CompTIA Sec +

TECHNOLOGY

Domain 2: Threats, Vulnerabilities, and Mitigations

Learning Objectives

By the end of this lesson, you will be able to:

- Compare and contrast various threat actors and their motivations to better anticipate and counter security breaches
- Understand common threat vectors and attack surfaces to enhance defensive strategies
- Identify different types of vulnerabilities to recognize potential security weaknesses
- Analyze indicators of malicious activity in different scenarios to aid a swift response
- Describe the purpose and effectiveness of mitigation techniques in securing enterprise operations

TECHNOLOGY

Threat Actors

Asset

An asset is any resource that adds value to an organization. It can be tangible or intangible.

Tangible:
Such as hardware and software

Intangible:
Include data, information, people, and reputation

Recognizing the range of organizational assets is vital in identifying potential vulnerabilities and safeguarding against threat actors.

Vulnerability

Vulnerability refers to a condition in a system that, whether intentionally or accidentally, causes a security flaw. This compromises the system's security.

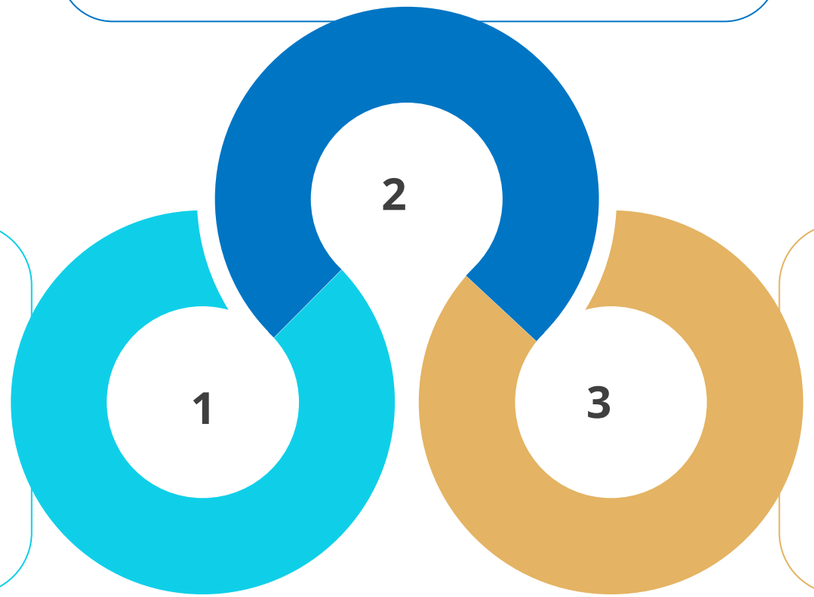
Examples: Unpatched software, buffer overflow, lack of awareness training

Effective management of vulnerabilities is crucial for enhancing system security and preventing breaches.

Threat

A threat is anything with the potential to cause harm to a system or data. The following are the different types of threats:

Intentional threats:
These are deliberate, malicious attempts to harm a system or steal data.



Unintentional threats:
These are accidental events that can cause damage, even when not intended to be malicious.

Natural threats:
Floods, earthquakes, fires, and other natural disasters can damage computer hardware and destroy data.

Threat Agents

A threat agent, also known as a threat actor, is an individual, group, or organization that can initiate an attack on a system or data.

Examples: Hackers and cybercriminals

Understanding the nature of threat agents is essential for developing effective security strategies and countermeasures.

Example of Threat to Asset

Asset

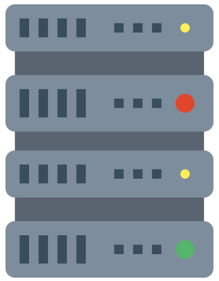
Organization's server

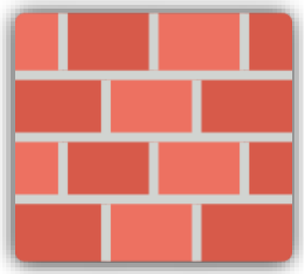
Vulnerability

Inadequate firewall rules

Threat

Cyber attack





Threat agent

Exposure

Unencrypted data (25%)

Risk

Loss of critical data

Countermeasure

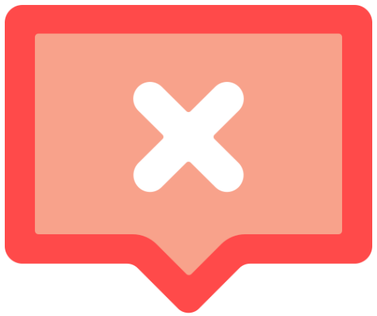
Reconfigure or replace the firewall

Risk

Risk is defined by the International Systems Audit and Control Association as the combination of the probability of an event and its consequences.

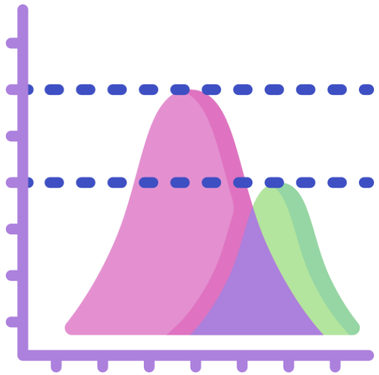
Effectively managing risk is crucial for minimizing potential negative outcomes and ensuring organizational resilience.

Key Terms Associated With Risk



Impact

The extent of damage that results from a threat exploiting a vulnerability



Likelihood

The probability that a threat will exploit a particular vulnerability

Examples of Risks

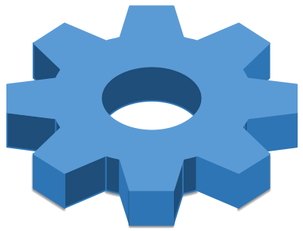
This table outlines key security risk factors from threat agents to resulting scenarios.

Threat Agent	Threat	Vulnerability	Risk Scenarios
Fire	Destruction of operating facility	Faulty fire detection or suppression equipment	Loss of life and property
Clueless user	Sharing of sensitive data using social engineering	Lack of security awareness training	Financial and reputation loss
Malicious insider	Data theft	Lack of adequate access controls on data	Legal risk and financial loss
Hacker	Unauthorized hacking	Unpatched server	Server unavailability and financial loss

Hackers

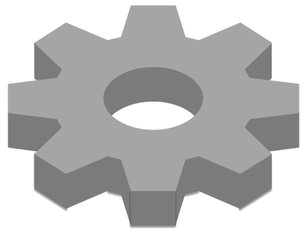
A hacker is someone who gains unauthorized access to computer systems. Originally, the term *hacker* neutrally described a person skilled in programming and system management.

The three major types of hackers are:



White Hat

Black Hat



Gray Hat

Script Kiddies

Script kiddies represent a unique cybersecurity threat, characterized by their lack of advanced skills and reliance on pre-made hacking tools.

Skill level

Lacking the expertise of skilled professional attackers, script kiddies often utilize attack tools crafted by other malicious programmers.

Threat potential

Despite their low skill level, they pose a real threat due to the sheer volume of individuals and the accessibility of powerful hacking tools.

Common activities

Commonly, they exploit known vulnerabilities in IT systems, focusing on easy targets that can be breached using readily available tools.

Motivation

Their primary aim is often to showcase their skills or gain peer recognition rather than cause serious harm.

Hacktivists

Hacktivists are individuals or groups who leverage their hacking skills for ideological, political, or social objectives.

Hacktivists use their extensive hacking skills to support causes and enact change.

They may release sensitive information, launch DoS attacks, or deface websites.

Their typical targets include the political, media, and financial sectors.

Groups like Anonymous, WikiLeaks, and LulzSec use cyber tactics for political goals.

Organized Crime

Organized crime has effectively extended its operations into the digital realm, seeking profit through cyber activities.

These groups have recognized the lucrative opportunities in digital spaces.

They mimic legitimate enterprises but engage in illegal cyber activities.

Key activities include ransomware attacks, credit card fraud, and identity theft.

Shadow IT

Shadow IT refers to the use of unauthorized technology within an organization without the IT department's approval.

Shadow IT includes software, applications, or devices used without formal oversight.

Employees often adopt these solutions to improve productivity or streamline work processes.

The use of shadow IT is typically not malicious but driven by the need for more efficient tools.

Nation-State Threat Actors

Nation-state threat actors are among the most formidable adversaries in cybersecurity.

They are government-sponsored entities conducting cyber operations to advance national interests.

With substantial resources and advanced technical capabilities, these actors can execute sophisticated attacks, including espionage, data theft, and sabotage.

Advance Persistent Threats

An Advanced Persistent Threat (APT) is a sophisticated cyberattack executed by well-funded and highly skilled entities, including nation-state actors and organized cybercriminal groups.

APTs excel in infiltrating specific systems or networks, maintaining stealth over prolonged periods.

These threats systematically extract valuable data or incrementally cause damage, thereby avoiding detection.

Criminal Syndicates

Criminal syndicates, also known as organized crime groups, are intricately structured organizations dedicated to profit-driven illegal activities.

Engagement: These syndicates are engaged in diverse criminal enterprises.

Activities: Their activities span drug trafficking, extortion, gambling, prostitution, and human trafficking.

Criminal Syndicates

Cybercrime has eclipsed physical crime in several countries, demonstrating its widespread impact through incidents and financial losses.

01 Operated across legal jurisdictions

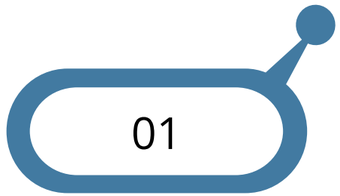
02 Driven by criminal profit

03 Well-resourced and funded

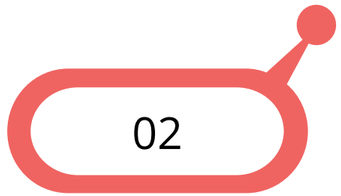
Competitors Espionage

Competitor-driven espionage is not only a strategy employed by state actors but is also increasingly utilized by businesses to gain competitive advantages over their rivals.

The two main types include:



Cyber espionage



Insider threat

Insider Threat

An insider threat arises when individuals, whether they have authorized access or not, potentially use their reach within an organization to intentionally or inadvertently cause harm.

A malicious insider threat actor:

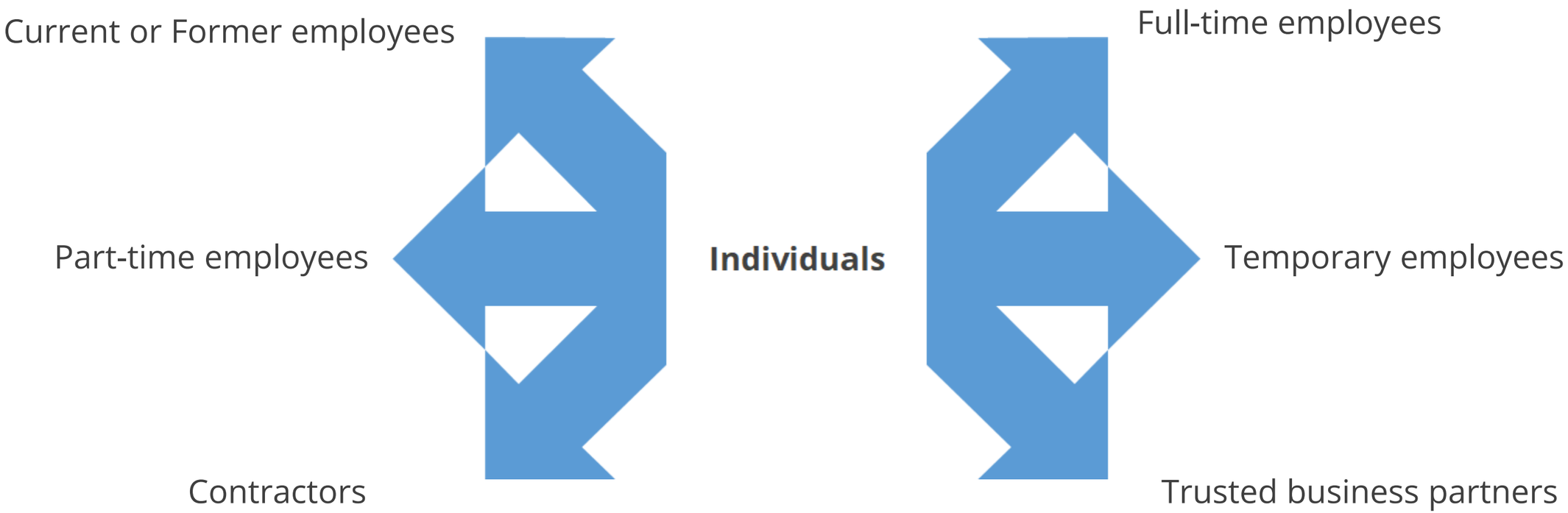
01 Possesses or holds authorized access to the organization's assets

02 Includes employees, contractors, and partners as potential threats

03 Engages in activities such as sabotage, financial gain, or seeking a business advantage

Individuals Involved in Insider Threat

Potential insider threats can come from a variety of roles within an organization, including:



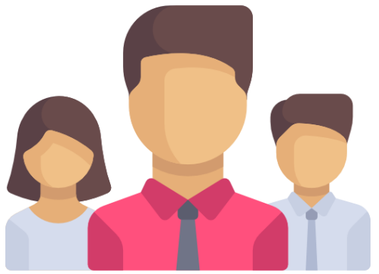
Organizational Assets Affected by Insider Threat

Insider threats can compromise various organizational assets, including:

Information

Technology

People



Facilities

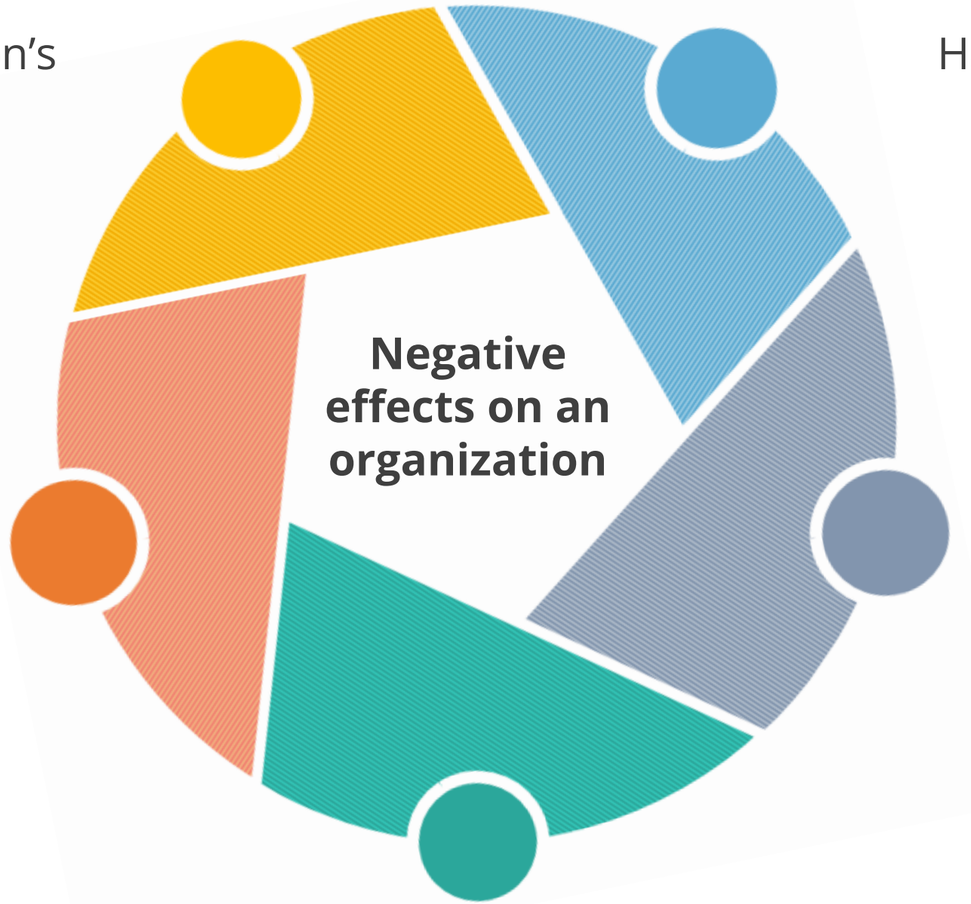
Intentional or Unintentional Insider Threat

Insider threats, whether intentional or unintentional, manifest in various forms, including:

Negative Effects Caused by Insider Threats to an Organization

Harm to the organization's customers

Harm to the organization's employees



Damage to the organization's reputation

Degradation of CIA of information or information systems

Disruption of the organization's ability to meet its mission

Comparison of Actors

The following table illustrates a comparative analysis of different cyber threat actors, highlighting their motivations, skill levels, resources, and potential impacts.

	Script Kiddies	Hacktivists	Organized crime	Nation state	Insider threat
Motivation	Thrill seeking	Political or social statement	Financial gain	Affect political outcomes	Revenge or financial gain
Skill level	Low	Low to high	High	High	Low to medium
Resources/ Funding	Low	Low to medium	High	High	Low to medium
Outcome	Service disruption	Service disruption	Financial loss of victim	Disable crucial infrastructure	Financial loss, disruption

Examples of Threat Agent

This table presents various cyber threat agents, detailing the associated threats they pose, vulnerabilities they exploit, and the nature of the resulting threats.

Threat agent	Threat	Vulnerability	Type of threat
Fire	Destruction of operating facility	Faulty fire detection or suppression equipment	Physical
Clueless user	Sharing of sensitive data using social engineering	Lack of security awareness training	Administrative
Malicious insider	Data theft	Lack of adequate access controls on data	Technical/physical
Hacker	Unauthorized hacking	Unpatched server	Technical

Insider Threat Actors

Unintentional insider threats often arise from organizational oversights and inadequate practices.

Examples could include:

01 Weak policies and procedures

02 Weak adherence to policies and procedures

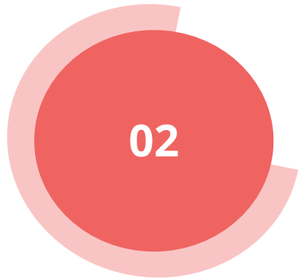
03 Lack of training or security awareness and shadow IT

Attributes of Actors

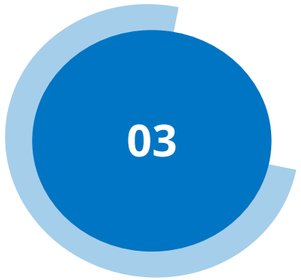
Attributes of Threat Actors

Threat analysis is the process of identifying the threat attributes with respect to:

Location (Internal or external)



Resource or funding availability



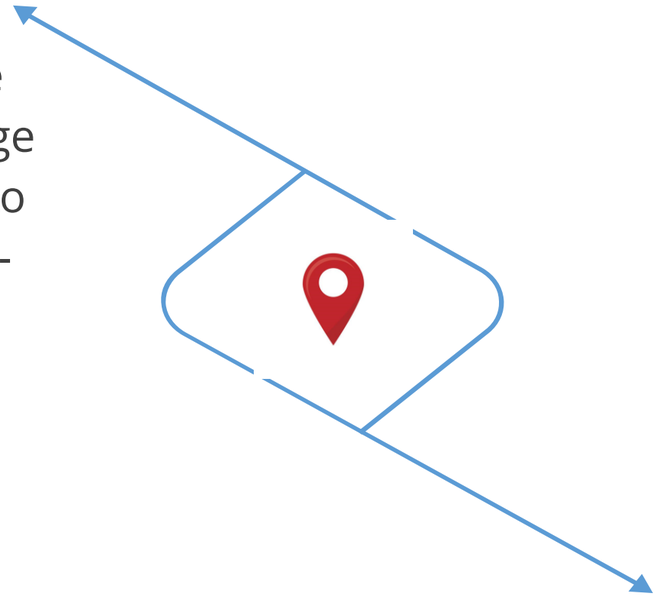
Level of sophistication or capability

Location

Location threat actors can be classified as:

External threat actor

These threats originate outside the organization and include a wide range of entities, from individual hackers to organized crime groups and nation-states.



