

# Endpoint Security Course

## Common Threats

### Threat Domains

With organizations facing an ever-growing number of cyber threats, it is critical that they have robust security solutions in place. But in order to protect themselves, organizations first need to know what vulnerabilities exist within their threat domains. A ‘threat domain’ is considered to be an area of control, authority or protection that attackers can exploit to gain access to a system.

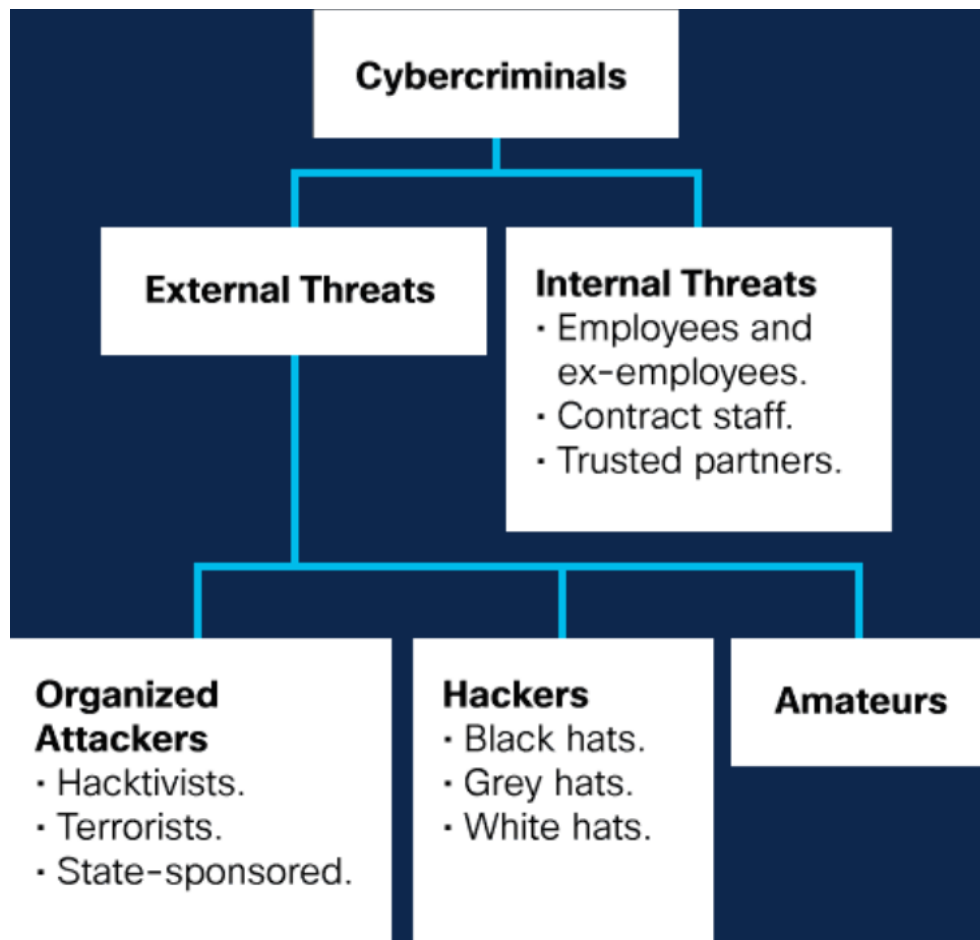
There are many ways that attackers can uncover vulnerabilities and exploit systems within a domain.

### Types of Cyber Threats

Cyber threats can be classified into different categories. This allows organizations to assess the likelihood of a threat occurring and understand the monetary impact of a threat so that they can prioritize their security efforts.

- **Software attacks**
  - A successful denial-of-service (DoS attack).
  - A computer virus.
- **Software errors**
  - A software bug.
  - An application going offline.
  - A cross-site script or illegal file server share.
- **Sabotage**
  - An authorized user successfully penetrating and compromising an organization’s primary database.
  - The defacement of an organization’s website.
- **Human error**
  - Inadvertent data entry errors.
  - A firewall misconfiguration.
- **Theft:** Laptops or equipment being stolen from an unlocked room.
- **Hardware failures:** Hard drive crashes.
- **Utility interruption**
  - Electrical power outages.
  - Water damage resulting from sprinkler failure.
- **Natural disasters:** Severe storms such as hurricanes or tornados, Earthquakes, Floods or Fires.

## Internal vs External Threats



Threats can originate from both within and outside of an organization, with attackers seeking access to valuable sensitive information such as personnel records, intellectual property, and financial data.

**Internal threats** are usually carried out by current or former employees and other contract partners who accidentally or intentionally mishandle confidential data or threaten the operations of servers or network infrastructure devices by connecting infected media or by accessing malicious emails or websites.

The source of an **external threat** typically stems from amateur or skilled attackers who can exploit vulnerabilities in networked devices or can use social engineering techniques, such as trickery, to gain access to an organization's internal resources.

*"Did you know that internal threats have the potential to cause greater damage than external threats? This is because employees or partners working within an organization have direct access to its premises and infrastructure devices. They will also have insider knowledge of the organization's network, resources and confidential data, as well as the security countermeasures in place."*

## User Threats and Vulnerabilities

A **user domain** includes anyone with access to an organization's information system, including employees, customers and contract partners. Users are often considered to be the weakest link in information security systems, posing a significant threat to the confidentiality, integrity and availability of an organization's data.

Let's reveal more information about the most common user threats found in many organizations.

- **No awareness of security:** Users must be aware of and understand an organization's sensitive data, security policies and procedures, technologies and countermeasures that are implemented in order to protect information and information systems.
- **Poorly enforced security policies:** All users must be aware of and understand an organization's security policies, as well as the consequences of non-compliance.
- **Data theft:** Data stolen by users can pose a significant financial threat to organizations, both in terms of the resulting damage to their reputation and/or the legal liability associated with the disclosure of sensitive information.
- **Unauthorized downloads and media:** Many network and device infections and attacks can be traced back to users who have downloaded unauthorized emails, photos, music, games, apps and videos to their computers, networks or storage devices, or used unauthorized media such as external hard disks and USB drives.
- **Unauthorized virtual private networks (VPNs):** VPNs can hide the theft of unauthorized information because the encryption normally used to protect confidentiality can stop a network administrator from tracking data transmission (unless they have permission to do so).
- **Unauthorized websites:** Accessing unauthorized websites can pose a risk to a user's data and devices, as well as the organization itself. Often, these websites prompt users to download scripts or plugins that contain malicious code or adware. Some of these sites can even take over user devices like cameras and applications.
- **Destruction of systems, applications or data:** The accidental or deliberate destruction or sabotage of systems, applications and data poses a serious risk to all organizations. Activists, disgruntled employees or industry competitors attempt to delete data and destroy or misconfigure devices, to make organizational data and information systems unavailable.

Always keep in mind that there are no technical solutions, controls or countermeasures that will make information systems any more secure than the behaviors and processes of the people who use these systems.

## Threats to Devices

- Any devices left powered on and unattended pose the risk of someone gaining unauthorized access to network resources.
- Downloading files, photos, music or videos from unreliable sources could lead to the execution of malicious code on devices.
- Cybercriminals often exploit security vulnerabilities within software installed on an organization's devices to launch an attack.
- An organization's information security teams must try to keep up to date with the daily discovery of new viruses, worms and other malware that pose a threat to their devices.
- Users who insert unauthorized USB drives, CDs or DVDs run the risk of introducing malware, or compromising data stored on their device.
- Policies are in place to protect an organization's IT infrastructure. A user can face serious consequences for purposefully violating such policies.
- Using outdated hardware or software makes an organization's systems and data more vulnerable to attack.

## Threats to the Local Area Network

The local area network (LAN) is a collection of devices, typically in the same geographic area, connected by cables (wired) or airwaves (wireless).

Because users can access an organization's systems, applications and data from the **LAN domain**, it is critical that it has strong security and stringent access controls.

### Some common threats posed to the LAN.

1. **Malware** – Malicious software such as viruses or worms can spread quickly across a LAN, damaging systems or stealing data.
2. **Unauthorized Access** – Intruders or unauthorized users gaining access to the network can compromise sensitive information.
3. **Denial-of-Service (DoS) Attacks** – These attacks flood the network with traffic, making it unusable for legitimate users.
4. **Man-in-the-Middle (MitM) Attacks** – Attackers intercept and potentially alter communication between two devices on the LAN.
5. **Eavesdropping** – Unencrypted traffic on the LAN can be intercepted and read by unauthorized users.
6. **Insider Threats** – Employees or users within the organization intentionally or unintentionally compromise network security.
7. **Rogue Devices** – Unauthorized devices connected to the LAN can introduce vulnerabilities or malicious software.

8. **Outdated Software or Firmware** – Unpatched systems can be exploited by attackers to gain control or access to the network.
9. **Phishing Attacks** – Users on the LAN may be tricked into revealing credentials or installing malware via deceptive emails or websites.
10. **Physical Security Breaches** – Gaining physical access to network hardware can lead to tampering or data theft.

### Threats to the Private Cloud

The private cloud domain includes any private servers, resources and IT infrastructure available to members of a single organization via the Internet. While many organizations feel that their data is safer in a private cloud, this domain still poses significant security threats, including:

- Unauthorized network probing and port scanning.
- Unauthorized access to resources.
- Router, firewall or network device operating system or software vulnerabilities.
- Router, firewall or network device configuration errors.
- Remote users accessing an organization's infrastructure and downloading sensitive data

### Threats to the Public Cloud

Where a private cloud domain hosts computing resources for a single organization, the **public cloud domain** is the entirety of computing services hosted by a cloud, service or Internet provider that are available to the public and shared across organizations.

There are three models of public cloud services that organizations may choose to use.

- **Software as a Service (SaaS):** This is a subscription-based model that provides organizations with software that is centrally hosted and accessed by users via a web browser, app or other software. In other words, this is software not stored locally but in the cloud.
- **Platform as a Service (PaaS):** This subscription-based model provides a platform that allows an organization to develop, run and manage its applications on the service's hardware, using tools that the service provides. This platform is accessed via the public cloud.
- **Infrastructure as a Service (IaaS):** This subscription-based model provides virtual computing resources such as hardware, software, servers, storage and other infrastructure components over the Internet. An organization will buy access to them and use them via the public cloud.

While public cloud service providers do implement security controls to protect the cloud environment, organizations are responsible for protecting their own resources on the cloud. Therefore, some of the most common threats to the public cloud domain include:

- Data breaches.
- Loss or theft of intellectual property.
- Compromised credentials or account hijacking.
- Social engineering attacks.
- Compliance violation.

## Threats to Applications

The **application domain** includes all of the critical systems, applications and data used by an organization to support operations. Increasingly, organizations are moving applications such as email, security monitoring and database management to the public cloud.

Common threats to applications include:

- Someone gaining unauthorized access to data centers, computer rooms, wiring closets or systems.
- Server downtime during maintenance periods.
- Network operating system software vulnerabilities.
- Data loss.
- Client-server or web application development vulnerabilities.

## Threat Complexity

Software vulnerabilities occur as a result of programming mistakes, protocol vulnerabilities or system misconfigurations. Cybercriminals seek to take advantage of such vulnerabilities and are becoming increasingly sophisticated in their attack methods.

- An **advanced persistent threat (APT)** is a continuous attack that uses elaborate espionage tactics involving multiple actors and/or sophisticated malware to gain access to and analyze a target's network.  
Attackers operate under the radar and remain undetected for a long period of time, with potentially devastating consequences. APTs typically target governments and high-level organizations and are usually well-orchestrated and well-funded.
- As the name suggests, **algorithm attacks** take advantage of algorithms in a piece of legitimate software to generate unintended behaviors. For example, algorithms used to track and report how much energy a computer consumes can be used to select targets or trigger false alerts. They can also disable a computer by forcing it to use up all its RAM or by overworking its central processing unit (CPU).

*“Many organizations rely on threat intelligence data to help them understand their overall risk, so that they can formulate and put in place effective preventative and response measures. Some of this data is closed source and requires a paid subscription for access. Other data is considered open source intelligence (OSINT) and can be accessed from publicly available information sources. In fact, sharing threat intelligence data is becoming more popular, with governments, universities, healthcare sector organizations and private businesses working together to improve everyone’s security.”*

## **Backdoors and Rootkits**

**Backdoors:** A **backdoor** is a covert method of bypassing normal authentication or encryption in a computer system, application, or network. They are often created by attackers after compromising a system, but sometimes exist due to poor software design or as deliberate features left by developers (often without proper documentation). Once in place, a backdoor allows attackers to re-enter the system at will, steal data, install more malware, or manipulate system functions—all without being detected by standard security mechanisms. **Key risk:** Backdoors enable attackers to maintain long-term, undetected access to systems, even after security patches are applied.

**Rootkits:** A **rootkit** is a set of malicious tools that allows an attacker to gain and maintain privileged (root-level) access to a system while actively hiding their presence. Rootkits often modify core parts of the operating system or install themselves at the firmware or kernel level, making them extremely difficult to detect or remove. They can be used to disable antivirus software, conceal other malware (like keyloggers or Trojans), intercept data, and manipulate logs. **Key risk:** Rootkits are dangerous because they operate at deep system levels, making them stealthy, persistent, and capable of fully controlling a compromised device or network.

Together, backdoors and rootkits are often part of advanced persistent threats (APTs), where attackers aim to remain undetected for long periods while extracting data or manipulating systems.

## **Threat Intelligence and Research Sources**

The United States Computer Emergency Readiness Team (US-CERT) and the U.S. Department of Homeland Security sponsor a dictionary of common vulnerabilities and exposures (CVE).

Each CVE entry contains a standard identifier number, a brief description of the security vulnerability and any important references to related vulnerability reports. The CVE list is maintained by a not-for-profit, the MITRE Corporation, on its public website.

Let's find out more about some other threat intelligence sources.

- **The dark web:** This refers to encrypted web content that is not indexed by conventional search engines and requires specific software, authorization or configurations to access. Expert researchers monitor the dark web for new threat intelligence.
- **Indicator of compromise (IOC):** IOCs such as malware signatures or domain names provide evidence of security breaches and details about them.
- **Automated Indicator Sharing (AIS):** Automated Indicator Sharing (AIS), a Cybersecurity and Infrastructure Security Agency (CISA) capability, enables the real-time exchange of cybersecurity threat indicators using a standardized and structured language called Structured Threat Information Expression (STIX) and Trusted Automated Exchange of Intelligence Information (TAXII).

## Deception

### Social Engineering

Social engineering is a non-technical strategy that attempts to manipulate individuals into performing certain actions or divulging confidential information.

Rather than software or hardware vulnerabilities, social engineering exploits human nature, taking advantage of people's willingness to help or preying on their weaknesses, such as greed or vanity.

Let's find out more about some common types of social engineering attacks.

- **Pretexting:** This type of attack occurs when an individual lies to gain access to privileged data. For example, an attacker pretends to need personal or financial data in order to confirm a person's identity.
- **Something for something (quid pro quo):** Quid pro quo attacks involve a request for personal information in exchange for something, like a gift. For example, a malicious email could ask you to give your sensitive personal details in exchange for a free vacation.
- **Identity fraud:** This is the use of a person's stolen identity to obtain goods or services by deception. For example, someone has acquired your data and is attempting to issue a credit card in your name.



## Social Engineering Tactics

Cybercriminals rely on several social engineering tactics to gain access to sensitive information.

- **Authority:** Attackers prey on the fact that people are more likely to comply when instructed by someone they perceive as an authority figure. For example, an executive opens what looks like an official subpoena attachment but is actually an infected PDF.
- **Intimidation:** Cybercriminals will often bully a victim into taking an action that compromises security. For example, a secretary receives a call that their boss is about to give an important presentation but the files are corrupt. The criminal on the phone claims it's the secretary's fault and pressures the secretary to send across the files immediately or risk dismissal.
- **Consensus:** Often called 'social proof,' consensus attacks work because people tend to act in the same way as other people around them, thinking that something must be right if others are doing it. For example, cybercriminals may publish a social media post about a 'business opportunity' and get dozens of legitimate or illegitimate accounts to comment on its validity underneath, which encourages unsuspecting victims to make a purchase.
- **Scarcity:** A well known marketing tactic, scarcity attacks work because attackers know that people tend to act when they think there is a limited quantity of something available. For example, someone receives an email about a luxury item being sold for very little money, but it states that there are only a handful available at this price, in an effort to spur the unsuspecting victim into taking action.
- **Urgency:** Similarly, people also tend to act when they think there is a limited time to do so. For example, cybercriminals promote a fake time-limited shipping offer to try and prompt victims to take action quickly.
- **Familiarity:** People are more likely to do what another person asks if they like this person. Therefore, attackers will often try to build a rapport with their victim in order to establish a relationship. In other cases, they may clone the social media profile of a friend of yours, in order to get you to think you are speaking to them.
- **Trust:** Building trust in a relationship with a victim may require more time to establish. For example, a cybercriminal disguised as a security expert calls the unsuspecting victim to offer advice. When helping the victim, the 'security expert' discovers a 'serious error' that needs immediate attention. The solution provides the cybercriminal with the opportunity to violate the victim's security.

*"Remember that cybercriminals repertory is vast and ever-evolving. Sometimes, they might combine two or more of the above tactics to increase their chances. It is up to cybersecurity professionals to raise awareness and educate other people in an organization about these tactics, to prevent them from falling victim to such attacks."*

## Shoulder Surfing and Dumpster Diving

Shoulder surfing is a simple attack that involves observing or literally looking over a target's shoulder to gain valuable information such as PINs, access codes or credit card details. Criminals do not always have to be near their victim to shoulder surf — they can use binoculars or security cameras to obtain this information. This is one reason why an ATM screen can only be viewed at certain angles. These types of safeguards make shoulder surfing much more difficult.

You may have heard of the phrase, 'one man's trash is another man's treasure.' Nowhere is this more true than in the world of dumpster diving — the process of going through a target's trash to see what information has been thrown out. This is why documents containing sensitive information should be shredded or stored in burn bags until they are destroyed by fire after a certain period of time.

## Impersonation and Hoaxes

**Impersonation:** Impersonation involves an attacker pretending to be someone the victim knows or trusts, such as a colleague, manager, or service provider. The goal is to manipulate the victim into taking an action that benefits the attacker, such as sharing sensitive information or transferring money. For example, a cybercriminal might impersonate a company executive via email and request a wire transfer, making the message appear urgent and legitimate to trick the employee into sending funds.

**Hoaxes:** Hoaxes are deliberately fabricated messages designed to mislead, scare, or manipulate individuals. They often take the form of fake alerts, virus warnings, or exaggerated claims and can cause users to take harmful actions or spread misinformation. For example, an employee receives an email warning of a widespread virus and is instructed to delete a system file to protect their computer. In reality, the file is essential, and deleting it causes damage to the system.

## Piggybacking and Tailgating

**Piggybacking:** Piggybacking occurs when an unauthorized person gains access to a restricted area by following closely behind an authorized person, typically with their knowledge or permission. This usually involves the attacker convincing the authorized individual to hold the door open or allow them entry. For example, an attacker carrying a stack of boxes asks an employee to hold the door open because they "forgot their badge," and the employee lets them in without verifying their identity.

**Tailgating:** Tailgating is similar to piggybacking but involves the unauthorized person slipping in behind someone without their knowledge. It relies on the momentary lapse in physical security and awareness. For example, an employee swipes their badge to enter a secure office, and an attacker quickly follows right behind before the door closes, gaining access without being noticed.

## Other Methods of Deception

Be aware that attackers have many more tricks up their sleeve to deceive their victims.

**Invoice scam:** Fake invoices are sent with the goal of receiving money from a victim by prompting them to put their credentials into a fake login screen. The fake invoice may also include urgent or threatening language.

**Watering hole attack:** A watering hole attack describes an exploit in which an attacker observes or guesses what websites an organization uses most often, and infects one or more of them with malware.

**Typosquatting:** This type of attack relies on common mistakes such as typos made by individuals when inputting a website address into their browser. The incorrect URL will bring the individuals to a legitimate-looking website owned by the attacker, whose goal is to gather their personal or financial information.

**Prepending:** Attackers can remove the ‘external’ email tag used by organizations to warn the recipient that an email has originated from an external source. This tricks individuals into believing that a malicious email was sent from inside their organization.

**Influence campaigns:** Often used in cyberwarfare, influence campaigns are usually very well coordinated and blend various methods such as fake news, disinformation campaigns and social media posts.

## Defending Against Deception

Organizations need to promote awareness of social engineering tactics and properly educate employees on prevention measures. Here are some top tips.

- Never disclose confidential information or credentials via email, chat, text messages, in person or over the phone to unknown parties.
- Resist the urge to click on enticing emails and web links.
- Be wary of uninitiated or automatic downloads.
- Establish and educate employees on key security policies.
- Encourage employees to take ownership of security issues.
- Do not give in to pressure by unknown individuals.

## Cyber Attacks

Cybercriminals use many different types of malicious software, or malware, to carry out attacks. Malware is any code that can be used to steal data, bypass access controls or cause harm to or compromise a system.

### Common types of malware

- **Viruses:** A virus is a type of computer program that, when executed, replicates and attaches itself to other files, such as a legitimate program, by inserting its own code into it. Some viruses are harmless yet others can be destructive, such as those that modify or delete data. Most viruses require end-user interaction to initiate activation, and can be written to act on a specific date or time. Viruses can be spread through removable media such as USB flash drives, Internet downloads and email attachments. The simple act of opening a file or executing a specific program can trigger a virus. Once a virus is active, it will usually infect other programs on the computer or other computers on the network. Viruses mutate to avoid detection. For example, the Melissa virus was released in 1999 and spread via email, affecting tens of thousands of users and causing an estimated \$1.2 billion in damage.
- **Worms:** A worm is a malicious software program that replicates by independently exploiting vulnerabilities in networks. Unlike a virus, which requires a host program to run, worms can run by themselves. Other than the initial infection of the host, they do not require user participation and can spread very quickly over the network, usually slowing it down. Worms share similar patterns: they exploit system vulnerabilities, they have a way to propagate themselves and they all contain malicious code (payload) to cause damage to computer systems or networks. Worms are responsible for some of the most devastating attacks on the Internet. In 2001, the Code Red worm had infected over 300,000 servers in just 19 hours.
- **Trojan horse:** A Trojan horse is malware that carries out malicious operations by masking its true intent. It might appear legitimate but is, in fact, very dangerous. Trojans exploit the privileges of the user who runs them. Unlike viruses, Trojans do not self-replicate but often bind themselves to non-executable files, such as image, audio or video files, acting as a decoy to harm the systems of unsuspecting users.

### Logic Bombs

A logic bomb is a malicious program that waits for a trigger, such as a specified date or database entry, to set off the malicious code. Until this trigger event happens, the logic bomb will remain inactive. Once activated, a logic bomb implements a malicious code that causes harm to a computer in various ways. It can sabotage database records, erase files and attack operating systems or applications. Cybersecurity specialists have recently discovered logic bombs that attack and destroy the hardware components in a device or server, including the cooling fans,

central processing unit (CPU), memory, hard drives and power supplies. The logic bomb overdrives these components until they overheat or fail.

## **Ransomware**

This malware is designed to hold a computer system or the data it contains captive until a payment is made. Ransomware usually works by encrypting your data so that you cannot access it. According to ransomware claims, once the ransom is paid via an untraceable payment system, the cybercriminal will supply a program that decrypts the files or send an unlock code — but in reality, many victims do not gain access to their data even after they have paid. Some versions of ransomware can take advantage of specific system vulnerabilities to lock it down.

Ransomware is often spread through phishing emails that encourage you to download a malicious attachment, or through software vulnerability.

## **Denial of Service Attacks**

Denials of service (DoS) attacks are a type of network attack that is relatively simple to conduct, even for an unskilled attacker. They are a major risk as they usually result in some sort of interruption to network services, causing a significant loss of time and money. Even operational technologies, hardware or software that controls physical devices or processes in buildings, factories or utility providers, are vulnerable to DoS attacks, which can cause a shutdown, in extreme circumstances. Distributed denials of service (DDoS) attacks are similar but originate from multiple coordinated sources. Here is how this happens:

- An attacker builds a network (botnet) of infected hosts called zombies, which are controlled by handler systems.
- The zombie computers constantly scan and infect more hosts, creating more and more zombies.
- When ready, the hacker will instruct the handler systems to make the botnet of zombies carry out a DDoS attack.

## **DNS (Domain Name System)**

There are many essential technical services needed for a network to operate — such as routing, addressing and domain naming. These are prime targets for attack.

Let's to find out how cybercriminals can take advantage of vulnerabilities in these services.

- **Domain reputation:** The Domain Name System (DNS) is used by DNS servers to translate a domain name, such as `www.cisco.com`, into a numerical IP address so that computers can understand it. If a DNS server does not know an IP address, it will ask another DNS server. An organization needs to monitor its domain reputation, including its IP address, to help protect against malicious external domains.

- **DNS spoofing:** DNS spoofing or DNS cache poisoning is an attack in which false data is introduced into a DNS resolver cache — the temporary database on a computer's operating system that records recent visits to websites and other Internet domains. These poison attacks exploit a weakness in the DNS software that causes the DNS servers to redirect traffic for a specific domain to the attacker's computer.
- **Domain hijacking:** When an attacker wrongfully gains control of a target's DNS information, they can make unauthorized changes to it. This is known as domain hijacking. The most common way of hijacking a domain name is to change the administrator's contact email address through social engineering or by hacking into the administrator's email account. The administrator's email address can be easily found via the WHOIS record for the domain, which is of public record.
- **Uniform resource location (URL):** A uniform resource locator (URL) is a unique identifier for finding a specific resource on the Internet. Redirecting a URL commonly happens for legitimate purposes. For example, you have logged into an eLearning portal to begin this Cybersecurity Essentials course. If you log out of the portal and return to it another time, the portal will redirect you back to the login page. It is this type of functionality that attackers can exploit. Instead of taking you to the eLearning login page, they can redirect you to a malicious site.

## Layer 2 Attacks

Layer 2 refers to the data link layer in the Open Systems Interconnection (OSI) data communication model.

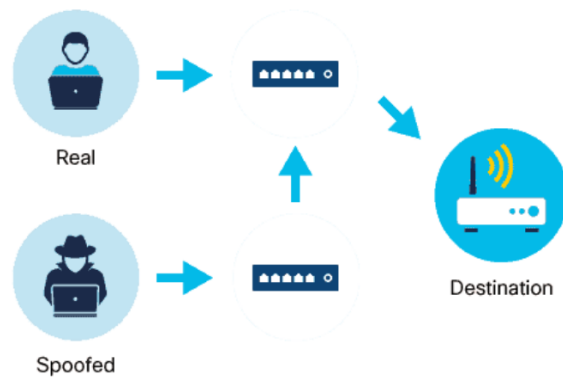
This layer is used to move data across a linked physical network. IP addresses are mapped to each physical device address (also known as media access control (MAC) address) on the network, using a procedure called address resolution protocol (ARP).

In its simplest terms, the MAC address identifies the intended receiver of an IP address sent over the network, and ARP resolves IP addresses to MAC addresses for transmitting data.

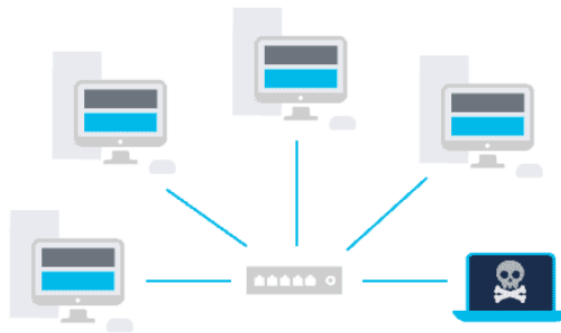
Attackers often take advantage of vulnerabilities in this layer 2 security.

### Examples

- **Spoofing:** Spoofing, or poisoning, is a type of impersonation attack that takes advantage of a trusted relationship between two systems.
  - MAC address spoofing occurs when an attacker disguises their device as a valid one on the network and can therefore bypass the authentication process.
  - ARP spoofing sends spoofed ARP messages across a LAN. This links an attacker's MAC address to the IP address of an authorized device on the network.
  - IP spoofing sends IP packets from a spoofed source address in order to disguise it.



- **MAC Flooding:** Devices on a network are connected via a network switch by using packet switching to receive and forward data to the destination device. MAC flooding compromises the data transmitted to a device. An attacker floods the network with fake MAC addresses, compromising the security of the network switch.



### Man-in-the-Middle and Man-in-the-Mobile Attacks

- **Man-in-the-Middle Attacks:** A man-in-the-middle (MitM) attack occurs when a cybercriminal secretly intercepts and possibly alters the communication between two parties who believe they are directly communicating with each other.
- **Man-in-the-Mobile Attacks:** A man-in-the-mobile (MitMo) attack is a variation of a MitM attack where malware is installed on a mobile device to intercept communications, such as text messages used for two-factor authentication, allowing attackers to bypass security measures.

*“A replay attack occurs when an attacker captures communication between two hosts and then retransmits the message to the recipient, to trick the recipient into doing what the attacker wants, thus circumventing any authentication mechanisms.”*

## **Zero-Day Attacks**

A zero-day attack or zero-day threat exploits software vulnerabilities before they become known or before they are disclosed by the software vendor.

A network is extremely vulnerable to attack between the time an exploit is discovered (zero hour) and the time it takes for the software vendor to develop and release a patch that fixes this exploit.

Defending against such fast-moving attacks requires network security professionals to adopt a more sophisticated and holistic view of any network architecture.

## **Keyboard Logging**

As the name suggests, keyboard logging or keylogging refers to recording or logging every key struck on a computer's keyboard.

Cybercriminals log keystrokes via software installed on a computer system or through hardware devices that are physically attached to a computer, and configure the keylogger software to send the log file to the criminal. Because it has recorded all keystrokes, this log file can reveal usernames, passwords, websites visited and other sensitive information.

Many anti-spyware suites can detect and remove unauthorized key loggers.

*“It is important to note that keylogging software can be legitimate. Many parents use it to keep an eye on their children's internet behavior.”*

## **Defending Against Attacks**

Organizations can take several steps to defend against various attacks. These include the following:

- Configure firewalls to remove any packets from outside the network that have addresses indicating that they originated from inside the network.
- Ensure patches and upgrades are current.
- Distribute the workload across server systems.
- Network devices use Internet Control Message Protocol (ICMP) packets to send error and control messages, such as whether or not a device can communicate with another on the network. To prevent DoS and DDoS attacks, organizations can block external ICMP packets with their firewalls.



# Wireless and Mobile Device Attacks

## Grayware and SMiShing

**Grayware** is any unwanted application that behaves in an annoying or undesirable manner. And while grayware may not carry any recognizable malware, it may still pose a risk to the user by, for example, tracking your location or delivering unwanted advertising.

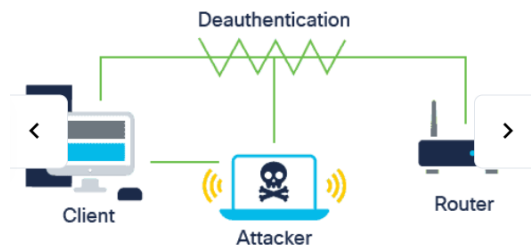
Authors of grayware typically maintain legitimacy by including these ‘gray’ capabilities in the small print of the software license agreement. This factor poses a growing threat to mobile security in particular, as many smartphone users install mobile apps without really considering this small print.

Short message service phishing or **SMiShing** is another tactic used by attackers to trick you. Fake text messages prompt you to visit a malicious website or call a fraudulent phone number, which may result in malware being downloaded onto your device or personal information being shared.

## Rogue Access Points

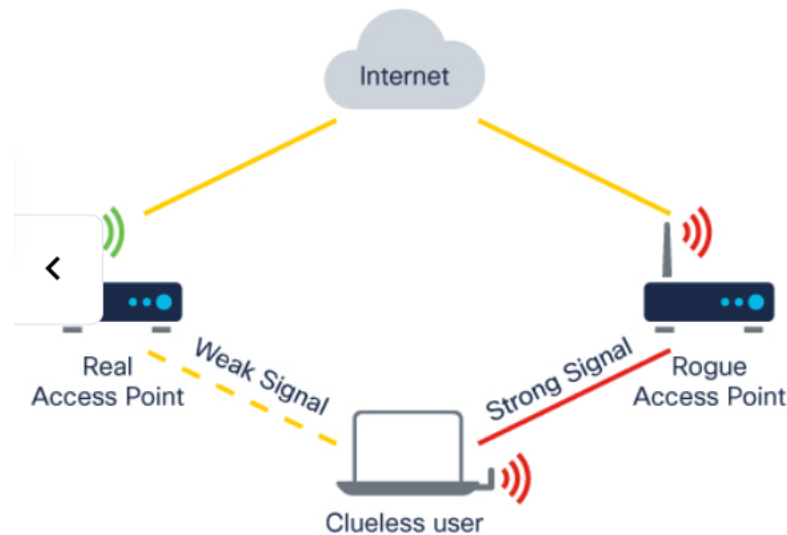
A rogue access point is a wireless access point installed on a secure network without explicit authorization. Although it could potentially be set up by a well-intentioned employee looking for a better wireless connection, it also presents an opportunity for attackers looking to gain access to an organization’s network.