Internal threat actor

These threats originate within an organization’s ranks, often taking advantage of their familiarity with systems, networks, and processes.

Resource Funding or Availability

The amount of resources and funding that threat actors have access to is commonly known as resources or funding availability. It is a key factor in determining their operational capabilities.

Well-resources

- These actors have access to substantial resources, which may include financial backing, advanced technology, or even government support.
- Nation-state and APT (Advanced Persistent Threat) actors fall into this category.

Limited resources

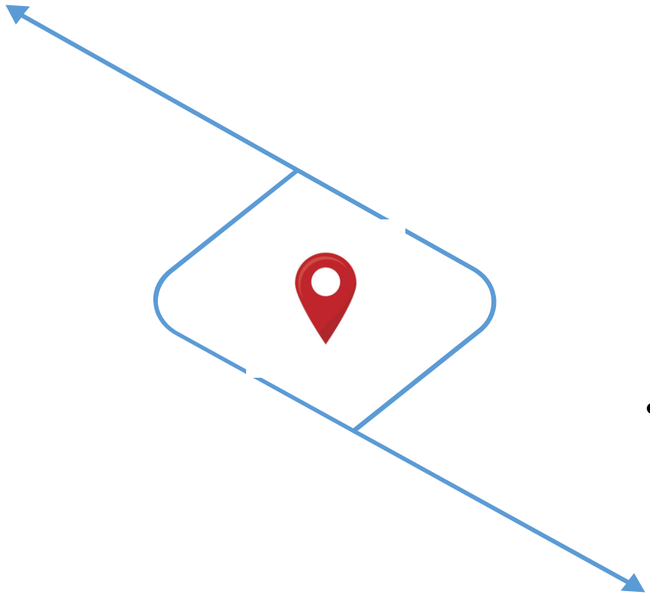
- Some threat actors, especially small-scale cybercriminals or unskilled attackers, operate with limited resources.
- They may rely on readily available hacking tools, social engineering, or other low-cost methods.

Level of Sophistications

The level of sophistication or capability of threat actors directly impacts the complexity and potential success of their attacks:

Highly sophisticated threat actors

- These actors possess advanced technical skills and deep knowledge of various attack vectors.
- Nation-states, APT groups, and certain organized crime syndicates often fall into this category.



Less sophisticated threat actors

- Unskilled attackers, script kiddies, and some cybercriminals operate with less advanced technical skills.
- They might rely on easily accessible tools, pre-made malware, and simpler attack methods.

TECHNOLOGY

Intent and Motivation

Intent and Motivation

Intent describes what an assailant believes the attack can achieve, while motivation is the reason for committing the attack.

Data exfiltration

Cyber espionage

Service disruptions

Intent and Motivation

Blackmail

Financial gain

Political beliefs

Intent and Motivation

Revenge

Disruption or chaos

War

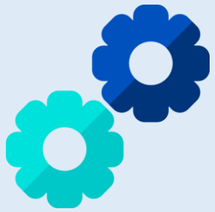
TECHNOLOGY

Attack Vectors

Attack Vectors

A threat actor's attack vector is the pathway to gain access to a secure system. Gaining access entails executing malicious code on the target system. The access can be as follows:

Goal: Hackers aim to steal sensitive data, acquire money, or disrupt operations.



Method: An attack vector is the method they use to achieve this.

Examples: Phishing emails, malware, unpatched software vulnerabilities, and weak passwords are all common attack vectors.

Different Types of Attack Vectors

Email

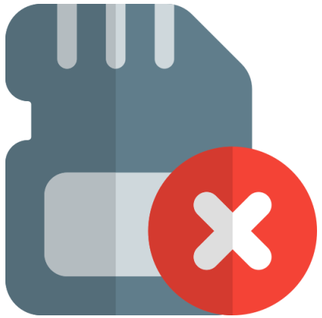
Instant message

File-based threat

Voice call

Short message service

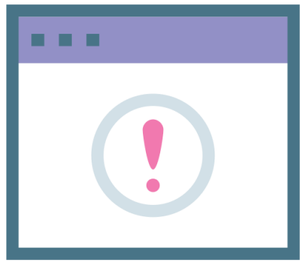
Image-based threat



Removable device

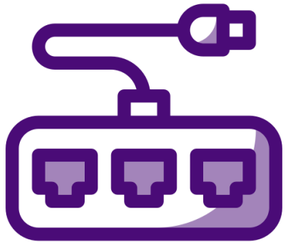
Vulnerable software

Different Types of Attack Vectors



Unsupported systems and applications

Unsecure networks



Open service ports

Default credentials

Supply chain

Human vectors/social engineering

Attack Vectors: Email

- Attackers frequently use email to spread malicious links or attachments that can cause a user's system to download malware.
- Phishing emails are common; they may pretend to be from reliable sources to trick users into disclosing personal or financial information.

Attack Vectors: Instant Message (IM)

- IM platforms are widely used for personal and business communication and are frequently targeted by cyber attackers.
- Attackers may use IM to spread malware via nefarious links or attachments, take advantage of holes in the IM software, or carry out phishing scams.

Attack Vectors: File-Based Threat

File-based threats use common files, such as documents, spreadsheets, or PDFs, to carry harmful scripts.

- These threats occur when malicious code is embedded within or attached to these files, which are then transmitted or shared to infect systems or networks.
- This type of threat is common in attachments sent via email, downloaded from websites, or transferred through file-sharing services.

Attack Vectors: Voice Call

- Voice call threats encompass a range of malicious activities conducted via phone calls, including deceptive practices such as vishing (voice phishing), unauthorized call interception, and fraudulent caller ID spoofing.
- Often, an attacker impersonates a legitimate entity to solicit personal or financial information or manipulates caller ID information to appear trustworthy.

Attack Vectors: Short Message Service (SMS)

- Due to the growing reliance on mobile devices, SMS vulnerabilities have become a prominent threat.
- SMS phishing (smishing) uses text messages to deceive users into revealing personal information or downloading malicious attachments.

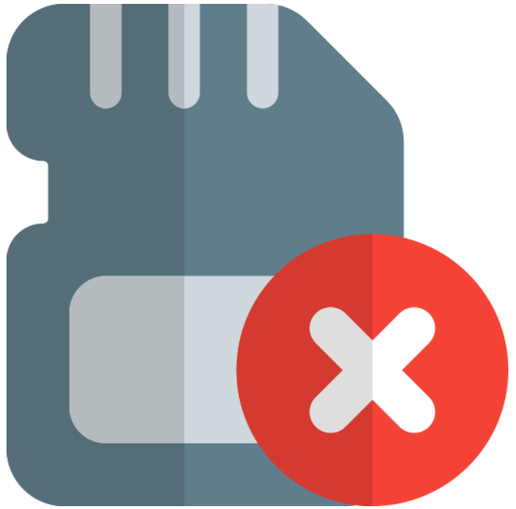
Attack Vectors: Image-Based Threat

Image-based threats involve manipulating digital images to hide or distribute malware, engage in phishing, or execute harmful actions.

- Attackers embed destructive code or manipulated image metadata to spread malware through email, social media, or other online platforms.
- When the image is opened, the hidden code can compromise the system.

Attack Vectors: Removable Device

- Portable storage devices like USB drives, external hard drives, or memory cards can introduce removable device threats, which can carry and transmit malware.
- When an infected removable device connects to a computer, it can execute malicious code, leading to data theft, system compromise, or malware spreading to other connected systems.



Attack Vectors: Vulnerable Software

- Vulnerable software has flaws or weaknesses in its code or design.
- Attackers can exploit vulnerable software to gain unauthorized access, disrupt operations, or cause other malicious activities.

Vulnerable Software - Prevention

Understanding the concepts of client-based and agentless security solutions is essential to avoid vulnerable software.

Client-based security

- It requires installing software (an agent) on a client device itself.
- The agent actively monitors and protects against malicious activities, such as exploiting software vulnerabilities.

Agentless security

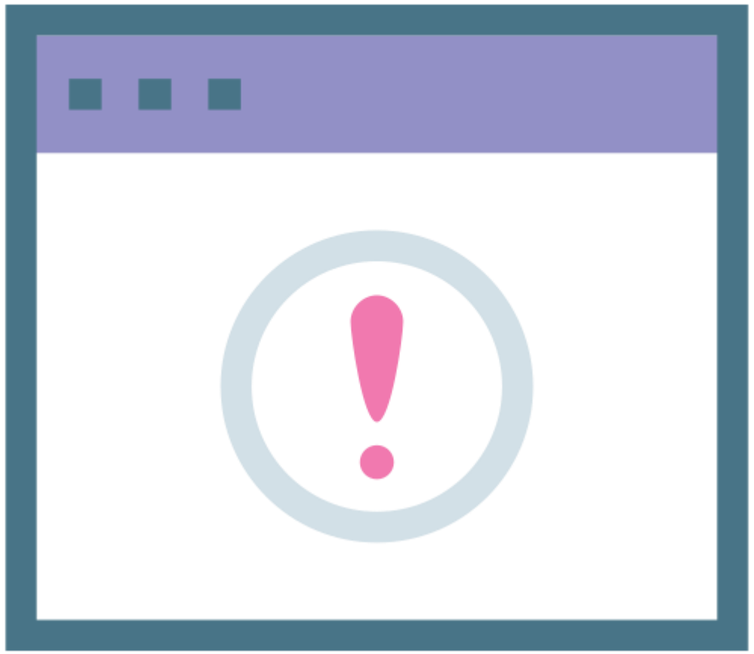
- It does not require installing software on individual client devices.
- Instead, it involves monitoring and enforcing security policies centrally, often through network devices or virtual appliances.

Attack Vectors: Unsupported Systems and Application

These are software tools or platforms that do not receive regular updates, security patches, or technical support from the developer or vendor.

1. This situation often arises when a software version reaches its official end-of-life (EOL) or the company that developed the software goes out of business or discontinues to support the products.

2. The security risks associated with unsupported systems and applications can be high, particularly when known vulnerabilities remain unaddressed.



Attack Vectors: Unsecure Networks

Unsecure networks are network, WIFI, or Bluetooth connections that one can join without a password or any other form of authentication.

- This lack of security makes them prime targets for hackers who can exploit these vulnerabilities to steal data or infect devices.

- Risks associated with unsecured networks are:
  - Interception of data
  - Man-in-the-middle attacks
  - Malware distribution

Types of Networks

Wireless networks

- Devices are connected without physical cables.
- Wireless networks that are improperly configured or lack robust encryption protocols can be susceptible to unauthorized access and eavesdropping.

Wired networks

- Devices are interconnected using physical cables.
- These are generally considered more secure than their wireless counterparts.
- They can still be vulnerable if proper segmentation and access controls are not implemented.

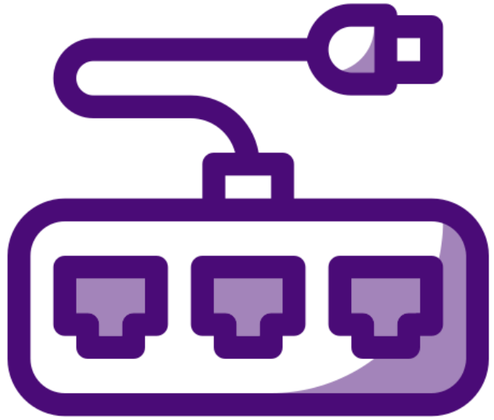
Bluetooth networks

- These networks allow short-range communication between devices.
- They can be exploited if devices are set to ‘discoverable’ mode or known Bluetooth protocol vulnerabilities are not patched.

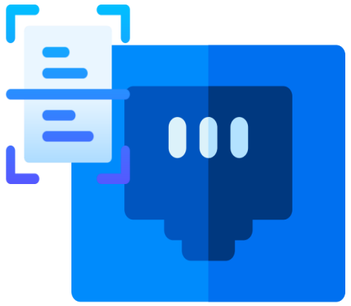
Attack Vectors: Open Service Ports

These are network communication endpoints that are left accessible and unguarded on a computer system.

- Applications use these ports to communicate with other devices over a network.
- Open service ports can present a significant security risk when not adequately secured.
- An open service port can be compared to an unlocked door in a building.
- Just as an unlocked door allows anyone to enter, an open service port can allow unauthorized access to an application or even the underlying operating system.



Mitigating Risks Associated with Open Ports



Scanning ports

Configuring firewalls

Monitoring and logging

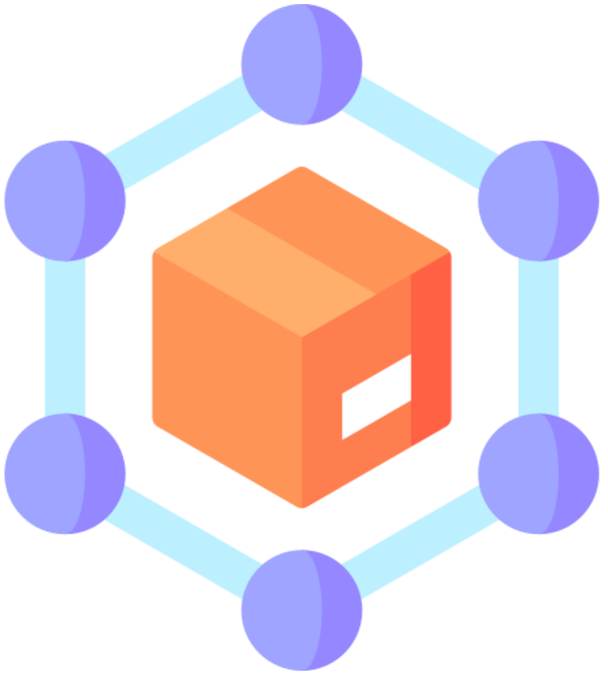
Patching and updating

Attack Vectors: Default Credentials

- Default credentials (often set by manufacturers for easy installation) are a glaring weakness.
- Attackers leverage default usernames and passwords to gain unauthorized access to systems and applications, and these default credentials are posted on several websites.
- Routers, switches, and other network device manufacturers often ship their products with simple default passwords, expecting the end user to change these credentials during initial setup.

Attack Vectors: Supply Chain

- A supply chain compromise occurs when an adversary jeopardizes a system's confidentiality, integrity, or availability of the information it processes, stores, or transmits.
- This chain, comprised of connected businesses, can be vulnerable at various points, making it a potential target for cybercriminals.



Attack Vectors: Social Engineering

Social Engineering is the exploitation of human behavior and trust.

- It is a strategy that relies on human emotion, deceptive tricks, and outright lies.
- Social engineers predate on people's intrinsic wants and needs.
- They are more knowledgeable of attributes and tailor their attacks accordingly.

Social Engineering

Examples of typical social engineering interference scenarios:

An attacker creates an executable file that prompts a user for their password and records whatever they type.

An intruder impersonates a remote sales agent seeking help to set up remote access and contacts the help desk.

An intruder sets off a fire alarm and connects a surveillance system to a network port while everyone is distracted.

Social Engineering Principles

Social engineering attacks rely on one or more of the following principles to be persuasive:

Familiarity or liking

- It creates trust.
- It makes the request appear reasonable and natural.

Consensus or social proof

- It utilizes courteous behaviors.
- It creates fabricated testimonials or contacts.

Authority and intimidation

- It makes the target fearful of refusing.
- It takes advantage of a lack of knowledge or awareness.

Scarcity and urgency

- It convinces the target to make a choice.

Phishing

Phishing is a hybrid of social engineering and spoofing.

It tricks the target into interacting with a malicious resource masked as a trusted entity, typically via email as the vector.

The user's login credentials are recorded as they authenticate with the spoofed site.

Phishing

The different types of phishing techniques include:

Spear phishing: It is a phishing scam in which the attacker possesses data that makes an individual target more likely to be deceived by the attack.

Whaling: It is a spear phishing attack directed specifically against upper management levels in the organization.

Vishing: It is a phishing attack conducted through a voice channel.

Smishing: It refers to the use of text communications via simple message service as the vector.

Impersonation

Impersonation involves pretending to be someone else to gain trust or access.

An attacker might impersonate a colleague, a boss, or even a family member to trick an individual into divulging sensitive information.

Training employees to verify identities through multiple channels can mitigate this risk.

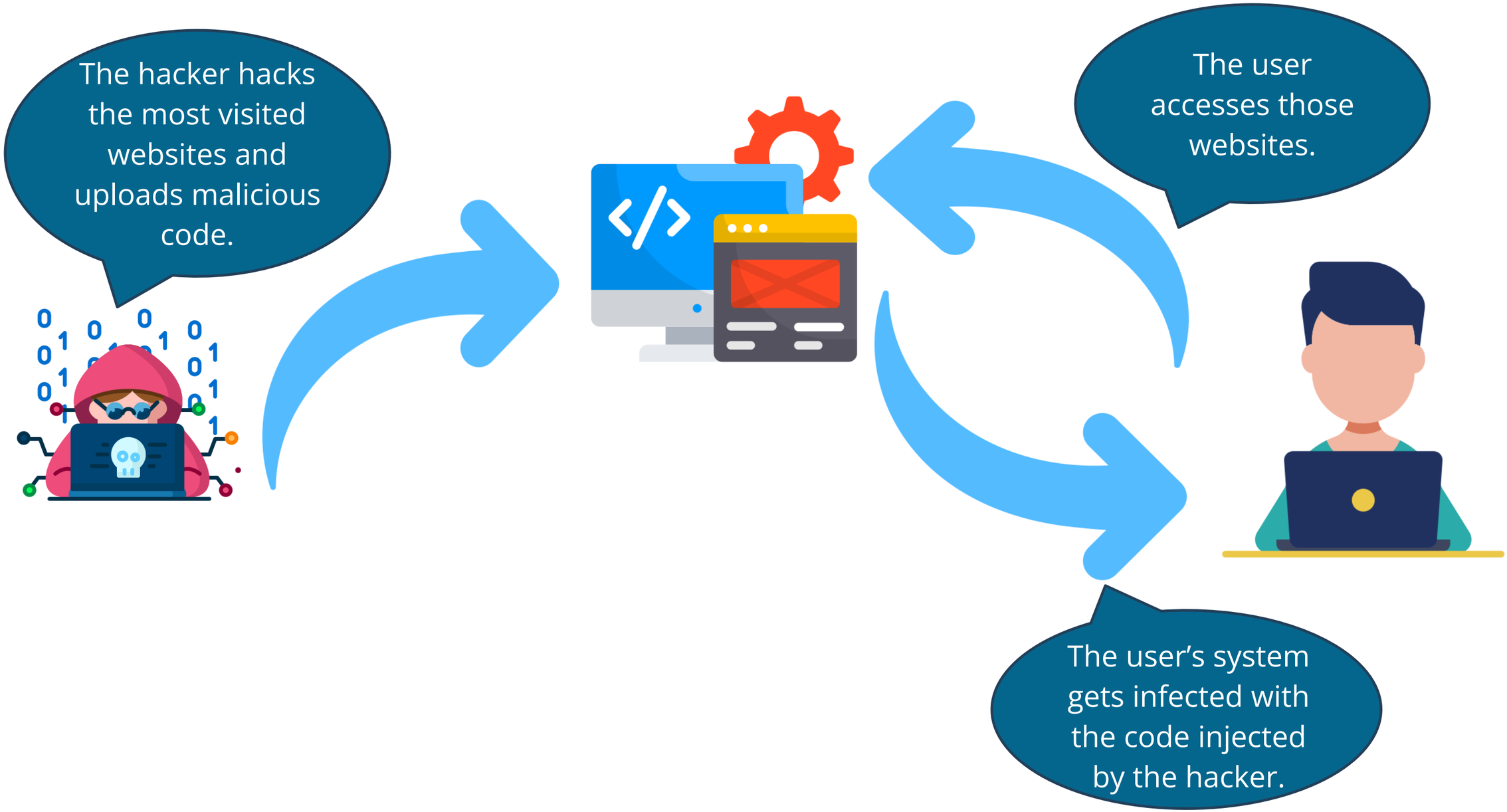
Watering Hole Attack

This cyberattack strategy targets specific users or organizations by compromising the websites they regularly visit.