- An attacker will often use social engineering tactics to gain physical access to an organization’s network infrastructure and install the rogue access point. Also known as a criminal’s access point, the access point can be set up as a MitM device to capture your login information.



This works by disconnecting the rogue access point, which triggers the network to send a deauthentication frame to disassociate the access point. This process is then exploited by spoofing your MAC address and sending a deauthentication data transmission to the wireless access point.

- **Evil twin attack:** An evil twin attack describes a situation where the attacker’s access point is set up to look like a better connection option. Once you connect to the evil access point, the attacker can analyze your network traffic and execute MitM attacks.



## Radio Frequency Jamming

Wireless signals are susceptible to electromagnetic interference (EMI), radio frequency interference (RFI) and even lightning strikes or noise from fluorescent lights.

Attackers can take advantage of this fact by deliberately jamming the transmission of a radio or satellite station to prevent a wireless signal from reaching the receiving station.

In order to successfully jam the signal, the frequency, modulation and power of the RF jammer needs to be equal to that of the device that the attacker is seeking to disrupt.

## Bluejacking and Bluesnarfing

- **Bluejacking:** Bluejacking is the practice of sending unsolicited messages to other Bluetooth-enabled devices nearby. It works by exploiting the way Bluetooth allows devices to exchange contact information (like vCards). A bluejacker sends a message disguised as a contact card, which pops up on the recipient's screen. Since Bluetooth range is limited (usually up to 10 meters), the attacker needs to be physically close. Bluejacking doesn't access or steal data; it just sends messages, so it's considered harmless and more of a prank. Bluejacking abuses Bluetooth's contact-sharing feature to send data.
- **Bluesnarfing:** Bluesnarfing is a hacking technique where an attacker exploits vulnerabilities in Bluetooth security to gain unauthorized access to data stored on a Bluetooth-enabled device. This can include contacts, calendar entries, emails, and even files. It happens without the user's knowledge and can be done remotely if the attacker is within Bluetooth range. Bluesnarfing targets flaws in Bluetooth protocols or weak device security, making it a serious privacy and security threat. Bluesnarfing abuses Bluetooth's file/data access protocols to steal data.

## Attacks against Wi-Fi Protocols

**Wired equivalent privacy (WEP)** and **Wi-Fi protected access (WPA)** are security protocols that were designed to secure wireless networks that are vulnerable to attacks.

WEP was developed to provide data transmitted over a wireless local area network (WLAN) with a level of protection comparable to what is usually expected of a traditional wired network. It added security to wireless networks by encrypting the data.

WEP used a key for encryption. The problem, however, was that WEP had no provision for key management and so the number of people sharing the same key continually grew, giving criminals access to a large amount of traffic data. Furthermore, WEP's initialization vector (IV), one of the key components of its encryption key, was too small, readable and static.

To address this and replace WEP, **WPA** and then **WPA2** were developed as improved security protocols. Unlike with WEP, an attacker cannot recover WPA2's encryption key by observing network traffic. However, they can still use a packet sniffer to analyze the packets going between an access point and a legitimate user.



## Wi-Fi and Mobile Defense

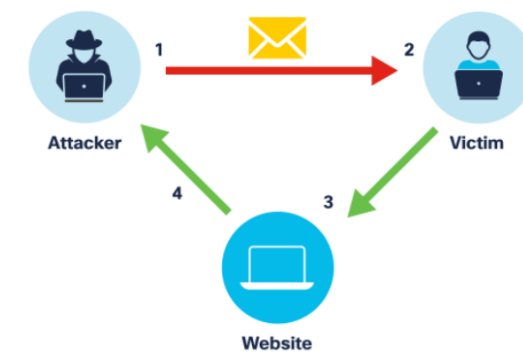
There are several steps that organizations and users need to take to defend against wireless and mobile device attacks. These include the following:

- Take advantage of basic wireless security features such as authentication and encryption by changing the default configuration settings.
- Restrict access point placement by placing these devices outside the firewall or within a demilitarized zone — a perimeter network that protects an organization's LAN from untrusted devices.

- Use WLAN tools such as NetStumbler to detect rogue access points or unauthorized workstations.
- Develop a policy for guest access to an organization's Wi-Fi network.
- Employees in an organization should use a remote access VPN for WLAN access.

## Application Attacks

### Cross-Site Scripting



Cross-site scripting (XSS) is a common vulnerability found in many web applications. This is how it works:

1. Cybercriminals exploit the XSS vulnerability by injecting scripts containing malicious code into a web page.
2. The web page is accessed by the victim, and the malicious scripts unknowingly pass to their browser.
3. The malicious script can access any cookies, session tokens or other sensitive information about the user, which is sent back to the cybercriminal.
4. Armed with this information, the cybercriminal can impersonate the user.

### Code Injection

Most modern websites use a database, such as a Structured Query Language (SQL) or an Extensible Markup Language (XML) database, to store and manage data. Injection attacks seek to exploit weaknesses in these databases

Common types of injection attacks

- **XML injection attack:** An XML injection attack can corrupt the data on the XML database and threaten the security of the website. It works by interfering with an application's processing of XML data or query entered by a user. Cybercriminals can manipulate this query by programming it to suit their needs. This will grant them access to all of the sensitive information stored on the database and allows them to make any number of changes to the website.

- **SQL injection attack:** Cybercriminals can carry out an SQL injection attack on websites or any SQL database by inserting a malicious SQL statement in an entry field. This attack takes advantage of a vulnerability in which the application does not correctly filter the data entered by a user for characters in an SQL statement. As a result, the cybercriminal can gain unauthorized access to information stored on the database, from which they can spoof an identity, modify existing data, destroy data or even become an administrator of the database server itself.
- **DLL injection attack:** A dynamic link library (DLL) file is a library that contains a set of code and data for carrying out a particular activity in Windows. Applications use this type of file to add functionality that is not built-in, when they need to carry out this activity. DLL injection allows a cybercriminal to trick an application into calling a malicious DLL file, which executes as part of the target process.
- **LDAP injection attack:** The Lightweight Directory Access Protocol (LDAP) is an open protocol for authenticating user access to directory services. An LDAP injection attack exploits input validation vulnerabilities by injecting and executing queries to LDAP servers, giving cybercriminals an opportunity to extract sensitive information from an organization's LDAP directory.

## **Buffer Overflow**

Buffers are memory areas allocated to an application. A buffer overflow occurs when data is written beyond the limits of a buffer. By changing data beyond the boundaries of a buffer, the application can access memory allocated to other processes. This can lead to a system crash or data compromise, or provide escalation of privileges.

These memory flaws can also give attackers complete control over a target's device. For example, an attacker can change the instructions of a vulnerable application while the program is loading in memory and, as a result, can install malware and access the internal network from the infected device.

## **Remote Code Executions**

Remote code execution allows a cybercriminal to take advantage of application vulnerabilities to execute any command with the privileges of the user running the application on the target device.

Privilege escalation exploits a bug, design flaw or misconfiguration in an operating system or software application to gain access to resources that are normally restricted.

Let's find out more about the Metasploit Project and this community's white hat cybersecurity tools

- **Metasploit Project** is an open-source cybersecurity framework used by professionals to test and improve system security through penetration testing and exploit development. It allows users to simulate attacks, deliver payloads, and assess vulnerabilities in networks and software.

The project offers ready-made exploit modules, payloads like Meterpreter, and tools for scanning and post-exploitation. It's widely used in ethical hacking, training, and responsible vulnerability research.

The Metasploit community is a collaborative group of white hat hackers and security researchers who contribute to its development, share knowledge, and promote ethical use of the tools for protecting systems.

## Other Application Attacks

Every piece of information that an attacker receives about a targeted system or application can be used as a valuable weapon for launching a dangerous attack. Let's find out more about some other types of application attacks.

- **Cross-site request forgery (CSRF):** CSRF describes the malicious exploit of a website where unauthorized commands are submitted from a user's browser to a trusted web application. A malicious website can transmit such commands through specially-crafted image tags, hidden forms or JavaScript requests — all of which can work without the user's knowledge.
- **Race condition attack:** Also known as a time of check (TOC) or a time of use (TOU) attack, a race condition attack happens when a computing system that is designed to handle tasks in a specific sequence is forced to perform two or more operations simultaneously. For example, operating systems are made up of threads — the smallest sequence of program instructions required to carry out a process. When two or more threads access shared data and try to change it at the exact same time, a race condition attack occurs.
- **Improper input handling attack:** Data inputted by a user that is not properly validated can affect the data flow of a program and cause critical vulnerabilities in systems and applications that result in buffer overflow or SQL injection attacks.
- **Error handling attack:** Attackers can use error messages to extract specific information such as the hostnames of internal systems and directories or files that exist on a given web server — as well as database, table and field names that can be used to craft SQL injection attacks.

- **Application programming interface (API) attack:** An API delivers a user response to a system and sends the system's response back to the user. An API attack occurs when a cybercriminal abuses an API endpoint.
- **Replay attack:** This describes a situation where a valid data transmission is maliciously or fraudulently repeated or delayed by an attacker, who intercepts, amends and resubmits the data to get the receiver to do whatever they want.
- **Directory traversal attack:** Directory traversal occurs when an attacker is able to read files on the webserver outside of the directory of the website. An attacker can then use this information to download server configuration files containing sensitive information, potentially expose more server vulnerabilities or even take control of the server!
- **Resource exhaustion attacks:** These attacks are computer security exploits that crash, hang or otherwise interfere with a targeted program or system. Rather than overwhelming network bandwidth like a DoS attack, resource exhaustion attacks overwhelm the hardware resources available on the target's server instead.

## Defending Against Application Attacks

There are several actions that you can take to defend against an application attack. You will find some of them outlined here.

- The first line of defense against an application attack is to write solid code.
- Prudent programming practice involves treating and validating all input from outside of a function as if it is hostile.
- Keep all software, including operating systems and applications, up to date and do not ignore update prompts. Remember that not all programs update automatically.

## Spam

Spam, also known as junk mail, is simply unsolicited email. In most cases, it is a method of advertising. However, a lot of spam is sent in bulk by computers infected by viruses or worms — and often contains malicious links, malware or deceptive content that aims to trick recipients into disclosing sensitive information, such as a social security number or bank account information.

Almost all email providers filter spam, but it still consumes bandwidth. And even if you have security features implemented, some spam might still get through to you. Look out for the following indicators of spam:

- The email has no subject line.
- The email asks you to update your account details.
- The email text contains misspelled words or strange punctuation.
- Links within the email are long and/or cryptic.
- The email looks like correspondence from a legitimate business, but there are tiny differences — or it contains information that does not seem relevant to you.
- The email asks you to open an attachment, often urgently.

If you receive an email that contains one or more of these indicators, you should not open the email or any attachments. Many organizations have an email policy that requires employees to report receipt of this type of email to their cybersecurity team for further investigation. If in doubt, always report.

### **Phishing and spear Phishing**

- Phishing is a broad cyberattack where attackers send **mass emails or messages** pretending to be a trustworthy entity (like a bank or popular service) to trick many people into revealing sensitive information—such as passwords, credit card numbers, or login credentials. These messages often contain links to fake websites designed to steal data. Phishing = mass, generic scam attempts.
- Spear phishing is a **targeted form of phishing**. Instead of sending generic messages to many people, attackers carefully research and customize their emails or messages to a specific individual or organization. Because the message looks highly relevant and personal, it's much more convincing and harder to detect. Spear Phishing = targeted, personalized scam attempts.

### **Vishing, Pharming and Whaling**

- **Vishing** (voice phishing) is a type of phishing attack that happens over the phone. Attackers call victims pretending to be legitimate organizations (like banks or government agencies) to trick them into giving sensitive information such as passwords, credit card details, or Social Security numbers. (**Vishing**: Phone call scams to steal info).
- **Pharming** is a cyberattack where victims are redirected from a legitimate website to a fake one without their knowledge. This often happens by exploiting vulnerabilities in DNS servers or by infecting the victim's computer with malware. The fake site looks real and steals login credentials or personal data. (**Pharming**: Redirecting users to fake websites).
- **Whaling** is a specific kind of spear phishing that targets high-profile individuals like CEOs, CFOs, or other executives. The attacker crafts highly personalized emails or messages to deceive these “big fish” into revealing confidential information or authorizing financial transactions. (**Whaling**: Targeted phishing at top executive).

### **Defending Against Email and Browser Attacks**

There are many actions that you can take to defend against email and browser attacks. Some of the most important ones are outlined here.

- It is difficult to stop spam, but there are ways to reduce its effects:
  - Most Internet service providers (ISPs) filter spam before it reaches the user's inbox.



- Many antivirus and email software programs automatically detect and remove dangerous spam from an email inbox.
- Organizations should educate employees about the dangers of unsolicited emails and make them aware of the dangers of opening attachments.
- Never assume that email attachments are safe, even when they come from a trusted contact. Always scan attachments before opening them.
- Become a member of the Anti-Phishing Working Group (APWG). It is an international association of companies focused on eliminating identity theft and fraud resulting from phishing and email spoofing.
- All software should be kept up-to-date, with the latest security patches applied to protect against any known security vulnerabilities.

### **There's More...**

#### **Physical attacks**

Physical attacks are intentional, offensive actions used to destroy, expose, alter, disable, steal or gain unauthorized access to an organization's infrastructure or hardware.

Examples of physical attacks include:

- Loading malware onto a USB flash drive that infects a device when plugged in.
- Fitting cables and plugs such as generic USB cables, mobile device charging cables and wall or power adapters with advanced technologies, such as a wireless chip, to allow an attacker to control or provide instructions to a device.
- Copying or skimming data from a credit or debit card using a specialized terminal to create a cloned card, which can be used to gain unauthorized access to the victim's accounts.

#### **Adversarial artificial intelligence attacks**

Machine learning is a method of automation that allows devices to carry out analysis and perform tasks without specifically being programmed to do so. It powers many of the applications we use today, such as web searching, photo tagging, spam detection, video surveillance, fraud detection and security automation.

Machine learning uses mathematical models to predict outcomes. However, these models are dependent on the data that is inputted. If the data is tainted, it can have a negative impact on the predicted outcome. Attackers can take advantage of this to perpetrate attacks against machine learning algorithms. For example, using tainted data to trick an autonomous vehicle into misinterpreting street signs

## Supply chain attacks

Many organizations interface with a third party for their systems management or to purchase components and software. Organizations may even rely on parts or components from a foreign source.

Attackers often find ways to intercept these supply chains. For example, software can be based on specific support agreements and subject to an end-of-life (EOL) date. Changing this date could mean that an organization is no longer eligible for service and maintenance support.

## Cloud-based attacks

Rather than developing systems on their own premises, more and more organizations are making the move toward cloud-based computing, as we discussed earlier in this module.

The advantage is that the cloud provider will maintain the equipment but this also opens up an organization to a host of potential threats. Attackers are constantly leveraging ways to exploit sensitive data stored on the cloud, as well as applications, platforms and infrastructure that is cloud-based, as we saw with SaaS, PaaS and IaaS.

## Securing network

### Networks Are Targets

Networks are routinely under attack. It is common to read in the news about yet another network that has been compromised. A quick internet search for network attacks will return many articles about network attacks, including news about organizations which have been compromised, the latest threats to network security, tools to mitigate attacks, and more.

To help you comprehend the gravity of the situation, Kaspersky maintains the interactive Cyberthreat Real-Time Map display of current network attacks. The attack data is submitted from Kaspersky network security products that are deployed worldwide. The figure displays a sample screenshot of this web tool, which shows these attacks in real time. Many similar tools are available on the internet and can be found by searching for cyberthreat maps.



## Reasons for Network Security

Network security relates directly to an organization's business continuity. Network security breaches can disrupt e-commerce, cause the loss of business data, threaten people's privacy, and compromise the integrity of information. These breaches can result in lost revenue for corporations, theft of intellectual property, lawsuits, and can even threaten public safety.

Maintaining a secure network ensures the safety of network users and protects commercial interests. Keeping a network secure requires vigilance on the part of an organization's network security professionals. They must constantly be aware of new and evolving threats and attacks to networks, and vulnerabilities of devices and applications.

Many tools are available to help network administrators adapt, develop, and implement threat mitigation techniques. For instance, the Cisco Talos Intelligence Group website, shown in the figure, provides comprehensive security and threat intelligence to defend customers and protect their assets.



Another group, called the Cisco Product Security Incident Response Team (PSIRT), is responsible for investigating and mitigating potential vulnerabilities in Cisco products. The figure displays a sample Cisco Security Advisories page which lists these vulnerabilities in real time and provides network administrators with information to help mitigate them.

tools.cisco.com/security/center/publicationListing.x

Worldwide (change) | Welcome | Account | Log Out | My Cisco

Products & Services | Support | How to Buy | Training & Events | Partners

Home / Cisco Security / Security Advisories

## Cisco Security

### Cisco Security Advisories

Vulnerabilities | Filter By Product

Quick Search

[Advanced Search](#)

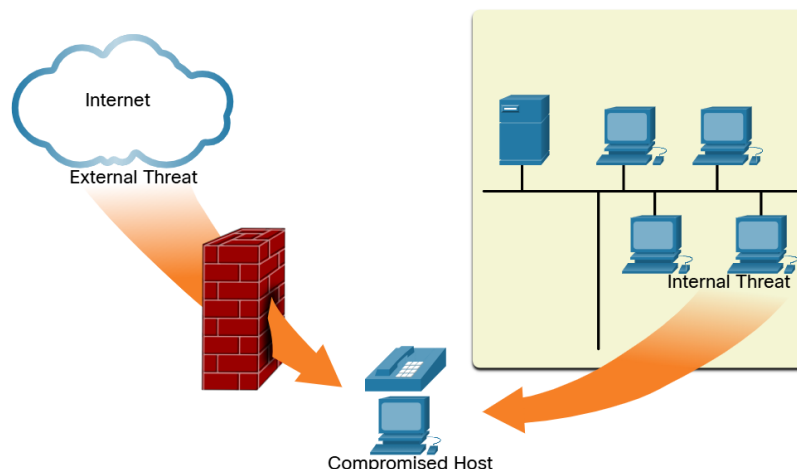
ADVISORY	IMPACT <input type="button" value="⌵"/>	CVE	LAST UPDATED <input type="button" value="⌵"/>	VERSION
<a href="#">Search Advisory Name</a>	All <input type="button" value="⌵"/>	<a href="#">Search CVE</a>	Most Recent <input type="button" value="⌵"/>	
▶  Cisco IOS XR Software DVMRP Memory Exhaustion Vulnerabilities	High	CVE-2020-3568 CVE-2020-3569	2020 Sep 01	2.1
▶  Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software Web Services Read-Only Path Traversal Vulnerability	High	CVE-2020-3452	2020 Aug 27	1.5
▶  Cisco FXOS and NX-OS Software Cisco Fabric Services Denial of Service Vulnerability	High	CVE-2020-3517	2020 Aug 26	1.1
▶  Cisco NX-OS Software Data Management Engine Remote Code Execution Vulnerability	High	CVE-2020-3415	2020 Aug 26	1.1
▶  Cisco Nexus 3000 and 9000 Series Switches Privilege Escalation Vulnerability	High	CVE-2020-3394	2020 Aug 26	1.1
▶  Cisco NX-OS Software Border Gateway Protocol Multicast VPN Session Denial of Service Vulnerability	High	CVE-2020-3398	2020 Aug 26	1.1
▶  Cisco NX-OS Software Border Gateway Protocol Multicast VPN	High	CVE-2020-3397	2020 Aug 26	1.1

Feedback

## Vectors of Network Attacks

An attack vector is a path by which a threat actor can gain access to a server, host, or network. Attack vectors originate from inside or outside the corporate network, as shown in the figure. For example, threat actors may target a network through the internet, to disrupt network operations and create a denial of service (DoS) attack.

### External and Internal Threats



**Note:** A DoS attack occurs when a network device or application is incapacitated and no longer capable of supporting requests from legitimate users.

An internal user, such as an employee, can accidentally or intentionally:

- Steal and copy confidential data to removable media, email, messaging software, and other media.
- Compromise internal servers or network infrastructure devices.
- Disconnect a critical network connection and cause a network outage.
- Connect an infected USB drive into a corporate computer system.

Internal threats have the potential to cause greater damage than external threats because internal users have direct access to the building and its infrastructure devices. Employees may also have knowledge of the corporate network, its resources, and its confidential data.

Network security professionals must implement tools and apply techniques for mitigating both external and internal threats.

## **Data Loss**

Data is likely to be an organization's most valuable asset. Organizational data can include research and development data, sales data, financial data, human resource and legal data, employee data, contractor data, and customer data.

Data loss, or data exfiltration, is when data is intentionally or unintentionally lost, stolen, or leaked to the outside world. The data loss can result in:

- Brand damage and loss of reputation
- Loss of competitive advantage
- Loss of customers
- Loss of revenue
- Litigation/legal action that results in fines and civil penalties
- Significant cost and effort to notify affected parties and recover from the breach

Network security professionals must protect the organization's data. Various Data Loss Prevention (DLP) controls must be implemented that combine strategic, operational, and tactical measures.

Common data loss vectors are displayed below.

- **Email/Social Networking:** The most common vector for data loss includes instant messaging software and social media sites. For instance, intercepted email or IM messages could be captured and reveal confidential information.

- **Unencrypted Devices:** A stolen corporate laptop typically contains confidential organizational data. If the data is not stored using an encryption algorithm, then the thief can retrieve valuable confidential data.
- **Cloud Storage Devices:** Saving data to the cloud has many potential benefits. However, sensitive data can be lost if access to the cloud is compromised due to weak security settings.
- **Removable Media:** One risk is that an employee could perform an unauthorized transfer of data to a USB drive. Another risk is that a USB drive containing valuable corporate data could be lost.
- **Hard Copy:** Corporate data should be disposed of thoroughly. For example, confidential data should be shredded when no longer required. Otherwise, a thief could retrieve discarded reports and gain valuable information.
- **Improper Access Control:** Passwords are the first line of defense. Stolen passwords or weak passwords which have been compromised can provide an attacker easy access to corporate data.

## Who is attacking Our Network?

### Threat, Vulnerability, and Risk

We are under attack and attackers want access to our assets. Assets are anything of value to an organization, such as data and other intellectual property, servers, computers, smart phones, tablets, and more.

To better understand any discussion of network security, it is important to know the following terms:

- **Threat:** A potential danger to an asset such as data or the network itself.
- **Vulnerability:** A weakness in a system or its design that could be exploited by a threat.
- **Attack surface:** An attack surface is the total sum of the vulnerabilities in a given system that are accessible to an attacker. The attack surface describes different points where an attacker could get into a system, and where they could get data out of the system. For example, your operating system and web browser could both need security patches. They are each vulnerable to attacks and are exposed on the network or the internet. Together, they create an attack surface that the threat actor can exploit.
- **Exploit:** The mechanism that is used to leverage a vulnerability to compromise an asset. Exploits may be remote or local. A remote exploit is one that works over the network without any prior access to the target system. The attacker does not need an account in the end system to exploit the vulnerability. In a local exploit, the threat actor has some type of user or administrative access to the end system. A local exploit does not necessarily mean that the attacker has physical access to the end system.

- **Risk:** The likelihood that a particular threat will exploit a particular vulnerability of an asset and result in an undesirable consequence.

Risk management is the process that balances the operational costs of providing protective measures with the gains achieved by protecting the asset. There are four common ways to manage risk, as shown below:

- **Risk acceptance:** This is when the cost of risk management options outweighs the cost of the risk itself. The risk is accepted, and no action is taken.
- **Risk avoidance:** This means avoiding any exposure to the risk by eliminating the activity or device that presents the risk. By eliminating an activity to avoid risk, any benefits that are possible from the activity are also lost.
- **Risk reduction:** This reduces exposure to risk or reducing the impact of risk by taking action to decrease the risk. It is the most commonly used risk mitigation strategy. This strategy requires careful evaluation of the costs of loss, the mitigation strategy, and the benefits gained from the operation or activity that is at risk.
- **Risk transfer:** Some or all of the risk is transferred to a willing third party such as an insurance company.

Other commonly used network security terms include:

- **Countermeasure** - The actions that are taken to protect assets by mitigating a threat or reducing risk.
- **Impact** - The potential damage to the organization that is caused by the threat.

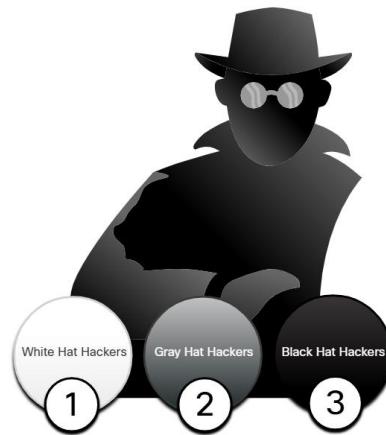
**Note:** A local exploit requires inside network access such as a user with an account on the network. A remote exploit does not require an account on the network to exploit that network's vulnerability.

## **Hacker vs Threat Actor**

As we know, "hacker" is a common term used to describe a threat actor. However, the term "hacker" has a variety of meanings, as follows:

- A clever programmer capable of developing new programs and coding changes to existing programs to make them more efficient.
- A network professional that uses sophisticated programming skills to ensure that networks are not vulnerable to attack.
- A person who tries to gain unauthorized access to devices on the internet.
- An individual who run programs to prevent or slow network access to a large number of users, or corrupt or wipe out data on servers.

An attack vector is a path by which a threat actor can gain access to a server, host, or network. Attack vectors originate from inside or outside the corporate network, as shown in the figure. For example, threat actors may target a network through the internet, to disrupt network operations and create a denial of service (DoS) attack.



As shown in the figure, the terms white hat hacker, black hat hacker, and grey hat hacker are often used to describe hackers.

1. **White hat** hackers are ethical hackers who use their programming skills for good, ethical, and legal purposes. They may perform network penetration tests in an attempt to compromise networks and systems by using their knowledge of computer security systems to discover network vulnerabilities. Security vulnerabilities are reported to developers and security personnel who attempt to fix the vulnerability before it can be exploited. Some organizations award prizes or bounties to white hat hackers when they provide information that helps to identify vulnerabilities.
2. **Grey hat** hackers are individuals who commit crimes and do arguably unethical things, but not for personal gain or to cause damage. An example would be someone who compromises a network without permission and then discloses the vulnerability publicly. Grey hat hackers may disclose a vulnerability to the affected organization after having compromised their network. This allows the organization to fix the problem.
3. **Black hat** hackers are unethical criminals who violate computer and network security for personal gain, or for malicious reasons, such as attacking networks. Black hat hackers exploit vulnerabilities to compromise computer and network systems.

*“Good or bad, hacking is an important aspect of network security. In this course, the term threat actor is used when referring to those individuals or groups that could be classified as gray or black hat hackers.”*



## Different types of threat actors.

- **Script kiddies:** Script kiddies emerged in the 1990s and refers to teenagers or inexperienced threat actors running existing scripts, tools, and exploits, to cause harm, but typically not for profit.
- **Vulnerability brokers:** Vulnerability brokers typically refers to grey hat hackers who attempt to discover exploits and report them to vendors, sometimes for prizes or rewards.
- **Hactivists:** Hactivists is a term that refers to grey hat hackers who rally and protest against different political and social ideas. Hactivists publicly protest against organizations or governments by posting articles, videos, leaking sensitive information, and performing distributed denial of service (DDoS) attacks.
- **Cybercriminals:** Cybercriminal is a term for black hat hackers who are either self-employed or working for large cybercrime organizations. Each year, cyber criminals are responsible for stealing billions of dollars from consumers and businesses.
- **State-sponsored:** State-Sponsored hackers are threat actors who steal government secrets, gather intelligence, and sabotage networks of foreign governments, terrorist groups, and corporations. Most countries in the world participate to some degree in state-sponsored hacking. Depending on a person's perspective, these are either white hat or black hat hackers.

## Cybercriminals

Cybercriminals are threat actors who are motivated to make money using any means necessary. While sometimes cybercriminals work independently, they are more often financed and sponsored by criminal organizations. It is estimated that globally, cybercriminals steal billions of dollars from consumers and businesses every year.

Cybercriminals operate in an underground economy where they buy, sell, and trade exploits and tools. They also buy and sell the personal information and intellectual property that they steal from victims. Cybercriminals target small businesses and consumers, as well as large enterprises and industries.

## Cybersecurity Tasks

Threat actors do not discriminate. They target the vulnerable end devices of home users and small-to-medium sized businesses, as well as large public and private organizations.

To make the internet and networks safer and more secure, we must all develop good cybersecurity awareness. Cybersecurity is a shared responsibility which all users must practice. For example, we must report cybercrime to the appropriate authorities, be aware of potential threats in email and the web, and guard important information from theft.

Organizations must take action and protect their assets, users, and customers. They must develop and practice cybersecurity tasks such as those listed in the figure.

## Cybersecurity checklist



## Attacking the foundation

### IP Vulnerabilities

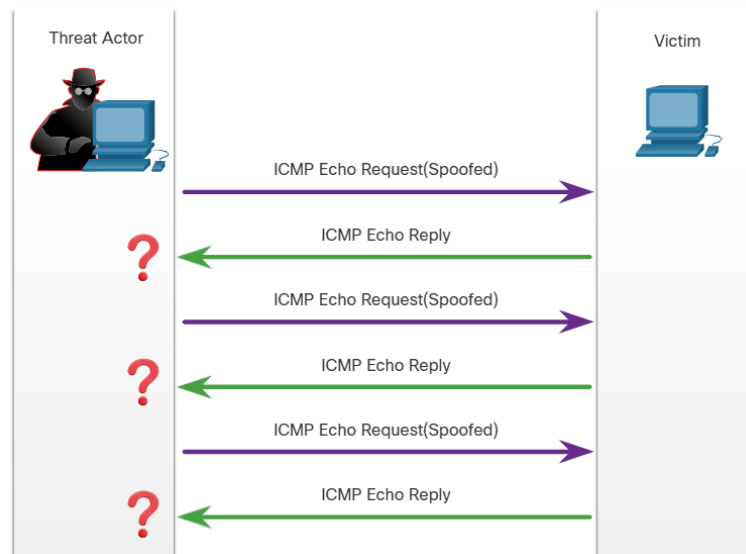
- **ICMP attacks:** Threat actors use Internet Control Message Protocol (ICMP) echo packets (pings) to discover subnets and hosts on a protected network, to generate DoS flood attacks, and to alter host routing tables.
- **Denial-of-Service (DoS) attacks:** Threat actors attempt to prevent legitimate users from accessing information or services.
- **Distributed Denial-of-Service (DDoS) attacks:** Similar to a DoS attack, but features a simultaneous, coordinated attack from multiple source machines.
- **Address spoofing attacks:** Threat actors spoof the source IP address in an attempt to perform blind spoofing or non-blind spoofing.
- **Man-in-the-middle attack (MiTM):** Threat actors position themselves between a source and destination to transparently monitor, capture, and control the communication. They could simply eavesdrop by inspecting captured packets or alter packets and forward them to their original destination.
- **Session hijacking:** Threat actors gain access to the physical network, and then use an MiTM attack to hijack a session

## ICMP Attacks

ICMP was developed to carry diagnostic messages and to report error conditions when routes, hosts, and ports are unavailable. ICMP messages are generated by devices when a network error or outage occurs. The ping command is a user-generated ICMP message, called an echo request that is used to verify connectivity to a destination.

Threat actors use ICMP for reconnaissance and scanning attacks. This enables them to launch information-gathering attacks to map out a network topology, discover which hosts are active (reachable), identify the host operating system (OS fingerprinting), and determine the state of a firewall.

Threat actors also use ICMP for DoS and DDoS attacks, as shown in the ICMP flood attack in the figure.



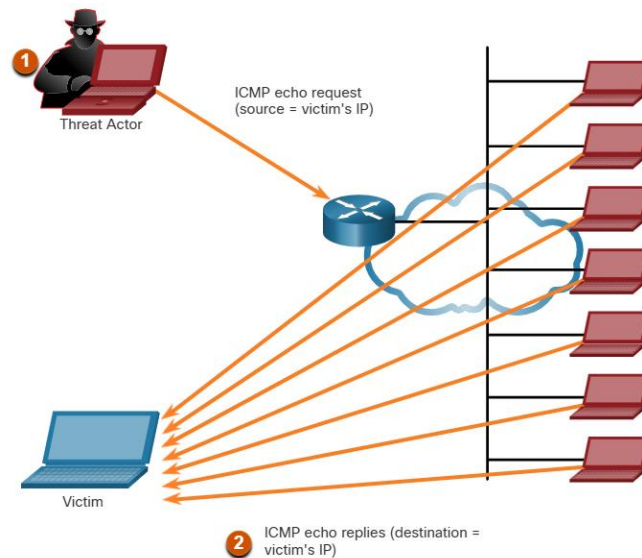
**Note:** ICMP for IPv4 (ICMPv4) and ICMP for IPv6 (ICMPv6) are susceptible to similar types of attacks. The following lists common ICMP messages of interest to threat actors.