\

- It is like a predator waiting near a watering hole in the wild, knowing their prey will eventually show up.
- To understand users' browsing habits, an attacker might guess or use direct observation.
- This type of attack may also incorporate other social engineering techniques, such as eavesdropping, pretexting, and phishing.

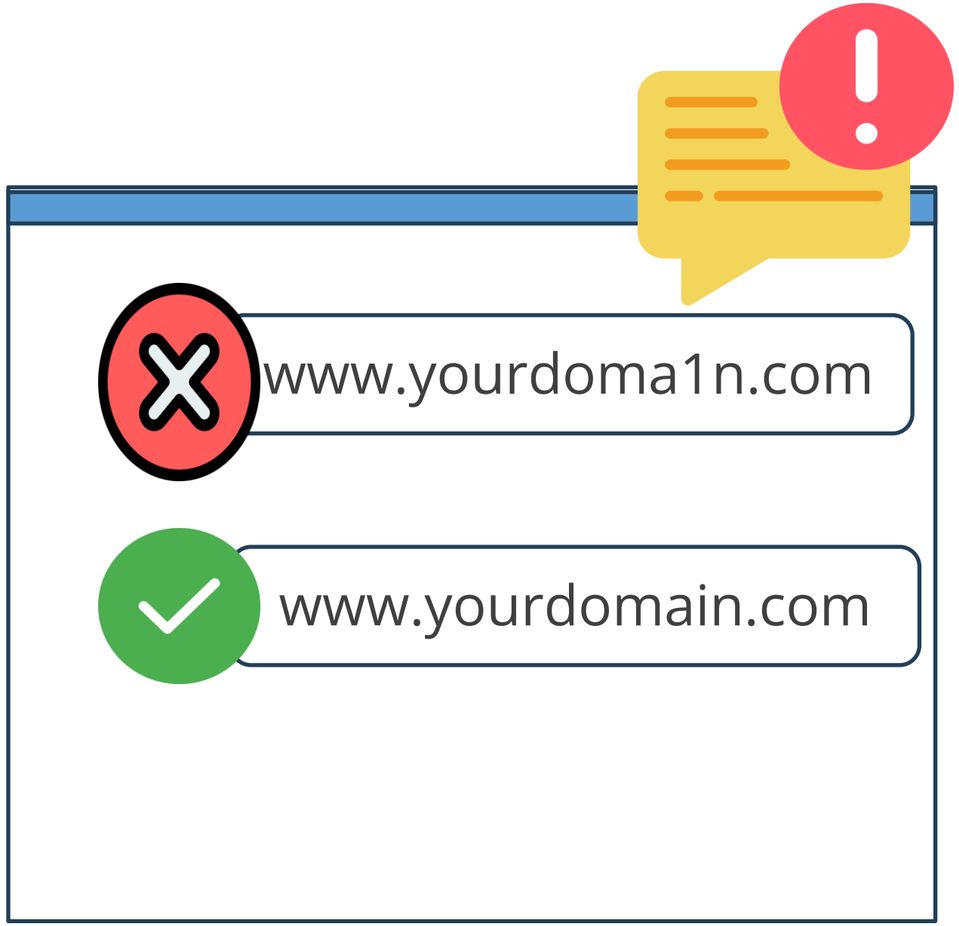
Watering Hole Attack



Typosquatting

Typosquatting is a technique that takes advantage of human error.

- Knowing that users often type URLs incorrectly, a typosquatter registers a domain that is a common typo of a legitimate site.
- They then impersonate the real website to host malware or perform other malicious activities to compromise users' systems.
- Example: An attacker might register the domain gogle.com to impersonate the website google.com and host malware or perform other malicious activities to compromise users' systems.



Brand Impersonation

Brand impersonation is a tactic in which attackers pretend to represent a trusted brand, such as a well-known bank or technology company.

- This impersonation can be used in phishing emails or fake websites to deceive victims into providing personal or financial information.
- Regular education, awareness training, and technical controls like email filtering can help individuals recognize and avoid these impersonation attempts.

TECHNOLOGY

Common Threat Vectors and Attack Surfaces

Introduction to Threat Actors and Attack Surface

Threat actors

- Threat actors are individuals or groups that pose a potential risk to an organization's security.
- Their motivations can vary and include financial gain, espionage, terrorism, or personal satisfaction.

Attack surface

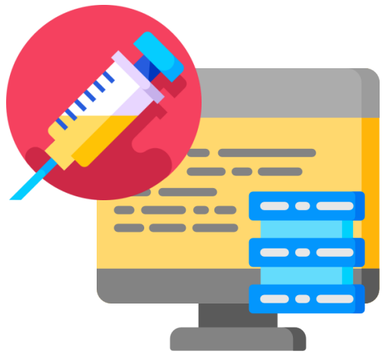
- The attack surface refers to all potential entry points a threat actor could exploit to gain unauthorized access to a system or network.
- It includes all vulnerabilities, exposed systems, and applications that could be targeted.

Application Vulnerability

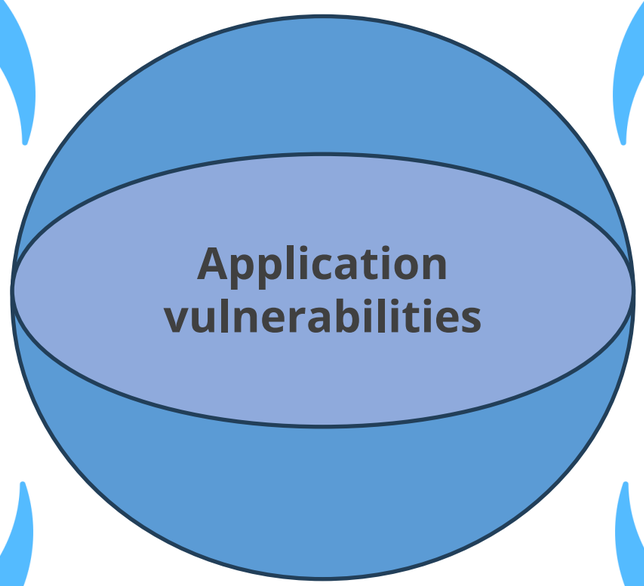
- The application layer is often a prime target for attackers because it serves as a gateway to user interactions and data.
- Vulnerabilities at this level can be especially detrimental, providing multiple avenues for malicious intrusion.
- Application vulnerabilities arise from weaknesses in how an application is designed, developed, or configured.
- Attackers can exploit these vulnerabilities to gain unauthorized access to systems or data.
- These vulnerabilities can exist in various applications, ranging from web browsers and mobile apps to enterprise software.

Types of Application Vulnerabilities

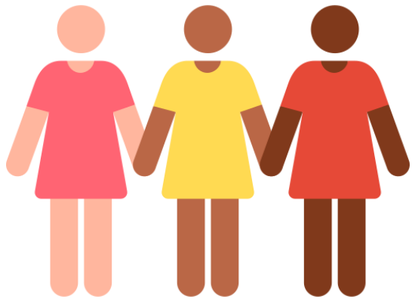
Memory injections



Buffer overflow



Race condition



Malicious update

Memory Injections

- A memory injection attack involves an attacker introducing (injecting) malicious code into a system's memory.
- Instead of executing malicious code directly on a host system, an attacker exploits a vulnerability in a legitimate process running on the system.
- This exploitation allows the injected code to run within the security context of the legitimate process.
- This makes detection more challenging because the malicious code appears to be part of a trusted operation.
- Memory injection attacks are particularly disastrous because they exploit legitimate processes to execute malicious code, making them difficult to detect.

Controls for Memory Injections

End Point Detections and Response (EDR)

It monitors abnormal behavior and flags anomalies.

1

2

Data execution prevention

It prevents code from being executed from data pages, blocking many types of memory injection attacks.

Whitelisting

It allows only pre-approved applications to run on the system.

3

4

User awareness training

It trains users to recognize phishing attempts and social engineering tactics.

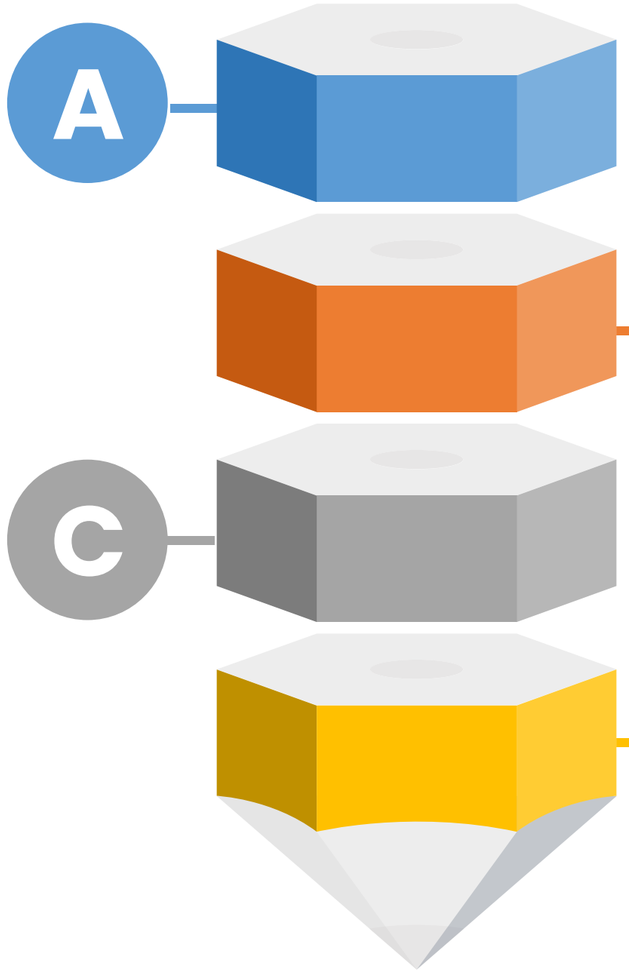
Buffer Overflow

- A buffer overflow, or buffer overrun, occurs when more data is placed into a fixed-length buffer than it can handle.
- This extra information overflows into adjacent memory space, corrupting or overwriting the data held there.

Buffer Overflow - Example

- One real-world example of a buffer overflow attack is the Slammer worm, also known as the SQL Slammer.
- In January 2003, this malicious software exploited a buffer overflow vulnerability in Microsoft SQL Server.
- The worm was spread rapidly by sending a small, specially crafted data packet to vulnerable servers, causing a buffer overflow in the server's memory.
- As a result of this overflow, the worm's code was executed in the server's memory space, generating a flood of network traffic as it attempted to infect other vulnerable systems.

Reason for Buffer Overflow



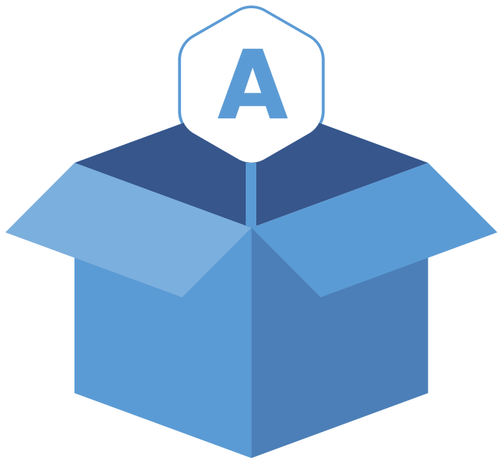
Poor programming practice

Programming language weakness

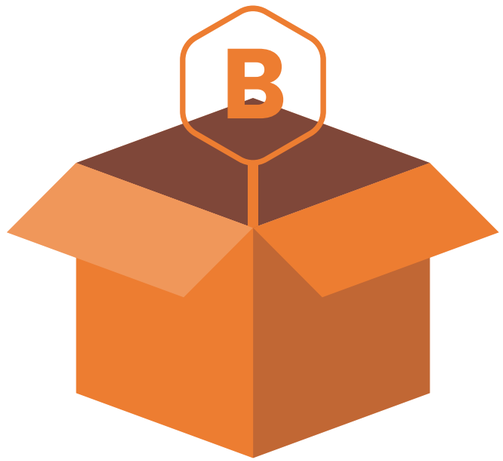
Lack of input validation

Poor management of memory allocation

Prevention of Buffer Overflow



Proper coding practice



Proper code review

Proper input validation

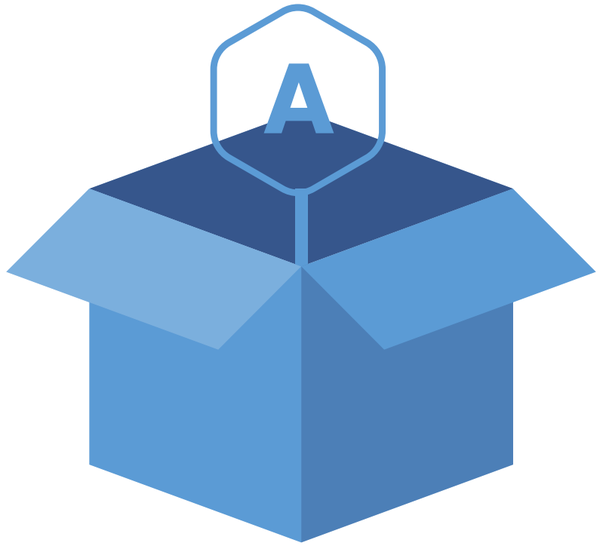
Malicious Update

- A malicious update occurs when legitimate software or firmware is altered or replaced with a version containing harmful code through an update mechanism.
- Attackers exploit the normal update process, disguising their destructive code as a routine update.
- Users believe they are simply updating their software or system, and unknowingly, they install the malicious version, leading to potential theft of sensitive information, unauthorized system access, or other damage.

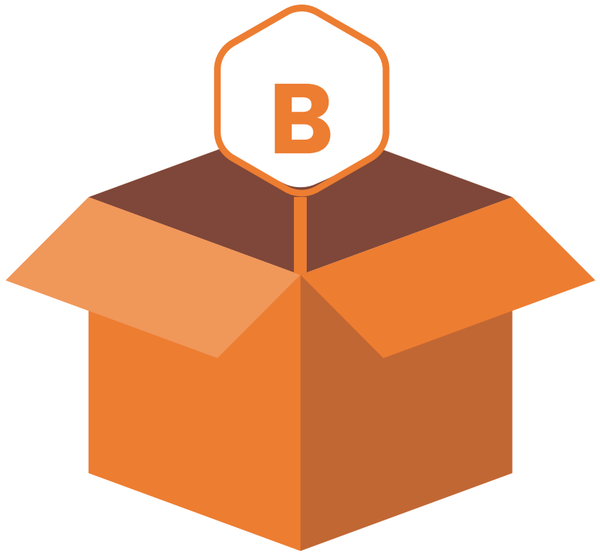
Malicious Update - Example

- CCleaner, a popular utility software used to clean and optimize computers, was compromised in 2017 when hackers successfully breached the supply chain of its parent company, Piriform.
- Hackers injected malicious code into a legitimate software update for CCleaner.
- This malicious update was distributed to millions of users who trusted the software's legitimacy.
- Once installed, the hidden malware allowed hackers to gain unauthorized access to infected systems, collect sensitive information, and deliver additional payloads for future attacks.

Prevention of Malicious Updates



Using secure channels for updates



Verifying updates with digital signatures

Educating users about the risks of updates from untrusted sources

Race Condition

- A race condition occurs when two instructions from separate threads attempt to access the same data simultaneously.
- Ideally, the developer should have programmed the threads to access the data sequentially.
- To illustrate, consider a scenario where one person is viewing a file's attributes while, simultaneously, another person accesses the same file.
- This phenomenon is referred to as **Time of Check to Time of Use** (TOC/TOU). In this situation, the individual accessing the file might modify its data, inadvertently overwriting the information being viewed by the first person.

Race Condition - Example

- An example of a race condition could involve an airline reservation system.
- Imagine two passengers, Alice and Bob, trying to book the last available seat on a flight simultaneously.
- Alice initiates the booking process and checks whether the last seat is available.
- Simultaneously, Bob starts the booking process and sees that the last seat is available. However, between Alice's check and booking confirmation, Bob confirms his booking.
- The system processes both transactions simultaneously.
- Due to the time gap between Alice's check and booking confirmation, both bookings are allowed to proceed, resulting in an overbooked flight.

OS-Based Vulnerabilities

- An OS-based vulnerability attack happens when hackers exploit weaknesses in the core software that manages a device's hardware and software resources.
- These vulnerabilities can arise from OS code, design, or configuration flaws.
- Adversaries may target these weaknesses to gain unauthorized access, disrupt operations, or extract sensitive data from a system.

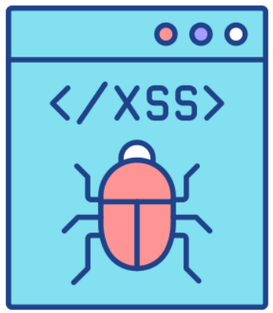
OS-Based Vulnerability - Example

- A prime example is the BlueKeep vulnerability that affected Microsoft Windows systems.
- This exploit allowed attackers to infiltrate unpatched systems remotely, compromising 1 million devices.

Web-Based Vulnerabilities

- Web-based vulnerabilities are weaknesses or flaws found in web applications that attackers can exploit to gain unauthorized access to data, systems, or entire networks.
- These vulnerabilities can exist on the server side (the code running on the web server) or the client side (the user's web browser).

Types of Web-Based Vulnerabilities



Cross-site scripting

SQL injections

Cross-site request forgery

SQL Injections

- These attacks allow a malicious individual to directly perform SQL transactions against the underlying database, bypassing the isolation model.
- SQL injection (SQLi) refers to an attack where an attacker can execute malicious SQL statements to control a web application’s database server.
- Such an attack can damage the database, retrieve information, or manipulate data.

SQL Attack Prevention

A. Update and patch

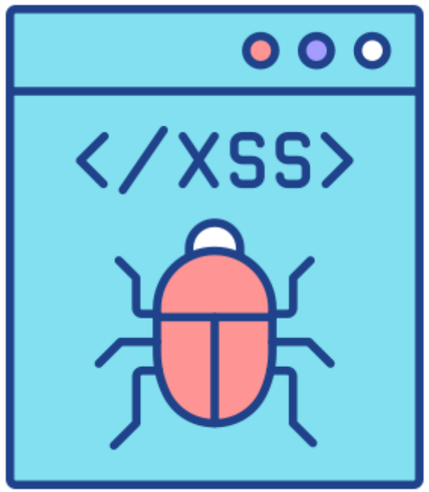
B. Perform input validation

C. Limit account privilege

D. Use stored procedure

Cross-Site Scripting

- Cross-site scripting (XSS) attacks involve injecting malicious scripts into otherwise benign and trusted websites.
- These attacks occur when an attacker uses a web application to send malicious code, typically in the form of a browser-side script, to a different end user.
- XSS enables attackers to inject client-side scripts into web pages viewed by other users.



Cross-Scripting Attack - Illustration

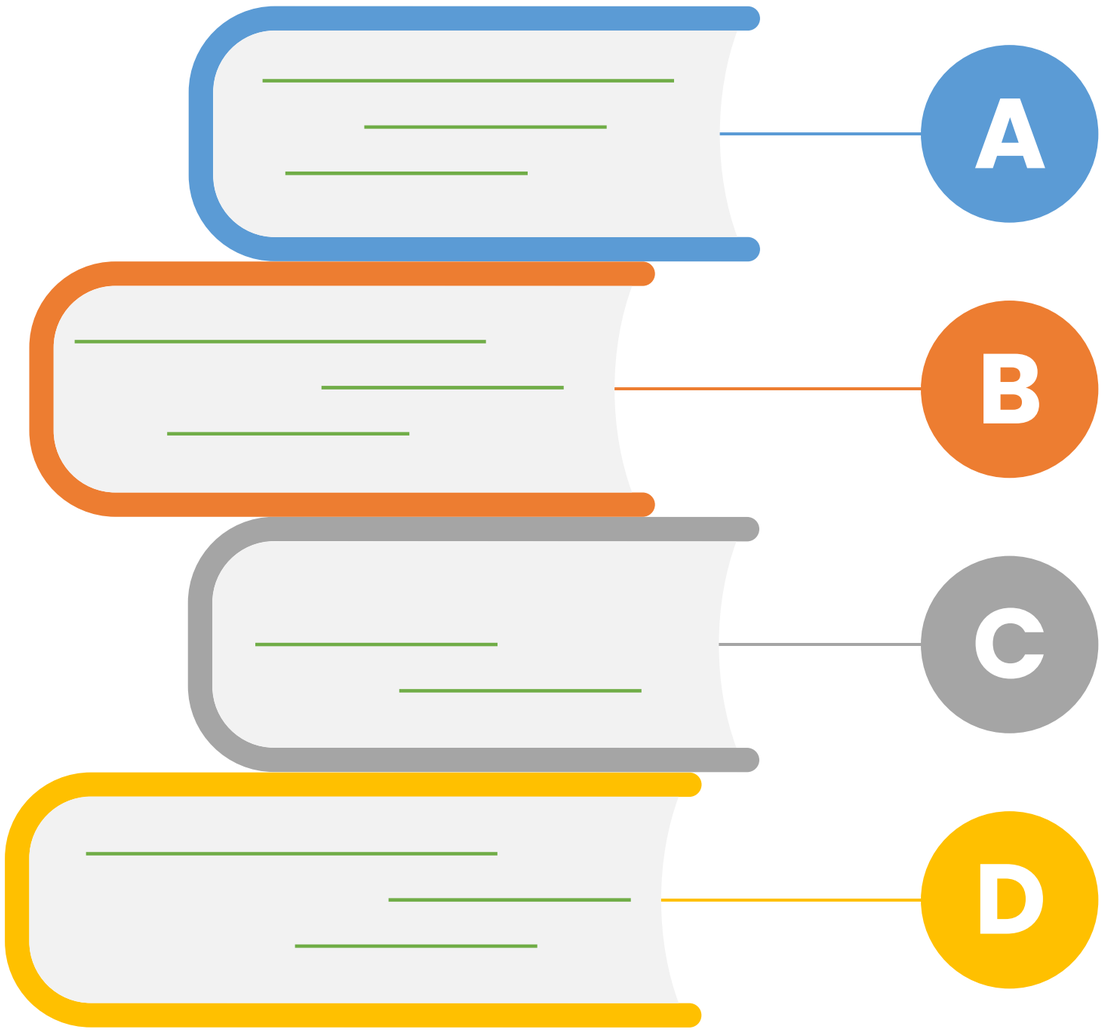
1. Suppose a web application, abc.com, is hosted on a server with an XSS vulnerability.

2. This XSS vulnerability in the web application server enables hackers to inject malicious scripts into the web server.

3. Now, a user attempts to access abc.com through their web browser for daily tasks or any other specific task.

4. The malicious script, injected by a hacker, is executed on the user's browser, enabling the hacker to steal valuable information or perform any designated task.

Impact of XSS



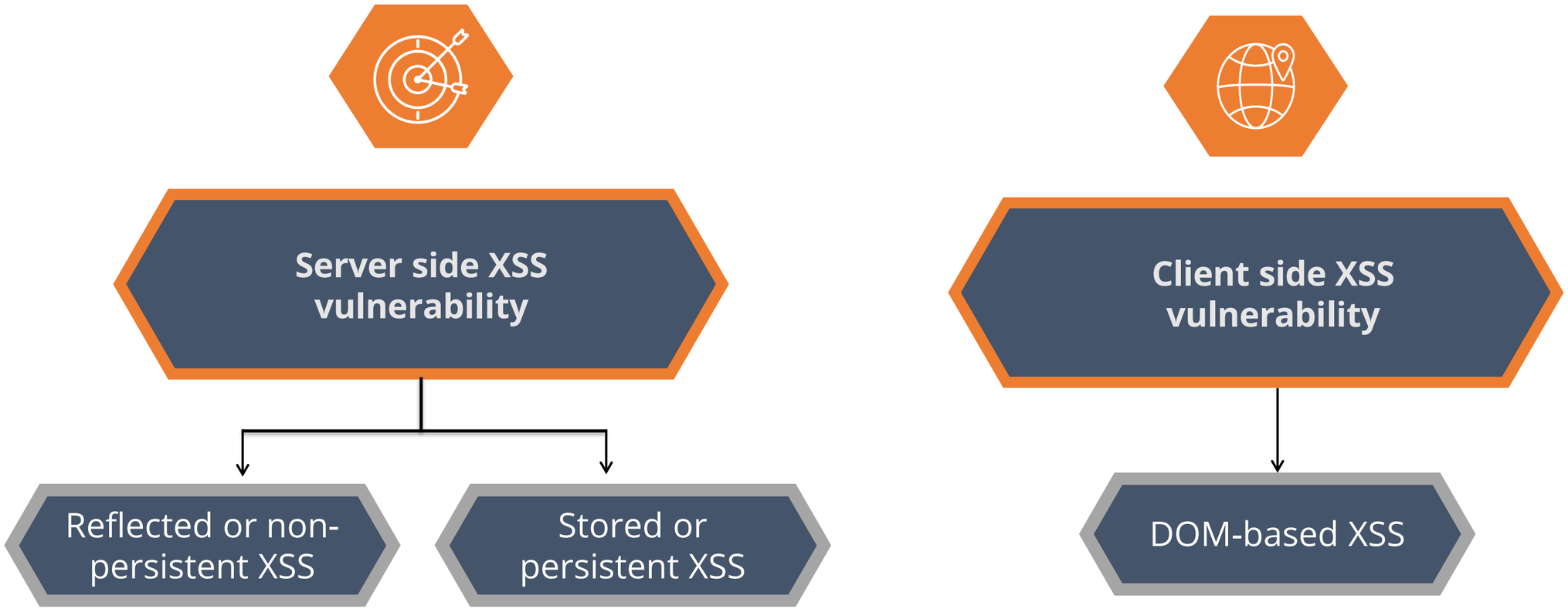
A. Session hijacking

B. Deploying hostile content

C. Impersonating user

D. Phishing

Types of Cross-Site Scripting



Types of XSS

Reflected or non-persistent XSS

- Reflected vulnerabilities occur when an attacker tricks the victim into processing a URL programmed with a rogue script to steal the victim's sensitive information (such as cookies, session IDs, etc.).
- The principle behind this attack lies in exploiting the lack of proper input or output validation on dynamic websites.

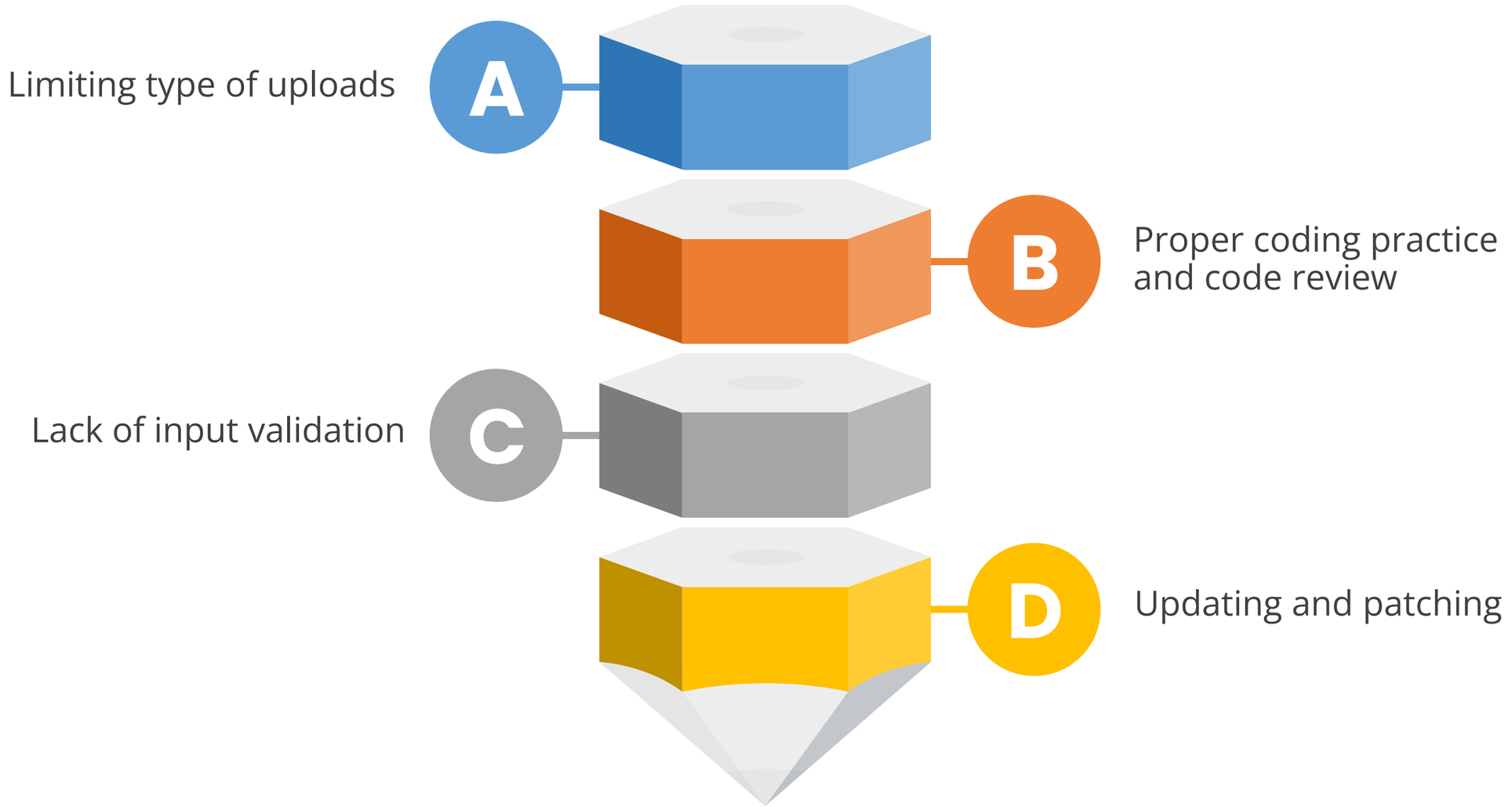
Non-Reflected or Persistent XSS

- These are also known as stored or second-order vulnerabilities and are generally targeted at websites that allow users to input data stored in a database or another location, such as forums, message boards, guest books, etc.
- The attacker posts text containing malicious JavaScript. When other users later view these posts, their browsers render the page and execute the attacker's JavaScript.

DOM-based XSS

- It is a client-side web application vulnerability that allows attackers to inject malicious scripts into the Document Object Model (DOM) of a web page.
- The DOM can be imagined as a blueprint for a house that represents the structure and content of a web page.
- It outlines how elements like rooms (sections), furniture (content), and hallways (navigation) are organized and interact within the browser.

Prevention of XSS

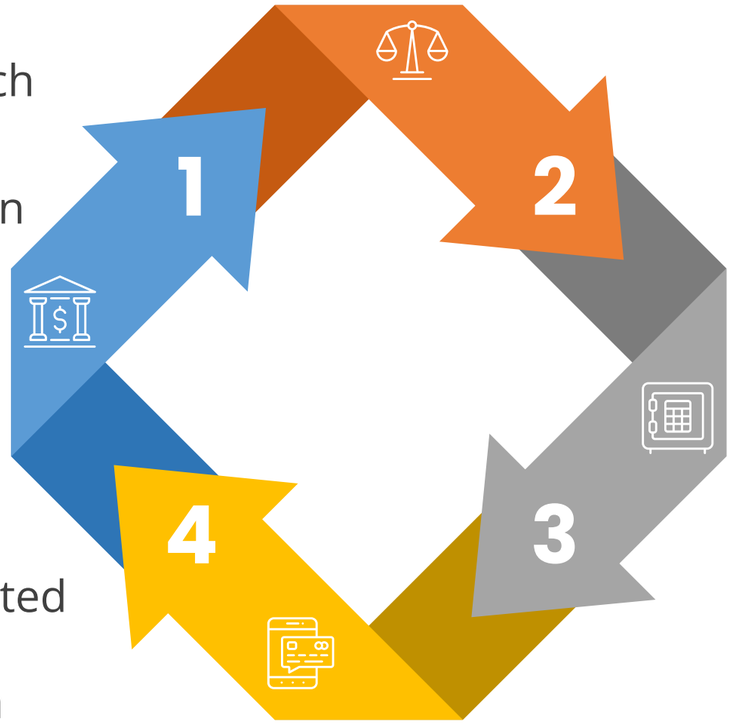


Cross-Site Request Forgery

- Cross-site request forgery (XSRF) attacks exploit unintended behaviors that are legitimate within defined use but occur under unauthorized circumstances.
- These attacks are executed against sites with authenticated users, leveraging the site's trust from a prior authentication event.
- The attacker tricks the user's browser into sending an HTTP request to the target site, thereby exploiting this trust.

Cross-Site Request Forgery

1. Imagine the user's bank lets users log in and perform financial transactions without needing to validate their authentication for each transaction. For example, the user would not be re-authenticated when transferring money to another account.



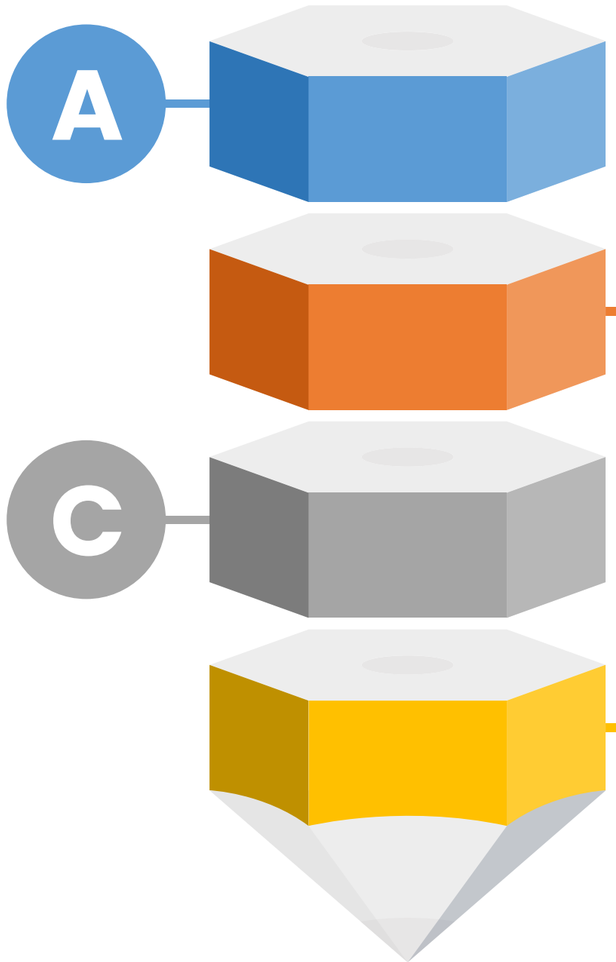
2. Now, the user opens a banking application and authenticates the banking website.

3. If the user is still logged in and has not closed their browser, an action in another browser tab could send a hidden request to the bank, resulting in a transaction that appears to be authorized but was not initiated by the user.

4. This transaction executes successfully because the banking application believes it is being initiated by the user. However, it is being executed by a malicious application opened in another tab or browser.