- **ICMP echo request and echo reply:** This is used to perform host verification and DoS attacks.
- **ICMP unreachable:** This is used to perform network reconnaissance and scanning attacks.
- **ICMP mask reply:** This is used to map an internal IP network.
- **ICMP redirects:** This is used to lure a target host into sending all traffic through a compromised device and create a MiTM attack.
- **ICMP router discovery:** This is used to inject bogus route entries into the routing table of a target host.

Networks should have strict ICMP access control list (ACL) filtering on the network edge to avoid ICMP probing from the internet. Security analysts should be able to detect ICMP-related attacks by looking at captured traffic and log files. In the case of large networks, security devices, such as firewalls and intrusion detection systems (IDS), should detect such attacks and generate alerts to the security analysts.

### Amplification and Reflection Attacks

Threat actors often use amplification and reflection techniques to create DoS attacks. The example in the figure illustrates how an amplification and reflection technique called a Smurf attack is used to overwhelm a target host.



1. **Amplification** - The threat actor forwards ICMP echo request message to many hosts. These messages contain the source IP address of the victim.
2. **Reflection** - These hosts all reply to the spoofed IP address of the victim to overwhelm it.

**Note:** Newer forms of amplification and reflection attacks such as DNS-based reflection and amplification attacks and Network Time Protocol (NTP) amplification attacks are now being used. Threat actors also use resource exhaustion attacks. These attacks consume the resources of a target host to either to crash it or to consume the resources of a network.

### Address Spoofing Attacks

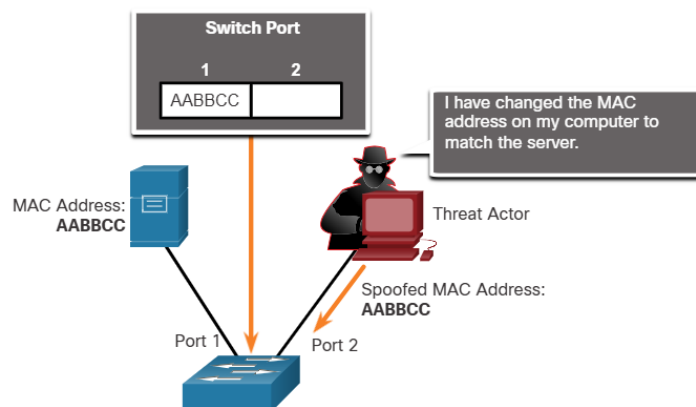
IP address spoofing attacks occur when a threat actor creates packets with false source IP address information to either hide the identity of the sender, or to pose as another legitimate user. The threat actor can then gain access to otherwise inaccessible data or circumvents security configurations. Spoofing is usually incorporated into another attack such as a Smurf attack.

Spoofing attacks can be non-blind or blind:

- **Non-blind spoofing** - The threat actor can see the traffic that is being sent between the host and the target. The threat actor uses non-blind spoofing to inspect the reply packet from the target victim. Non-blind spoofing determines the state of a firewall and sequence-number prediction. It can also hijack an authorized session.
- **Blind spoofing** - The threat actor cannot see the traffic that is being sent between the host and the target. Blind spoofing is used in DoS attacks.

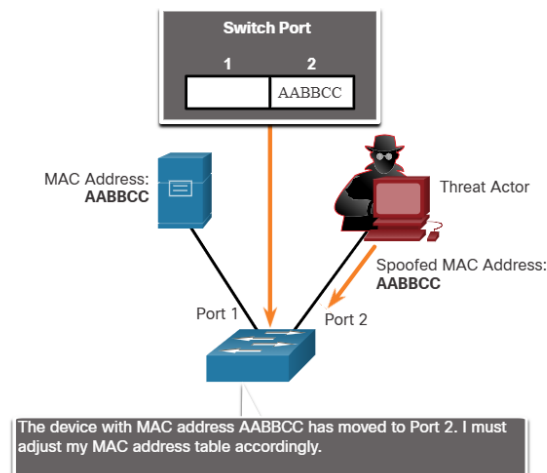
MAC address spoofing attacks are used when threat actors have access to the internal network. Threat actors alter the MAC address of their host to match another known MAC address of a target host, as shown in the figure. The attacking host then sends a frame throughout the network with the newly-configured MAC address. When the switch receives the frame, it examines the source MAC address.

Threat Actor Spoofs a server's MAC Address



The switch overwrites the current CAM table entry and assigns the MAC address to the new port, as shown in the figure. It then forwards frames destined for the target host to the attacking host.

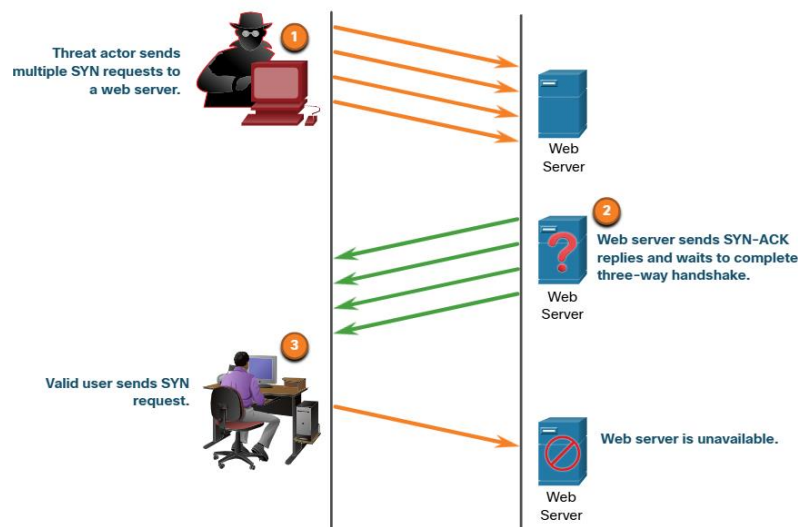
Switch Updates CAM Table with Spoofed Address



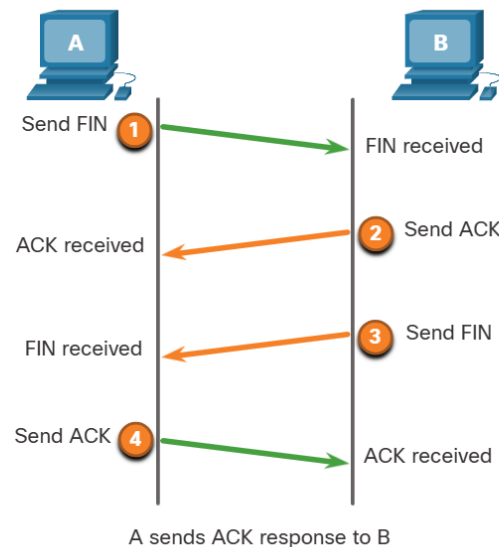
Application or service spoofing is another spoofing example. A threat actor can connect a rogue DHCP server to create an MiTM condition.

## TCP and UDP Vulnerabilities

- **TCP SYN Flood Attack:** The TCP SYN Flood attack exploits the TCP three-way handshake. The figure shows a threat actor continually sending TCP SYN session request packets with a randomly spoofed source IP address to a target. The target device replies with a TCP SYN-ACK packet to the spoofed IP address and waits for a TCP ACK packet. Those responses never arrive. Eventually the target host is overwhelmed with half-open TCP connections, and TCP services are denied to legitimate users.



1. The treat actor sends multiple SYN requests to the web server.
  2. The web server replies with SYN-ACK's for each SYN request and wait for to complete the three way handshake.The treat actor does not respond to the SYN-ACK's.
  3. The valid user cannot access the web server beacuse the web server has too many half-opened TCP connections.
- **TCP Reset Attack:** A TCP reset attack can be used to terminate TCP communications between two hosts. The figure displays how TCP uses a four-way exchange to close the TCP connection using a pair of FIN and ACK segments from each TCP endpoint. A TCP connection terminates when it receives an RST bit. This is an abrupt way to tear down the TCP connection and inform the receiving host to immediately stop using the TCP connection. A threat actor could do a TCP reset attack and send a spoofed packet containing a TCP RST to one or both endpoints.



Terminating a TCP session uses the following four-way exchange process:

1. When the client has no more data to send in the stream, it send a segment with the FIN flag set.
  2. The server sends an ACK to acknowledge the receipt of the FIN to terminate the session from client to server.
  3. The server sends the FIN to the client to terminate the server-to-client session.
  4. The client responds with an ACK to acknowledge the FIN from server.
- **TCP Session Hijacking:** TCP session hijacking is another TCP vulnerability. Although difficult to conduct, a threat actor takes over an already-authenticated host as it communicates with the target. The threat actor must spoof the IP address of one host, predict the next sequence number, and send an ACK to the other host. If successful, the threat actor could send, but not receive, data from the target device.

## UDP Attacks

UDP is not protected by any encryption. You can add encryption to UDP, but it is not available by default. The lack of encryption means that anyone can see the traffic, change it, and send it on to its destination. Changing the data in the traffic will alter the 16-bit checksum, but the checksum is optional and is not always used. When the checksum is used, the threat actor can create a new checksum based on the new data payload, and then record it in the header as a new checksum. The destination device will find that the checksum matches the data without knowing that the data has been altered. This type of attack is not widely used.

**UDP Flood Attacks:** You are more likely to see a UDP flood attack. In a UDP flood attack, all the resources on a network are consumed. The threat actor must use a tool like UDP Unicorn or Low Orbit Ion Cannon. These tools send a flood of UDP packets, often from a spoofed host, to a server on the subnet. The program will sweep through all the known ports trying to find closed

ports. This will cause the server to reply with an ICMP port unreachable message. Because there are many closed ports on the server, this creates a lot of traffic on the segment, which uses up most of the bandwidth. The result is very similar to a DoS attack.

## ARP Vulnerabilities

Hosts broadcast an ARP Request to other hosts on the network segment to determine the MAC address of a host with a particular IP address. All hosts on the subnet receive and process the ARP Request. The host with the matching IP address in the ARP Request sends an ARP Reply.

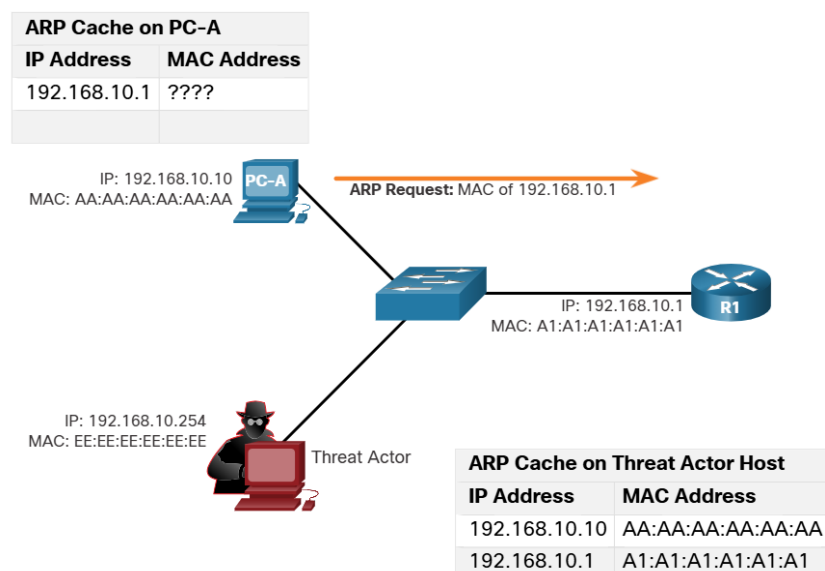
Any client can send an unsolicited ARP Reply called a “gratuitous ARP.” This is often done when a device first boots up to inform all other devices on the local network of the new device’s MAC address. When a host sends a gratuitous ARP, other hosts on the subnet store the MAC address and IP address contained in the gratuitous ARP in their ARP tables.

However, this feature of ARP also means that any host can claim to be the owner of any IP/MAC they choose. A threat actor can poison the ARP cache of devices on the local network, creating an MiTM attack to redirect traffic. The goal is to associate the threat actor’s MAC address with the IP address of the default gateway in the ARP caches of hosts on the LAN segment. This positions the threat actor in between the victim and all other systems outside of the local subnet.

## ARP Cache Poisoning

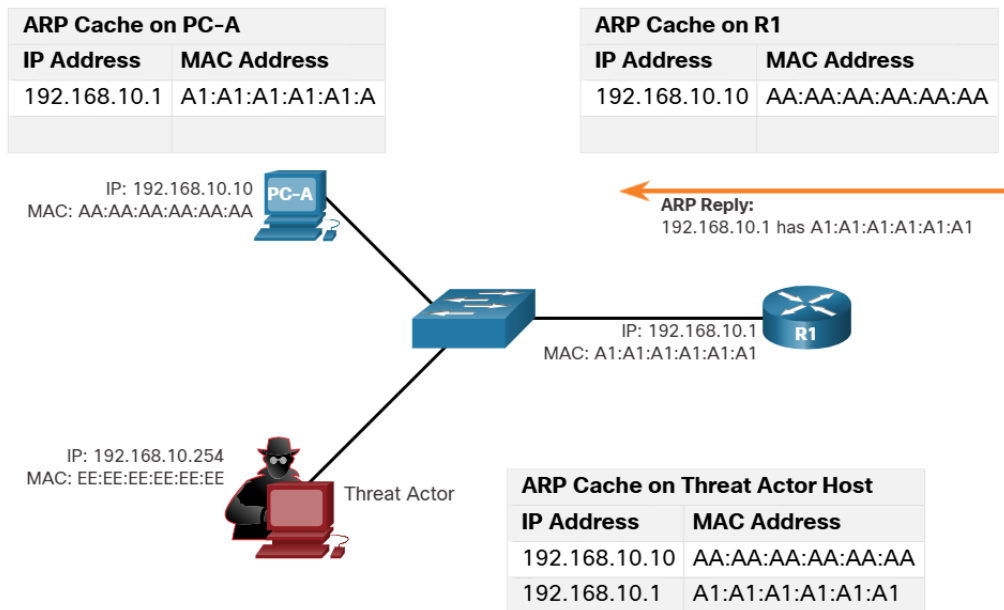
ARP cache poisoning can be used to launch various man-in-the-middle attacks. ARP cache poisoning process is the following:

- **ARP request:** The figure shows how ARP cache poisoning works. PC-A requires the MAC address of its default gateway (R1); therefore, it sends an ARP Request for the MAC address of 192.168.10.1.

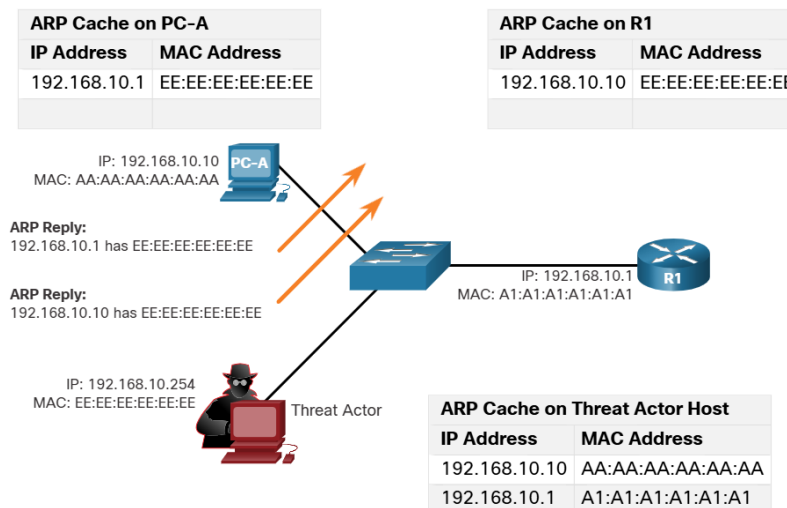




- **ARP reply:** In this figure, R1 updates its ARP cache with the IP and MAC addresses of PC-A. R1 sends an ARP Reply to PC-A, which then updates its ARP cache with the IP and MAC addresses of R1.



- **Spoofed gratuitous ARP Replies:** In the figure, the threat actor sends two spoofed gratuitous ARP Replies using its own MAC address for the indicated destination IP addresses. PC-A updates its ARP cache with its default gateway which is now pointing to the threat actor's host MAC address. R1 also updates its ARP cache with the IP address of PC-A pointing to the threat actor's MAC address. The threat actor's host is executing an ARP poisoning attack. The ARP poisoning attack can be passive or active. Passive ARP poisoning is where threat actors steal confidential information. Active ARP poisoning is where threat actors modify data in transit, or inject malicious data.



**Note:** There are many tools available on the internet to create ARP MiTM attacks including dsniff, Cain & Abel, ettercap, Yersinia, and others.

## **DNS Attacks**

The Domain Name Service (DNS) protocol defines an automated service that matches resource names, such as `www.cisco.com`, with the required numeric network address, such as the IPv4 or IPv6 address. It includes the format for queries, responses, and data and uses resource records (RR) to identify the type of DNS response.

Securing DNS is often overlooked. However, it is crucial to the operation of a network and should be secured accordingly.

DNS attacks include the following:

- DNS open resolver attacks
- DNS stealth attacks
- DNS domain shadowing attacks
- DNS tunneling attacks

**DNS Open Resolver Attacks:** Many organizations use the services of publicly open DNS servers such as GoogleDNS (8.8.8.8) to provide responses to queries. This type of DNS server is called an open resolver. A DNS open resolver answers queries from clients outside of its administrative domain. DNS open resolvers are vulnerable to multiple malicious activities described in the table.

**DNS Domain Shadowing Attacks:** Domain shadowing involves the threat actor gathering domain account credentials in order to silently create multiple sub-domains to be used during the attacks. These subdomains typically point to malicious servers without alerting the actual owner of the parent domain.

## **DHCP Attacks**

A DHCP spoofing attack occurs when a rogue DHCP server is connected to the network and provides false IP configuration parameters to legitimate clients. A rogue server can provide a variety of misleading information:

- **Wrong default gateway** - Threat actor provides an invalid gateway, or the IP address of its host to create a MiTM attack. This may go entirely undetected as the intruder intercepts the data flow through the network.
- **Wrong DNS server** - Threat actor provides an incorrect DNS server address pointing the user to a malicious website.

- **Wrong IP address** -Threat actor provides an invalid IP address, invalid default gateway IP address, or both. The threat actor then creates a DoS attack on the DHCP client.

Assume a threat actor has successfully connected a rogue DHCP server to a switch port on the same subnet as the target clients. The goal of the rogue server is to provide clients with false IP configuration information.

## Email threats

- **Attachment-based attacks:** Threat actors embed malicious content in business files such as an email from the IT department. Legitimate users open malicious content. Malware is used in broad attacks often targeting a specific business vertical to seem legitimate, enticing users working in that vertical to open attachments, or click embedded links.
- **Email spoofing:** Threat actors create email messages with a forged sender address that is meant to fool the recipient into providing money or sensitive information. For example, a bank sends you an email asking you to update your credentials. When this email displays the identical bank logo as mail you have previously opened that was legitimate, it has a higher chance of being opened, having attachments opened and links clicked. The spoofed email may even ask you to verify your credentials so that the bank is assured that you are you, exposing your login information.
- **Spam email:** Threat actors send unsolicited email containing advertisements or malicious files. This type of email is sent most often to solicit a response, telling the threat actor that the email is valid and a user has opened the spam.
- **Open mail relay server:** Threat actors take advantage of enterprise servers that are misconfigured as open mail relays to send large volumes of spam or malware to unsuspecting users. The open mail relay is an SMTP server that allows anybody on the internet to send mail. Because anyone can use the server, they are vulnerable to spammers and worms. Very large volumes of spam can be sent by using an open mail relay. It is important that corporate email servers are never set up as an open relay. This will considerably reduce the amount of unsolicited emails.
- **Homoglyphs:** Threat actors can use text characters that are very similar or even identical to legitimate text characters. For example, it can be difficult to distinguish between an O (upper case letter O) and a 0 (number zero) or a l (lower case “L”) and a 1 (number one). These can be used in phishing emails to make them look very convincing. In DNS, these characters are very different from the real thing. When the DNS record is searched, a completely different URL is found when the link with the homoglyph is used in the search.

Just like any other service that is listening to a port for incoming connections, SMTP servers also may have vulnerabilities. Always keep SMTP software up to date with security and software patches and updates. To further prevent threat actors from completing their task of fooling the end user, implement countermeasures. Use a security appliance specific to email such as the Cisco Email Security Appliance. This will help to detect and block many known types of threats such as phishing, spam, and malware. Also, educate the end user. When attacks make it by the security measures in place, and they will sometimes, the end user is the last line of defense. Teach them how to recognize spam, phishing attempts, suspicious links and URLs, homoglyphs, and to never open suspicious attachments.

## **Web-Exposed Databases**

Web applications commonly connect to a relational database to access data. Because relational databases often contain sensitive data, databases are a frequent target for attacks.

Code injection: Attackers are able to execute commands on a web server's OS through a web application that is vulnerable. This might occur if the web application provides input fields to the attacker for entering malicious data. The attacker's commands are executed through the web application and have the same permissions as the web application. This type of attack is used because often there is insufficient validation of input. An example is when a threat actor injects PHP code into an insecure input field on server page.

SQL injection: SQL is the language used to query a relational database. Threat actors use SQL injections to breach the relational database, create malicious SQL queries, and obtain sensitive data from the relational database. One of the most common database attacks is the SQL injection attack. The SQL injection attack consists of inserting a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify database data, execute administration operations on the database, and sometimes, issue commands to the operating system. Unless an application uses strict input data validation, it will be vulnerable to the SQL injection attack. If an application accepts and processes user-supplied data without any input data validation, a threat actor could submit a maliciously crafted input string to trigger the SQL injection attack. Security analysts should be able to recognize suspicious SQL queries in order to detect if the relational database has been subjected to SQL injection attacks. They need to be able to determine which user ID was used by the threat actor to log in, then identify any information or further access the threat actor could have leveraged after a successful login.

**Cross-Site Scripting :** Not all attacks are initiated from the server side. Cross-Site Scripting (XSS) is where web pages that are executed on the client-side, within their own web browser, are injected with malicious scripts. These scripts can be used by Visual Basic, JavaScript, and others to access a computer, collect sensitive information, or deploy more attacks and spread malware. As with SQL injection, this is often due to the attacker posting content to a trusted website with a lack of input validation. Future visitors to the trusted web site will be exposed to the content provided by the attacker.

These are the two main types of XSS:

- Stored (persistent) -This is permanently stored on the infected server and is received by all visitors to the infected page.
- Reflected (non-persistent) -This only requires that the malicious script is located in a link and visitors must click the infected link to become infected.

These are some ways to prevent or reduce XSS attacks:

- Be sure that web application developers are aware of XSS vulnerabilities and how to avoid them.
- Use an IPS implementation to detect and prevent malicious scripts.
- Use a web proxy to block malicious sites.
- Use a service such as Cisco Umbrella to prevent users from navigating to web sites that are known to be malicious.
- As with all other security measures, be sure to educate end users. Teach them to identify phishing attacks and notify infosec personnel when they are suspicious of anything security-related.

## **Mitigating Common Network Attacks**

### **Defending the Network**

Constant vigilance and ongoing education are required to defend your network against attack. The following are best practices for securing a network:

- Develop a written security policy for the company.
- Educate employees about the risks of social engineering, and develop strategies to validate identities over the phone, via email, or in person.
- Control physical access to systems.
- Use strong passwords and change them often.
- Encrypt and password-protect sensitive data.
- Implement security hardware and software such as firewalls, intrusion prevention systems (IPS), virtual private network (VPN) devices, antivirus software, and content filtering.
- Perform backups and test the backed-up files on a regular basis.
- Shut down unnecessary services and ports.
- Keep patches up-to-date by installing them weekly or daily, if possible, to prevent buffer overflow and privilege escalation attacks.

- Perform security audits to test the network.

## **Mitigating Malware**

Malware, including viruses, worms, and Trojan horses, can cause serious problems on networks and end devices. Network administrators have several means of mitigating these attacks.

**Note:** Mitigation techniques are often referred to in the security community as “countermeasures”.

One way of mitigating virus and Trojan horse attacks is antivirus software. Antivirus software helps prevent hosts from getting infected and spreading malicious code. It requires much more time to clean up infected computers than it does to maintain up-to-date antivirus software and antivirus definitions on the same machines.

Antivirus software is the most widely deployed security product on the market today. Several companies that create antivirus software, such as Symantec, McAfee, and Trend Micro, have been in the business of detecting and eliminating viruses for more than a decade. Many corporations and educational institutions purchase volume licensing for their users. The users are able to log in to a website with their account and download the antivirus software on their desktops, laptops, or servers.

Antivirus products have update automation options so that new virus definitions and new software updates can be downloaded automatically or on demand. This practice is the most critical requirement for keeping a network free of viruses and should be formalized in a network security policy.

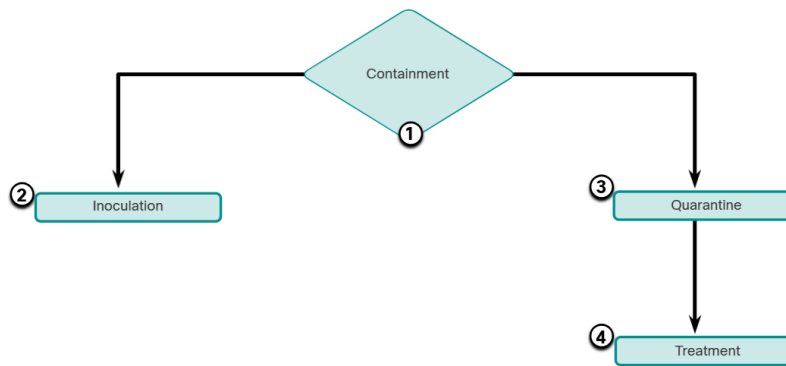
Antivirus products are host-based. These products are installed on computers and servers to detect and eliminate viruses. However, they do not prevent viruses from entering the network, so a network security professional must be aware of the major viruses and keep track of security updates regarding emerging viruses.

Another way to mitigate malware threats is to prevent malware files from entering the network at all. Security devices at the network perimeter can identify known malware files based on their indicators of compromise. The files can be removed from the incoming data stream before they can cause an incident. Unfortunately, threat actors are aware of this countermeasure and frequently alter their malware enough that it evades detection. These exploits will enter the network and will also evade antivirus software. No mitigation technique can be 100% effective. Security incidents are going to happen.

## **Mitigating Worms**

Worms are more network-based than viruses. Worm mitigation requires diligence and coordination on the part of network security professionals.

As shown in the figure, the response to a worm attack can be broken down into four phases: containment, inoculation, quarantine, and treatment.



- **Containment:** The containment phase involves limiting the spread of a worm infection to areas of the network that are already affected. This requires compartmentalization and segmentation of the network to slow down or stop the worm and to prevent currently infected hosts from targeting and infecting other systems. Containment requires using both outgoing and incoming ACLs on routers and firewalls at control points within the network.
- **Inoculation:** The inoculation phase runs parallel to or subsequent to the containment phase. During the inoculation phase, all uninfected systems are patched with the appropriate vendor patch. The inoculation process further deprives the worm of any available targets.
- **Quarantine:** The quarantine phase involves tracking down and identifying infected machines within the contained areas and disconnecting, blocking, or removing them. This isolates these systems appropriately for the treatment phase.
- **Treatment:** The treatment phase involves actively disinfecting infected systems. This can involve terminating the worm process, removing modified files or system settings that the worm introduced, and patching the vulnerability the worm used to exploit the system. Alternatively, in more severe cases, the system may need to be reinstalled to ensure that the worm and its by-products are removed.

## Mitigating Reconnaissance Attacks

Reconnaissance attacks are typically the precursor to other attacks that have the intent of gaining unauthorized access to a network or disrupting network functionality. A network security professional can detect when a reconnaissance attack is underway by receiving notifications from preconfigured alarms. These alarms are triggered when certain parameters are exceeded, such as the number of ICMP requests per second. A variety of technologies and devices can be used to monitor this type of activity and generate an alarm. Cisco's Adaptive Security Appliance (ASA) provides intrusion prevention in a standalone device. Additionally, enterprise routers, such as Cisco Integrated Services Routers (ISR), support network-based intrusion prevention with additional software.

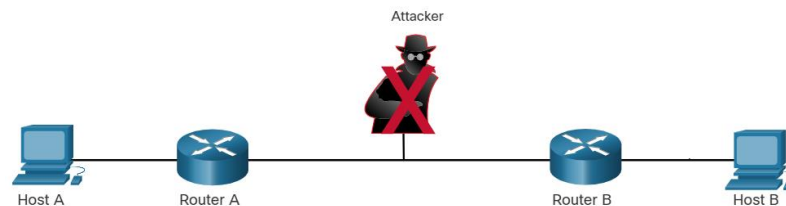
Reconnaissance attacks can be mitigated in several ways, including the following:

- Implementing authentication to ensure proper access.
- Using encryption to render packet sniffer attacks useless.
- Using anti-sniffer tools to detect packet sniffer attacks.
- Implementing a switched infrastructure.
- Using a firewall and IPS.

Anti-sniffer software and hardware tools detect changes in the response time of hosts to determine whether the hosts are processing more traffic than their own traffic loads would indicate. While this does not completely eliminate the threat, as part of an overall mitigation system, it can reduce the number of instances of threat.

Encryption is also effective for mitigating packet sniffer attacks. If traffic is encrypted, using a packet sniffer is of little use because captured data is not readable.

It is impossible to mitigate port scanning but using an intrusion prevention system (IPS) and firewall can limit the information that can be discovered with a port scanner. Ping sweeps can be stopped if ICMP echo and echo-reply are turned off on edge routers; however, when these services are turned off, network diagnostic data is lost. Additionally, port scans can be run without full ping sweeps. The scans simply take longer because inactive IP addresses are also scanned.



## Mitigating Access Attacks

Several techniques are available for mitigating access attacks. These include strong password security, principle of minimum trust, cryptography, and applying operating system and application patches.

A surprising number of access attacks are carried out through simple password guessing or brute-force dictionary attacks against passwords. To defend against this, create and enforce a strong authentication policy which includes:

- Use strong passwords -Strong passwords are at least eight characters and contain uppercase letters, lowercase letters, numbers, and special characters.
- Disable accounts after a specified number of unsuccessful logins has occurred -This practice helps to prevent continuous password attempts.



The network should also be designed using the principle of minimum trust. This means that systems should not use one another unnecessarily. For example, if an organization has a trusted server that is used by untrusted devices, such as web servers, the trusted server should not trust the untrusted devices unconditionally.

Cryptography is a critical component of any modern secure network. Using encryption for remote access to a network is recommended. Routing protocol traffic should also be encrypted. The more that traffic is encrypted, the fewer opportunities hackers have for intercepting data with man-in-the-middle attacks.

The use of encrypted or hashed authentication protocols, along with a strong password policy, greatly reduces the probability of successful access attacks.

Finally, educate employees about the risks of social engineering, and develop strategies to validate identities over the phone, via email, or in person. Multifactor authentication (MFA) has become increasingly common. In this approach, authentication requires two or more independent means of verification. For example, a password may be combined with a code that is sent over a text message. Software or separate devices may be used to generate tokens that are good for only one use. These token values, when provided with a password, provide an additional layer of security that prevents the use of passwords that have been guessed or stolen by threat actors.

In general, access attacks can be detected by reviewing logs, bandwidth utilization, and process loads. The network security policy should specify that logs are formally maintained for all network devices and servers. By reviewing logs, network security personnel can determine if an unusual number of failed login attempts have occurred.

## **Mitigating DoS Attacks**

One of the first signs of a DoS attack is a large number of user complaints about unavailable resources or unusually slow network performance. To minimize the number of attacks, a network utilization software package should be running at all times. Network behavior analysis can detect unusual patterns of usage that indicate that a DoS attack is occurring. A means of detecting unusual network behavior should be required by the organization's network security policy. A network utilization graph showing unusual activity could also indicate a DoS attack.

DoS attacks could be a component of a larger offensive. DoS attacks can lead to problems in the network segments of the computers being attacked. For example, the packet-per-second capacity of a router between the internet and a LAN might be exceeded by an attack, compromising not only the target system but also the network devices that the traffic must pass through. If the attack is conducted on a sufficiently large scale, entire geographical regions of internet connectivity could be compromised. Historically, many DoS attacks were sourced from spoofed addresses. Cisco routers and switches support a number of antispoofing technologies, such as port security, Dynamic Host Configuration Protocol (DHCP) snooping, IP Source Guard, Dynamic Address Resolution Protocol (DAI) Inspection, and access control lists (ACLs).

## Secure WLANs

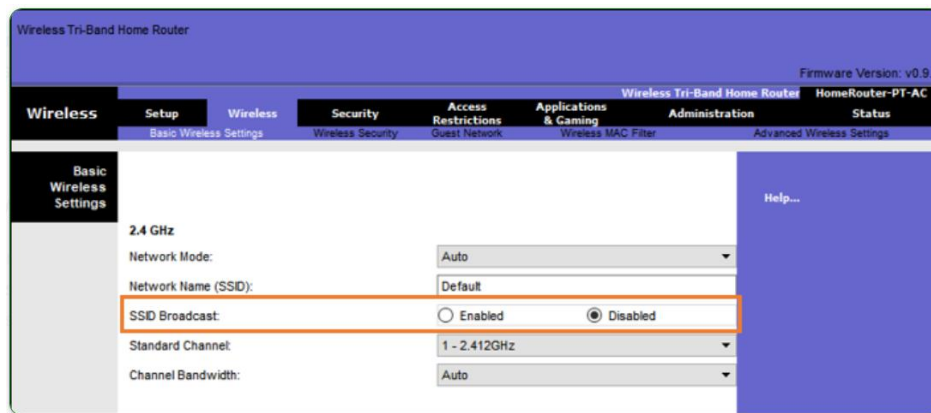
### SSID Cloaking and MAC Address Filtering

Wireless signals can travel through solid matter, such as ceilings, floors, walls, outside of the home, or office space. Without stringent security measures in place, installing a WLAN can be the equivalent of putting Ethernet ports everywhere, even outside.

To address the threats of keeping wireless intruders out and protecting data, two early security features were used and are still available on most routers and APs: SSID cloaking and MAC address filtering.

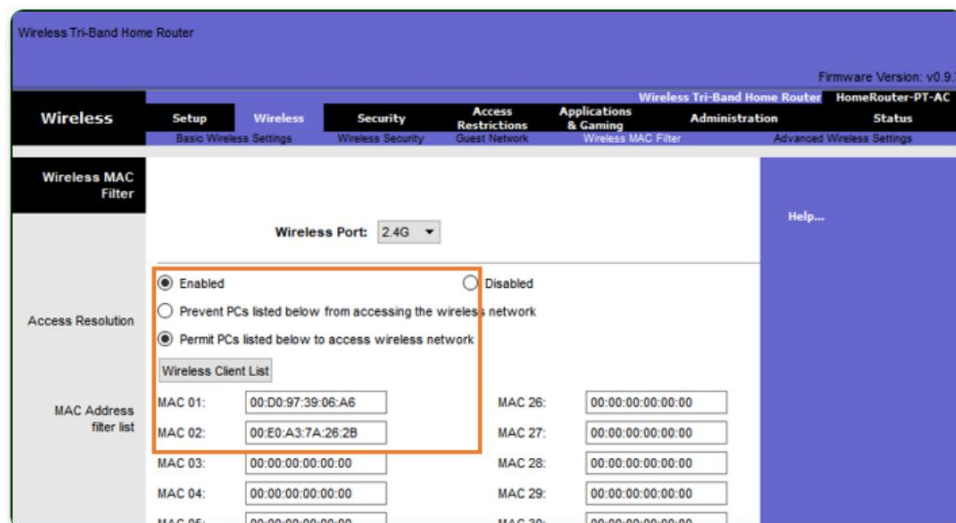
### SSID Cloaking

APs and some wireless routers allow the SSID beacon frame to be disabled, as shown in the figure. Wireless clients must manually configure the SSID to connect to the network.



### MAC Addresses Filtering

An administrator can manually permit or deny clients wireless access based on their physical MAC hardware address. In the figure, the router is configured to permit two MAC addresses. Devices with different MAC addresses will not be able to join the 2.4GHz WLAN.



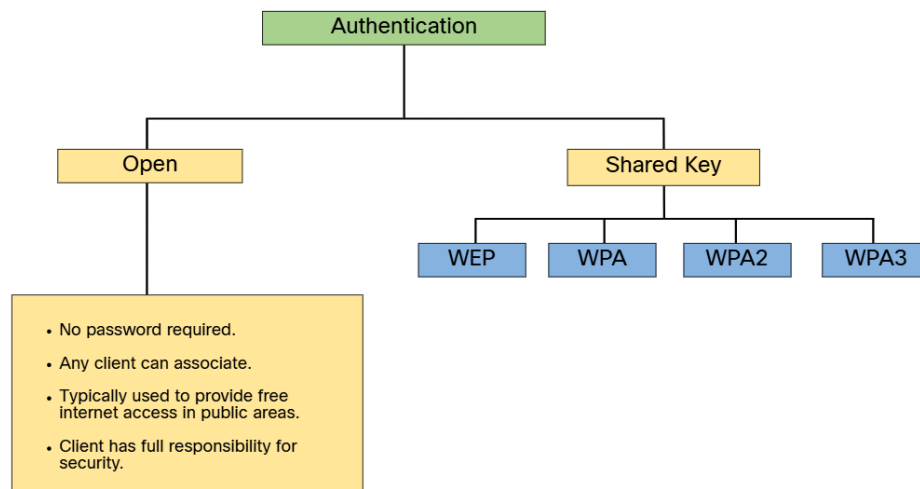
## 802.11 Original Authentication Methods

Although these two features would deter most users, the reality is that neither SSID cloaking nor MAC address filtering would deter a crafty intruder. SSIDs are easily discovered even if APs do not broadcast them and MAC addresses can be spoofed. The best way to secure a wireless network is to use authentication and encryption systems.

Two types of authentication were introduced with the original 802.11 standard:

- **Open system authentication-** Any wireless client should easily be able to connect and should only be used in situations where security is of no concern, such as those providing free internet access like cafes, hotels, and in remote areas. The wireless client is responsible for providing security such as using a virtual private network (VPN) to connect securely. VPNs provide authentication and encryption services. VPNs are beyond the scope of this topic.
- **Shared key authentication-** Provides mechanisms, such as WEP, WPA, WPA2, and WPA3 to authenticate and encrypt data between a wireless client and AP. However, the password must be pre-shared between both parties to connect.

The following chart summarizes these authentication methods.



## Shared Key Authentication Methods

There are four shared key authentication techniques available, as described in the table. Until the availability of WPA3 devices becomes ubiquitous, wireless networks should use the WPA2 standard.

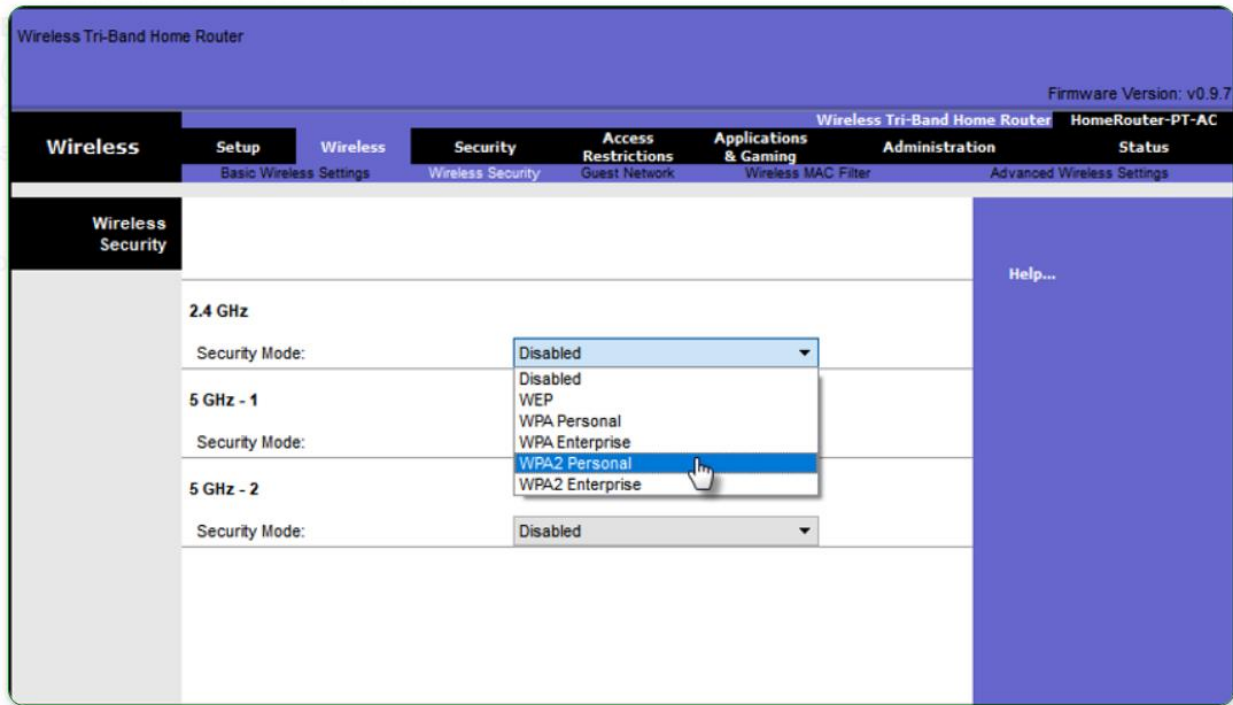
Authentication Method	Description
Wired Equivalent Privacy (WEP)	The original 802.11 specification designed to secure the data using the Rivest Cipher 4 (RC4) encryption method with a static key. However, the key never changes when exchanging packets. This makes it easy to hack. WEP is no longer recommended and should never be used.
Wi-Fi Protected Access (WPA)	A Wi-Fi Alliance standard that uses WEP, but secures the data with the much stronger Temporal Key Integrity Protocol (TKIP) encryption algorithm. TKIP changes the key for each packet, making it much more difficult to hack.
WPA2	WPA2 is the current industry standard for securing wireless networks. It uses the Advanced Encryption Standard (AES) for encryption. AES is currently considered the strongest encryption protocol.
WPA3	The next generation of Wi-Fi security. All WPA3-enabled devices use the latest security methods, disallow outdated legacy protocols, and require the use of Protected Management Frames (PMF). However, devices with WPA3 are not yet readily available.

### Authenticating a Home User

Home routers typically have two choices for authentication: WPA and WPA2. WPA2 is the stronger of the two. The figure shows the option to select one of two WPA2 authentication methods:

- **Personal** - Intended for home or small office networks, users authenticate using a pre-shared key (PSK). Wireless clients authenticate with the wireless router using a pre-shared password. No special authentication server is required.
- **Enterprise** - Intended for enterprise networks but requires a Remote Authentication Dial-In User Service (RADIUS) authentication server. Although more complicated to set up, it provides additional security. The device must be authenticated by the RADIUS server and then users must authenticate using 802.1X standard, which uses the Extensible Authentication Protocol (EAP) for authentication.

In the figure, the administrator is configuring the wireless router with WPA2 Personal authentication on the 2.4 GHz band.



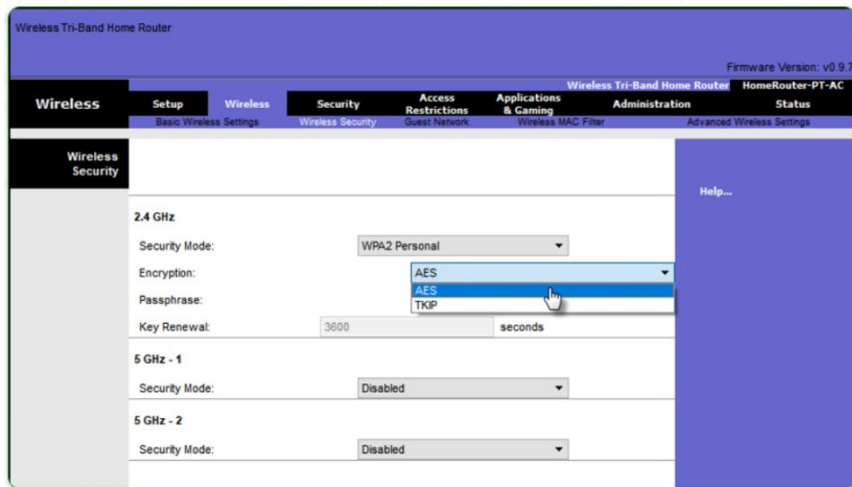
## Encryption Methods

Encryption is used to protect data. If an intruder has captured encrypted data, they would not be able to decipher it in any reasonable amount of time.

The WPA and WPA2 standards use the following encryption protocols:

- **Temporal Key Integrity Protocol (TKIP)** - TKIP is the encryption method used by WPA. It provides support for legacy WLAN equipment by addressing the original flaws associated with the 802.11 WEP encryption methods. It makes use of WEP, but encrypts the Layer 2 payload using TKIP, and carries out a Message Integrity Check (MIC) in the encrypted packet to ensure the message has not been altered.
- **Advanced Encryption Standard (AES)** - AES is the encryption method used by WPA2. It is the preferred method because it is a far stronger method of encryption. It uses the Counter Cipher Mode with Block Chaining Message Authentication Code Protocol (CCMP) that allows destination hosts to recognize if the encrypted and non-encrypted bits have been altered.

In the figure, the administrator is configuring the wireless router to use WPA2 with AES encryption on the 2.4 GHz band.

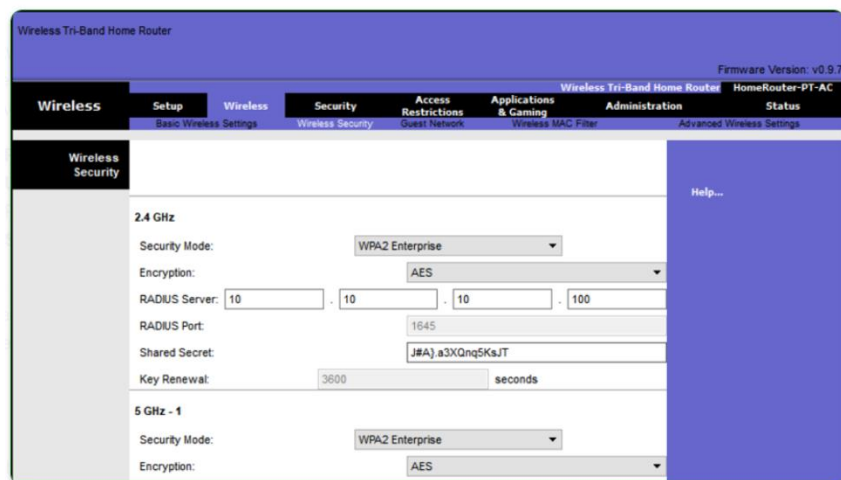


## Authentication in the Enterprise

In networks that have stricter security requirements, an additional authentication or login is required to grant wireless clients such access. The Enterprise security mode choice requires an Authentication, Authorization, and Accounting (AAA) RADIUS server.

- **RADIUS Server IP address** - This is the reachable address of the RADIUS server.
- **UDP port numbers** - Officially assigned UDP ports 1812 for RADIUS Authentication, and 1813 for RADIUS Accounting, but can also operate using UDP ports 1645 and 1646, as shown in the figure.
- **Shared key** - Used to authenticate the AP with the RADIUS server.

In the figure, the administrator is configuring the wireless router with WPA2 Enterprise authentication using AES encryption. The RADIUS server IPv4 address is configured as well with a strong password to be used between the wireless router and the RADIUS server.



The shared key is not a parameter that must be configured on a wireless client. It is only required on the AP to authenticate with the RADIUS server. User authentication and authorization is

handled by the 802.1X standard, which provides a centralized, server-based authentication of end users.

The 802.1X login process uses EAP to communicate with the AP and RADIUS server. EAP is a framework for authenticating network access. It can provide a secure authentication mechanism and negotiate a secure private key which can then be used for a wireless encryption session using TKIP or AES encryption.

## WPA3

At the time of this writing, devices that support WPA3 authentication were not readily available. However, WPA2 is no longer considered secure. WPA3, if available, is the recommended 802.11 authentication method. WPA3 includes four features:

- WPA3-Personal
- WPA3-Enterprise
- Open Networks
- Internet of Things (IoT) Onboarding

**WPA3-Personal:** In WPA2-Personal, threat actors can listen in on the “handshake” between a wireless client and the AP and use a brute force attack to try and guess the PSK. WPA3-Personal thwarts this attack by using Simultaneous Authentication of Equals (SAE), a feature specified in the IEEE 802.11-2016. The PSK is never exposed, making it impossible for the threat actor to guess.

**WPA3-Enterprise:** WPA3-Enterprise still uses 802.1X/EAP authentication. However, it requires the use of a 192-bit cryptographic suite and eliminates the mixing of security protocols for previous 802.11 standards. WPA3-Enterprise adheres to the Commercial National Security Algorithm (CNSA) Suite which is commonly used in high security Wi-Fi networks.

**Open Networks:** Open networks in WPA2 send user traffic in unauthenticated, clear text. In WPA3, open or public Wi-Fi networks still do not use any authentication. However, they do use Opportunistic Wireless Encryption (OWE) to encrypt all wireless traffic.

**IoT Onboarding:** Although WPA2 included Wi-Fi Protected Setup (WPS) to quickly onboard devices without configuring them first, WPS is vulnerable to a variety of attacks and is not recommended. Furthermore, IoT devices are typically headless, meaning they have no built-in GUI for configuration, and needed any easy way to get connected to the wireless network. The Device Provisioning Protocol (DPP) was designed to address this need. Each headless device has a hardcoded public key. The key is typically stamped on the outside of the device or its packaging as a Quick Response (QR) code. The network administrator can scan the QR code and quickly onboard the device. Although not strictly part of the WPA3 standard, DPP will replace WPS over time.

## **Operating System Vulnerabilities**

Operating systems consist of millions of lines of code. Installed software can also contain millions of lines of code. With all this code come vulnerabilities. Vulnerability is some flaw or weakness that can be exploited by an attacker to reduce the viability of a computer's information. To take advantage of operating system vulnerability, the attacker must use a technique or a tool to exploit the vulnerability. The attacker can then use the vulnerability to get the computer to act in a fashion outside of its intended design. In general, the goal is to gain unauthorized control of the computer, change permissions, or to manipulate or steal data.

Let's see some common Windows OS security recommendations:

### **Virus or malware protection**

- By default, Windows uses Windows Defender for malware protection.
- Windows Defender provides a suite of protection tools built into the system.
- If Windows Defender is turned off, the system becomes more vulnerable to attacks and malware.

### **Unknown or unmanaged services**

- There are many services that run behind the scenes.
- It is important to make sure that each service is identifiable and safe.
- With an unknown service running in the background, the computer can be vulnerable to attack.

### **Encryption**

- When data is not encrypted, it can easily be gathered and exploited.
- This is not only important for desktop computers, but especially mobile devices.

### **Security policy**

- A good security policy must be configured and followed.
- Many settings in the Windows Security Policy control can prevent attacks.

### **Firewall**

- By default, Windows uses Windows Firewall to limit communication with devices on the network.
- Over time, rules may no longer apply.
- For example, a port may be left open that should no longer be readily available.



- It is important to review firewall settings periodically to ensure that the rules are still applicable and remove any that no longer apply.

### **File and share permissions**

- These permissions must be set correctly.
- It is easy to just give the “Everyone” group Full Control, but this allows all people to do what they want to all files.
- It is best to provide each user or group with the minimum necessary permissions for all files and folders.

### **Weak or no password**

- Many people choose weak passwords or do not use a password at all.
- It is especially important to make sure that all accounts, especially the Administrator account, have a very strong password.

### **Login as Administrator**

- When a user logs in as an administrator, any program that they run will have the privileges of that account.
- It is best to log in as a Standard User and only use the administrator password to accomplish certain tasks.

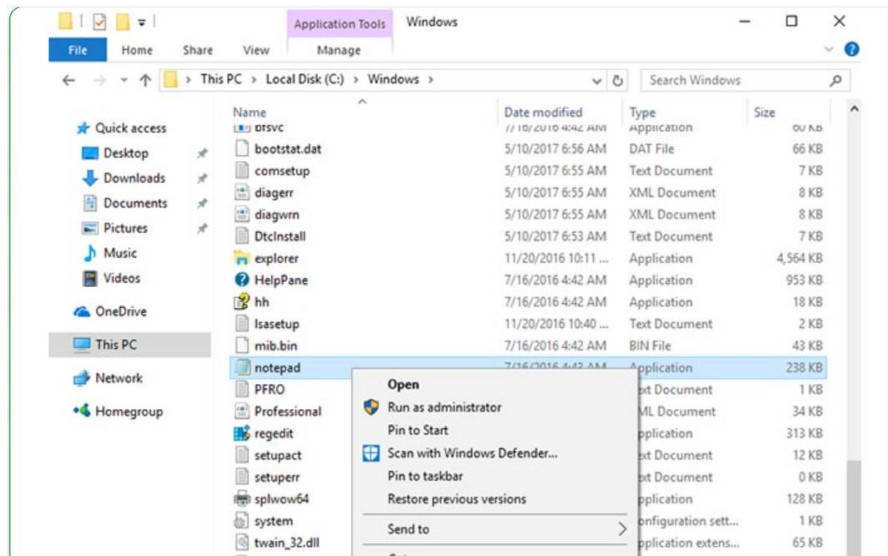
## **Windows Configuration and Monitoring**

### **Run as Administrator**

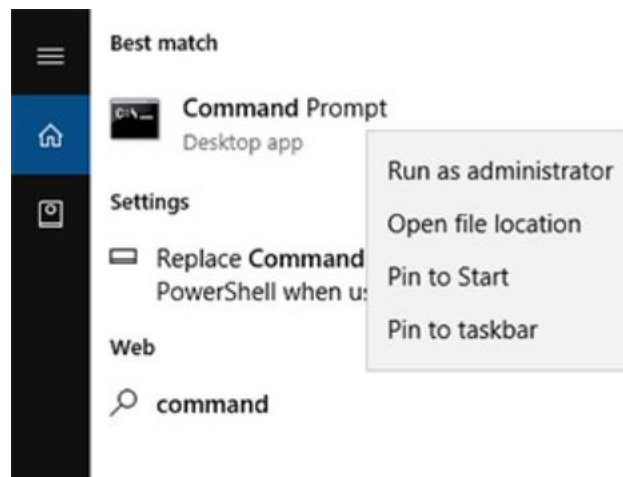
As a security best practice, it is not advisable to log on to Windows using the Administrator account or an account with administrative privileges. This is because any program that is executed while logged on with those privileges will inherit administrative privileges. Malware that has administrative privileges has full access to all the files and folders on the computer.

Sometimes, it is necessary to run or install software that requires the privileges of the Administrator. To accomplish this, there are two different ways to install it.

- Administrator: Right-click the command in the Windows File Explorer and choose Run as Administrator from the Context Menu.



- Administrator CMD: Search for **command**, right-click the executable file, and choose Run as Administrator from the Context Menu. Every command that is executed from this command line will be carried out with the Administrator privileges, including installation of software.



## Local Users and Domains

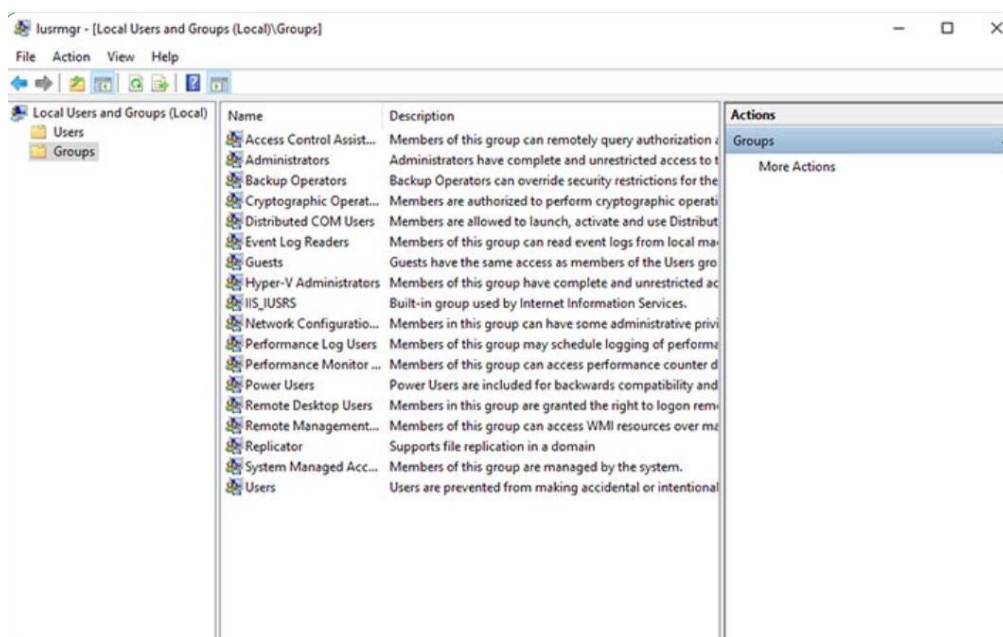
When you start a new computer for the first time, or you install Windows, you will be prompted to create a user account. This is known as a local user. This account will contain all of your customization settings, access permissions, file locations, and many other user-specific data. There are also two other accounts that are present, the guest, and the administrator. Both of these accounts are disabled by default.

As a security best practice, do not enable the Administrator account and do not give standard users administrative privileges. If a user needs to perform any function that requires administrative privileges, the system will ask for the Administrator password and allow only that task to be performed as an administrator. Requiring the administrator password protects the

computer by preventing any software that is not authorized from installing, executing, or accessing files.

The Guests account should not be enabled. The guest account does not have a password associated with it because it is created when a computer is going to be used by many different people who do not have accounts on the computer. Each time the guest account logs on, a default environment is provided to them with limited privileges.

To make administration of users easier, Windows uses groups. A group will have a name and a specific set of permissions associated with it. When a user is placed into a group, the permissions of that group are given to that user. A user can be placed into multiple groups to be provided with many different permissions. When the permissions overlap, certain permissions, like “explicitly deny” will override the permission provided by a different group. There are many different user groups built into Windows that are used for specific tasks. For example, the Performance Log Users group allows members to schedule logging of performance counters and collect logs either locally or remotely. Local users and groups are managed with the lusrmgr.msc control panel applet, as shown in the figure.



In addition to groups, Windows can also use domains to set permissions. A domain is a type of network service where all of the users, groups, computers, peripherals, and security settings are stored on and controlled by a database. This database is stored on special computers or groups of computers called domain controllers (DCs). Each user and computer on the domain must authenticate against the DC to logon and access network resources. The security settings for each user and each computer are set by the DC for each session. Any setting supplied by the DC defaults to the local computer or user account setting.

## CLI and PowerShell

The Windows command line interface (CLI) can be used to run programs, navigate the file system, and manage files and folders. In addition, files called batch files can be created to execute multiple commands in succession, much like a basic script.

To open the Windows CLI, search for **cmd.exe** and click the program. Remember that right-clicking the program provides the option to run as administrator, giving much more power to the commands that will be used.

The prompt displays the current location within the file system. These are a few things to remember when using the CLI:

- The file names and paths are not case-sensitive, by default.
- Storage devices are assigned a letter for reference. The drive letter is followed by a colon and backslash (\). This indicates the root, or highest level, of the device. Folder and file hierarchy on the device is indicated by separating them with the backslash. For example, the path C:\Users\Jim\Desktop\file.txt refers to a file called file.txt that is in the Desktop folder within the Jim folder within the Users folder at the root of drive C:.
- Commands that have optional switches use the forward slash (/) to delineate between the command and the switch option.
- You can use the **Tab** key to auto-complete commands when directories or files are referenced.
- Windows keeps a history of the commands that were entered during a CLI session. Access previously entered commands by using the up and down arrow keys.
- To switch between storage devices, type the letter of the device, followed by a colon, and then press **Enter**.

Even though the CLI has many commands and features, it cannot work together with the core of Windows or the GUI. Another environment, called the Windows PowerShell, can be used to create scripts to automate tasks that the regular CLI is unable to create. PowerShell also provides a CLI for initiating commands. PowerShell is an integrated program within Windows and can be opened by searching for “powershell” and clicking the program. Like the CLI, PowerShell can also be run with administrative privileges.

These are the types of commands that PowerShell can execute:

- **cmdlets** - These commands perform an action and return an output or object to the next command that will be executed.
- **PowerShell scripts** - These are files with a **.ps1** extension that contain PowerShell commands that are executed.
- **PowerShell functions** - These are pieces of code that can be referenced in a script.

To see more information about Windows PowerShell and get started using it, type help in PowerShell, as shown in the command output.

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Try the new cross-platform PowerShell https://aka.ms/pscore6
PS C:\WINDOWS\system32> help
TOPIC
    Windows PowerShell Help System
SHORT DESCRIPTION
    Displays help about Windows PowerShell cmdlets and concepts.
LONG DESCRIPTION
    Windows PowerShell Help describes Windows PowerShell cmdlets,
    functions, scripts, and modules, and explains concepts, including
    the elements of the Windows PowerShell language.
    Windows PowerShell does not include help files, but you can read the
    help topics online, or use the Update-Help cmdlet to download help files
    to your computer and then use the Get-Help cmdlet to display the help
    topics at the command line.
    You can also use the Update-Help cmdlet to download updated help files
    as they are released so that your local help content is never obsolete.
    Without help files, Get-Help displays auto-generated help for cmdlets,
    functions, and scripts.
ONLINE HELP
    You can find help for Windows PowerShell online in the TechNet Library
    beginning at http://go.microsoft.com/fwlink/?LinkID=108518.
    To open online help for any cmdlet or function, type:
    Get-Help -Online
UPDATE-HELP
    To download and install help files on your computer:
        1. Start Windows PowerShell with the "Run as administrator" option.
        2. Type:
            Update-Help
    After the help files are installed, you can use the Get-Help cmdlet to
    display the help topics. You can also use the Update-Help cmdlet to
    download updated help files so that your local help files are always
    up-to-date.
    For more information about the Update-Help cmdlet, type:
    Get-Help Update-Help -Online
-- More --
```

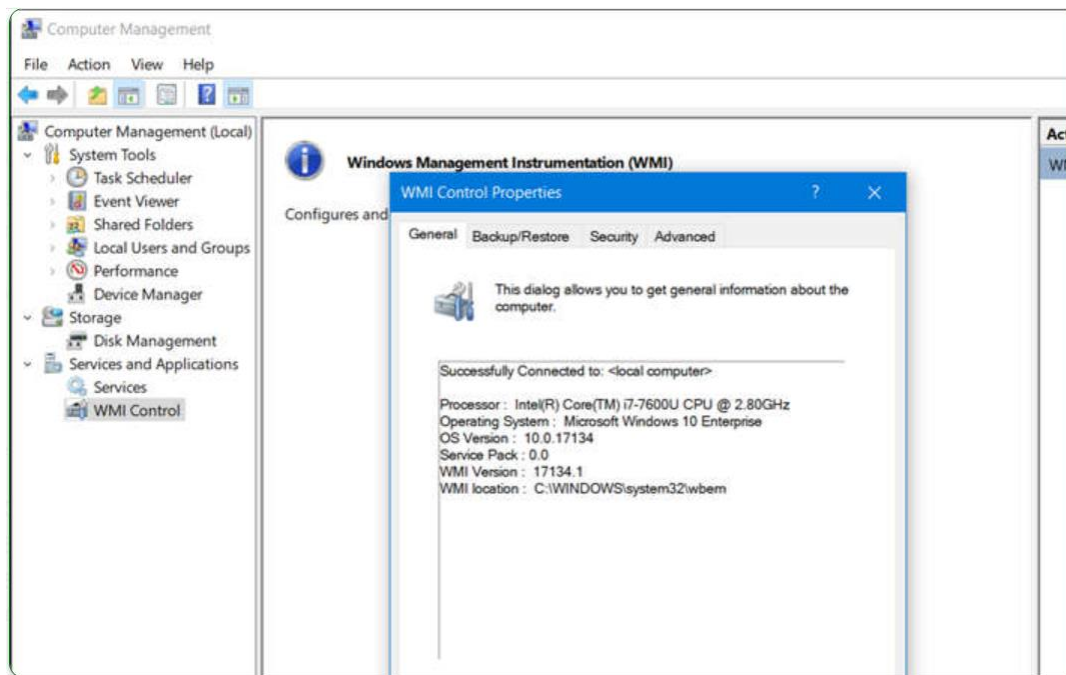
There are four levels of help in Windows PowerShell:

- **get-help** PS command - Displays basic help for a command
- **get-help** PS command [-examples] - Displays basic help for a command with examples
- **get-help** PS command [-detailed] - Displays detailed help for a command with examples
- **get-help** PS command [-full] - Displays all help information for a command with examples in greater depth

## Windows Management Instrumentation

Windows Management Instrumentation (WMI) is used to manage remote computers. It can retrieve information about computer components, hardware and software statistics, and monitor the health of remote computers. To open the WMI control from the Control Panel, double-click **Administrative Tools > Computer Management** to open the Computer Management window, expand the **Services and Applications** tree and right-click the **WMI Control icon > Properties**.

The WMI Control Properties window is shown in the figure.



These are the four tabs in the WMI Control Properties window:

- **General** - Summary information about the local computer and WMI
- **Backup/Restore** - Allows manual backup of statistics gathered by WMI
- **Security** - Settings to configure who has access to different WMI statistics
- **Advanced** - Settings to configure the default namespace for WMI

Some attacks today use WMI to connect to remote systems, modify the registry, and run commands. WMI helps them to avoid detection because it is common traffic, most often trusted by the network security devices and the remote WMI commands do not usually leave evidence on the remote host. Because of this, WMI access should be strictly limited.

## The net Command

Windows has many commands that can be entered at the command line. One important command is the **net** command, which is used in the administration and maintenance of the OS. The **net** command supports many subcommands that follow the **net** command and can be combined with switches to focus on specific output.

To see a list of the many **net** commands, type **net help** at the command prompt. The command output shows the commands that the net command can use. To see verbose help about any of the net commands, type `C:\> net help`, as shown below.