Prevention of CSRF

Train and maintaining awareness

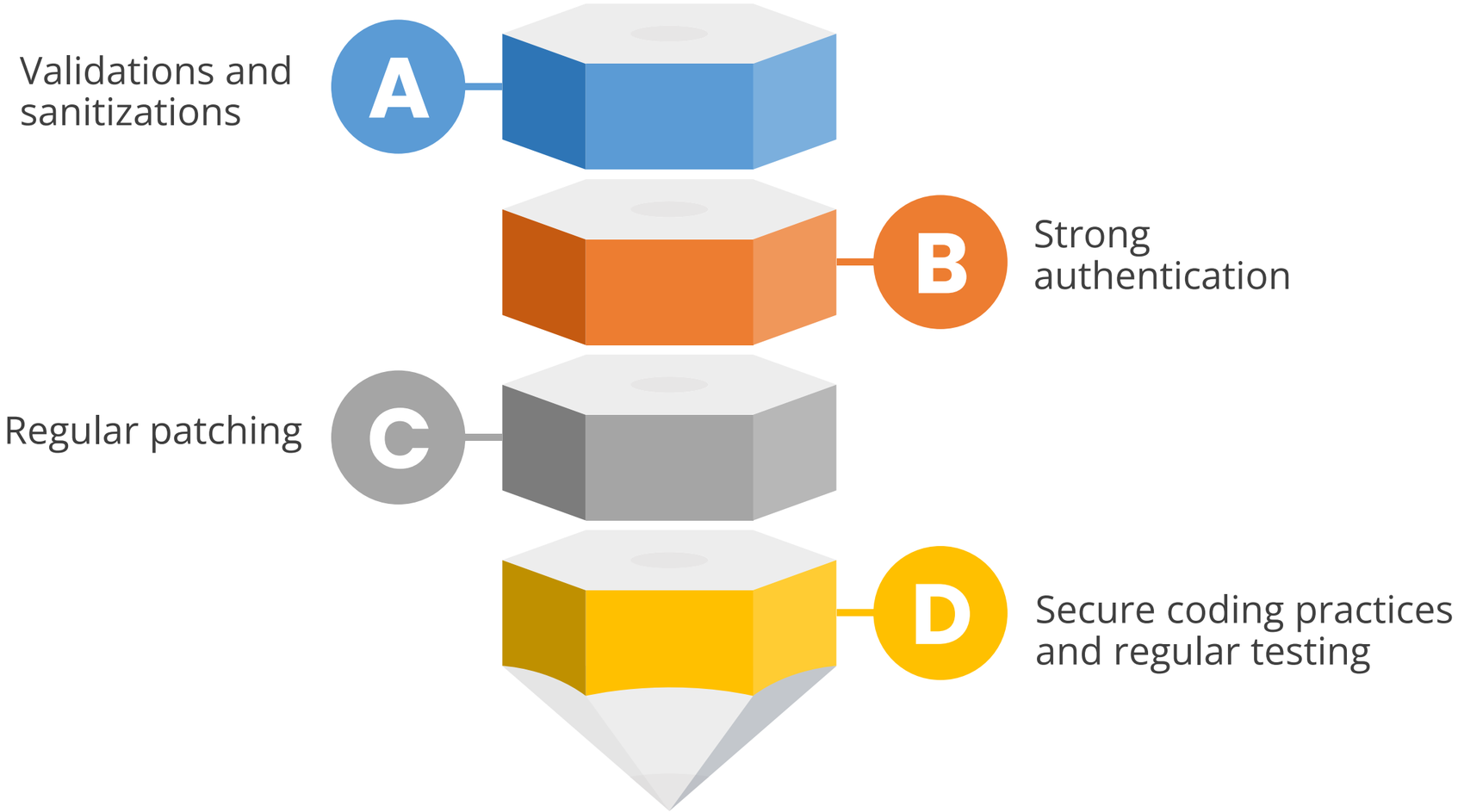


Scan and testing regularly

Limit authentication time

Set cookie expiration

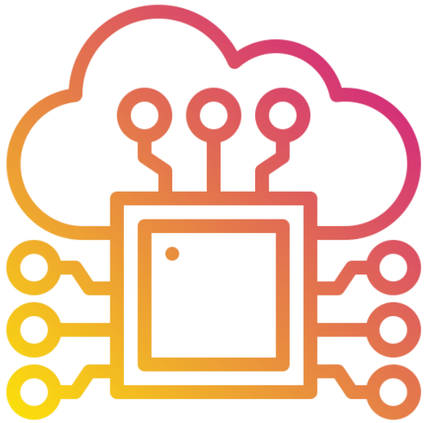
Controls for Web Application Vulnerability



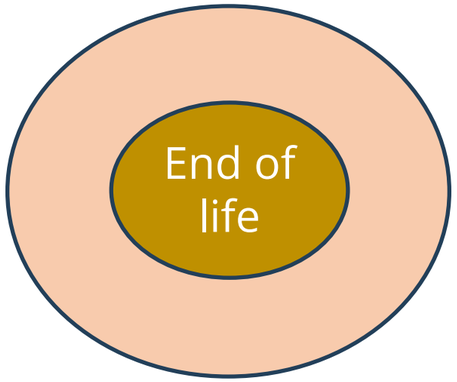
Hardware Vulnerabilities

- Hardware vulnerabilities are flaws in a computer system's physical components that attackers can exploit to gain unauthorized access to data or take control of the system.
- These vulnerabilities can exist in a variety of devices, including computers, servers, mobile devices, and even Internet of Things (IoT) devices.

Types of Hardware Vulnerabilities



Firmware

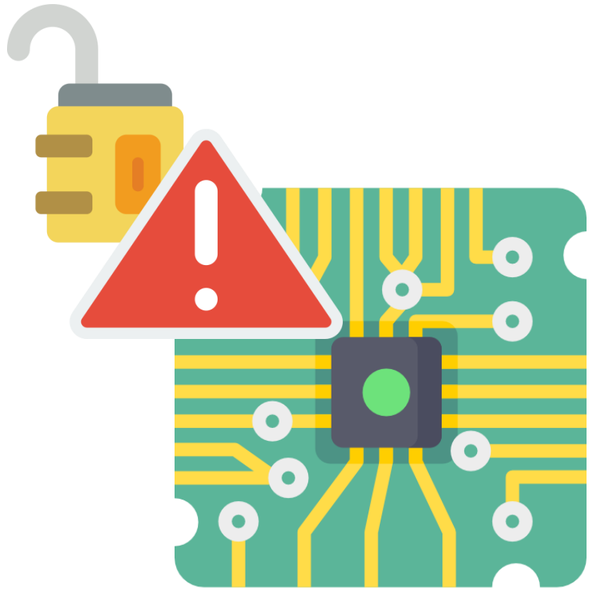


End of life

Legacy platforms

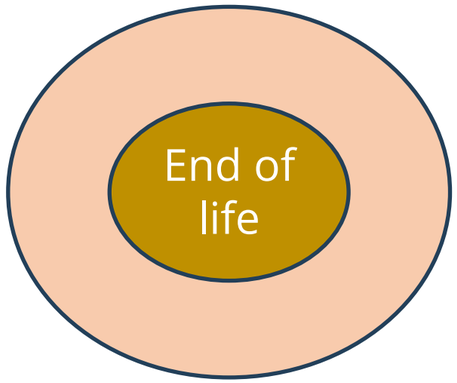
Firmware Vulnerability

- A firmware vulnerability refers to a weakness in the low-level code that controls a device's hardware.
- These weaknesses can be exploited by attackers to gain unauthorized access, steal data, or disrupt the device's functionality.
- Firmware is essentially the hidden software that acts as an intermediary between the physical components and the operating system.



End of Life

- End-of-life (EOL) hardware refers to hardware that has reached the stage in its lifecycle when the manufacturer no longer supports it.
- This lack of support often means that the hardware does not receive essential security updates or patches, making it especially susceptible to exploitation.
- The most effective way to mitigate EOL hardware vulnerabilities is through a proactive replacement or upgrading process to ensure that hardware components remain current and supported.



Enhancing Server Security

Duration: 10 Min.

Problem Statement:

As a Windows Server Administrator, you have been tasked with enhancing the security of Windows Server 2022. The primary objectives include disabling guest and local administrator accounts, restricting remote access, configuring account lockout policies, and disabling unnecessary services. These actions are essential to mitigate cyber threats and ensure the secure operation of the server.

Note: Refer to the demo document for detailed steps:
01_Enhancing_Server_Security

ASSISTED PRACTICE

Assisted Practice: Guidelines

Steps to be followed are:

1. Disable guest user accounts
2. Disable the local administrator account
3. Create a new, unique administrator account
4. Restrict remote access
5. Configure account lockout policy per best practices
6. Disable any unnecessary service

Legacy Hardware

- Legacy hardware vulnerabilities are security weaknesses in older computer equipment that can be especially dangerous due to a lack of support and updates.

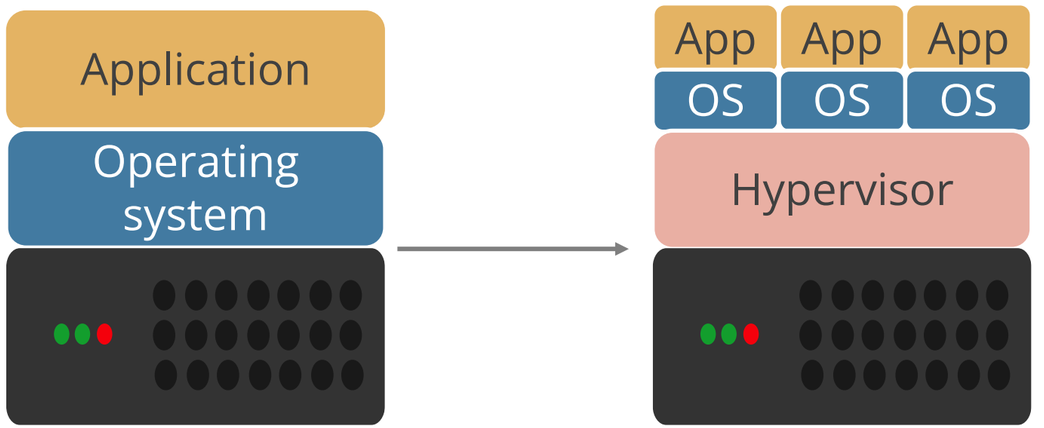
- These vulnerabilities are like cracks in an aging foundation, making the system much easier for attackers to break into.

- Issues with legacy hardware include:
  a) Missing security patches
  b) Outdated security patches
  c) Limited functionality
  d) End-of-life status

Virtualization

Virtualization is a technology that enables multiple operating systems to run side-by-side on the same processing hardware.

It adds a software layer between an operating system and the underlying computer hardware.



Traditional architecture

Virtual architecture

Its benefits include efficiency, higher availability, and lower costs.

Hypervisor

A hypervisor is software that is installed to virtualize a given computer.

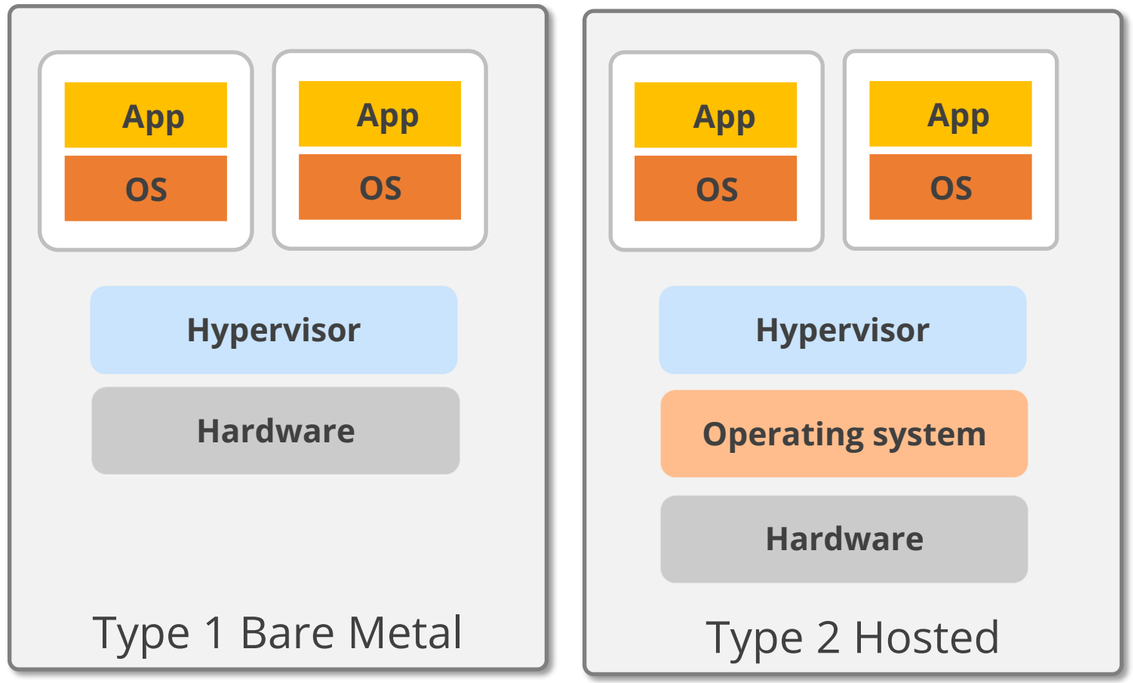
- **Host machine:** A computer on which a hypervisor is installed
- **Guest machine:** Every virtual machine

Type 1 hypervisors run directly on the host machine's hardware.

- Examples: Microsoft Hyper-V, VMware ESX/ESXi

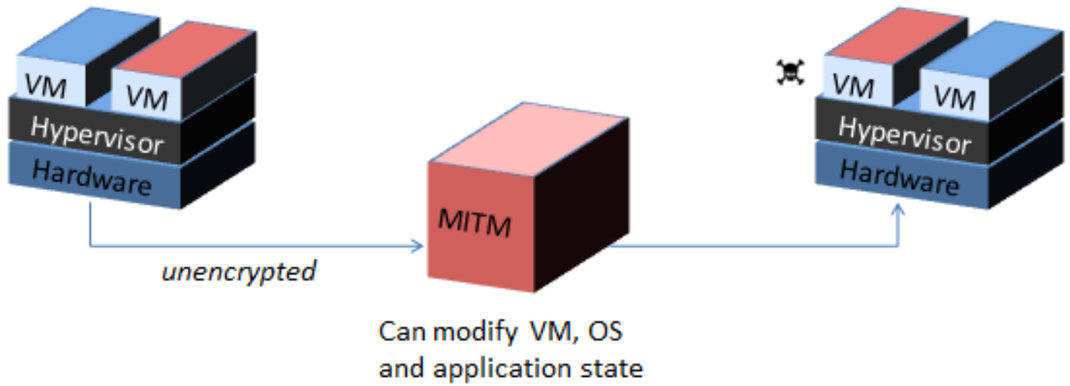
Type 2 hypervisors run within an existing operating system environment.

- Examples: VMware Workstation, VirtualBox



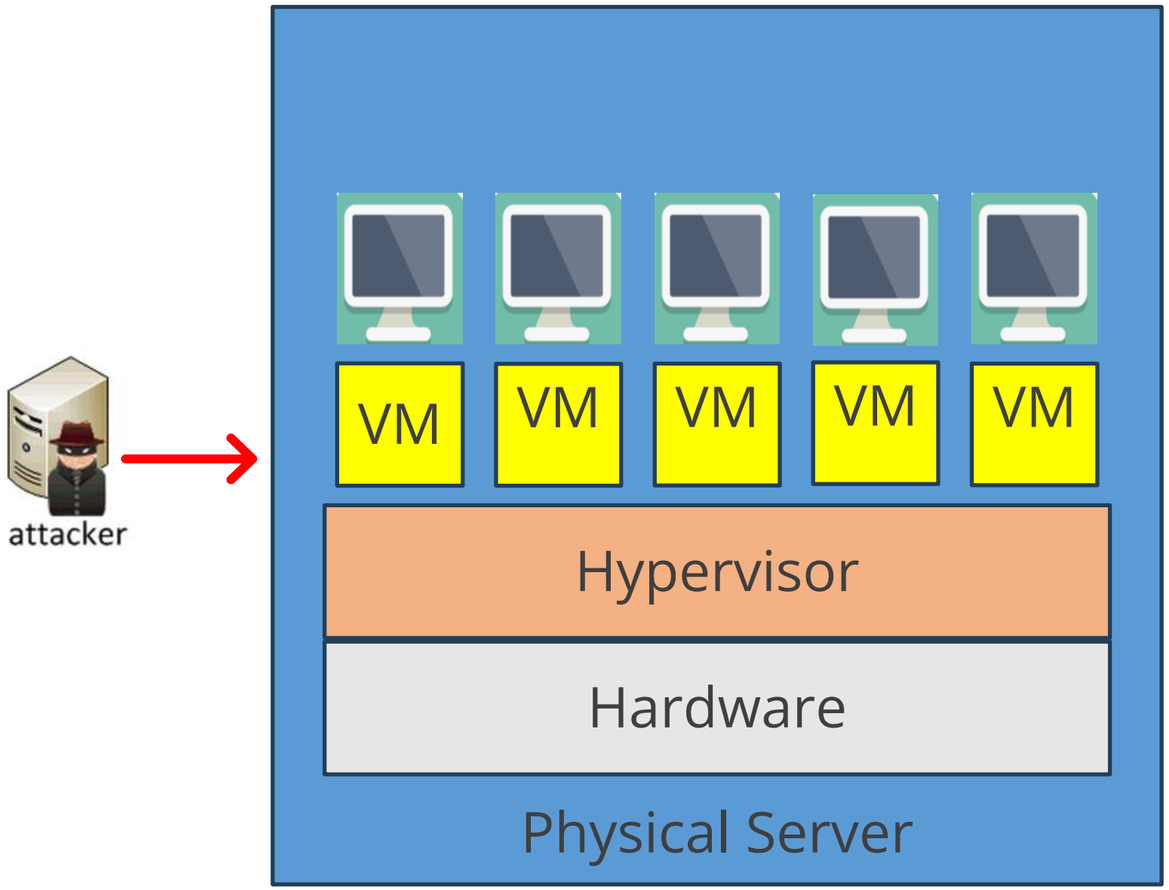
VM Attacks

- Cloud servers contain numerous VMs, which may be either active or offline, and regardless of their state, they are susceptible to attacks.
- Active VMs are vulnerable to all traditional attacks that can affect physical servers.
- An Offline VM is stored as a file and needs to be protected.
- Once a VM is compromised, VMs on the same physical server can attack each other because they share the same hardware and software resources, including memory, device drivers, storage, and hypervisor software.