```
C:\> net help
The syntax of this command is:
NET HELP
command
-or-
NET command /HELP
Commands available are:
NET ACCOUNTS          NET HELPMMSG          NET STATISTICS
NET COMPUTER          NET LOCALGROUP        NET STOP
NET CONFIG            NET PAUSE              NET TIME
NET CONTINUE          SESSION               NET USE
NET FILE              NET SHARE              NET USER
NET GROUP             NET START              NET VIEW
NET HELP
NET HELP NAMES explains different types of names in NET HELP syntax lines.
NET HELP SERVICES lists some of the services you can start.
NET HELP SYNTAX explains how to read NET HELP syntax lines.
NET HELP command | MORE displays Help one screen at a time.
C:\>
```

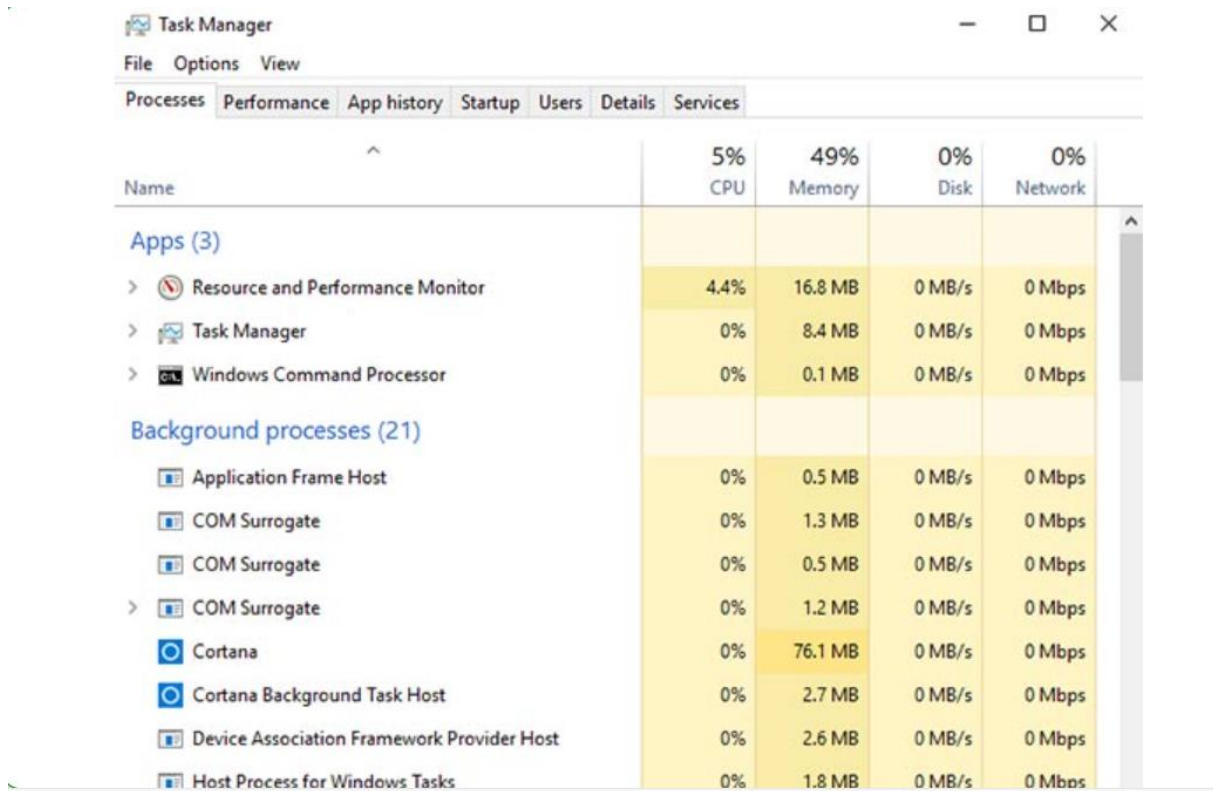
Let us learn more about some common net commands.

- **net accounts:** Sets password and logon requirements for users
- **net session:** Lists or disconnects sessions between a computer and other computers on the network
- **net share:** Creates, removes, or manages shared resources
- **net start:** Starts a network service or lists running network services
- **net stop:** Stops a network service
- **net use:** Connects, disconnects, and displays information about shared network resources
- **net view:** Shows a list of computers and network devices on the network

## Task Manager and Resource Monitor

There are two very important and useful tools to help an administrator to understand the many different applications, services, and processes that are running on a Windows computer. These tools also provide insight into the performance of the computer, such as CPU, memory, and network usage. These tools are especially useful when investigating a problem where malware is suspected. When a component is not performing the way that it should be, these tools can be used to determine what the problem might be.

**Task Manager:** The Task Manager, which is shown in the figure, provides a lot of information about the software that is running and the general performance of the computer.



The screenshot shows the Windows Task Manager application with the 'Performance' tab selected. The top bar displays overall system performance: CPU at 5%, Memory at 49%, Disk at 0%, and Network at 0%. The main area is divided into two sections: 'Apps (3)' and 'Background processes (21)'. The 'Apps' section lists three foreground applications, and the 'Background processes' section lists various system services. Each process is shown with its name, icon, and resource usage across the four categories.

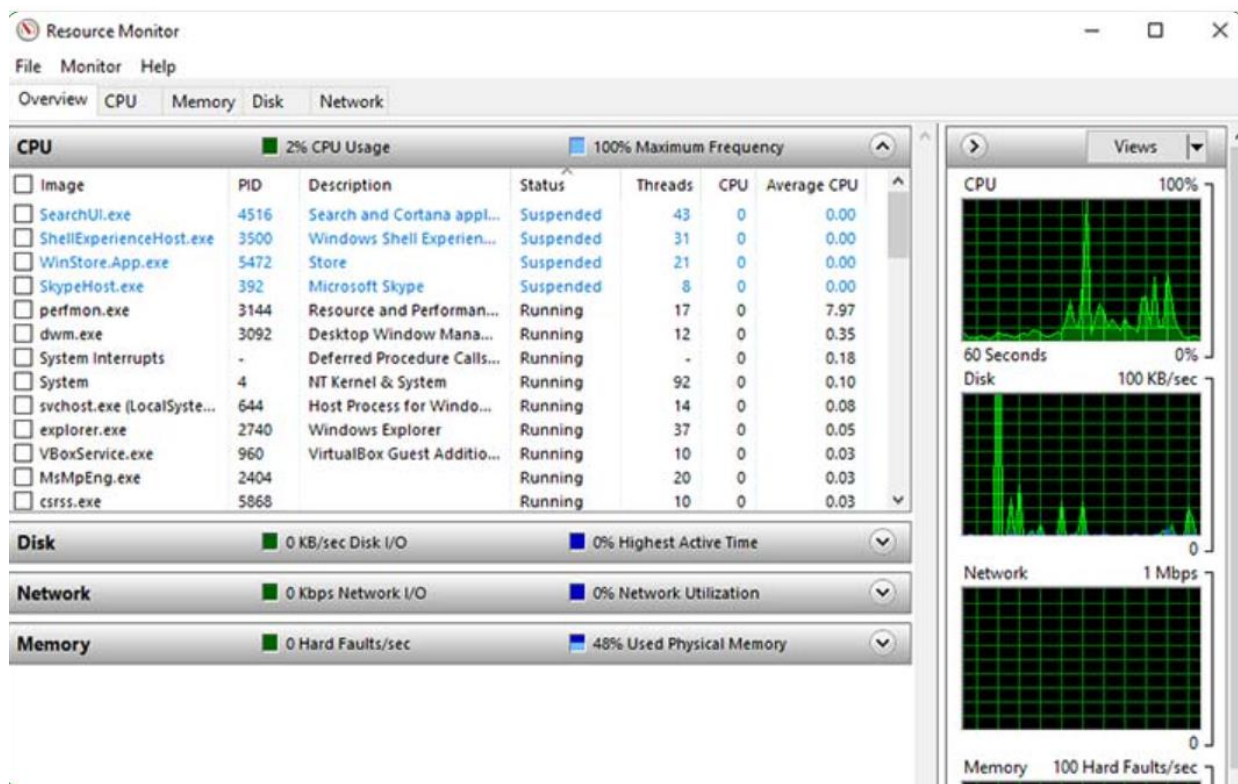
Name	5% CPU	49% Memory	0% Disk	0% Network
<b>Apps (3)</b>				
Resource and Performance Monitor	4.4%	16.8 MB	0 MB/s	0 Mbps
Task Manager	0%	8.4 MB	0 MB/s	0 Mbps
Windows Command Processor	0%	0.1 MB	0 MB/s	0 Mbps
<b>Background processes (21)</b>				
Application Frame Host	0%	0.5 MB	0 MB/s	0 Mbps
COM Surrogate	0%	1.3 MB	0 MB/s	0 Mbps
COM Surrogate	0%	0.5 MB	0 MB/s	0 Mbps
COM Surrogate	0%	1.2 MB	0 MB/s	0 Mbps
Cortana	0%	76.1 MB	0 MB/s	0 Mbps
Cortana Background Task Host	0%	2.7 MB	0 MB/s	0 Mbps
Device Association Framework Provider Host	0%	2.6 MB	0 MB/s	0 Mbps
Host Process for Windows Tasks	0%	1.8 MB	0 MB/s	0 Mbps

- **Processes**
  - Lists all of the programs and processes that are currently running.
  - Displays the CPU, memory, disk, and network utilization of each process.
  - The properties of a process can be examined or ended if it is not behaving properly or has stalled.
- **Performance**
  - A view of all the performance statistics provides a useful overview of the CPU, memory, disk, and network performance.
  - Clicking each item in the left pane will show detailed statistics of that item in the right pane.



- **App history**
  - The use of resources by application over time provides insight into applications that are consuming more resources than they should.
  - Click **Options** and **Show history for all processes** to see the history of every process that has run since the computer was started.
- **Startup**
  - All of the applications and services that start when the computer is booted are shown in this tab.
  - To disable a program from starting at startup, right-click the item and choose Disable.
- **Users**
  - All of the users that are logged on to the computer are shown in this tab.
  - Also shown are all the resources that each user's applications and processes are using.
  - From this tab, an administrator can disconnect a user from the computer.
- **Details**
  - Similar to the Processes tab, this tab provides additional management options for processes such as setting a priority to make the processor devote more or less time to a process.
  - CPU affinity can also be set which determines which core or CPU a program will use.
  - Also, a useful feature called Analyze wait chain shows any process for which another process is waiting.
  - This feature helps to determine if a process is simply waiting or is stalled.
- **Services**
  - All the services that are loaded are shown in this tab.
  - The process ID (PID) and a short description are also shown along with the status of either Running or Stopped.
  - At the bottom, there is a button to open the Services console which provides additional management of services.

**Resource Monitor:** When more detailed information about resource usage is needed, you can use the Resource Monitor, as shown in the figure.



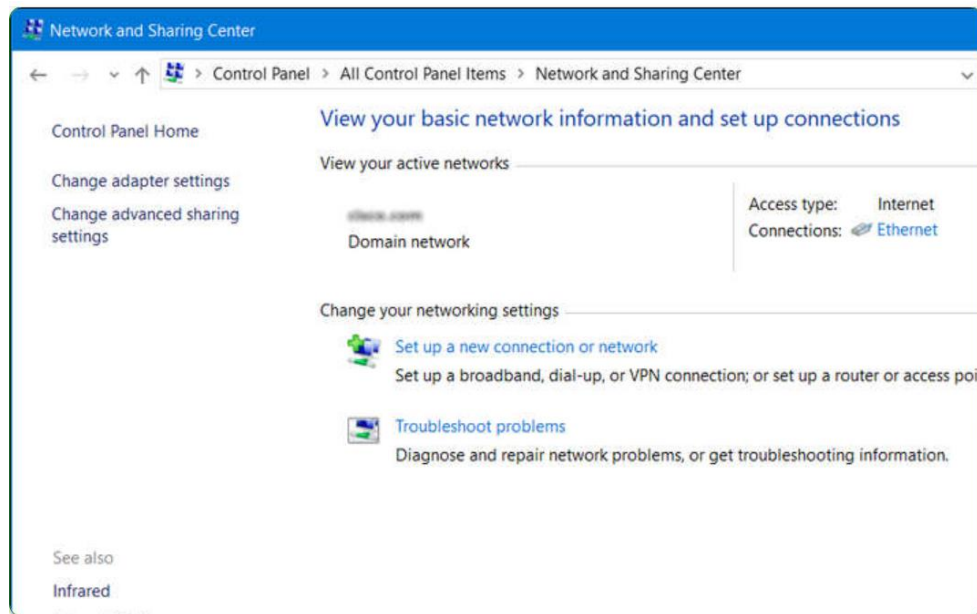
When searching for the reason a computer may be acting erratically, the Resource Monitor can help to find the source of the problem.

- **Overview**
  - The tab displays the general usage for each resource.
  - If you select a single process, it will be filtered across all of the tabs to show only that process's statistics.
- **CPU**
  - The PID, number of threads, which CPU the process is using, and the average CPU usage of each process is shown.
  - Additional information about any services that the process relies on, and the associated handles and modules can be seen by expanding the lower rows.
- **Memory**
  - All of the statistical information about how each process uses memory is shown in this tab.
  - Also, an overview of usage of the entire RAM is shown below the Processes row.
- **Disk:** All of the processes that are using a disk are shown in this tab, with read/write statistics and an overview of each storage device.

- **Network**

- All of the processes that are using the network are shown in this tab, with read/write statistics.
- Most importantly, the current TCP connections are shown, along with all of the ports that are listening.
- This tab is very useful when trying to determine which applications and processes are communicating over the network.
- It makes it possible to tell if an unauthorized process is accessing the network, listening for a communication, and the address with which it is communicating.

**Networking:** One of the most important features of any operating system is the ability for the computer to connect to a network. Without this feature, there is no access to network resources or the internet. To configure Windows networking properties and test networking settings, the Network and Sharing Center is used. The easiest way to run this tool is to search for it and click it. Use the Network and Sharing Center to verify or create network connections, configure network sharing, and change network adapter settings.

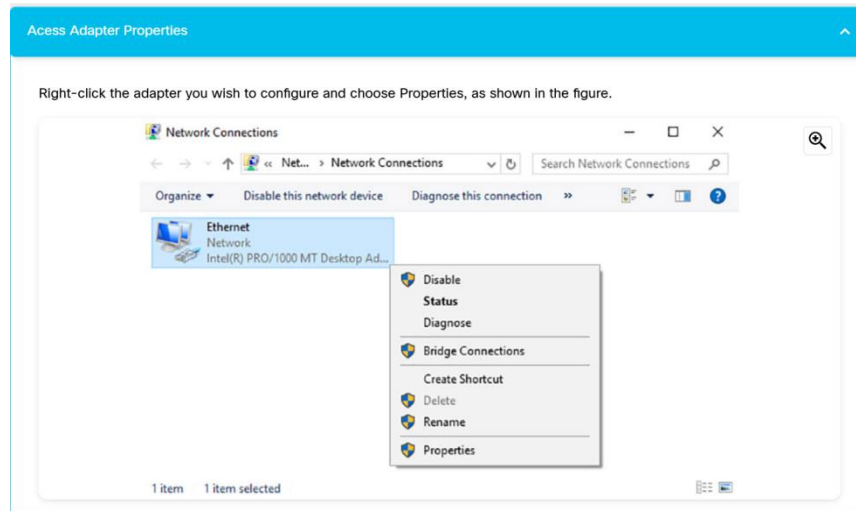


The initial view shows an overview of the active network. This view shows whether there is internet access and if the network is private, public, or guest. The type of network, either wired or wireless, is also shown. From this window, you can see the HomeGroup the computer belongs to, or create one if it is not already part of a HomeGroup. This tool can also be used to change adapter settings, change advance sharing settings, set up a new connection, or troubleshoot problems. Note that HomeGroup was removed from Windows 10 in version 1803.

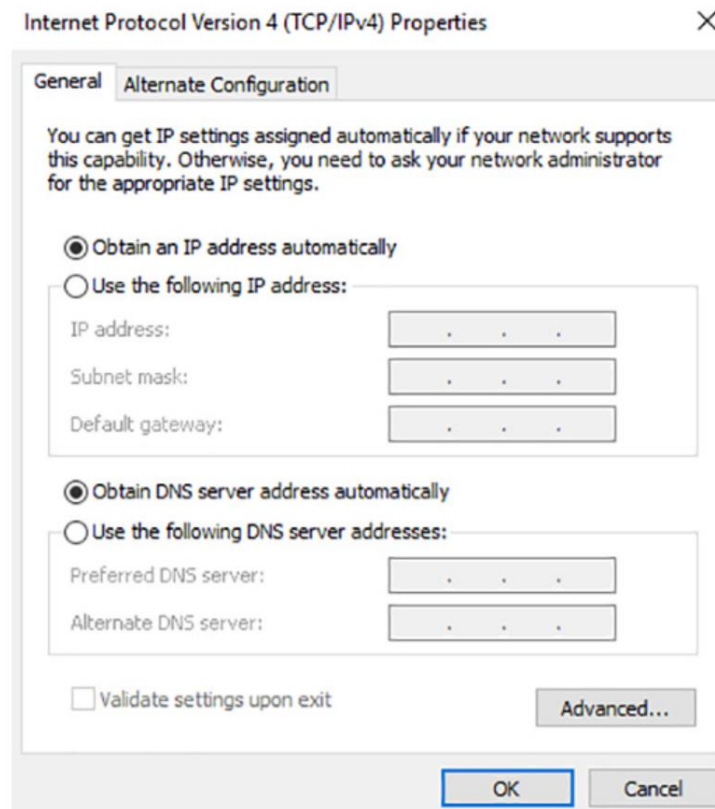
**Change Adapter Settings** To configure a network adapter, choose Change adapter settings in the Networking and Sharing Center to show all of the network connections that are available.

Select the adapter that you want to configure. In this case, we change an Ethernet adapter to acquire its IPv4 address automatically from the network.

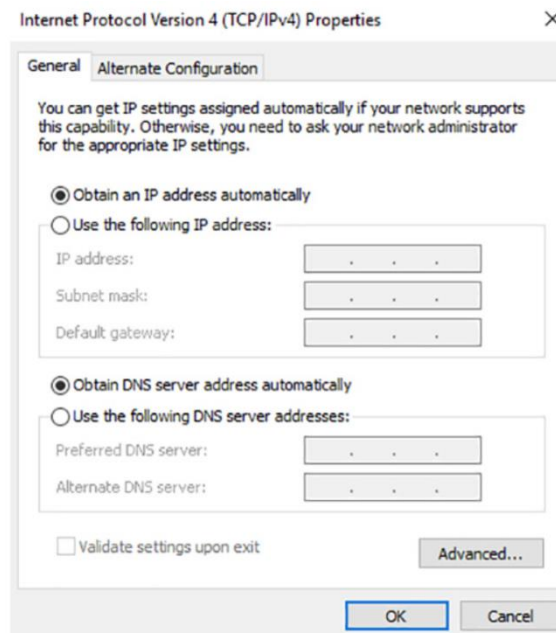
- **Access Adapter Properties:** Right-click the adapter you wish to configure and choose Properties, as shown in the figure.



- **Access TCP/IPV4 Properties:** This connection uses the following items: **Internet Protocol Version 4 (TCP/IPv4)** or **Internet Protocol Version 6 (TCP/IPv6)** depending on which version you wish to use. In the figure, IPv4 is being selected.



- **Change settings:** Click **Properties** to configure the adapter. In the **Properties** dialogue box, shown in the figure, you can choose to **Obtain an address automatically** if there is a DHCP server available on the network. If you wish to configure addressing manually, you can fill in the address, subnet, default gateway, and DNS servers to configure the adapter. Click **OK** to accept the changes. You can also use the netsh.exe tool to configure networking parameters from a command prompt. This program can display and modify the network configuration. Type **netsh /?** at the command prompt to see a list of all the switches that can be used with this command.



**nslookup and netstat:** Domain Name System (DNS) should also be tested because it is essential to finding the address of hosts by translating it from a name, such as a URL. Use the nslookup command to test DNS. Type nslookup cisco.com at the command prompt to find the address of the Cisco webserver. When the address is returned, you know that DNS is functioning correctly. You can also check to see what ports are open, where they are connected, and what their current status is. Type netstat at the command line to see details of active network connections, as shown in the command output. The netstat command will be examined further later in this module.

```
C:\Users\USER>netstat
```

```
Active Connections
```

Proto	Local Address	Foreign Address	State
TCP	127.0.0.1:3030	USER-VGFFA:58652	ESTABLISHED
TCP	127.0.0.1:3030	USER-VGFFA:62114	ESTABLISHED
TCP	&127.0.0.1:3030	USER-VGFFA:62480	TIME_WAIT
TCP	127.0.0.1:3030	USER-VGFFA:62481	TIME_WAIT
TCP	127.0.0.1:3030	USER-VGFFA:62484	TIME_WAIT

## Accessing Network Resources

Like other operating systems, Windows uses networking for many different applications such as web, email, and file services. Originally developed by IBM, Microsoft aided in the development of the Server Message Block (SMB) protocol to share network resources. SMB is mostly used for accessing files on remote hosts. The Universal Naming Convention (UNC) format is used to connect to resources, for example:

`\\servername\sharename\file`

In the UNC, `servername` is the server that is hosting the resource. This can be a DNS name, a NetBIOS name, or simply an IP address. The `sharename` is the root of the folder in the file system on the remote host, while the `file` is the resource that the local host is trying to find. The file may be deeper within the file system and this hierarchy will need to be indicated.

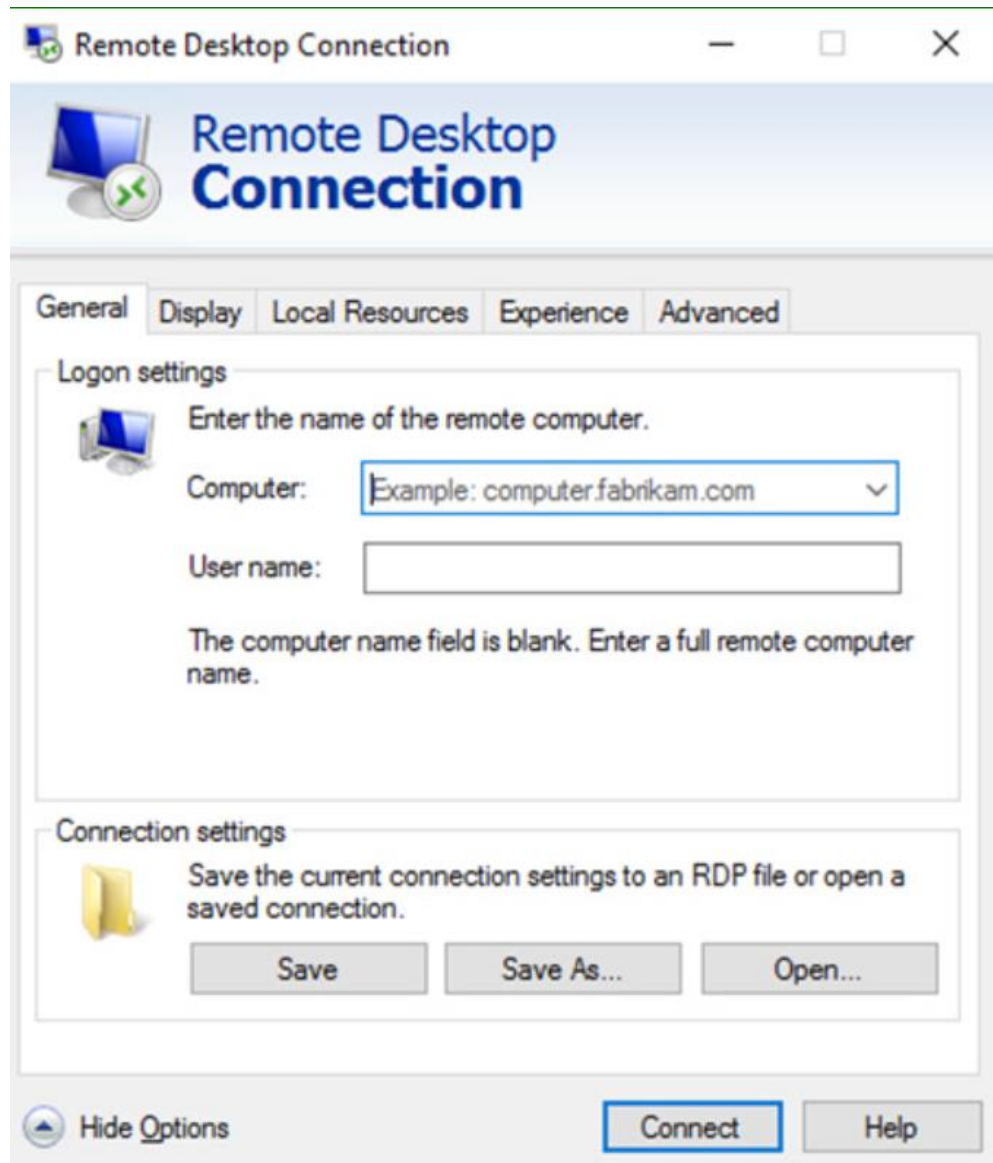
When sharing resources on the network, the area of the file system that will be shared will need to be identified. Access control can be applied to the folders and files to restrict users and groups to specific functions such as read, write, or deny. There are also special shares that are automatically created by Windows. These shares are called administrative shares. An administrative share is identified by the dollar sign (\$) that comes after the share name. Each disk volume has an administrative share, represented by the volume letter and the \$ such as C\$, D\$, or E\$. The Windows installation folder is shared as `admin$`, the printers' folder is shared as `print$`, and there are other administrative shares that can be connected. Only users with administrative privileges can access these shares.

The easiest way to connect to a share is to type the UNC of the share into the Windows File Explorer, in the box at the top of the screen which shows the breadcrumb listing of the current file system location. When Windows tries to connect to the share, you will be asked to provide credentials for accessing the resource. Remember that because the resource is on a remote computer, the credentials need to be for the remote computer, not the local computer.

Besides accessing shares on remote hosts, you can also log in to a remote host and manipulate that computer, as if it were local, to make configuration changes, install software, or troubleshoot an issue. In Windows, this feature uses the Remote Desktop Protocol (RDP). When investigating security incidents, a security analyst uses RDP often to access remote computers. To start RDP and connect to a remote computer, search for remote desktop and click the application. The Remote Desktop Connection window is shown in the figure.

Because RDP is designed to permit remote users to control individual hosts, it is a natural target for threat actors. Care should be taken when activating RDP, especially on unpatched legacy versions of Windows such as those that are still found in industrial control systems. Care should

be taken to limit the exposure of RDP to the internet, and security approaches and access control policies, such as Zero Trust, should be used to limit access to internal hosts.



## Windows Server

Most Windows installations are performed as desktop installations on desktops and laptops. There is another edition of Windows that is mainly used in data centers called Windows Server. This is a family of Microsoft products that began with Windows Server 2003. Windows Server hosts many different services and can fulfill different roles within a company.

Note: Although there is a Windows Server 2000, it is considered a client version of Windows NT 5.0. Windows Server 2003 is a server based on NT 5.2 and begins a new family of Windows Server versions.



These are some of the services that Windows Server provides:

- **Network Services** - DNS, DHCP, Terminal services, Network Controller, and Hyper-V Network virtualization
- **File Services** - SMB, NFS, and DFS
- **Web Services** - FTP, HTTP, and HTTPS
- **Management** - Group policy and Active Directory domain services control

## Windows Security

### The netstat Command

When malware is present in a computer, it will often open communication ports on the host to send and receive data. The **netstat** command can be used to look for inbound or outbound connections that are not authorized. When used on its own, the **netstat** command will display all of the active TCP connections.

By examining these connections, it is possible to determine which of the programs are listening for connections that are not authorized. When a program is suspected of being malware, a little research can be performed to determine its legitimacy. From there, the process can be shut down with Task Manager, and malware removal software can be used to clean the computer.

To make this process easier, you can link the connections to the running processes that created them in Task Manager. To do this, open a command prompt with administrative privileges and enter the **netstat -abno** command, as shown in the command output.