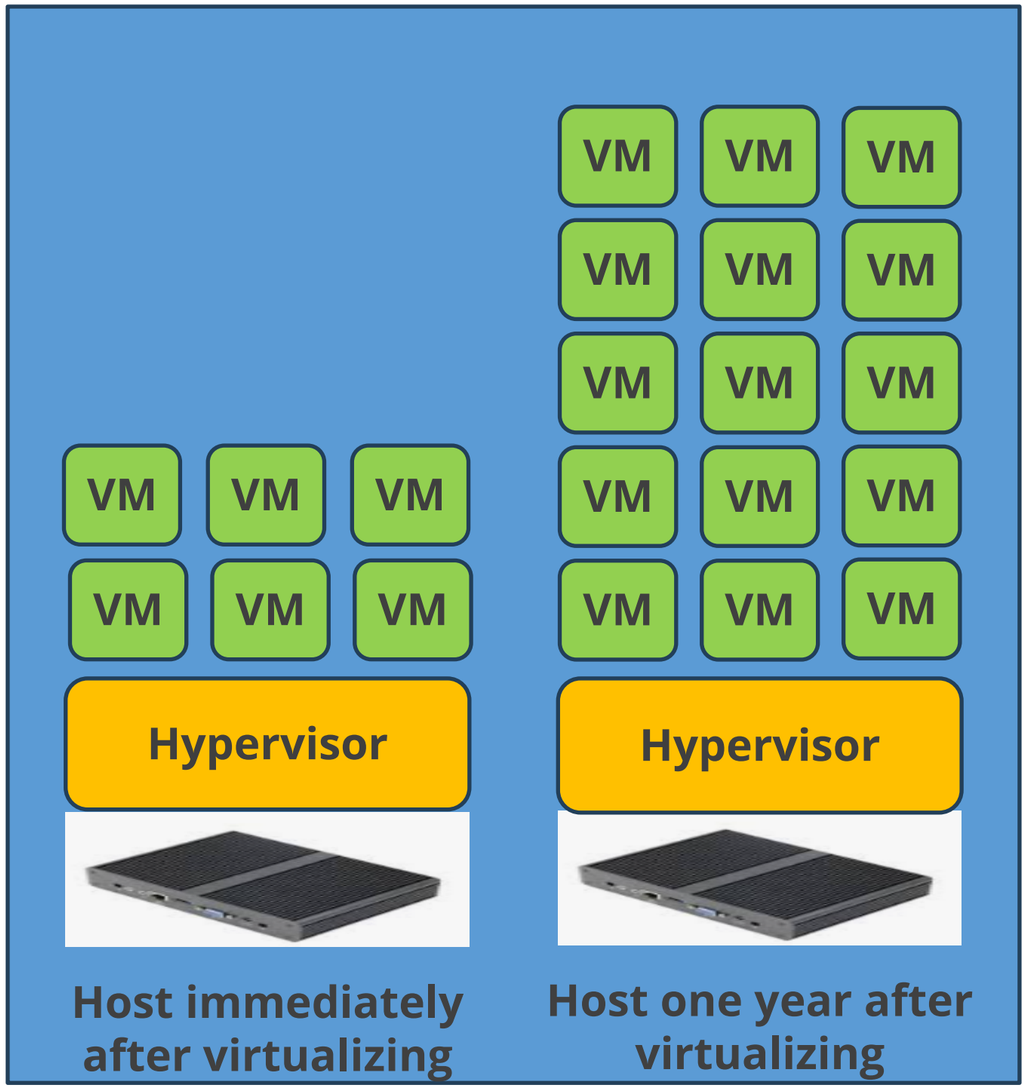
Hyperjacking

- Hyperjacking is an attack in which a hacker takes malicious control over the hypervisor, which creates the virtual environment within a virtual machine (VM) host.
- It involves installing a malicious, fake hypervisor that can manage the entire server system.
- Regular security measures are ineffective because the operating system will not know that the machine has been compromised.
- The hypervisor represents a single point of failure while securing and protecting sensitive information.
- While an actual hyperjacking incident has yet to be reported, it is hypothetically possible.



VM Sprawl

- Sprawl refers to the uncontrolled spreading and disorganization of resources, assets, or systems due to the absence of an organizational structure when numerous similar elements need to be managed.
- VM sprawl, also known as virtualization sprawl, happens when an administrator can no longer effectively control and manage all the virtual machines on a network.
- VMs are essentially files that contain a copy of a working machine's disk and memory structures, and management is easy when the numbers are small.
- However, as the number of VMs rapidly grows over time, sprawl can become an issue. VM sprawl is a symptom of a disorganized structure.



Resource Usage

- Resource sharing is a key advantage of virtualization, but improper allocation and management can lead to performance issues and resource contention.
- If resources aren't sanitized before reuse, sensitive data may be compromised.
- Excessive resource consumption by one VM can impact the performance of others on the same host, leading to resource exhaustion.

What Is Cloud?

- The cloud refers to a network of servers around the world. These servers store data, run applications, and deliver services like webmail, video streaming, and social media.
- Instead of having your own physical computer to store files or run programs, you can access them through the internet from any device.

Cloud Vulnerabilities

- Cloud vulnerabilities are security weaknesses or gaps within a cloud computing environment that malicious actors can exploit.
- These weaknesses can be found in various cloud components, and a few of them will be mentioned in the next slide.

Cloud Vulnerabilities

Risk of shared tenancy

In a public cloud, multiple tenants share the same environment. Without proper isolation, this can result in data breaches and unauthorized access.

Inadequate configuration management

In cloud services, poorly managed intricate settings, configurations, and permissions can expose resources or facilitate infiltration.

Identity and access management flaws

In cloud environments, compromised credentials, weak authentication, and user permissions can lead to unauthorized access and compromised accounts.

Insecure interfaces and APIs

In cloud services, APIs (Application Programming Interfaces) are vital for interaction. However, insecure APIs can be exploited by attackers.

Supply Chain Risk

The supply chain is the network of individuals, organizations, resources, activities, and technologies involved in creating and delivering a product from suppliers to end users.

Supply chain risk management (SCRM) is the process of identifying, monitoring, detecting, and mitigating threats to supply chain continuity and profitability.

A supply chain compromise is an incident within the supply chain where an adversary jeopardizes the confidentiality, integrity, or availability of a system or the information it processes, stores, or transmits.

This compromise can happen at any point within the system development life cycle of the product or service.

Supply Chain Vulnerabilities

Service provider vulnerabilities

Businesses outsourcing functions increase reliance on external entities, leading to security breaches and service interruptions if third-party relationships are poorly managed.

Hardware provider vulnerabilities

Counterfeit hardware or compromised components can enter the supply chain, posing potential threats to system integrity, resilience, and data confidentiality.

Software provider vulnerabilities

Software provider vulnerabilities are weaknesses or flaws in software applications exploited by malicious actors to gain unauthorized access or control over a system, having severe consequences for both the software provider and their users.

Risks Associated with Hardware, Software, and Services

Here are a few risks associated with hardware, software, and services:

Counterfeit hardware or hardware with embedded malware

Poor information security practices by lower-tier suppliers

Software security vulnerabilities in supply chain management or supplier systems

Compromised software or hardware purchased from suppliers

Cryptographic Vulnerability

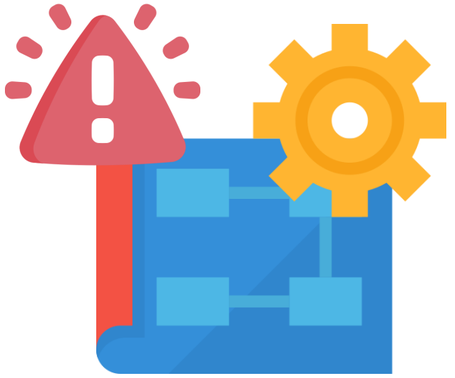
- A cryptographic vulnerability is a weakness in the systems and processes used to secure information.
- Cryptographic vulnerabilities, specifically weaknesses within certificates and encryption, require thorough evaluation and scrutiny.
- These vulnerabilities can expose sensitive data or allow attackers to bypass security measures.

Cryptography Vulnerabilities

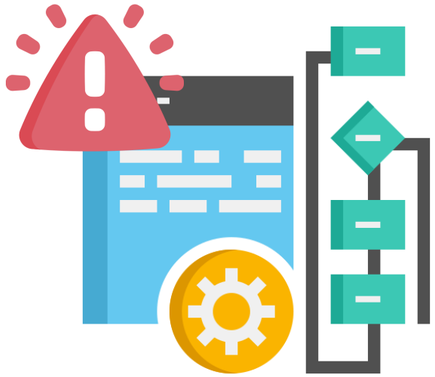
CA compromise

Key compromise

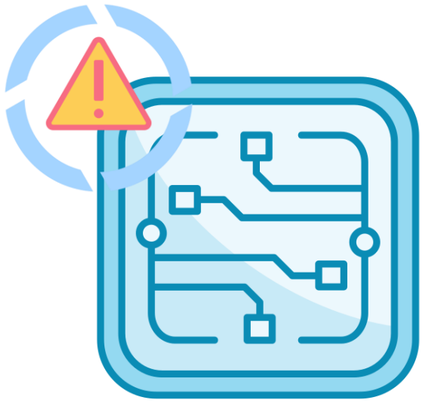
Flawed implementation



Outdated algorithm



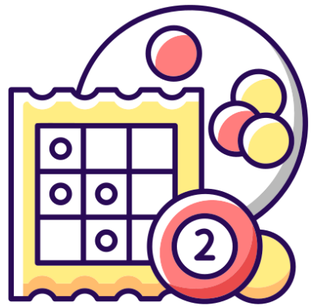
Side-channel attacks



Backdoor exploitation

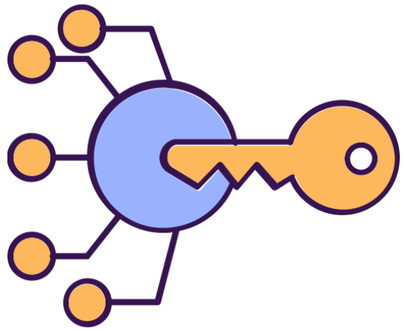
Cryptography Vulnerabilities

Random number generation



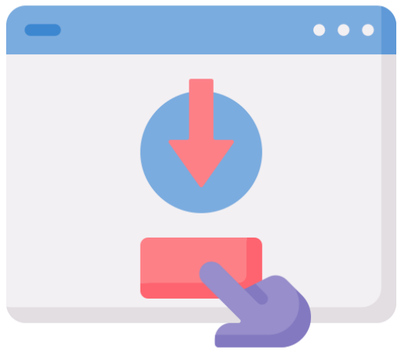
Certification revocation lists/online certificate status protocol

Secure key management



SSL striping

SSL/TLS downgrade



Ransomware

Cryptographic Vulnerabilities

Certificate Authority (CA) compromise

- Certificate Authorities (CAs) issue digital certificates on which the digital world relies.
- If a CA is compromised, attackers can generate fraudulent certificates, leading to the interception of encrypted communications and potentially causing widespread breaches.

Key compromise

- The strength of cryptographic systems is entirely dependent on the strength of their keys.
- Keys can be compromised due to theft, weak generation, or poor key management, which can lead to unauthorized data access, manipulation, or decryption.

Flawed implementation

- Flawed cryptographic implementations can lead to the failure of even robust processes.
- Poorly coded encryption routines and weak key management can create openings that adversaries can exploit.

Cryptographic Vulnerabilities

Outdated algorithm

- Cryptographic algorithms that were once secure may become vulnerable to emerging attack techniques or increased computational power.
- Outdated algorithms may expose data to potential breaches.

Side-channel attacks

- Cryptographic operations can inadvertently leak information through side channels such as power consumption, timing, or electromagnetic radiation.
- Attackers skilled in exploiting these side channels can compromise encryption keys or data.

Backdoor implementations

- Deliberate or unintentional backdoors within cryptographic systems can provide attackers with unauthorized access, effectively rendering the encryption useless.

Cryptographic Vulnerabilities

Random generations

- Secure encryption relies on truly random numbers to generate cryptographic keys.
- Flawed or predictable random number generation leads to weak keys and compromised security.

Certification revocations lists/OCSP

- Compromised certificates are annulled, and any keys listed on the CRL are unequivocally invalidated to prevent unauthorized utilization.
- These measures are vital tools for maintaining the integrity of the trust infrastructure.

Secure key management

- Secure key management requires strict policies to ensure keys are generated securely, stored safely, and rotated regularly.
- Weak key management provides a common vector for attacks.
- Effective key management involves securely storing keys in HSM or key escrow services.

Cryptographic Vulnerabilities

SSL striping	SSL stripping is an attack where attackers conduct an SSL downgrade attack, bypassing certificate-based protection and converting a secure session into an HTTP session.
SSL/TLS downgrade	An SSL/TLS downgrade attack manipulates a web browser and server into negotiating a weaker version of the protocol or a less secure cipher suite (a set of encryption algorithms) than they normally would.
Insecure communication channel	If data is either transmitted unencrypted over a network or encrypted at rest, it can be intercepted by attackers.

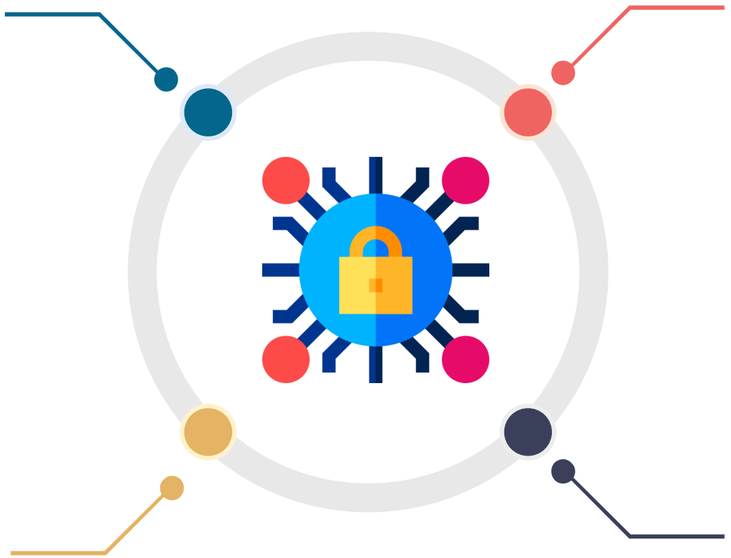
Causes of Cryptography

Uses outdated cryptography

As newer, stronger algorithms emerge, outdated algorithms leave data vulnerable.

Generates insufficient randomness

Cryptographic systems rely on high entropy and unpredictable random number generation for secure key creation.



Implements weak custom cryptography

Non-established, non-vetted cryptographic libraries and protocols are unsafe.

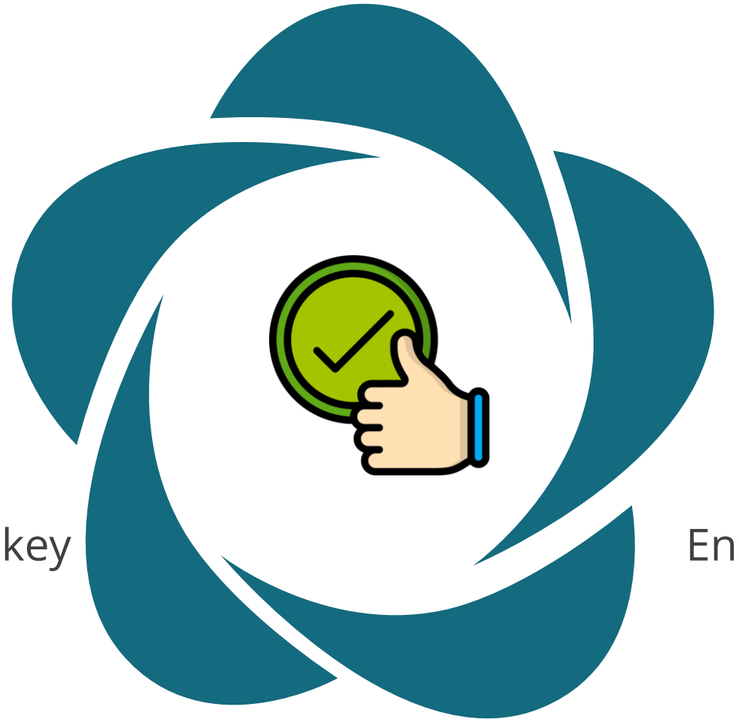
Encounters physical security violations

If attackers gain physical access to devices storing cryptographic keys, they can steal the keys and decrypt protected data.

Best Practices for Protection against Cryptography

Stay up-to-date

Leverage strong algorithm



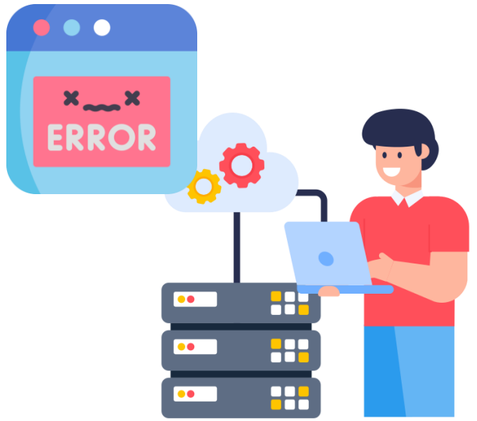
Prioritize physical security

Implement secure key management

Encrypt data in transit and at rest

Misconfiguration Vulnerability

- Misconfiguration vulnerabilities are security weaknesses arising from improper settings or errors in configuring computer systems, applications, or cloud services.
- These vulnerabilities can be exploited by attackers to gain unauthorized access to data, systems, or functionality.



Causes of Misconfiguration

Human error

Simple mistakes during system setup, configuration changes, or applying security patches can introduce vulnerabilities.

Complexity

Modern systems have numerous configuration options, making it challenging to ensure that everything is securely set.

Default setting

Many systems come with default configurations that prioritize ease of use over security. These defaults often need to be changed to enhance security.

Lack of awareness

Sometimes, system administrators or users might not be fully aware of the security implications of specific configuration settings.

Types of Misconfiguration Vulnerabilities

Unnecessary accounts and privileges: Leaving unused accounts active or assigning excessive privileges to users can create security risks.

Weak passwords: Using default or easily guessable passwords for accounts or systems makes them vulnerable to brute-force attacks.

Insecure remote access: Enabling remote access features without proper security measures, such as strong passwords or two-factor authentication, creates vulnerabilities.

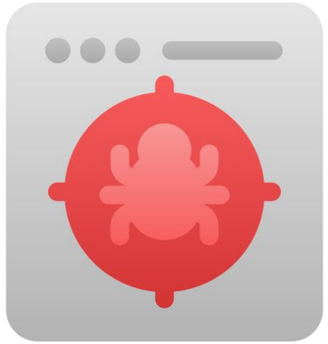
Unpatched software: Running outdated software with known vulnerabilities can lead to exploitation if not patched promptly.

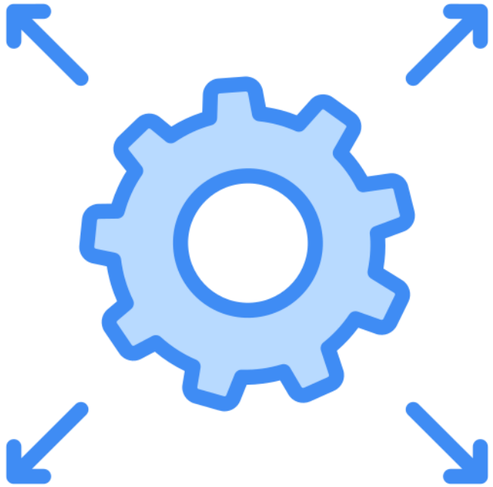
Open ports and services: Keeping unnecessary ports or services running on a system can provide entry points for attackers.

Impact of Misconfiguration Vulnerability

Data breaches

Malware infection





System outages

Compliance violation

Prevention of Misconfiguration Vulnerabilities

Standardization: Implementing standardized configurations to ensure consistency and reduce the risk of errors

Automation: Automating configuration tasks whenever possible to minimize human error

Configuration management tools: Using configuration management tools to track and enforce secure configurations across systems

Prevention of Misconfiguration Vulnerabilities

Security best practices: Adhering to security best practices for system configuration, password management, and access controls

Regular security audits: Conducting regular security audits to identify and address misconfiguration vulnerabilities

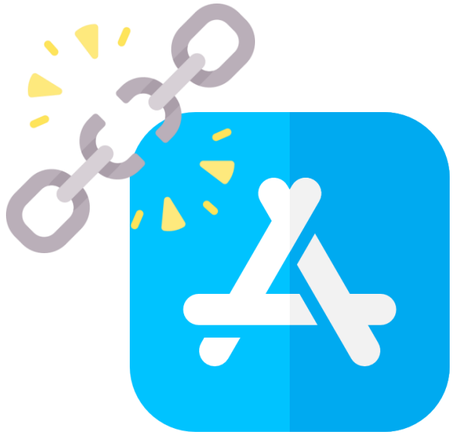
Security awareness training: Training system administrators and users about secure configuration practices

Mobile Device Vulnerability

- Mobile devices are essential parts of our lives, but they also carry a lot of sensitive information.
- They seamlessly integrate into our modern lives, serving as channels for communication, information, and entertainment.
- They have vulnerabilities that encompass security weaknesses within smartphones, tablets, and other portable devices.
- These vulnerabilities may include insecure data storage, weak authentication mechanisms, or outdated operating systems.