```
Microsoft Windows [Version 10.0.18363.720]
(c) 2019 Microsoft Corporation. All rights reserved.
C:\WINDOWS\system32> netstat -abno

Active Connections
Proto Local Address           Foreign Address         State       PID
TCP   0.0.0.0:80                0.0.0.0:0               LISTENING   4
Can not obtain ownership information
TCP   0.0.0.0:135               0.0.0.0:0               LISTENING   952
RpcSs
[svchost.exe]
TCP   0.0.0.0:445               0.0.0.0:0               LISTENING   4
Can not obtain ownership information
TCP   0.0.0.0:623               0.0.0.0:0               LISTENING   14660
[LMS.exe]
TCP   0.0.0.0:3389              0.0.0.0:0               LISTENING   1396
TermService
[svchost.exe]
TCP   0.0.0.0:5040              0.0.0.0:0               LISTENING   9792
CDPSvc
[svchost.exe]
TCP   0.0.0.0:5357              0.0.0.0:0               LISTENING   4
Can not obtain ownership information
TCP   0.0.0.0:5593              0.0.0.0:0               LISTENING   4
Can not obtain ownership information
TCP   0.0.0.0:8099              0.0.0.0:0               LISTENING   5248
[SolarWinds TFTP Server.exe]
TCP   0.0.0.0:16992             0.0.0.0:0               LISTENING   14660
```

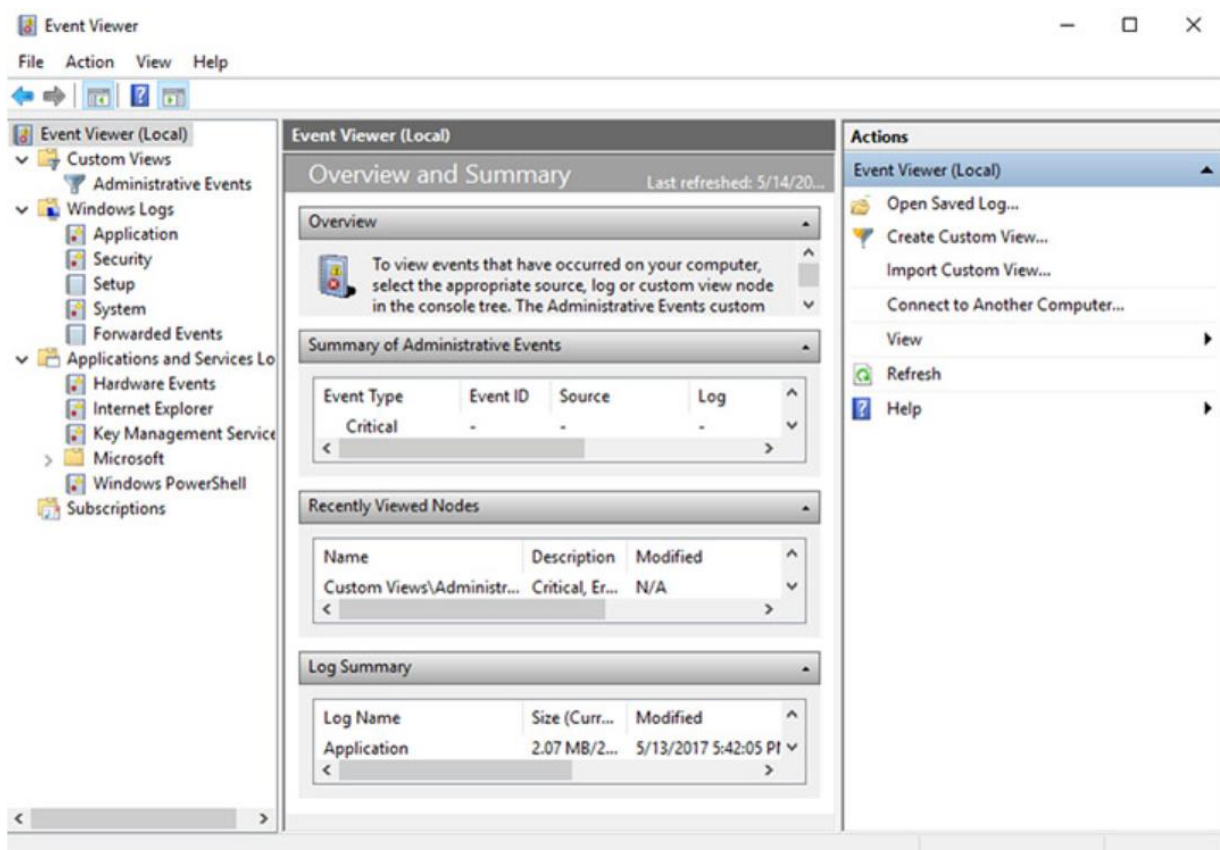


**Note:** If you are not in administrator mode, a “The requested operation requires elevation” message will appear. Search for Command Prompt. Right-click on **Command Prompt** and chose **Run as administrator**.

By examining the active TCP connections, an analyst should be able to determine if there are any suspicious programs that are listening for incoming connections on the host. You can also trace that process to the Windows Task Manager and cancel the process. There may be more than one process listed with the same name. If this is the case, use the PID to find the correct process. Each process running on the computer has a unique PID. To display the PIDs for the processes in the Task Manager, open the **Task Manager**, right-click the table heading and select **PID**.

## Event Viewer

Windows Event Viewer logs the history of application, security, and system events. These log files are a valuable troubleshooting tool because they provide information necessary to identify a problem. To open the Event Viewer, search for it and click the program icon, as shown in the figure.



Windows includes two categories of event logs: Windows Logs, and Application and Services Logs. Each of these categories has multiple log types. Events that are displayed in these logs have a level: information, warning, error, or critical. They also have the date and time that the event occurred, along with the source of the event and an ID which relates to that type of event.

It is also possible to create a custom view. This is useful when looking for certain types of events, finding events that happened during a certain time period, displaying events of a certain level, and many other criteria. There is a built-in custom view called Administrative Events that shows all critical, error, and warning events from all of the administrative logs. This is a good view to start with when trying to troubleshoot a problem.

Security event logs are found under Windows Logs. They use event IDs to identify the type of event.

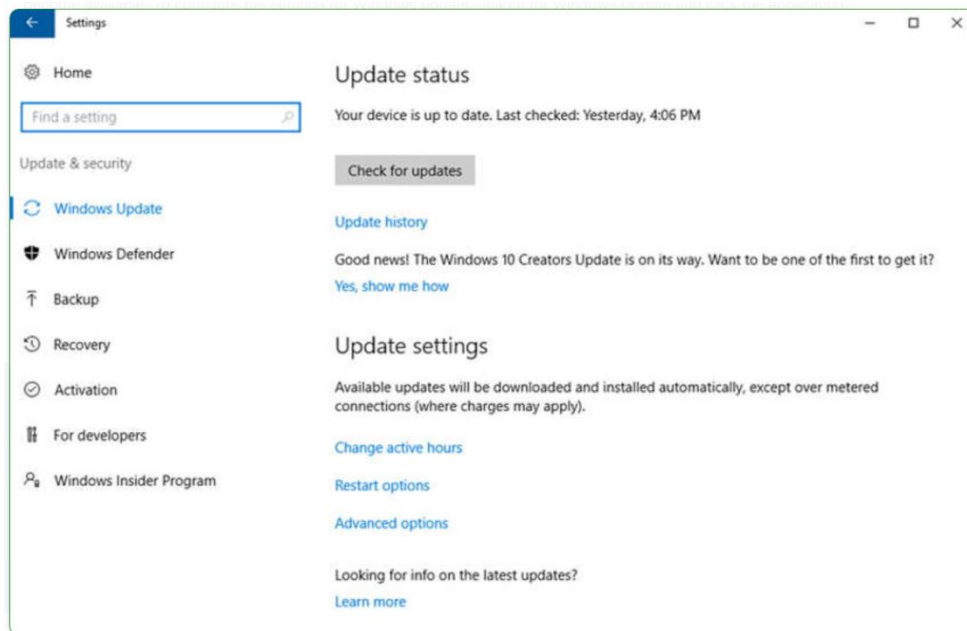
## **Windows Update Management**

No software is perfect, and the Windows operating system is no exception. Attackers are constantly coming up with new ways to compromise computers and exploit bad code. Some of these attacks come so quickly that defenses against them have not yet been devised and distributed. These are called zero-day exploits. Microsoft and security software developers are always trying to stay ahead of the attackers, but they are not always successful. To ensure the highest level of protection against these attacks, always make sure Windows is up to date with the latest service packs and security patches.

Patches are code updates that manufacturers provide to prevent a newly discovered virus or worm from making a successful attack. From time to time, manufacturers combine patches and upgrades into a comprehensive update application called a service pack. Many devastating virus attacks could have been much less severe if more users had downloaded and installed the latest service pack. It is highly desirable that enterprises utilize systems that automatically distribute, install, and track security updates.

Windows routinely checks the Windows Update website for high-priority updates that can help protect a computer from the latest security threats. These updates include security updates, critical updates, and service packs. Depending on the setting you choose, Windows automatically downloads and installs any high-priority updates that your computer needs or notifies you as these updates become available. To configure the settings for Windows update, search for Windows Update and click the application.

Update status, shown in the figure, allows you to check for updates manually and see the update history of the computer.

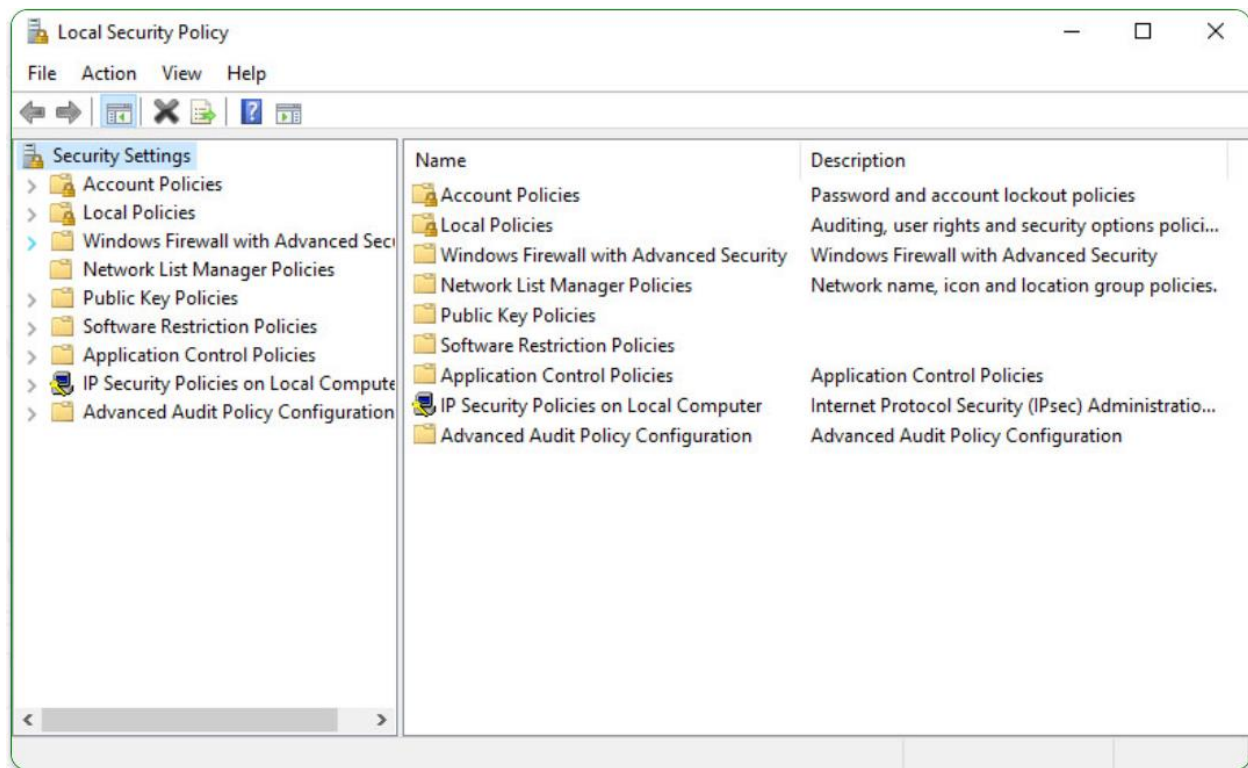


There are also settings for the hours where the computer will not automatically restart, for example during regular business hours. You can also choose when to restart the computer after an update, if necessary, with the Restart options. Advanced options are also available to choose how updates are installed how other Microsoft products are updated.

## Local Security Policy

A security policy is a set of objectives that ensures the security of a network, the data, and the computer systems in an organization. The security policy is a constantly evolving document based on changes in technology, business, and employee requirements.

In most networks that use Windows computers, Active Directory is configured with Domains on a Windows Server. Windows computers join the domain. The administrator configures a Domain Security Policy that applies to all computers that join the domain. Account policies are automatically set when a user logs in to a computer that is a member of a domain. Windows Local Security Policy, shown in the figure, can be used for stand-alone computers that are not part of an Active Directory domain. To open the Local Security Policy applet, search for Local Security Policy and click the program.



Password guidelines are an important component of a security policy. Any user that must log on to a computer or connect to a network resource should be required to have a password.

Passwords help prevent theft of data and malicious acts. Passwords also help to confirm that the logging of events is valid by ensuring that the user is the person that they say they are. In the Local Security Policy, Password Policy is found under Account Policies and defines the criteria for the passwords for all of the users on the local computer.

Use the Account Lockout Policy in Account Policies to prevent brute-force login attempts. For example, you can set the policy to allow the user to enter a wrong username and/or password five times. After five attempts, the account is locked for 30 minutes. After 30 minutes, the number of attempts is reset to zero and the user can attempt to login again.

It is important to make sure that computers are secure when users are away. A security policy should contain a rule about requiring a computer to lock when the screensaver starts. This will ensure that after a short time away from the computer, the screen saver will start and then the computer cannot be used until the user logs in.

If the Local Security Policy on every stand-alone computer is the same, then use the Export Policy feature. Save the policy with a name, such as workstation.inf. Copy the policy file to an external media or network drive to use on other stand-alone computers. This is particularly helpful if the administrator needs to configure extensive local policies for user rights and security options.

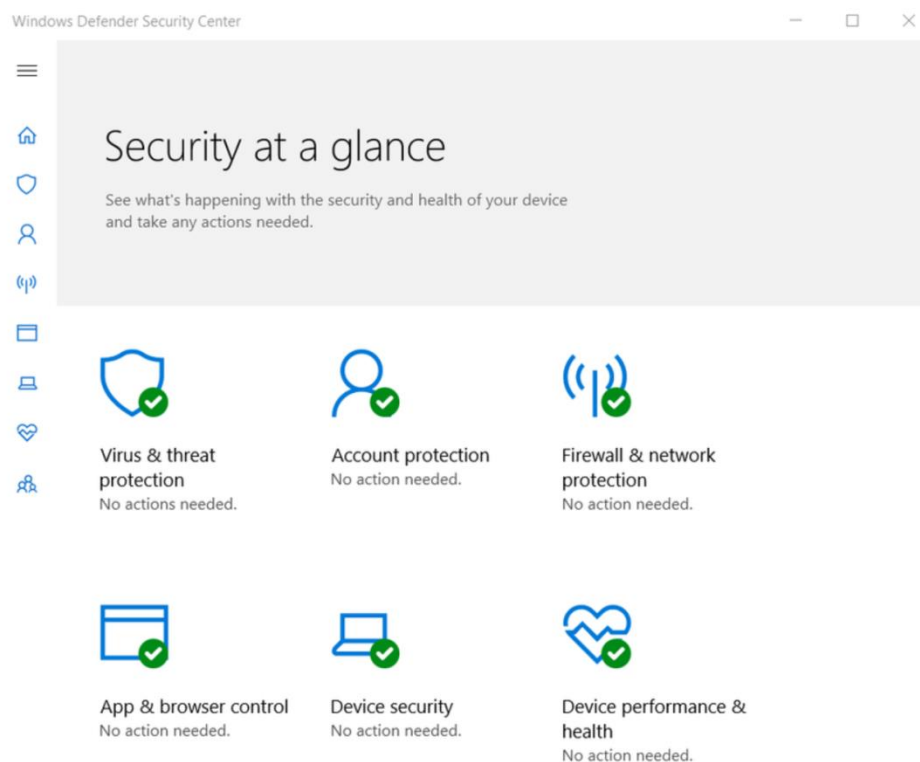
The Local Security Policy applet contains many other security settings that apply specifically to the local computer. You can configure User Rights, Firewall Rules, and even the ability to restrict the files that users or groups are allowed to run with the AppLocker.

## Windows Defender

Malware includes viruses, worms, Trojan horses, keyloggers, spyware, and adware. These are designed to invade privacy, steal information, damage the computer, or corrupt data. It is important that you protect computers and mobile devices using reputable antimalware software.

It may take several different programs and multiple scans to completely remove all malicious software. Run only one malware protection program at a time.

Several reputable security organizations such as McAfee, Symantec, and Kaspersky offer all-inclusive malware protection for computers and mobile devices. Windows has built-in virus and spyware protection called Windows Defender, as shown in the figure. Windows Defender is turned on by default to provide real-time protection against infection.



To open Windows Defender, search for it and click the program. Although Windows Defender works in the background, you can perform manual scans of the computer and storage devices. You can also manually update the virus and spyware definitions in the Update tab. Also, to see all of the items that were found during previous scans, click the History tab.

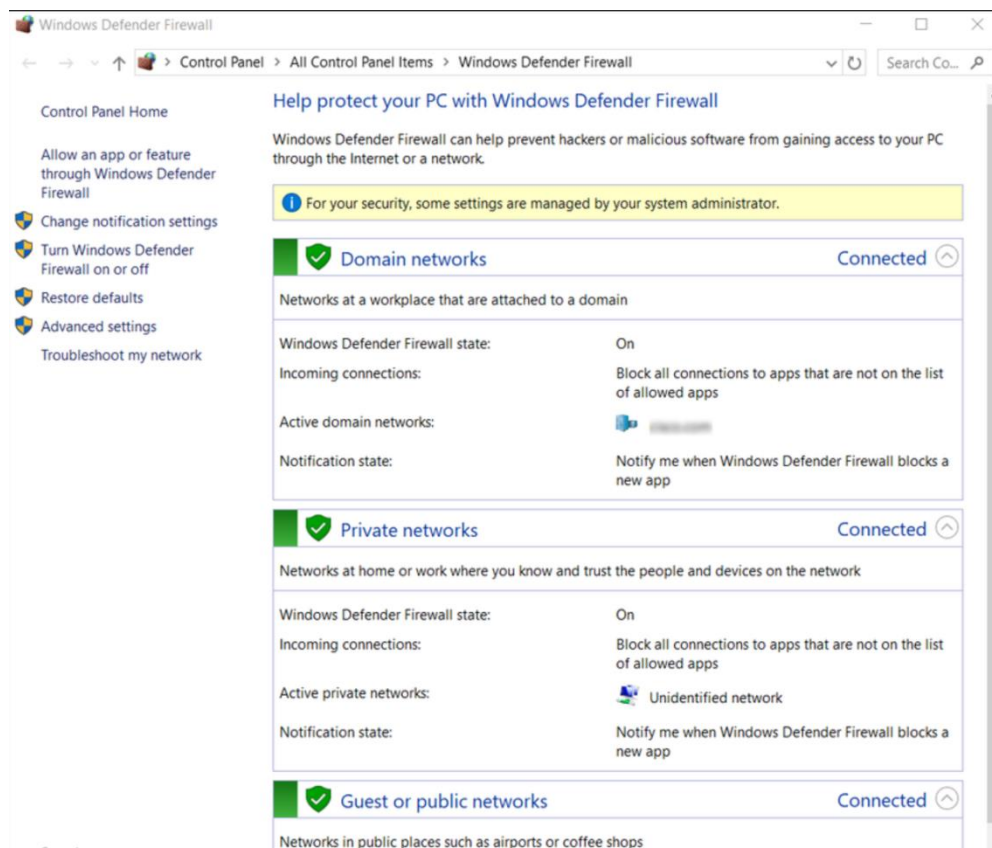
## Windows Defender Firewall

A firewall selectively denies traffic to a computer or network segment. Firewalls generally work by opening and closing the ports used by various applications. By opening only the required ports on a firewall, you are implementing a restrictive security policy. Any packet not explicitly permitted is denied. In contrast, a permissive security policy permits access through all ports, except those explicitly denied. In the past, software and hardware were shipped with permissive settings. As users neglected to configure their equipment, the default permissive settings left many devices exposed to attackers. Most devices now ship with settings as restrictive as possible, while still allowing easy setup.

To allow program access through the Windows Defender Firewall, search for **Control Panels**. Under **Systems and Security**, locate **Windows Defender Firewall**. Click **Allow an app or feature through Windows Defender Firewall**, as shown in the figure.

If you wish to use a different software firewall, you will need to disable Windows Firewall. To disable the Windows Firewall, click **Turn Windows Firewall on or off**.

Many additional settings can be found under **Advanced settings**. Here you can create inbound or outbound traffic rules based on different criteria. You can also import and export policies or monitor different aspects of the firewall.



# Linux

## The Value of Linux

Linux is often the operating system of choice in the Security Operations Center (SOC). These are some of the reasons to choose Linux:

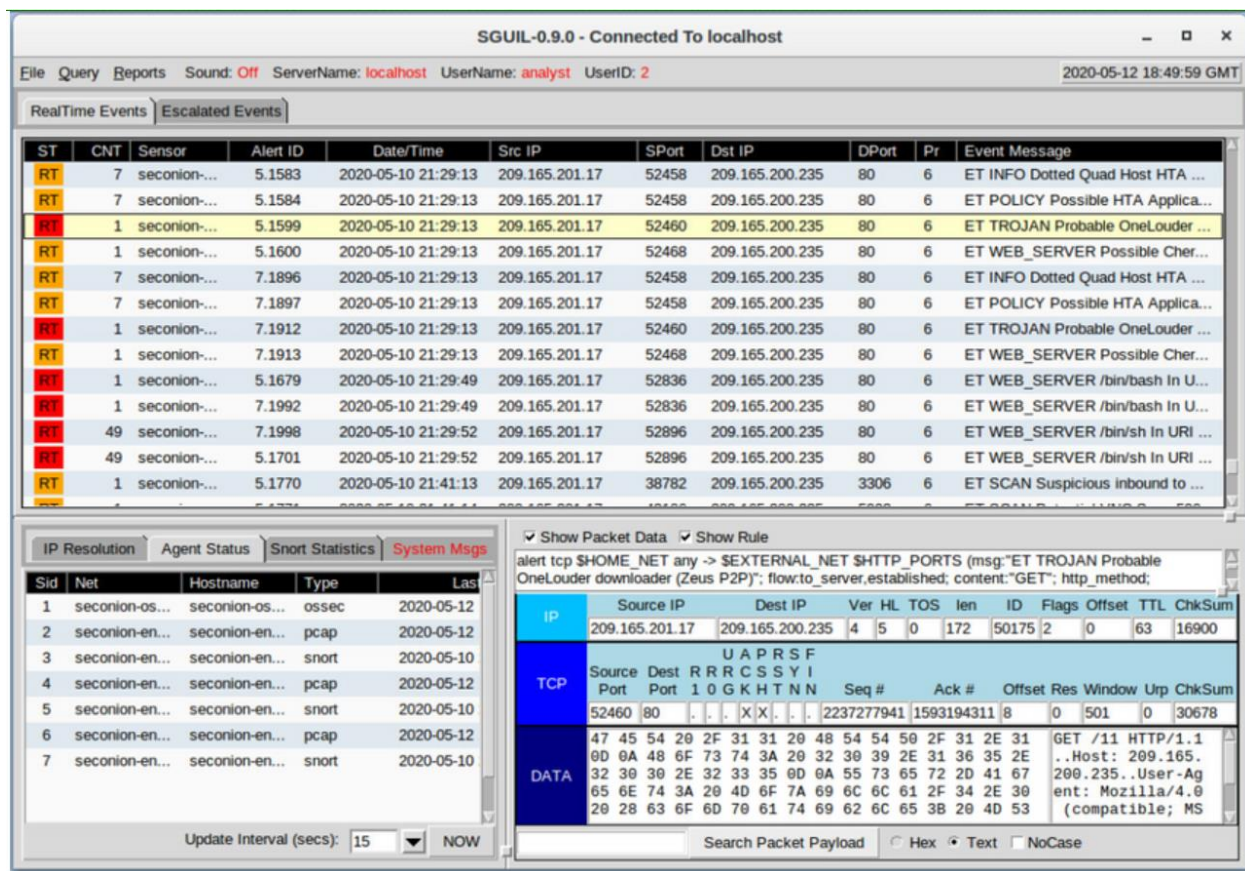
- **Linux is open source** - Any person can acquire Linux at no charge and modify it to fit specific needs. This flexibility allows analysts and administrators to tailor-build an operating system specifically for security analysis.
- **The Linux CLI is very powerful** - While a GUI makes many tasks easier to perform, it adds complexity and requires more computer resources to run. The Linux Command Line Interface (CLI) is extremely powerful and enables analysts to perform tasks not only directly on a terminal, but also remotely.
- **The user has more control over the OS** - The administrator user in Linux, known as the root user, or superuser, has absolute power over the computer. Unlike other operating systems, the root user can modify any aspect of the computer with a few keystrokes. This ability is especially valuable when working with low level functions such as the network stack. It allows the root user to have precise control over the way network packets are handled by the operating system.
- **It allows for better network communication control** - Control is an inherent part of Linux. Because the OS can be adjusted in practically every aspect, it is a great platform for creating network applications. This is the same reason that many great network-based software tools are available for Linux only.

## Linux in the SOC

The flexibility provided by Linux is a great feature for the SOC. The entire operating system can be tailored to become the perfect security analysis platform. For example, administrators can add only the necessary packages to the OS, making it lean and efficient. Specific software tools can be installed and configured to work in conjunction, allowing administrators to build a customized computer that fits perfectly in the workflow of a SOC.

The figure shows Sguil, which is the cybersecurity analyst console in a special version of Linux called Security Onion. Security Onion is an open source suite of tools that work together for network security analysis.





Let us find out more about tools that are often found in a SOC.

- **Network packet capture software**
  - A crucial tool for a SOC analyst as it makes it possible to observe and understand every detail of a network transaction.
  - Wireshark is a popular packet capture tool.
- **Malware analysis tools:** These tools allow analysts to safely run and observe malware execution without the risk of compromising the underlying system.
- **Intrusion detection systems (IDSs)**
  - These tools are used for real-time traffic monitoring and inspection.
  - If any aspect of the currently flowing traffic matches any of the established rules, a pre-defined action is taken.
- **Firewalls:** This software is used to specify, based on pre-defined rules, whether traffic is allowed to enter or leave a network or device.
- **Log managers:** Log files are used to record events, because a network can generate a very large number of log entries, log manager software is employed to facilitate log monitoring.

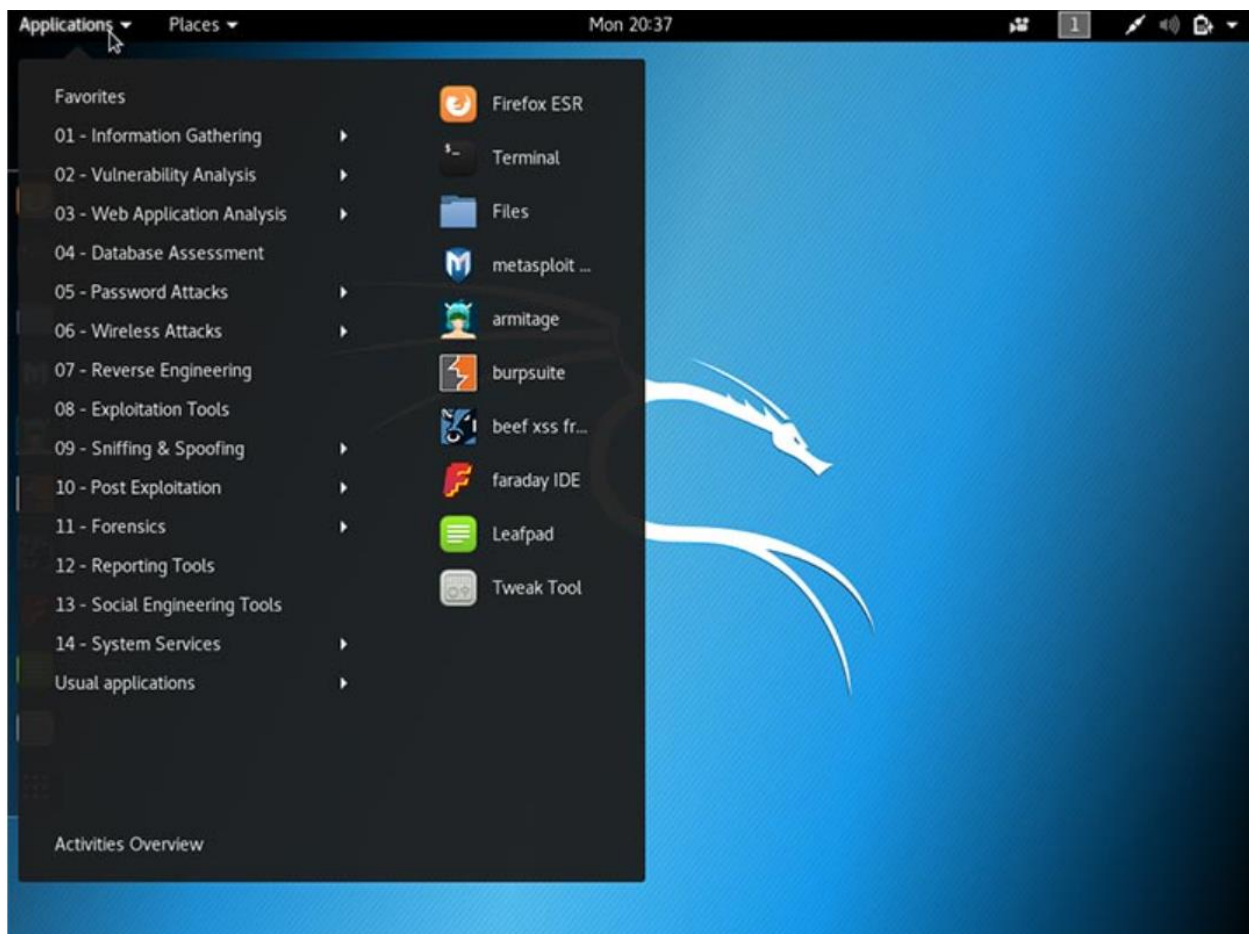


- **Security information and event management (SIEM):** SIEMs provide real-time analysis of alerts and log entries generated by network appliances such as IDSs and firewalls.
- **Ticketing systems:** Task ticket assignment, editing, and recording is done through a ticket management system. Security alerts are often assigned to analysts through a ticketing system.

## Linux Tools

In addition to SOC-specific tools, Linux computers that are used in the SOC often contain penetration testing tools. Also known as PenTesting, a penetration test is the process of looking for vulnerabilities in a network or computer by attacking it. Packet generators, port scanners, and proof-of-concept exploits are examples of PenTesting tools.

Kali Linux is a Linux distribution groups many penetration tools together in a single Linux distribution. Kali contains a great selection of tools. The figure shows a screenshot of Kali Linux. Notice all the major categories of penetration testing tools.



## The Linux Shell

In Linux, the user communicates with the OS by using the CLI or the GUI. Linux often starts in the GUI by default. This hides the CLI from the user. One way to access the CLI from the GUI is through a terminal emulator application. These applications provide user access to the CLI and are often named as some variation of the word “terminal”. In Linux, popular terminal emulators are Terminator, eterm, xterm, konsole, and gnome-terminal.

Fabrice Bellard has created JSLinux which allows an emulated version of Linux to run in a browser. Search for it on the internet. Open a Linux console in JSLinux and type the **ls** command to list the current directory content. Keep the tab open if you would like to try out some of the other commands discussed in this chapter.

The figure shows gnome-terminal, a popular Linux terminal emulator.

**Note:** The terms shell, console, console window, CLI terminal, and terminal window are often used interchangeably.

### Basic commands

- **mv** – Moves or renames files and directories. Example: `mv file.txt /home/user/`
- **chmod** – Changes file or directory permissions. Example: `chmod 755 script.sh`
- **chown** – Changes file or directory ownership. Example: `chown user:group file.txt`
- **dd** – Copies and converts data, often used for disk cloning. Example: `dd if=/dev/sda of=/dev/sdb`
- **pwd** – Prints the current working directory. Example: `pwd`
- **ps** – Displays running processes. Example: `ps aux`
- **su** – Switches to another user account (usually root). Example: `su -`
- **sudo** – Runs commands with superuser privileges. Example: `sudo apt-get update`
- **grep** – Searches for patterns in text. Example: `grep "error" logfile.txt`
- **ifconfig** – Shows or configures network interfaces. Example: `ifconfig eth0`
- **apt-get** – Installs, updates, or removes software packages. Example: `sudo apt-get install curl`
- **iwconfig** – Configures wireless network interfaces. Example: `iwconfig wlan0 essid "MyNetwork"`
- **shutdown** – Shuts down or restarts the system. Example: `shutdown -h now`
- **passwd** – Changes a user’s password. Example: `passwd username`
- **cat** – Displays the contents of a file. Example: `cat file.txt`
- **man** – Displays the manual for a command. Example: `man ls`

## File and Directory Commands

- **ls** – Lists files and directories. Example: `ls -l`
- **cd** – Changes the current directory. Example: `cd /home/user/`
- **mkdir** – Creates a new directory. Example: `mkdir new_folder`
- **cp** – Copies files or directories. Example: `cp file.txt /home/user/`
- **mv** – Moves or renames files and directories. Example: `mv file.txt /home/user/`
- **rm** – Removes files or directories. Example: `rm -r folder/`
- **grep** – Searches for patterns in files. Example: `grep "error" logfile.txt`
- **cat** – Displays file contents. Example: `cat file.txt`

## Working with Text Files

Linux has many different text editors, with various features and functions. Some text editors include graphical interfaces while others are command-line only tools. Each text editor includes a feature set designed to support a specific type of task. Some text editors focus on the programmer and include features such as syntax highlighting, brackets and parenthesis check, and other programming-focused features.

While graphical text editors are convenient and easy to use, command line-based text editors are very important for Linux users. The main benefit of command-line-based text editors is that they allow for text file editing from a remote computer.

Consider the following scenario: a user must perform administrative tasks on a Linux computer but is not sitting in front of that computer. Using SSH, the user starts a remote shell to the remote computer. Under the text-based remote shell, the graphical interface is not available, which makes it impossible to rely on tools such as graphical text editors. In this type of situation, text-based programs are crucial.

The figure shows nano, a popular command-line text editor. The administrator is editing firewall rules. Text editors are often used for system configuration and maintenance in Linux.