Mobile Vulnerabilities

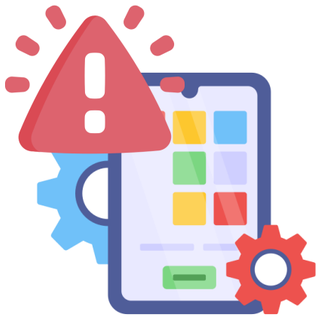
Jailbreaking



Rooting

Sideloading

Counterfeits apps



OS vulnerabilities

Device vulnerabilities

Mobile Vulnerabilities

Jailbreaking

Jailbreaking applies specifically to Apple devices and allows users to bypass manufacturer or operating system restrictions, providing more control over the device.

Rooting

Rooting allows users to bypass manufacturer or operating system restrictions on Android devices, providing more control over the device.

Sideloading

Sideloading refers to installing applications on a mobile device from sources outside the official app store. It can introduce vulnerabilities, as these applications may contain malicious code or bypass security controls.

Mobile Vulnerabilities

Counterfeit apps

Unregulated stores can host third-party counterfeit or modified versions of legitimate apps carrying hidden malware.

OS vulnerability

Software vulnerabilities are flaws in the core software that powers a mobile device, such as Android or iOS, which attackers can exploit to gain root access and complete control over the system.

Device vulnerabilities

Hardware vulnerabilities are physical weaknesses in a mobile device itself, such as flaws in the hardware or a poorly secured boot process, which attackers can exploit to install malware or steal data directly from the device's memory.

Zero-Day Attacks

- A zero-day attack is a cyberattack that exploits a recently discovered software vulnerability that the software vendor or developer is unaware of.
- Imagine a hole in a wall that no one knows exists; that's what a zero-day vulnerability is like for a computer system.
- **Zero:** This highlights the fact that software developers have no time to address the issue because attackers have already found it.
- **Day:** This refers to the day the vulnerability is discovered.

Best Practices for Protection against Zero Day Attack

Keep software updated

Be cautious with links and attachments

Use security software

Use strong password

Stay informed

Indicators, Indicators of Compromise, and Indicators of Attack

Indicators

- Signs of possible malicious actions within a system or network indicate that an issue may exist.
- Behaviors, patterns, or anomalies indicate unauthorized access, malware infection, or other cyber threats.
- Observation and analysis of these indicators are essential for security, allowing early detection and response to threats and developing effective defense mechanisms.

Examples of Indicators

Account lockout

Account lockouts can be early warnings of unauthorized access attempts, especially for privileged accounts.

Concurrent usage

Concurrent user sessions showing sudden increases may indicate unauthorized access or a breach.

Impossible travel

Impossible travel with multiple logins from geographically distant locations in an unrealistically short timeframe may indicate a potential account compromise.

Resource consumption

Unusual spikes in resource consumption, such as excessive CPU or memory usage, may indicate a malware infection or a DDoS attack on your systems.

Resource inaccessibility

Sudden inaccessibility of critical resources may indicate a cyberattack, such as a DDoS attack.

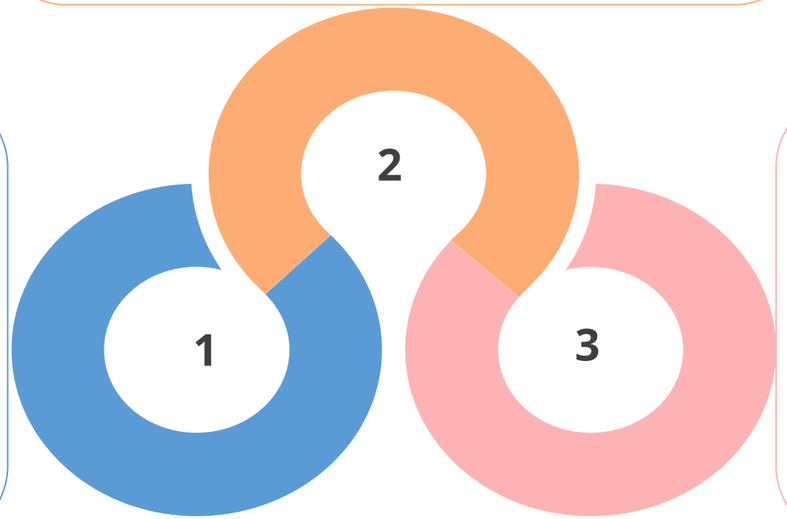
Out-of-cycle logging

Irregular log generation times may indicate suspicious activities and warrant investigation.

Indicators of Compromise

Indicators of Compromise (IoCs) serve as evidence of a cyberattack, indicating that a system is being compromised by unauthorized activity.

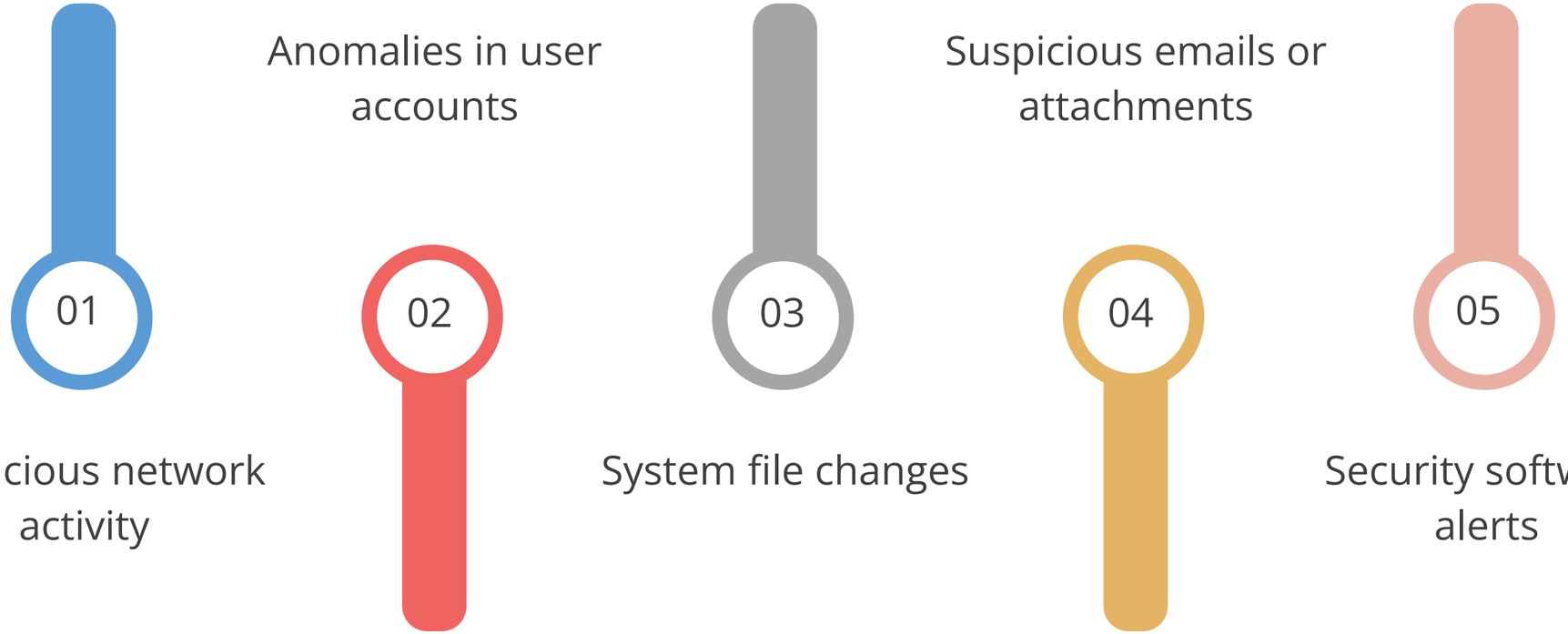
Artifacts detected on a network or within an operating system serve as strong indicators of a computer intrusion.



Modern antimalware systems use known indicators of compromise to detect threats early, proactively preventing and protecting data and IT systems.

Indicators of Compromise

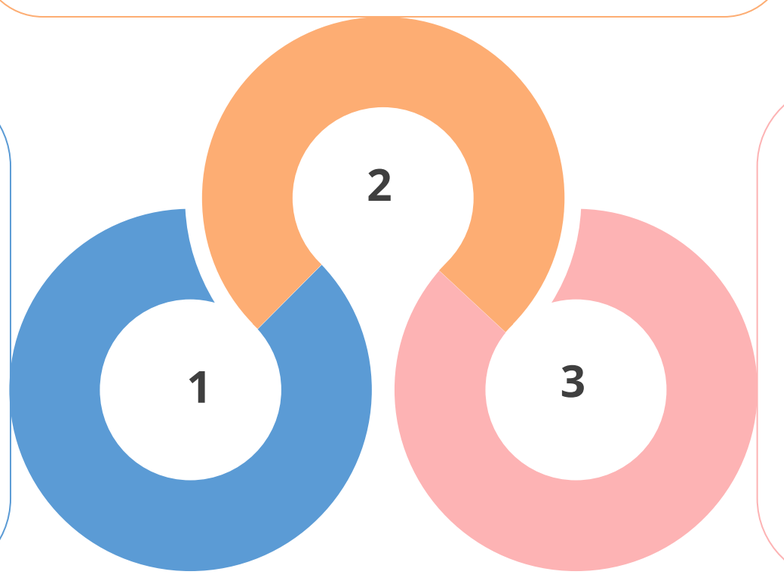
Rundown of some IoCs:



Indicators of Attacks

Indicate potential ongoing attacks or high risks of attacks by resembling suspicious behavior and being more dynamic in nature

Provide early warnings of potential threats by identifying suspicious activities or behaviors within a network, helping organizations proactively defend against cyberattacks



Identify signs and behaviors suggesting an ongoing or imminent cyberattack, unlike Indicators of Compromise (IoCs) that focus on evidence of a successful attack

Indicators of Attacks

Rundown of some IoAs:

01

Unusual login attempts

02

Escalation of user privileges

03

Abnormal data transfer patterns

04

Modification of critical system files

05

Traffics originating from high-risk location

IOC vs IOA

	Feature	Indicator of compromise	Indicator of attack
1	Focus	Evidence of past compromise	Signs of ongoing attack
2	Nature	Specific, static digital evidence	Broader, dynamic patterns of activity
3	Detection	Identify already compromised systems	Proactively identify potential attacks
4	Example	Known malware signature	Unusual login attempts

Investigating DoS and MITM Attacks Using Wireshark

Duration: 10 Min.

Problem Statement:

As a Network Security Analyst, you are tasked with investigating potential Denial of Service (DoS) and Man-in-the-Middle (MITM) attacks. Using Wireshark, you need to filter and analyze network traffic to identify anomalies such as excessive packet counts, IP duplication, and irregular ARP entries. This investigation aims to detect and mitigate security threats to maintain network integrity and protect against malicious activities.

Note: Refer to the demo document for detailed steps:
02_Investigating_DoS_and_MITM_attacks_using_Wireshark

ASSISTED PRACTICE

Assisted Practice: Guidelines

Steps to be followed are:

1. Analyze the MITM.pcapng file
2. Analyze the NmapScanANDDoS.pcapng file
3. Mitigate MITM and DoS attacks

TECHNOLOGY

Malware Attacks

Malware

Malware, or malicious software, encompasses various harmful programs intentionally designed to execute unauthorized actions on a target system.

It includes software that disrupts or damages computers and networks.

It executes malicious actions to fulfill an attacker's goals, like data theft or system sabotage.

Impacts of Malware

Malware can have various detrimental effects on systems, including:

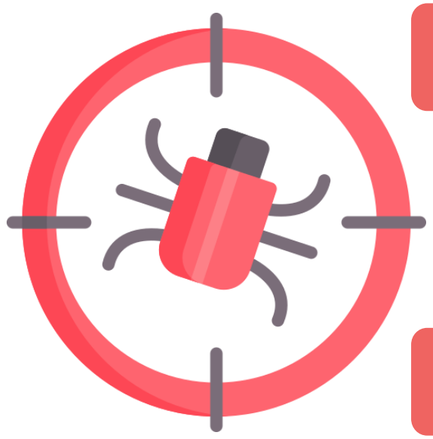
01 Stealing personal information

02 Deleting files

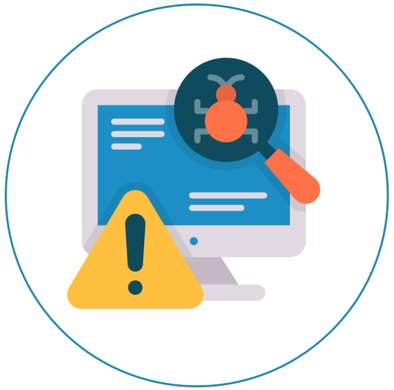
03 Conducting click fraud

04 Stealing software serial numbers

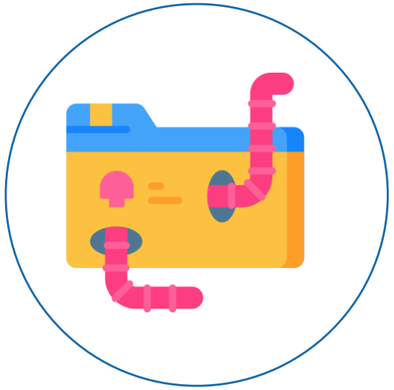
05 Using your computer as a relay



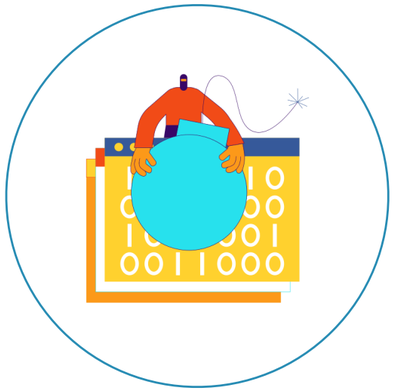
Types of Malware



Virus

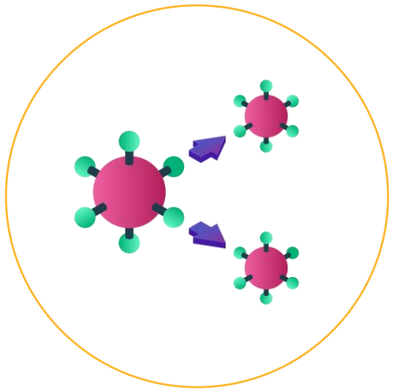


Worms



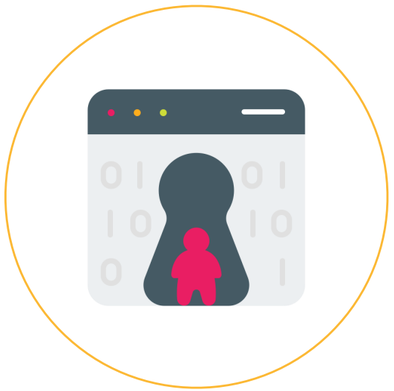
Logic bombs

Spyware



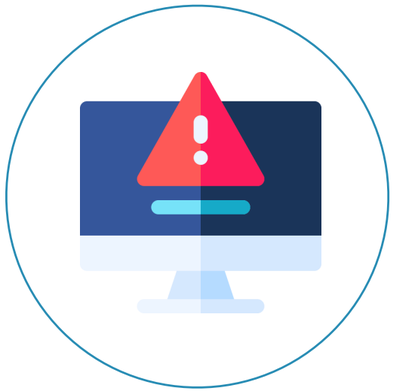
Polymorphic virus

Trojan horse



Backdoor

Types of Malware



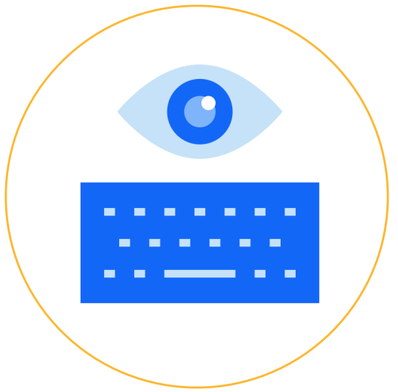
Potentially unwanted programs

Ransomware

Adware

Bloatware

Rootkits

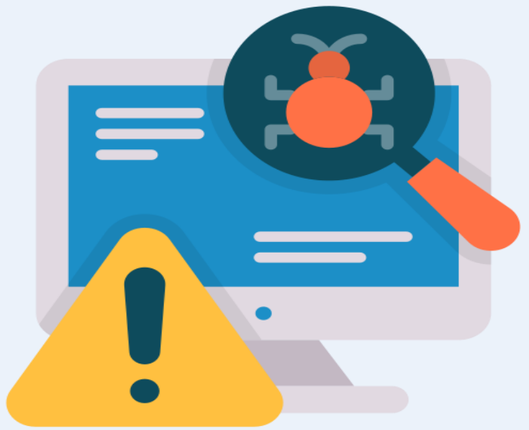


Keyloggers

Virus

A virus is malicious code that replicates by attaching itself to another piece of executable code.

- It executes when the host code runs, infecting other files and performing harmful actions.
- It can significantly slow down or crash your system, potentially leading to data loss.



Worms

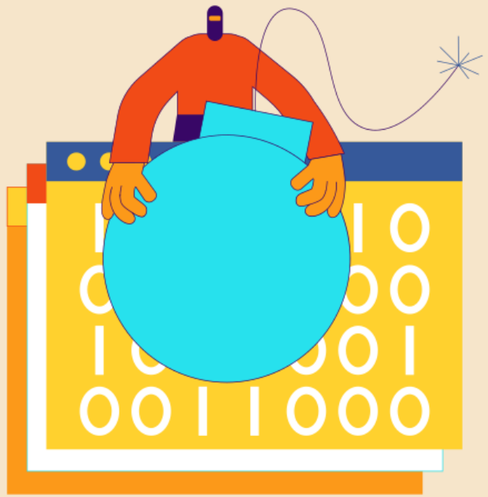
Worms are self-replicating pieces of code designed to penetrate networks and computer systems.

- They replicate and spread independently, similar to biological organisms.
- They exploit vulnerabilities to move through networks, consuming bandwidth and rapidly infecting new hosts.

Logic Bombs

Logic bombs are malicious code objects that infect a system and lie dormant until triggered by specific conditions, such as:

- A specific time
- A program launch
- A website login
- Other predefined events



Trojan Horse

A Trojan horse is a type of malicious software that disguises itself as legitimate software to trick users.

- Trojans appear to perform a useful function but secretly execute malicious actions.
- They are standalone programs that need to be installed by the user, often through deception.
- They are designed to trick users into downloading or executing harmful software by mimicking legitimate files or programs.