```
GNU nano 4.9.2                                fw_rules
sudo iptables -t nat -A POSTROUTING -o r1-eth0 -j MASQUERADE
sudo iptables -A FORWARD -i r1-eth0 -o r1-eth1 -m state --state RELATED,ESTABLISHED -j ACCEPT
sudo iptables -A FORWARD -i r1-eth1 -o r1-eth0 -j ACCEPT
sudo iptables -N LOGGING
sudo iptables -A FORWARD -j LOGGING
#sudo iptables -A LOGGING -j LOG --log-prefix "IPTables-Dropped: " --log-level 7
sudo iptables -A LOGGING -j ULOG --ulog-prefix "IPTables-Dropped"
sudo iptables -A LOGGING -j DROP

^G Get Help      ^O Write Out    ^W Where Is     ^K Cut Text     ^J Justify      ^C Cur Pos      M-U Undo        M-A Mark Text
^X Exit          ^R Read File    ^\ Replace      ^U Paste Text   ^T To Spell     ^_ Go To Line    M-E Redo        M-6 Copy Text
```

Due to the lack of graphical support, nano (or GNU nano) can only be controlled with the keyboard. For example, **CTRL+O** saves the current file; **CTRL+W** opens the search menu. GNU nano uses a two-line shortcut bar at the bottom of the screen, where commands for the current context are listed. Press **CTRL+G** for the help screen and a complete list of commands.

## The Importance of Text Files in Linux

In Linux, everything is treated as a file. This includes the memory, the disks, the monitor, and the directories. For example, from the operating system standpoint, showing information on the display means to write to the file that represents the display device. It should be no surprise that the computer itself is configured through files. Known as configuration files, they are usually text files used to store adjustments and settings for specific applications or services. Practically everything in Linux relies on configuration files to work. Some services have not one, but several configuration files.

Users with proper permission levels can use text editors to change the contents of configuration files. After the changes are made, the file is saved and can be used by the related service or application. Users are able to specify exactly how they want any given application or service to behave. When launched, services and applications check the contents of specific configuration files to adjust their behavior accordingly.

In the figure, the administrator opened the host configuration file in **nano** for editing. The host file contains static mappings of host IP addresses to names. The names serve as shortcuts that allow connecting to other devices by using a name instead of an IP address. Only the superuser can change the host file.

**Note:** The administrator used the command **sudo nano /etc/hosts** to open the file. The command **sudo** (short for “superuser do”) invokes the superuser privilege to use the nano text editor to open the host file.

```
GNU nano 4.9.2 /etc/hosts
# Static table lookup for hostnames.
# See hosts(5) for details.
127.0.0.1    localhost
::1         localhost
127.0.0.1    secOps.localdomain secOps

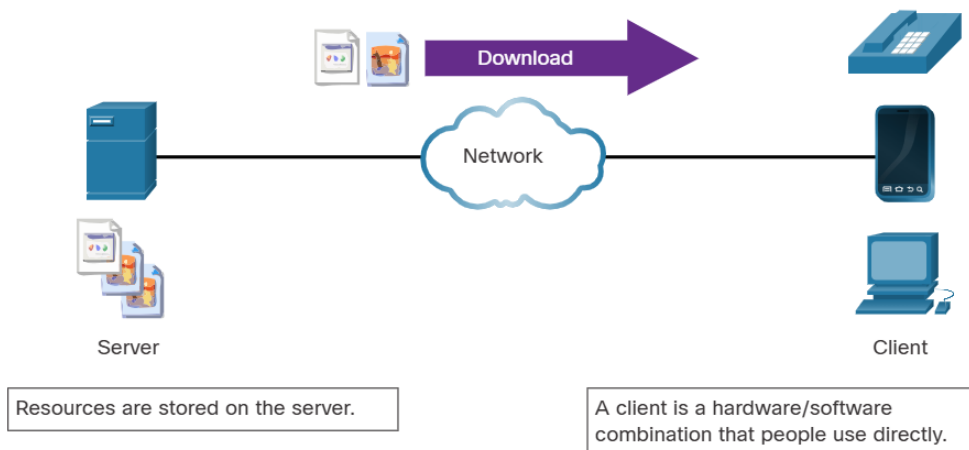
[ Read 5 lines ]
^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos   M-U Undo     M-A Mark Text
^X Exit      ^R Read File ^\ Replace   ^U Paste Text ^T To Spell  ^_ Go To Line M-E Redo     M-G Copy Text
```

## Linux Servers and Clients

### An Introduction to Client-Server Communications

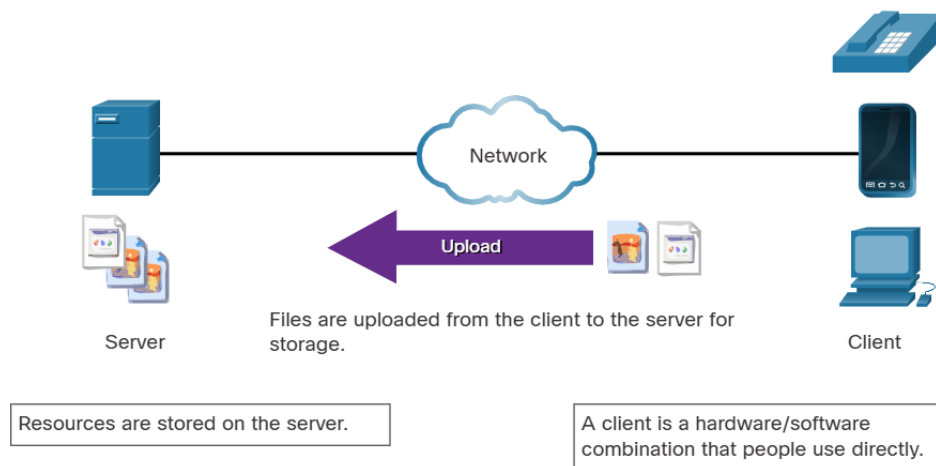
Servers are computers with software installed that enables them to provide services to clients across the network. There are many types of services. Some provide external resources such as files, email messages, or web pages to clients upon request. Other services run maintenance tasks such as log management, memory management, disk scanning, and more. Each service requires separate server software. For example, the server in the figure uses file server software to provide clients with the ability to retrieve and submit files

Files are downloaded from the server to the client.



## Clients

Clients are programs or applications designed to communicate with a specific type of server. Also known as client applications, clients use a well-defined protocol to communicate with the server. Web browsers are web clients that are used to communicate with web servers through the Hyper Text Transfer Protocol (HTTP) on port 80. The File Transfer Protocol (FTP) client is software used to communicate with an FTP server. The figure shows a client uploading files to a server.



## Monitoring Service Logs

- `/var/log/messages` - General system messages and errors, typically on RHEL, CentOS, and Fedora systems.
- `/var/log/syslog` - General system messages and events, mostly on Debian and Ubuntu systems.
- `/var/log/auth.log` - Authentication-related logs such as `sudo`, `ssh`, and login attempts, found on Debian/Ubuntu.
- `/var/log/secure` - Authentication logs on RHEL, CentOS, and Fedora systems.
- `/var/log/boot.log` - Logs generated during the system boot process.
- `/var/log/dmesg` - Kernel ring buffer logs showing hardware detection and kernel messages; also viewable via the `dmesg` command.
- `/var/log/kern.log` - Detailed kernel messages.
- `/var/log/cron` - Logs related to scheduled jobs run by `cron`.
- `/var/log/mysqld.log` or `/var/log/mysql.log` - MySQL or MariaDB database server logs; location depends on distribution and configuration.
- `/var/log/maillog` or `/var/log/mail.log` - Logs from mail server services, if running.

Running `sudo cat /var/log/messages` will display the entire contents of the `/var/log/messages` file, which contains general system messages and errors on your Linux system. Since this file can be very large, it's usually better to use commands that let you view it page by page or monitor it live, like:

- `sudo less /var/log/messages` — to scroll through the file comfortably
- `sudo tail -n 50 /var/log/messages` — to see the last 50 lines
- `sudo tail -f /var/log/messages` — to watch new entries as they come in

## The File System Types in Linux

There are many different kinds of file systems, varying in properties of speed, flexibility, security, size, structure, logic and more. It is up to the administrator to decide which file system type best suits the operating system and the files it will store.

- **ext2** – Lightweight Linux file system without journaling; stores general data; used on `/boot`, USB drives.
- **ext3** – ext2 + journaling for crash recovery; stores general Linux files; used on root or data partitions.
- **ext4** – Modern Linux default file system with better performance and large file support; used on `/`, `/home`, etc.
- **XFS** – High-performance journaling FS for large files and parallel I/O; often used for `/home` or data volumes.
- **Btrfs** – Advanced Linux FS with snapshots and built-in RAID; stores system/data files; used on `/`, `/data`.
- **ReiserFS** – Older FS optimized for small files; used on root or data partitions (now mostly deprecated).
- **F2FS** – Flash-optimized FS minimizing writes; used on `/data`, SD cards, SSDs.
- **NTFS** – Windows-native FS; used on `/mnt/windows` or external drives for cross-platform access.
- **VFAT / FAT32 / exFAT** – Windows-compatible FS for USBs/SD cards; mounted under `/media/` or `/mnt/`.
- **NFS** – Networked FS allowing remote file access; mounted under `/mnt/nfs` or similar paths.
- **CDFS (ISO 9660)** – Read-only FS for CDs/DVDs; auto-mounted under `/media/` or `/run/media/`.
- **tmpfs** – RAM-based FS for temporary files; mounted at `/tmp`, `/run`, `/dev/shm`.
- **procfs** – Virtual FS exposing kernel/process info; always mounted at `/proc`.
- **sysfs** – Virtual FS showing hardware and driver data; mounted at `/sys`.
- **Swap** – Disk-based memory extension used when RAM is full; not mounted, listed in `swapon --show`.

- **HFS+** – Apple FS with journaling; used for mounting Mac drives; usually mounted under /mnt/hfs or /media/.
- **APFS** – New Apple FS with encryption/snapshots; limited Linux support; mounted read-only if supported.
- **ISO 9660** – Standard FS for ISO/CD images; mounted under /media/cdrom or /mnt/iso.
- **MBR** – Not a file system; stores bootloader and partition table; located at first 512 bytes of disk (/dev/sdX).

## Linux Roles and File Permissions

In Linux, most system entities are treated as files. In order to organize the system and enforce boundaries within the computer, Linux uses file permissions. File permissions are built into the file system structure and provide a mechanism to define permissions on every file. Every file in Linux carries its file permissions, which define the actions that the owner, the group, and others can perform with the file. The possible permission rights are Read, Write and Execute. The `ls` command with the `-l` parameter lists additional information about the file.

Consider the output of the `ls -l` command in the command output.

```
[analyst@secOps ~]$ ls -l space.txt
-rwxrw-r-- 1 analyst staff 253 May 20 12:49 space.txt
      (1)  (2)  (3)   (4)  (5)   (6)       (7)
```

The output provides a lot of information about the file `space.txt`.

The first field of the output displays the permissions that are associated with `space.txt` (`-rwxrw-r--`). File permissions are always displayed in the User, Group, and Other order.

The file `space.txt` has the following permissions:

- The dash (-) means that this is a file. For directories, the first dash would be a “d”.
- The first set of characters is for user permission (**rwX**). The user, **analyst**, who owns the file can **Read**, **Write** and **eXecute** the file.
- The second set of characters is for group permissions (**rw-**). The group, **staff**, who owns the file can **Read** and **Write** to the file.
- The third set of characters is for any other user or group permissions (**r--**). Any other user or group on the computer can only Read the file.

The second field defines the number of hard links to the file (the number 1 after the permissions). A hard link creates another file with a different name linked to the same place in the file system (called an inode). This is in contrast to a symbolic link, which is discussed on the next page.



The third and fourth field display the user (**analyst**) and group (**staff**) who own the file, respectively.

The fifth field displays the file size in bytes. The **space.txt** file has 253 bytes.

The sixth field displays the date and time of the last modification.

The seventh field displays the file name.

The figure shows a breakdown of file permissions in Linux.

Binary	Octal	Permission	Description
000	0	---	No access
001	1	--x	Execute only
010	2	-w-	Write only
011	3	-wx	Write and Execute
100	4	r--	Read only
101	5	r-x	Read and Execute
110	6	rw-	Read and Write
111	7	rwX	Read, Write and Execute

File permissions are a fundamental part of Linux and cannot be broken. A user has only the rights to a file that the file permissions allow. The only user that can override file permission on a Linux computer is the root user. Because the root user has the power to override file permissions, the root user can write to any file. Because everything is treated as a file, the root user has full control over a Linux computer. Root access is often required before performing maintenance and administrative tasks. Because of the power of the root user, root credentials should use strong passwords and not be shared with anyone other than system administrators and other high-level users.

## Installing and Running Applications on a Linux Host

Many end-user applications are complex programs written in compiled languages. To aid in the installation process, Linux often includes programs called package managers. A package is the term used to refer to a program and all its supporting files. By using a package manager to install a package, all the necessary files are placed in the correct file system location.

Package managers vary depending on Linux distributions. For example, **pacman** is used by Arch Linux while **dpkg** (Debian package) and **apt** (Advanced Packaging Tool) are used in Debian and Ubuntu Linux distributions.

The command output shows the output of a few **apt-get** commands used in Debian distributions.

```
analyst@cuckoo:~$ sudo apt-get update
[sudo] password for analyst:
Hit:1 http://us.archive.ubuntu.com/ubuntu xenial InRelease
Get:2 http://us.archive.ubuntu.com/ubuntu xenial-updates InRelease [102 kB]
Get:3 http://security.ubuntu.com/ubuntu xenial-security InRelease [102 kB]
Get:4 http://us.archive.ubuntu.com/ubuntu xenial-backports InRelease [102 kB]
Get:5 http://us.archive.ubuntu.com/ubuntu xenial-updates/main amd64 Packages [534 kB]
Fetched 4,613 kB in 4s (1,003 kB/s)
Reading package lists... Done
analyst@cuckoo:~$
analyst@cuckoo:~$ sudo apt-get upgrade
Reading package lists Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
The following packages have been kept back:
linux-generic-hwe-16.04 linux-headers-generic-hwe-16.04
linux-image-generic-hwe-16.04
The following packages will be upgraded:
firefox firefox-locale-en glib2.0-gtk2 libjavascriptcoregtk-4.0-18
libwebkit2gtk-4.0-37 libwebkit2gtk-4.0-37-gtk2 libxen-4.6 libxenstore3.0 linux-libc-dev logrotate
openssh-client
qemu-block-extra qerau-kvm qemu-system-common qemu-system-x86 qemu-utils
```

The **apt-get update** command is used to get the package list from the package repository and update the local package database. The **apt-get upgrade** command is used to update all currently installed packages to their latest versions.

## Keeping the System Up to Date

Task	Arch	Debian / Ubuntu
Install a package by name	pacman -S	apt install
Remove a package by name	pacman -Rs	apt remove
Update a local package	pacman -Syy	apt-get update
Upgrade all currently installed packages	pacman -Syu	apt-get upgrade

A Linux GUI can also be used to manually check and install updates. In Ubuntu for example, to install updates you would click Dash Search Box, type software updater , and then click the Software Updater icon, as shown in the figure.

## Processes and Forks

- **ps aux** — List all running processes
  - Example: `ps aux | grep firefox`
  - *Outcome*: Shows all Firefox processes with details.
- **top** — Real-time process monitor
  - Example: Run top and press q to quit
  - *Outcome*: Displays CPU, memory usage, and active processes live.
- **pidof name** — Get PID of a process
  - Example: `pidof bash`
  - *Outcome*: Prints PID(s) of running bash shells.
- **pgrep name** — Find processes by name
  - Example: `pgrep sshd`
  - *Outcome*: Lists PIDs of all sshd processes.
- **kill PID** — Send termination signal (SIGTERM)
  - Example: `kill 1234`
  - *Outcome*: Gracefully stops process with PID 1234.
- **kill -9 PID** — Force kill (SIGKILL)
  - Example: `kill -9 1234`
  - *Outcome*: Immediately terminates process 1234 (cannot be ignored).
- **jobs** — List background jobs in current shell
  - Example: `jobs`
  - *Outcome*: Lists running or stopped jobs started from this shell.

- **fg %1** — Bring job #1 to foreground
  - Example: fg %1
  - *Outcome*: Resumes job #1 in the foreground.
- **Ctrl+Z** — Suspend current foreground job
  - *Outcome*: Pauses current process, moves it to background stopped state.
- **./script.sh &** — Run script in background
  - *Outcome*: Starts script asynchronously, shell prompt returns immediately.
- **ps tree** — Show process hierarchy
  - Example: ps tree -p
  - *Outcome*: Visual tree of processes with PIDs.

## Malware on a Linux Host

Linux malware includes viruses, Trojan horses, worms, and other types of malware that can affect the operating system. Due to a number of design components such as file system structure, file permissions, and user account restrictions, Linux operating systems are generally regarded as better protected against malware.

While arguably better protected, Linux is not immune to malware. Many vulnerabilities have been found and exploited in Linux. These range from server software to kernel vulnerabilities. Attackers are able to exploit these vulnerabilities and compromise the target. Because Linux is open source, fixes and patches are often made available within hours of the discovery of such problems.

If a malicious program is executed, it will cause damage, regardless of the platform. A common Linux attack vector is its services and processes. Vulnerabilities are frequently found in server and process code running on computers connected to the network. An outdated version of the Apache web server could contain an unpatched vulnerability which can be exploited by an attacker, for example. Attackers often probe open ports to assess the version and nature of the server running on that port. With that knowledge, attackers can research if there are any known issues with that particular version of that particular server to support the attack. As with most vulnerabilities, keeping the computer updated and closing any unused services and ports is a good way to reduce the opportunities for attack in a Linux computer.

The command output shows an attacker using the Telnet command to probe the nature and version of a web server (port 80).

```
analyst@secOps ~]$ telnet 209.165.200.224 80
Trying 209.165.200.224...
Connected to 209.165.200.224.
Escape character is '^]'.
HTTP/1.1 400 Bad Request
Server: nginx/1.12.0
Date: Wed, 17 May 2017 14:27:30 GMT
Content-Type: text/html
Content-Length: 173
Connection: close
<html>
<head><title>400 Bad Request</title></head>
<body bgcolor="white">
<center><h1>400 Bad Request</h1></center>
<hr><center>nginx/1.12.0</center>
</body>
</html >
Connection closed by foreign host.
analyst@secOps ~]$
```

The attacker has learned that the server in question is running nginx version 1.12.0. The next step would be to research known vulnerabilities in the nginx 1.12.0 code.

## Rootkit Check

A rootkit is a type of malware that is designed to increase an unauthorized user's privileges or grant access to portions of the software that should not normally be allowed. Rootkits are also often used to secure a backdoor to a compromised computer.

The installation of a rootkit can be automated (done as part of an infection) or an attacker can manually install it after compromising a computer. A rootkit is destructive because it changes kernel code and its modules, changing the most fundamental operations of the OS itself. With such a deep level of compromise, rootkits can hide the intrusion, remove any installation tracks, and even tamper with troubleshooting and diagnostic tools so that their output now hides the presence of the rootkit. While a few Linux vulnerabilities through history have allowed rootkit installation via regular user accounts, the vast majority of rootkit compromises require root or administrator access.

Because the very nature of the computer is compromised, rootkit detection can be very difficult. Typical detection methods often include booting the computer from trusted media such as a diagnostics operating system live CD. The compromised drive is mounted and, from the trusted system toolset, trusted diagnostic tools can be launched to inspect the compromised file system. Inspection methods include behavioral-based methods, signature scanning, difference scanning, and memory dump analysis.

Rootkit removal can be complicated and often impossible, especially in cases where the rootkit resides in the kernel; re-installation of the operating system is usually the only real solution to the problem. Firmware rootkits usually require hardware replacement.

**chkrootkit** is a popular Linux-based program designed to check the computer for known rootkits. It is a shell script that uses common Linux tools such as **strings** and **grep** to compare the signatures of core programs. It also looks for discrepancies as it traverses the /proc file system comparing the signatures found there with the output of **ps**.

While helpful, keep in mind that programs to check for rootkits are not 100% reliable.

The command output shows the output of chkrootkit on an Ubuntu Linux.

```
analyst@cuckoo:~$ sudo ./chkrootkit
[sudo] password for analyst:
ROOTDIR is '/'
Checking 'amd'... not found
Checking 'basename'... not infected
Checking 'biff'... not found
Checking 'chfn'... not infected
Checking 'chsh'... not infected
Checking 'cron'... not infected
Checking 'crontab'... not infected
Checking 'date'... not infected
Checking 'du'... not infected
Checking 'dirname'... not infected
Checking 'echo'... not infected
Checking 'egrep'... not infected
Checking 'env'... not infected
Checking 'find'... not infected
Checking 'fingerd'... not found
Checking 'gpm'... not found
Checking 'grep'... not infected
Checking 'hdparm'... not infected
Checking 'su'... not infected
Checking 'ifconfig'... not infected
Checking 'inetd'... not tested
Checking 'inetdconf'... not found
```

## Piping Commands

Although command line tools are usually designed to perform a specific, well-defined task, many commands can be combined to perform more complex tasks by a technique known as piping. Named after its defining character, the pipe (**|**), piping consists of chaining commands together, feeding the output of one command into the input of another.

For example, the `ls` command is used to display all the files and directories of a given directory. The **grep** command compares searches through a file or text looking for the specified string. If found, **grep** displays the entire contents of the folder where the string was found.

The two commands, `ls` and **grep**, can be piped together to filter out the output of `ls`. This is shown in the output of the `ls -l | grep host` command and the `ls -l | grep file` command.

```
[analyst@secOps ~]$ ls -l
total 40
drwxr-xr-x 2 analyst analyst 4096 Mar 22 2018 Desktop
drwxr-xr-x 3 analyst analyst 4096 April 2 14:44 Downloads
-rw-r--r-- 1 analyst analyst 9 May 20 10:51 hostfile1.txt
-rw-r--r-- 1 analyst analyst 9 May 20 10:51 hostfile2.txt
-rw-r--r-- 1 analyst analyst 9 May 20 10:52 hostfile3.txt
drwxr-xr-x 9 analyst analyst 4096 Jul 19 2018 lab.support.files
-rw-r--r-- 1 analyst analyst 19 May 20 10:53 mytest.com
-rw-r--r-- 1 analyst analyst 228844 May 20 10:54 rkhunter-1.4.6-1-any.pkg.tar.xz
drwxr-xr-x 2 analyst analyst 4096 Mar 21 2018 second_drive
-rw-r--r-- 1 analyst analyst 257 May 20 10:52 space.txt
[analyst@secOps ~]$
[analyst@secOps ~]$ ls -l | grep host
-rw-r--r-- 1 analyst analyst 9 May 20 10:51 hostfile1.txt
-rw-r--r-- 1 analyst analyst 9 May 20 10:51 hostfile2.txt
-rw-r--r-- 1 analyst analyst 9 May 20 10:52 hostfile3.txt
[analyst@secOps ~]$
[analyst@secOps ~]$ ls -l | grep file
-rw-r--r-- 1 analyst analyst 9 May 20 10:51 hostfile1.txt
-rw-r--r-- 1 analyst analyst 9 May 20 10:51 hostfile2.txt
-rw-r--r-- 1 analyst analyst 9 May 20 10:52 hostfile3.txt
drwxr-xr-x 9 analyst analyst 4096 Jul 19 2018 lab.support.files
[analyst@secOps ~]$
```

## System and Endpoint Protection

The operating system plays a critical role in maintaining the security of a network and is the target of many attacks. So, our first job as cybersecurity professionals is to secure the operating system.

### Operating System Security

What does an organization need to do to **harden** an operating system and keep it secure?

- **A good administrator:** A good administrator will configure the operating system to protect against outside threats. That means removing any unnecessary programs and services, and making sure that security patches and updates are installed in a timely manner to correct faults and mitigate risks.
- **A systematic approach:** It's important to have a systematic approach in place for addressing system updates. An organization should:
  - establish procedures for monitoring security-related information
  - evaluate updates for applicability
  - plan the installation of application updates and patches
  - Install updates using a documented plan.
- **A baseline:** Another critical way to secure an operating system is to identify potential vulnerabilities. To do this, establish a baseline to compare how a system is performing against baseline expectations.

### Points to Remember

- Watch out for rogue antivirus products: Be cautious of malicious rogue antivirus products that appear while browsing the Internet. Most of these display an ad or popup that looks like an actual Windows warning. They warn that malware is infecting the computer and prompt the user to clean it. But they do not come from legitimate sources, and clicking anywhere inside the window may download and install malware instead.
- Fileless attacks are difficult to detect and remove: Fileless malware uses legitimate programs to infect a computer. Going straight into memory, this type of malware doesn't rely on files, so it leaves no footprint. A fileless attack ends when the system is rebooted. Fileless viruses use scripting languages such as Windows PowerShell and are hard to detect.
- Scripts can also be malware: Scripting languages such as Python, Bash (the command-line language for Apple's macOS and most Linux distributions) or Visual Basic for Applications (or VBA, used in Microsoft macros) can be used to create scripts that are malware.



- Always remove unapproved software: Unapproved or non-compliant software may be unintentionally installed on a computer. Users may also intentionally install unauthorized programs. Although unapproved software may not be malicious, it can still violate the security policy and interfere with the organization's software or network services. Non-compliant software should be removed immediately.

## Patch Management

Cybercriminals work relentlessly to exploit weakness in computer systems. To stay one step ahead, keep systems secure and up to date by regularly installing patches.

Let us learn more about what patches are and how they work.

- **What are patches?**
  - Patches are code updates that prevent a new virus, worm, or other malware from making a successful attack. Patches and upgrades are often combined into a service pack. Many malware attacks could have been avoided if users had installed the latest service pack.
  - Operating systems such as Windows routinely check for updates that can protect a computer from the latest security threats. These include security updates, critical updates and service packs. Windows can be configured to automatically download and install any high-priority updates or to notify the user as these become available.
- **What do you need to do?**
  - As a cybersecurity professional, it's good practice to test a patch before deploying it throughout the organization. A patch management tool can be used to manage patches locally instead of using the vendor's online update service.
  - An automated patch service provides administrators with a more controlled setting. Let's look at the benefits:
    - Administrators can approve or decline updates.
    - Administrators can force the update of systems on a specific date.
    - Administrators can obtain reports on the update(s) needed by each system.
    - There is no need for each computer to connect to the vendor's service to download patches; instead, it gets the verified update from a local server.
    - Users cannot disable or circumvent updates.
- **A proactive approach:** As well as securing the operating system, it's important to update third-party applications such as Adobe Acrobat, Java and Chrome to address vulnerabilities that could be exploited. A proactive approach to patch management provides network security while helping to prevent ransomware and other threats.

## Endpoint Security

A host-based solution is a software application that runs on a local device (or endpoint) to protect it. The software works with the operating system to help prevent attacks.

### 1. **Host-Based Firewall** – Controls network traffic at the device level.

A host-based firewall is installed directly on an endpoint (like a PC or server) and filters inbound and outbound traffic according to predefined rules. Unlike a network firewall, it protects the individual host from threats that may have bypassed perimeter defenses or originated internally. It helps stop unauthorized applications or users from sending or receiving data over the network.

### 2. **HIDS (Host-based Intrusion Detection System)** – Detects abnormal behavior on an endpoint.

HIDS monitors files, logs, and system behavior on the host to identify potentially malicious activity or policy violations. It compares current system state with a known baseline, alerts administrators when changes occur, and can help detect rootkits, unauthorized access, or configuration changes. However, HIDS is passive—its job is to detect and alert, not block.

### 3. **HIPS (Host-based Intrusion Prevention System)** – Prevents and blocks attacks in real-time.

HIPS build on the capabilities of HIDS by adding the power to actively block threats. It watches for suspicious behavior (like buffer overflows, privilege escalation, or script injection) and takes immediate action, such as terminating a process or isolating the host. HIPS operates close to the system kernel, offering deep protection against exploits targeting applications or the OS.

### 4. **EDR (Endpoint Detection and Response)** – Monitors, detects, and responds to endpoint threats.

EDR tools provide real-time visibility and analytics on endpoint activity. They collect detailed data (processes, file changes, registry activity, network connections), and use machine learning or behavioral analysis to detect advanced threats, even zero-days. Security teams can use EDR for forensic investigations, threat hunting, and automated or manual incident response. EDR is essential for detecting stealthy attacks like fileless malware.

### 5. **DLP (Data Loss Prevention)** – Stops sensitive data from leaving the endpoint.

DLP solutions identify, monitor, and protect sensitive data at rest, in motion, or in use on endpoints. They enforce policies to block unauthorized sharing, copying, printing, or uploading of protected data. For example, DLP can prevent users from emailing client SSNs or uploading confidential documents to cloud storage. It's especially important in compliance-heavy environments (HIPAA, GDPR, etc.).

**6. NGFW (Next-Generation Firewall)** – Provides advanced traffic filtering with context-aware protection.

NGFWs combine traditional firewall functionality with deep packet inspection, intrusion prevention, application control, and threat intelligence integration. When deployed on endpoints (as part of endpoint protection suites), NGFW features help monitor all traffic entering or leaving the device, even encrypted traffic NGFWs can identify apps (e.g., blocking specific cloud apps), enforce security policies, and detect/block known and unknown threats using threat intel feeds□

Endpoint Security Tools – Summary Table

Security Tool	Primary Function	Prevention	Detection	Response
Host Firewall	Traffic control	Yes	No	No
HIDS	Behavior monitoring	No	Yes	No
HIPS	Threat blocking	Yes	Yes	Yes
EDR	Threat visibility	No	Yes	Yes
DLP	Data protection	Yes	Yes	Yes
NGFW	Intelligent filtering	Yes	Yes	Yes

## Host Encryption

The Windows Encrypting File System (EFS) feature allows users to encrypt files, folders or an entire hard drive. Full disk encryption (FDE) encrypts the entire contents of a drive (including temporary files and memory). Microsoft Windows uses **BitLocker** for FDE.

To use BitLocker, the user needs to enable Trusted Platform Module (TPM) in the BIOS. The TPM is a specialized chip on the motherboard that stores information about the host system, such as encryption keys, digital certificates and passwords. When enabled, BitLocker can use the TPM chip.

Similarly, **BitLocker To Go** is a tool that encrypts removable drives. It does not use a TPM chip, but still encrypts the data, requiring a password to decrypt it. Meanwhile, a self-encrypting drive automatically encrypts all data in the drive to prevent attackers from accessing the data through their operating system.

## Boot Integrity

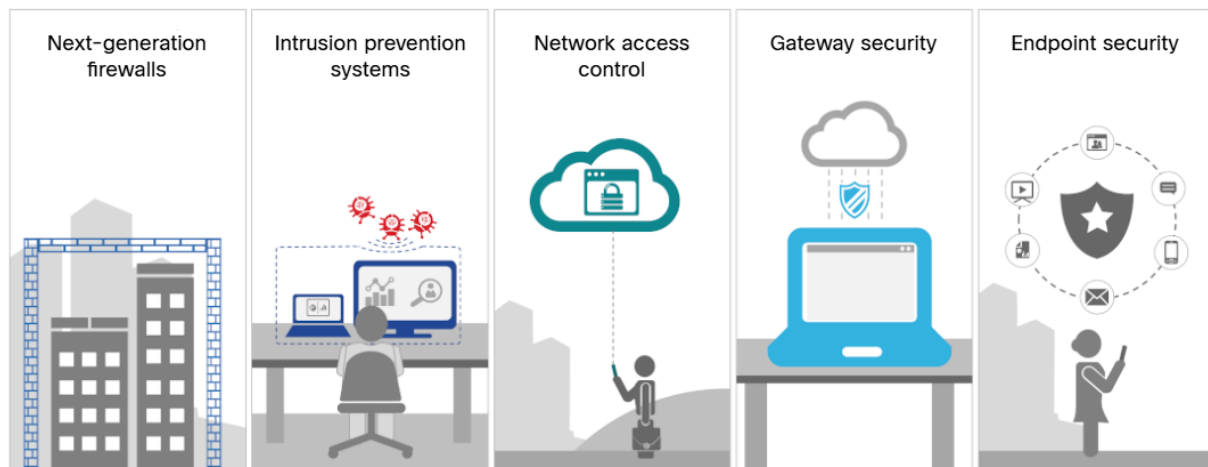
Attackers can strike at any moment, even in the short space of time it takes for a system to start up. It is critical to ensure that systems and devices remain secure when booting up.

- **What is boot integrity?**
  - Boot integrity ensures that the system can be trusted and has not been altered while the operating system loads.
  - Firmware — software instructions about basic computer functions — is stored on a small memory chip on the motherboard. The basic input/output system (BIOS) is the first program that runs when you turn on the computer.
  - Unified Extensible Firmware Interface (UEFI), a newer version of BIOS, defines a standard interface between the operating system, firmware and external devices. A system that uses UEFI is preferred over one that uses BIOS because a UEFI system can run in 64-bit mode.
- **How does Secure Boot work?**
  - Secure Boot is a security standard to ensure that a device boots using trusted software. When a computer system boots, the firmware checks the signature of each piece of boot software, including UEFI firmware drivers, UEFI applications and the operating system. If the signatures are valid, the system boots, and the firmware gives control to the operating system.
- **What is Measured Boot?**
  - Measured Boot provides stronger validation than Secure Boot. Measured Boot measures each component starting with the firmware through to the boot start drivers, and stores the measurements in the TPM chip to create a log. The log can be tested remotely to verify the boot state of the client. Measured Boot can identify untrusted applications trying to load, and it also allows antimalware to load earlier.

## Physical Protection of Devices

- **Computer equipment :** To physically protect computer equipment:
  - Use cable locks to secure devices
  - Keep telecommunication rooms locked
  - Use security cages (Faraday cages) around equipment to block electromagnetic fields.
- **Door locks:** A standard keyed entry lock is the most common type of door lock. They are often easy to force open. A deadbolt lock can be added for extra security. Any lock that requires a key is vulnerable if the keys are lost, stolen or duplicated. A cipher lock uses buttons that are pressed in a given sequence to open the door. It can be programmed so that a user's code may only work during certain days or times. It can also keep a record of when the door opened, and the code used to open it.

## Network-Based Malware Protection



New security architectures for the borderless network address security challenges by having endpoints use network scanning elements. These devices provide many more layers of scanning than a single endpoint possibly could. Network-based malware prevention devices are also capable of sharing information among themselves to make better informed decisions.

Protecting endpoints in a borderless network can be accomplished using network-based, as well as host-based techniques, as shown in the figure above. The following are examples of devices and techniques that implement host protections at the network level.

- **Advanced Malware Protection (AMP)** - This provides endpoint protection from viruses and malware.
- **Email Security Appliance (ESA)** - This provides filtering of SPAM and potentially malicious emails before they reach the endpoint. An example is the Cisco ESA.
- **Web Security Appliance (WSA)** - This provides filtering of websites and blocklisting to prevent hosts from reaching dangerous locations on the web. The Cisco WSA provides control over how users access the internet and can enforce acceptable use policies, control access to specific sites and services, and scan for malware.
- **Network Admission Control (NAC)** - This permits only authorized and compliant systems to connect to the network.

## Host-Based Firewalls

Host-based personal firewalls are standalone software programs that control traffic entering or leaving a computer. Firewall apps are also available for Android phones and tablets.

Host-based firewalls may use a set of predefined policies, or profiles, to control packets entering and leaving a computer. They also may have rules that can be directly modified or created to control access based on addresses, protocols, and ports. Host-based firewall applications can also

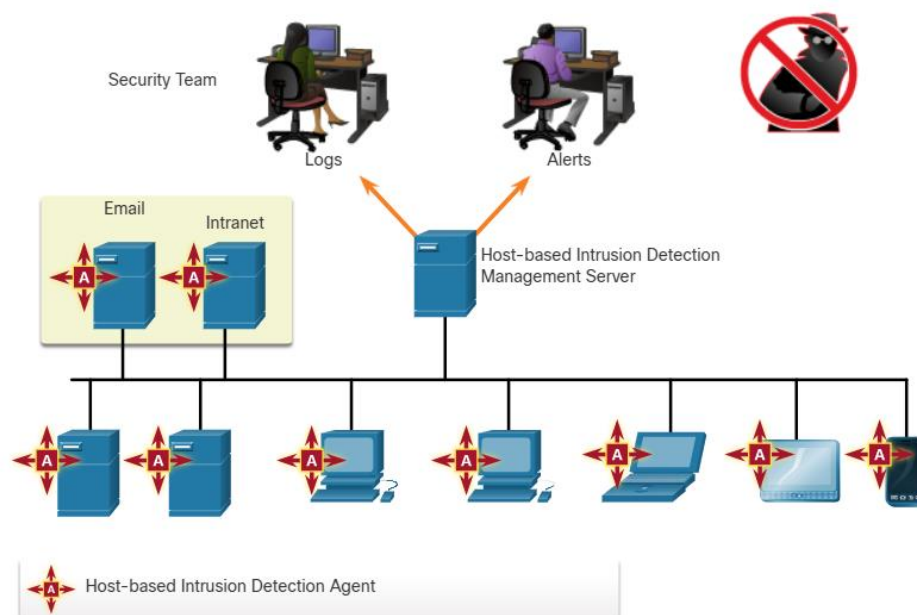
be configured to issue alerts to users if suspicious behavior is detected. They can then offer the user the ability to allow an offending application to run or to be prevented from running in the future.

Logging varies depending on the firewall application. It typically includes the date and time of the event, whether the connection was allowed or denied, information about the source or destination IP addresses of packets, and the source and destination ports of the encapsulated segments. In addition, common activities such as DNS lookups and other routine events can show up in host-based firewall logs, so filtering and other parsing techniques are useful for inspecting large amounts of log data.

One approach to intrusion prevention is the use of distributed firewalls. Distributed firewalls combine features of host-based firewalls with centralized management. The management function pushes rules to the hosts and may also accept log files from the hosts.

### Host-Based Intrusion Detection

It can be said that host-based security systems function as both detection and prevention systems because they prevent known attacks and detect unknown potential attacks. A HIDS uses both proactive and reactive strategies. A HIDS can prevent intrusion because it uses signatures to detect known malware and prevent it from infecting a system. However, this strategy is only good against known threats. Signatures are not effective against new, or zero day, threats. In addition, some malware families exhibit polymorphism. This means that variations of a type, or family, of malware may be created by attackers that will evade signature-based detections by changing aspects of the malware signature just enough so that it will not be detected.



- **HIDS Products**

- There are a number of HIDS products on the market today. Most of them utilize software on the host and some sort of centralized security management functionality that allows integration with network security monitoring services and threat intelligence. Examples are Cisco AMP, AlienVault USM, Tripwire, and Open Source HIDS SECurity (OSSEC).
- OSSEC uses a central manager server and agents that are installed on individual hosts. Currently, agents are available for Mac, Windows, Linux, and Solaris platforms. The OSSEC server, or Manager, can also receive and analyze alerts from a variety of network devices and firewalls over syslog. OSSEC monitors system logs on hosts and also conducts file integrity checking. OSSEC can detect rootkits and other malware, and can also be configured to run scripts or applications on hosts in response to event triggers.
- Search the internet for OSSEC to learn more.

## **Attack Surface**

Recall that vulnerability is a weakness in a system or its design that could be exploited by a threat. An attack surface is the total sum of the vulnerabilities in a given system that is accessible to an attacker. The attack surface can consist of open ports on servers or hosts, software that runs on internet-facing servers, wireless network protocols, and even users.

The attack surface is continuing to expand, as shown in the figure. More devices are connecting to networks through the Internet of Things (IoT) and Bring Your Own Device (BYOD). Much of network traffic now flows between devices and some location in the cloud. Mobile device use continues to increase. All of these trends contribute to a prediction that global IP traffic will increase threefold in the next five years.

The SANS Institute describes three components of the attack surface:

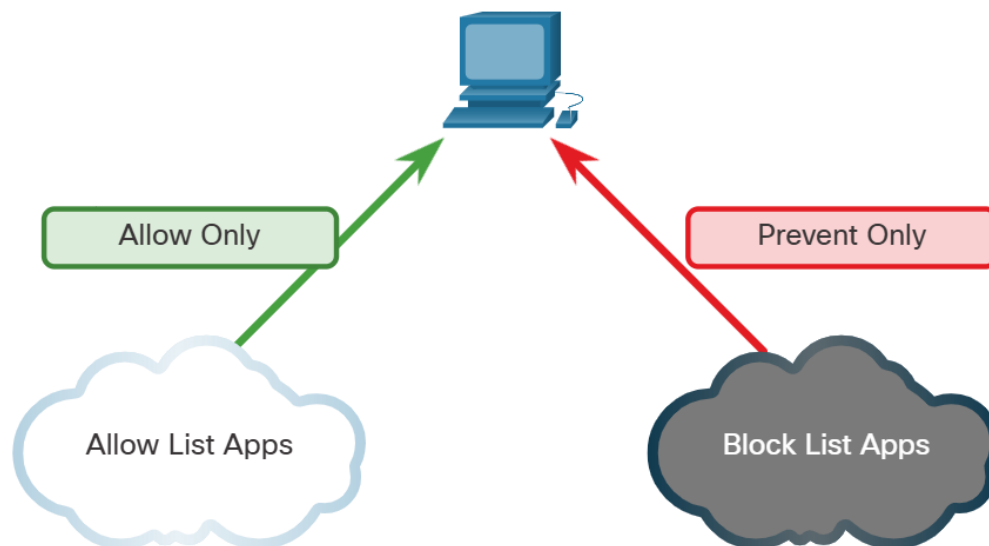
- **Network Attack Surface:** The attack exploits vulnerabilities in networks. This can include conventional wired and wireless network protocols, as well as other wireless protocols used by smartphones or IoT devices. Network attacks also exploit vulnerabilities at the network and transport layers.
- **Software Attack Surface:** The attack is delivered through exploitation of vulnerabilities in web, cloud, or host-based software applications.
- **Human Attack Surface:** The attack exploits weaknesses in user behavior. Such attacks include social engineering, malicious behavior by trusted insiders, and user error.

## Application Block list and Allow list

One way of decreasing the attack surface is to limit access to potential threats by creating lists of prohibited applications. This is known as blocklisting.

Application blocklists can dictate which user applications are not permitted to run on a computer. Similarly, allow lists can specify which programs are allowed to run, as shown in the figure. In this way, known vulnerable applications can be prevented from creating vulnerabilities on network hosts.

Allow lists are created in accordance with a security baseline that has been established by an organization. The baseline establishes an accepted amount of risk, and the environmental components that contribute to that level of risk. Non-allowlisted software can violate the established security baseline by increasing risk.

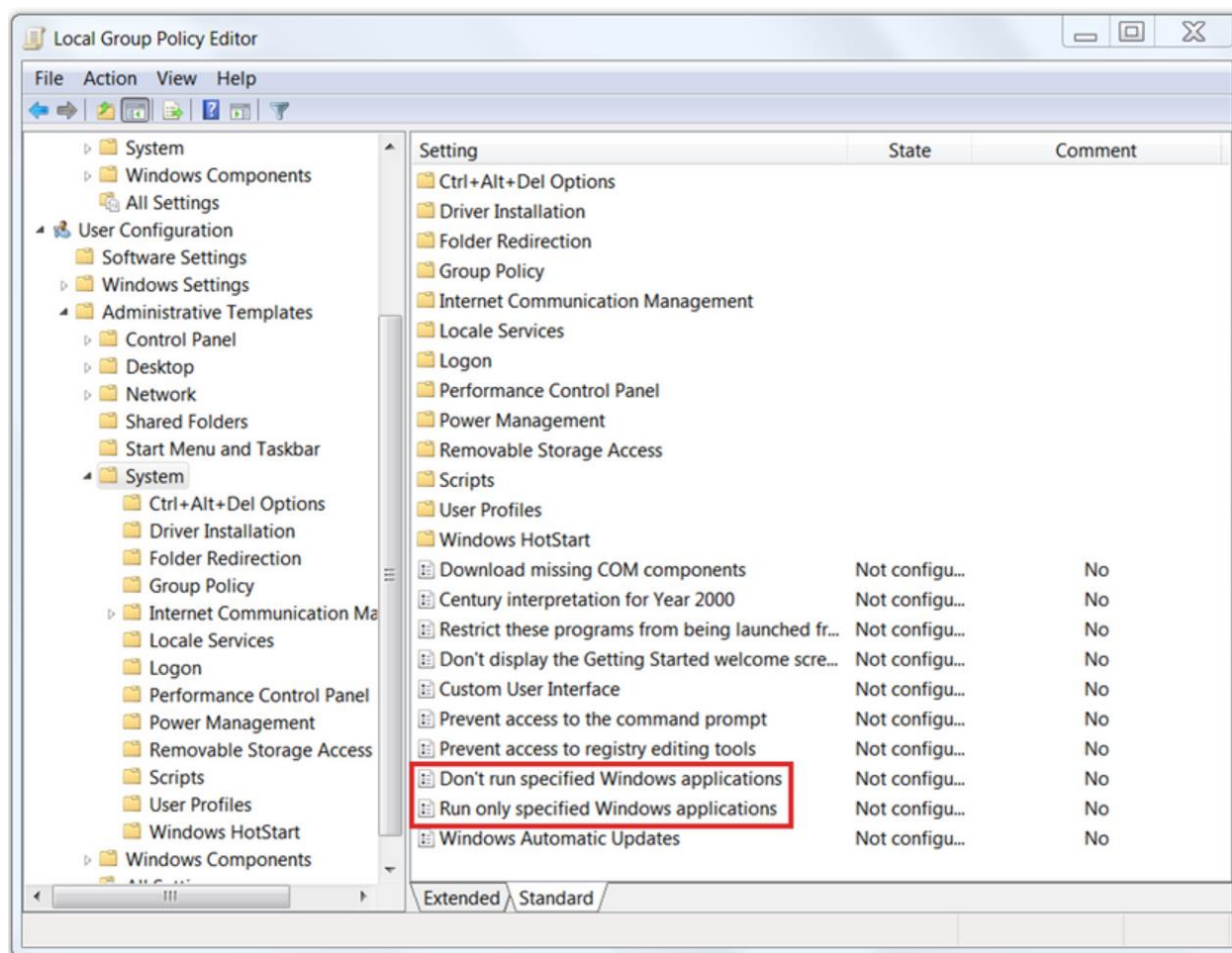


The figure shows the Windows Local Group Policy Editor blacklisting and whitelisting settings

Websites can also be whitelisted and blacklisted. These blacklists can be manually created, or they can be obtained from various security services. Blacklists can be continuously updated by security services and distributed to firewalls and other security systems that use them. Cisco's Firepower security management system is an example of a system that can access the Cisco Talos security intelligence service to obtain blacklists. These blacklists can then be distributed to security devices within an enterprise network.



Search the internet for The **Spamhaus Project**, which is an example of a free blacklist service.



## System-Based Sandboxing

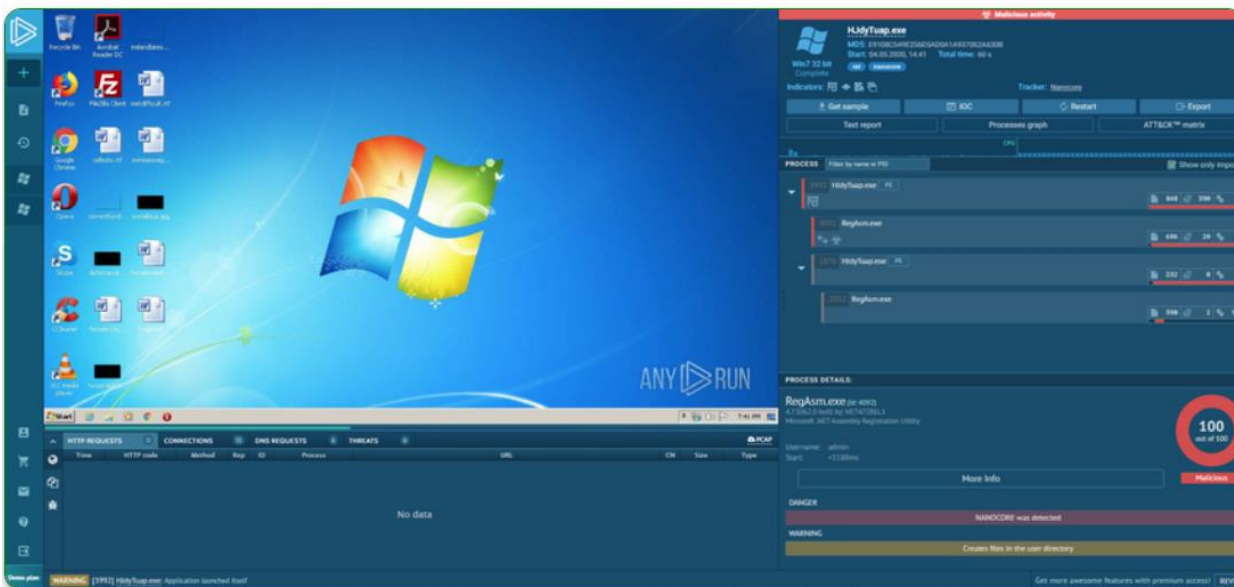
Sandboxing is a technique that allows suspicious files to be executed and analyzed in a safe environment. Automated malware analysis sandboxes offer tools that analyze malware behavior. These tools observe the effects of running unknown malware so that features of malware behavior can be determined and then used to create defenses against it.

As mentioned previously, polymorphic malware changes frequently and new malware appears regularly. Malware will enter the network despite the most robust perimeter and host-based security systems. HIDS and other detection systems can create alerts on suspected malware that may have entered the network and executed on a host. Systems such as Cisco AMP can track the trajectory of a file through the network, and can “roll back” network events to obtain a copy of the downloaded file. This file can then be executed in a sandbox, such as Cisco Threat Grid Glovebox, and the activities of the file documented by the system. This information can then be used to create signatures to prevent the file from entering the network again. The information can

also be used to create detection rules and automated plays that will identify other systems that have been infected.

Cuckoo Sandbox is a popular free malware analysis system sandbox. It can be run locally and have malware samples submitted to it for analysis. A number of other online public sandboxes exist. These services allow malware samples to be uploaded for analysis. Some of these services are VirusTotal, Joe Sandbox, and CrowdStrike Falcon Sandbox.

An interesting online tool is ANY.RUN, which is shown in the figure. It offers the ability to upload a malware sample for analysis like any online sandbox. However, it offers a very rich interactive reporting functionality that is full of details regarding the malware sample. ANY.RUN runs the malware and captures a series of screen shots of the malware if it has interactive elements that display on the sandbox computer screen. You can view public samples that have been submitted by ANY.RUN users to investigate information about newly discovered malware or malware that is currently circulating on the internet. Reports include network and internet activity of the malware, including HTTP requests and DNS queries. Files that are executed as part of the malware process are shown and rated for threat. Details are available for the files including multiple hash values, hexadecimal and ASCII views of the file contents, and the system changes made by the files. In addition, identifying indicators of compromise, such as the malware file hashes, DNS requests, and the IP connections that are made by the malware are also shown. Finally, the tactics taken by the malware are mapped to the MITRE ATT&CK Matrix with each tactic linked to details on the MITRE website.



# Cybersecurity Principles, Practices, and Processes

## CIA Triad – The Principle of Confidentiality

- To accomplish confidentiality without using encryption, **tokenization** is a substitution technique that can isolate data elements from exposure to other data systems. A random value with no mathematical relationship replaces original data. Outside the system, a token has no value and is meaningless. Tokenization can preserve the data format (its type and data length), which makes it useful for databases and card payment processing.
- Rights management covers both **digital rights management (DRM)** and **information rights management (IRM)**. Both protect data from unauthorized access by using encryption. DRM protects copyrighted material like music, films, or books. When any such content appears in digital form — for instance on CD, mp3, or e-book — it is encrypted, so the media cannot be copied without the decryption key. The decryption key is available only to licensed parties. IRM is used with email and other files that are relevant to the activities and communications of an organization. When this information is shared with others, IRM allows the document owner, the organization, or one of its members to control and manage access to the document.

*“Some organizations deploy privacy enhancement technologies including anonymization, data minimization and tokenization to help resolve data privacy concerns. Data anonymization works by obscuring privately identifiable data stored in a clear format, and turning that data into irreversible anonymous information. This might be something that @Apollo might think about implementing as its business grows.”*

## Data Integrity

Integrity is the accuracy, consistency, and trustworthiness of data across its entire lifecycle.

Data undergoes several operations, such as capture, storage, retrieval, update, and transfer. Data must remain unaltered by unauthorized entities during all these operations.

Methods used to ensure data integrity include hashing, data validation checks, data consistency checks, and access controls. Data integrity systems can include one or more of these methods.

Data integrity is a fundamental component of information security. Ensuring data integrity is a constant challenge for most organizations. Loss of data integrity can render entire data resources unreliable or unusable.

However, the importance of data integrity varies based on how an organization uses its data. For example, a bank or financial organization assigns a higher importance to data integrity than a social media channel.

- **Critical level of need:** in a healthcare organization, data integrity might be a matter of life or death prescription information must be accurate. Therefore, all data is continuously validated, tested and verified.
- **High level of need:** in an e-commerce or analytics-based organization, transactions and customer accounts must be accurate. All data is validated and verified at frequent intervals.
- **Mid level of need:** online sales and search engines collect data that has been publically posted. Little verification is performed, and data is not completely trustworthy.
- **Low level of need:** Blogs, forums and personal pages on a social media are powered by public options and open contribution. Data may not be verified at all, and there is a low level of trust in the content.

## Ensuring Availability

Availability refers to the need to maintain availability of information whenever it is needed. Cyberattack and system failures can prevent access to information, systems and services. There are many measures that organizations can implement to ensure the availability of their services and systems.

- **Equipment maintenance:** Regular equipment maintenance can dramatically improve system uptime. Maintenance includes component replacement, cleaning and alignment.
- **Operating systems and software updates and patches:** Modern operating systems, applications and software are continuously updated to correct errors and eliminate vulnerabilities. In every organization, all systems, applications and software should be updated to a regular schedule. Cybersecurity professionals can subscribe to alerts that announce new update releases.
- **Backup testing:** Backup of organization data, configuration data and personal data helps ensures availability. Backup systems and backed up data should also be tested to ensure they work properly, and that data can be recovered in the event of data loss.
- **Disaster planning:** Planning for disasters is a critical part of increasing system availability. Employees and customers should know how to respond to a disaster. The cybersecurity team should practice response protocols, test backup systems and be familiar with procedures for restoring critical systems.
- **New technology implementations:** High availability requires continuous evaluation and testing of new technologies to counter new threats and attacks. Cybercriminals use the latest tools and tricks, so cyber professionals are also required to keep up, using new technologies, products and devices.
- **Activity monitoring:** Continuous system monitoring increases system availability. Monitoring event logs, system alerts and access logs provides the cybersecurity professional with real-time system information. Such monitoring can identify attacks within seconds and enable cybersecurity professionals to fend them off quickly, when they occur.

- **Availability testing:** All systems should be tested to find vulnerabilities. Testing can include port scans, vulnerability scans and penetration tests.

## Data at Rest

‘Data at rest’ refers to data that is in storage. Simply put, it is the state data is in when no user or process is accessing, requesting or amending it. Data at rest can be stored on local devices such as a hard disk in a user’s computer, or centralized on a network, such as an organization’s server.

Data that is not in transit or in-process is considered data at rest. If you have data that you need to store and will want to access later, a number of storage options exist.

- **Direct-attached storage (DAS):** This type of storage is connected to a computer. A hard drive or USB flash drive is an example of direct-attached storage. By default, systems are not set up to share direct-attached storage with other computers on their network.
- **Redundant array of independent disks (RAID):** These professional storage solutions use multiple hard drives in an array, which is a method of combining multiple disks so that the operating system sees them as a single disk. RAID provides improved performance and fault tolerance.
- **Network attached storage (NAS) device:** This is a storage device connected to a network that allows storage and retrieval of data from a centralized location by authorized network users. NAS devices are flexible and scalable, meaning administrators can increase their capacity as needed.
- **Storage area network (SAN):** SAN architecture is a network-based storage system. SAN systems connect to the network using high-speed interfaces, which allows for improved performance and the ability to connect multiple servers to a centralized disk storage repository.
- **Cloud storage:** This is a remote storage option that uses space on a data center provider and is accessible from any computer with Internet access, usually upon subscription. Google Drive, iCloud, and Dropbox are all examples of cloud storage providers.

## Challenges of Protecting Stored Data

To improve data storage protection, organizations can automate and centralize data backups.

- Direct-attached storage can be one of the most difficult types of data storage to manage and control. Direct-attached storage is vulnerable to malicious attacks on the local host.
- Data at rest also includes backup data (when it is not being written or in transit). Backups can be manual or automatic. To boost security and decrease data loss, organizations should limit the types of data stored on direct-attached storage devices.
- Network storage systems offer a more secure option. Network storage systems including RAID, SAN and NAS provide greater performance and redundancy. However, network

storage systems are more complicated to configure and manage. They also handle more data, posing a greater risk to the organization if the device fails. The unique challenges of network storage systems include configuring, testing and monitoring the system.

*“@company has decided not to store its data using direct-attached methods. Instead, the organization opted for network storage systems. They employ an IT technician to manage this, as many organizations find protecting their stored data a growing challenge, with cybersecurity attacks becoming more sophisticated and frequent.”*

## Methods of Transmitting Data

Data in transit is the second state of data we are going to look at, referring simply to data which is being transmitted — it is neither at rest nor in use

Data transmission involves sending information from one device to another, and protecting data in transit poses challenges. There are numerous ways to transmit data between devices.

- **A sneaker net:** A sneaker net uses removable media to physically move data from one computer to another. Organizations will never be able to fully eliminate the use of a sneaker net as a way to transmit data between devices.
- **Wired networks:** Wired networks include copper and fiber optic media and can serve a local area network (LAN) or span great distances in wide area networks (WAN).
- **Wireless networks:** Wireless networks use radio waves to transmit data. Wireless networks are replacing wired networks as they become faster and able to handle more traffic. Wireless networks increase the number of guest users with mobile devices on small office home office (SOHO) and enterprise networks. This also increases the attack surface of the network.

Both wired and wireless networks transmit packets. The term packet refers to a unit of data that travels between a source and a destination on the network. Standard protocols such as the Internet Protocol (IP) and Hypertext Transfer Protocol (HTTP) define the structure and format of data packets. These standards are open source and fully available to the public. Protecting the confidentiality, integrity, and availability of transmitted data is one of the most important responsibilities of a cybersecurity professional.

## Challenges of Data in Transit

The protection of data in transit is one of the most challenging jobs of a cybersecurity professional. With the growth in mobile and wireless devices, and the increasing amounts of data collected and stored by organizations, cybersecurity professionals are responsible for protecting massive amounts of data crossing their network daily.

We have several challenges to deal with if we want to protect this data.

- **Protecting the confidentiality of data in transit:** Cybercriminals can capture, save, or steal data in transit. Cybersecurity professionals must take steps to safeguard data in transit, such as implementing VPNs, using SSL and IPsec, and various other methods of encrypting data for transmission.
- **Protecting the integrity of data in transit:** Cybercriminals can intercept and alter data in transit. Cybersecurity professionals deploy data integrity systems that test the integrity and authenticity of transmitted data to counter these actions. These systems include, for example, hashing and data redundancy.
- **Protecting the availability of data in transit:** Cybercriminals can use rogue or unauthorized devices to interrupt data availability, capturing it in transit. A simple mobile device can pose as a local wireless access point and trick unsuspecting users into associating with it. The cybercriminal can then hijack an authorized connection to a protected service or device. As data is being transmitted to and from the victim's device, the cybercriminal can intercept and even delete it, affecting its availability. Network security professionals can implement mutual authentication systems to counter these actions. A mutual authentication system requires the user to authenticate to the server and requests the server to authenticate to the user. This way, a user's device can tell when it is being contacted or it is receiving data requests from unauthenticated, rogue systems, such as the attacker's in the example above.

## Data in Process

Data in process refers to data during initial input, modification, computation or output. It is the state that data is in when it is neither in transit nor at rest — in simple terms, it is data that is being processed.

- **Input:** Protection of data integrity starts with the initial input of data. Organizations use several methods to collect data, each posing a potential threat to data integrity: data entry, scanning forms, file uploads and data collected from sensors. Corruption during the input process may include mislabeling and incorrect or mismatched data formats, data entry errors or disconnected and/or malfunctioning or inoperable system sensors.
- **Modification:** Data modification is any change made to original data, such as users manually modifying data, and programs processing and changing data. These changes are intentional. Processes like encoding/decoding, compression/decompression and encryption/decryption are all examples of data modification too. But changes to data can be unintentional or malicious. When data is modified in a way that stops it from being readable or usable, this is often referred to as data corruption. For instance, equipment failing can result in data corruption. Malicious code can also cause data corruption.

- **Output:** Data output refers to outputting data to output devices, such as printers, electronic displays and speakers. The accuracy of output data is critical because output provides information and influences decision-making. Examples of output data corruption include the incorrect use of data delimiters, incorrect communication configurations and improperly configured printers.

## Hardware-Based and Software-Based Technologies

In the world of cybersecurity, both software and hardware are utilized to protect the data and systems of organizations. Administrators can install the following software-based countermeasures or safeguards on individual hosts or servers: Software safeguards include programs and services that protect operating systems, databases and other services operating on workstations, portable devices and servers.

- **Software firewalls:** These control remote access to a system. Operating systems typically include a firewall, or a user can purchase or download software from a third party.
- **Network and port scanners:** These discover and monitor open ports on a host or server.
- **Protocol analyzers:** Otherwise known as signature analyzers, these are devices that collect and examine network traffic. They identify performance problems, detect misconfigurations, identify misbehaving applications, establish baseline and normal traffic patterns and debug communication problems.
- **Vulnerability scanners:** These are programs designed to assess weaknesses on computers or networks.
- **Host-based intrusion detection systems (IDS):** These examine activity on host systems only. An IDS generates log files and alarm messages when it detects unusual activity. A system storing sensitive data or providing critical services is a candidate for host-based IDS.

There are several hardware-based technologies used to safeguard an organization's assets too. They include:

- **Firewalls:** These block unwanted traffic. Firewalls contain customizable rules that define the traffic allowed into and out of a network.
- **Proxy servers:** Proxy servers use a network addressing scheme to present one organization-wide IP address to the Internet. A proxy server thus functions on behalf of the client when requesting service, potentially masking the true origin of the request to the resource server.
- **Hardware-based access control:** This term refers to devices that utilize biometric technology, such as fingerprint or iris scanners, to confirm the identity of anyone trying to access servers, data and systems.



- **Network switches:** Integral parts to networking, switches are commonly used as a connection point, linking other devices together, for example in a local area network. Their features enable them to add to the security efficiency of the network.

## **Establishing a Culture of Cybersecurity Awareness**

Investing a lot of money in technology will not make a difference if the people within the organization are not trained in cybersecurity.

A security awareness program and solid, comprehensive security policies are extremely important for any organization. An employee might not be purposefully malicious but just unaware of what the proper procedures are and still cause great harm. There are several ways to implement training to prevent this and to ensure all employees feel knowledgeable and confident to make cybersecurity best practices part of their day-to-day activities.

- **Education and training:**
  - Make security awareness training a part of an organization 's on-boarding process.
  - Tie security awareness to job requirement or performance evaluations.
  - Conduct in-person training sessions using gamification and activities (for example capture the flag scenarios)
  - Complete online modules and course such as CISCO endpoint security
- **Security awareness programs:** An active security awareness program depends on:
  - The organization's environment and network
  - The level of threat
  - The nature and demands of the data organization holds

**NOTE:** People are the first line of defense in cybersecurity, and every organization is only as strong as its weakest link. Every member of an organization must be aware of its security policies and implement them in their day-to-day activities.

## **Policies**

A security policy sets out the security objectives, rules of behavior and system requirements to be adhered to. A comprehensive security policy accomplishes several tasks:

- It demonstrates an organization's commitment to security.
- It sets the rules for expected behavior.
- It ensures consistency in system operations and software and hardware acquisition, use, and maintenance.
- It defines the legal consequences of violations.
- It gives security staff the backing of management.

Security policies inform users, staff and managers of the organization's requirements, which protect technology and information assets. A security policy also specifies the mechanisms needed to meet security requirements.

- **Identification and authentication policies:** Specify authorized persons that can have access to network resources and outlines verification procedures for said users.
- **Password policies:** Ensure passwords meet minimum requirements and are changed regularly.
- **Acceptable use policies:** Identify network resources and usage that are acceptable to the organization. It may also identify ramifications for policy violations.
- **Remote access policies:** Identify how remote users can access a network and what is remotely accessible.
- **Network maintenance policies:** Specify network device operating systems and end-user application update procedures.
- **Incident handling policies:** Describe how security incidents are to be handled.

One of the most common security policy components is an acceptable use policy (AUP). This component defines what users can and cannot do on the various system components. The AUP should be as explicit as possible, to avoid misunderstandings. For example, an AUP lists specific websites, newsgroups or bandwidth-intensive applications that users cannot access using the organization's computers or while on the organization's network.

## Standards

Standards help IT staff maintain consistency in operating the network.

- Security policies inform users, staff, and managers of the organization's technology and information asset protection requirements. This helps IT staff improve efficiency and simplicity in design, maintenance and troubleshooting.
- One of the most important security principles is consistency. For this reason, it is necessary for organizations to establish standards. Each organization develops standards that support its unique operating environment.
- An example of a standard would be an organization's password policy. For instance, the standard could stipulate that passwords require a minimum of eight uppercase and lowercase alphanumeric characters, including at least one special character. In addition, the password policy may specify that users must change their passwords every 30 days. A password history may be kept for the 12 most recent passwords to prevent anyone from reusing the same passwords during a twelve-month period.

## **Guidelines**

Guidelines are a list of suggestions on how to do things more efficiently and securely. They are similar to standards but are more flexible and are not usually mandatory.

Guidelines define how standards are developed and guarantee adherence to general security policies. Some of the most helpful guidelines make up an organization's best practices.

In addition to an organization's defined best practices, guidelines are also available from the following:

- National Institute of Standards and Technology (NIST) Computer Security Resource Center.
- National Security Agency (NSA) Security Configuration Guides.
- The Common Criteria standard.

Using the password policy example, a guideline can be a suggestion that the user takes a phrase that is memorable to them, like 'I have a dream,' and converts it to a strong password by replacing letters with characters, e.g. Ihv@dr3@m. The user can create other passwords from the same phrase by changing the number, moving the symbol or changing the punctuation mark.