Remote Access Trojans

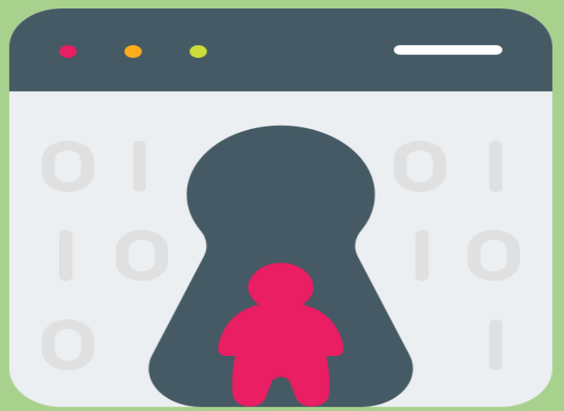
Remote Access Trojans (RATs) are modern-day versions of Trojan horses in the cyber realm.

- They are stealthy infiltrators concealed within legitimate files, granting cybercriminals remote control over compromised systems.
- They allow command and control of the computer, enabling remote access for malicious activities such as data theft or malware installation.

Backdoor

Backdoor programs allow attackers to maintain access to a system after unauthorized entry. These programs:

- Ensure unrestricted access even if the initial entry method is blocked
- Allow installation inadvertently by authorized users via Trojan horses



Spyware

Spyware is malicious software that secretly gathers your personal information and activities.

- Installs itself without your knowledge or consent
- Transmits stolen data to a third party, posing a significant threat to privacy and security

Ransomware

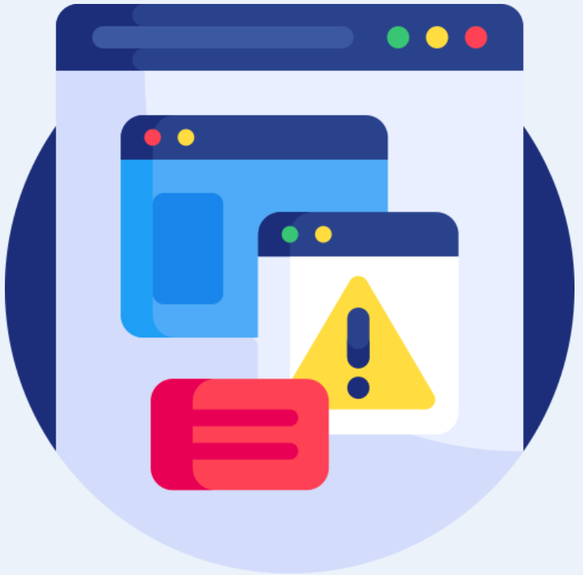
Ransomware is a type of malicious software designed to extort money by encrypting the victim’s files, making them inaccessible until a ransom is paid.

- It infects systems by taking control of the victim's machine, including files and documents.
- It is typically installed through malicious email attachments, links in instant messages, or visits to compromised websites.

Adware

Adware is a type of malware that displays unwanted ads and pop-ups. These programs:

- Bombard you with endless ads and pop-up windows, potentially dangerous to your device
- Often gather personal information, though most adware is considered safe



Bloatware

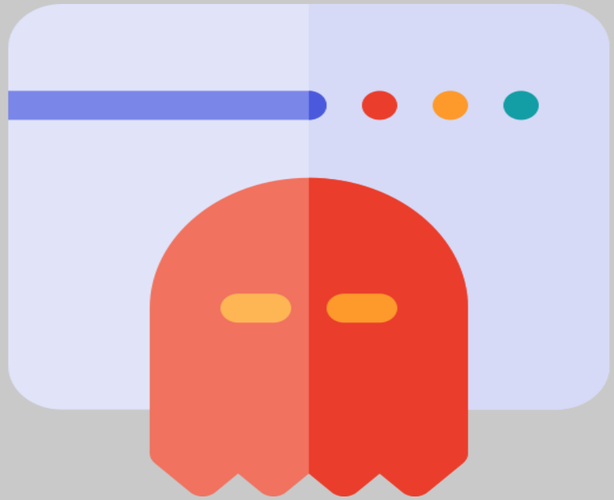
Bloatware is unwanted software pre-installed on new devices.

- It hogs storage space and slows down your device.
- Examples: Trial versions of software, manufacturer-branded apps, promotional software, and unnecessary background programs

Rootkits

Rootkits are a very stealthy type of malware designed to provide attackers with unauthorized, privileged access to a computer system. These programs:

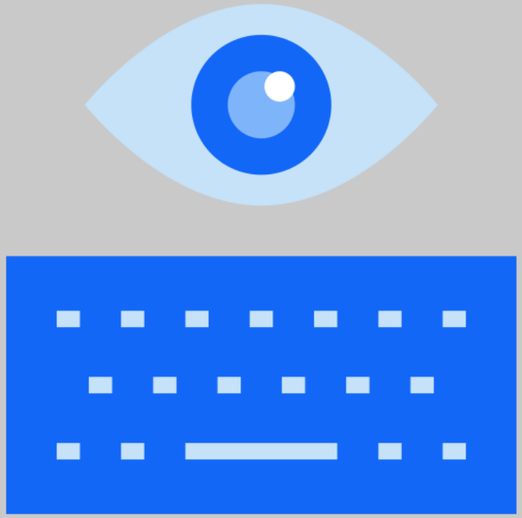
- Dig deep into the system, usually at the root level, hiding their presence while giving attackers full control over the infected device
- Alter the operation of the operating system to enable nonstandard functionality



Keylogger

A keylogger is a type of malware designed to covertly record everything you type on your keyboard. These programs:

- Act like digital eavesdroppers, capturing keystrokes including passwords, credit card numbers, and messages
- Transmit stolen information to attackers, posing a significant threat to privacy and security



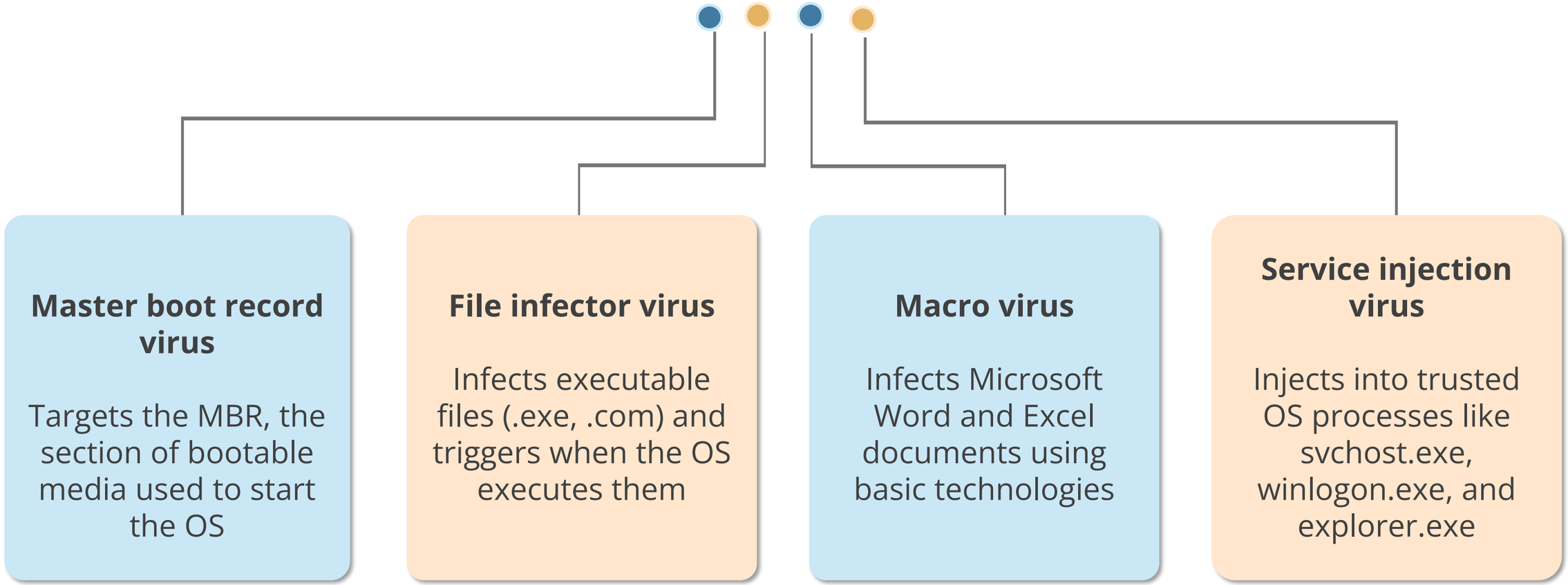
Potentially Unwanted Programs

Potentially Unwanted Programs (PUPs), also known as Potentially Unwanted Applications (PUAs), are software that may install themselves without clear consent and can affect device performance.

- Often bundled with other software, when installed without the user's full knowledge or explicit consent
- Tends to overconsume resources, slowing down the computer system
- Considered grayware due to its ambiguous nature: not fully malicious but still unwanted

Virus Propagation Techniques

Viruses use various methods to spread and infect systems. These include:



Virus Technologies

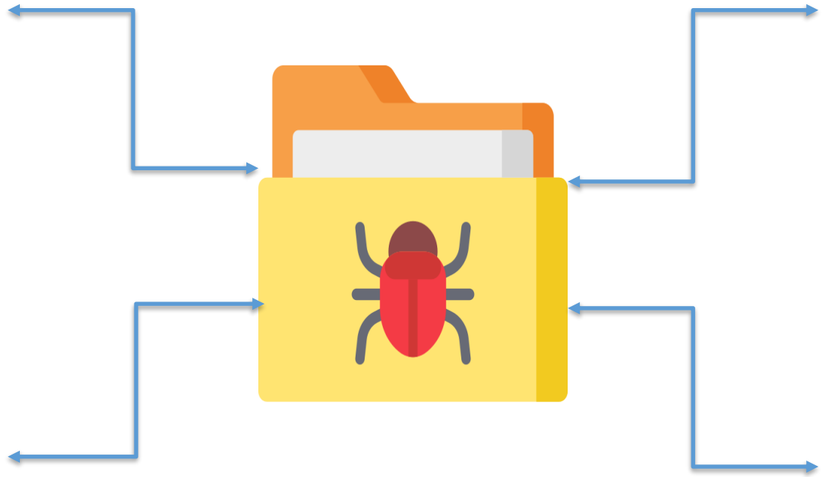
Viruses employ various techniques to evade detection and propagate within systems. These include:

Multipartite viruses

Use multiple propagation techniques to penetrate systems

Stealth viruses

Hide by tampering with the OS to avoid detection



Polymorphic viruses

Modify their code as they travel from system to system

Encrypted viruses

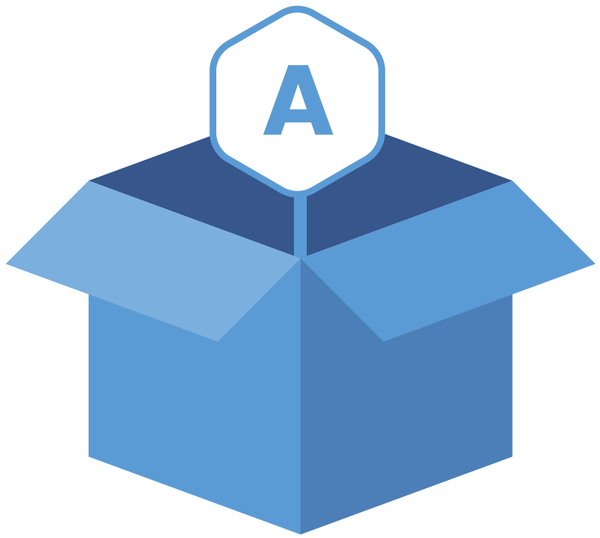
Use cryptographic techniques to avoid detection

Preventive Measures for Malware Control

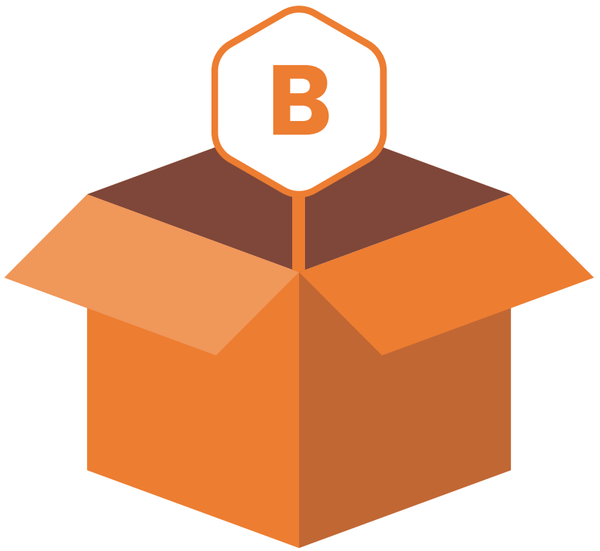
A few preventive measures to protect your system from malware are as follows:

Detective Measures for Malware Control

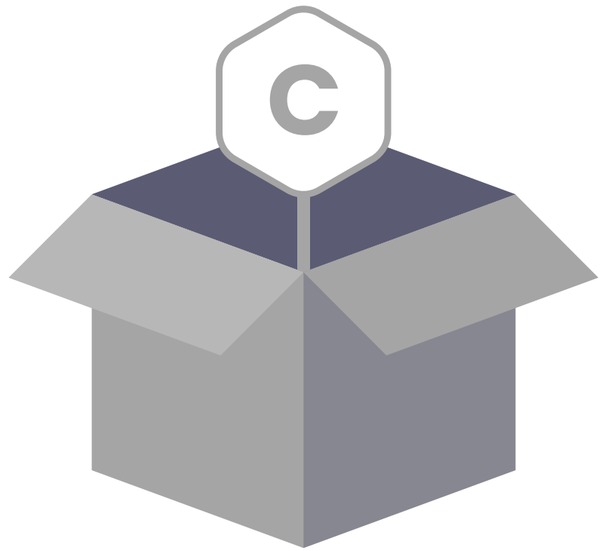
Detective measures are essential to identify and mitigate malware threats. These include:



Regular malware scans



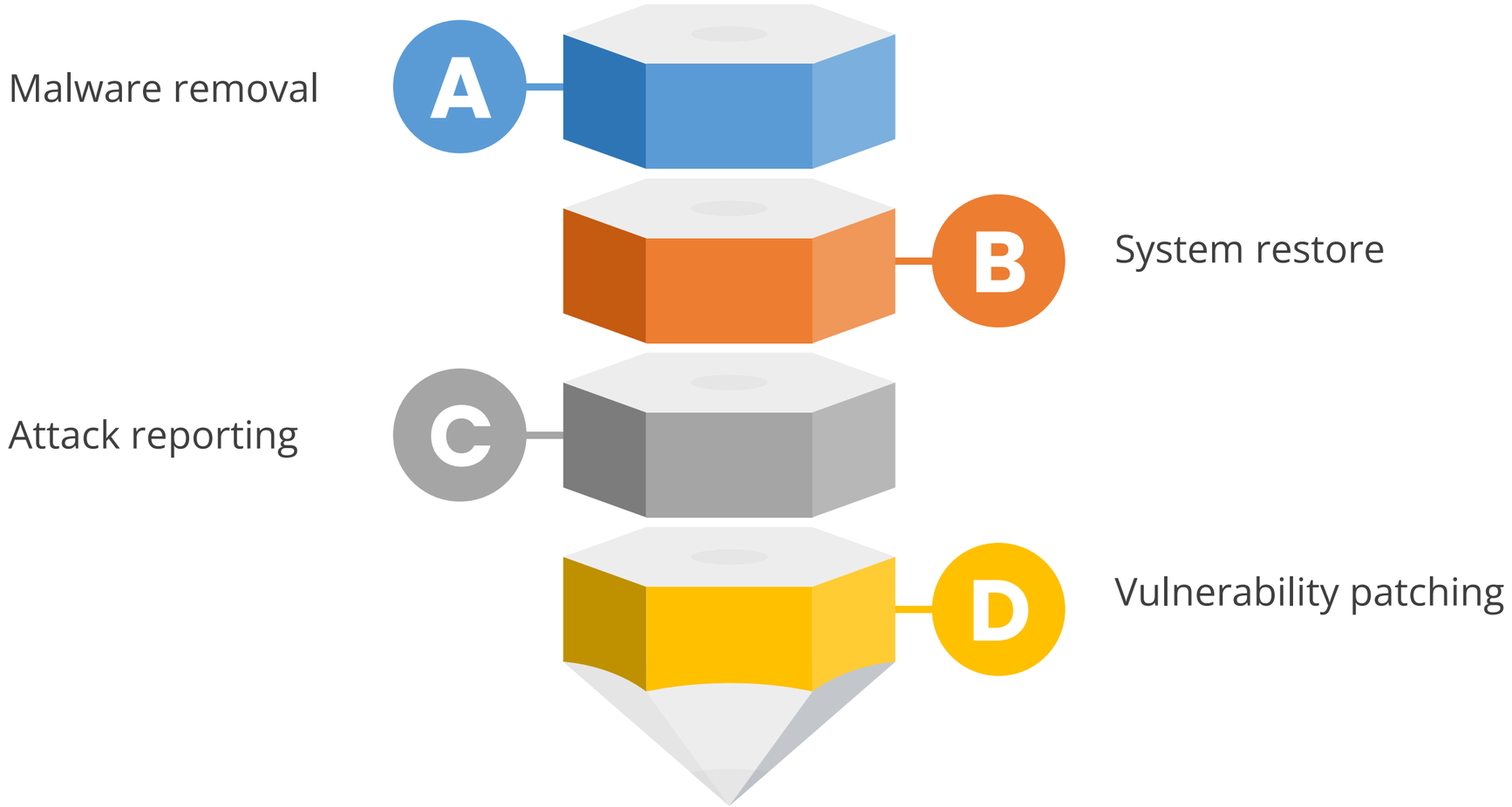
System monitoring



Security software alerts

Corrective Measures for Malware Control

Corrective measures help mitigate the impact of malware after detection. These include:



Malware: Technical Controls

Antivirus and antimalware software

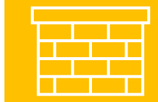
Scans for malicious software, identifies threats, and removes or blocks them

Endpoint detection and response

Provides continuous monitoring and analysis to detect suspicious behaviors

Application whitelisting

Restricts the system to run only authorized applications



Firewalls

Filters network traffic to block malicious patterns

Email security solutions

Filters incoming emails, blocking phishing and other email-borne threats

Data loss prevention

Prevents malware from exfiltrating sensitive data

Malware: Technical Controls

Security information and event management

Collects and analyzes security logs to identify potential threats

Network segmentation

Divides the network into segments to contain malware spread

Operating system and application hardening

Configures the system with security best practices, disabling exploitable features

Analyzing Malware Reports Using VirusTotal

Duration: 10 Min.

Problem Statement:

As a cybersecurity analyst, you are tasked with conducting a comprehensive malware analysis. This involves using VirusTotal to examine file hashes, gather IP information, and utilize graph visualization tools. The goal is to understand the malware's behavior and its network relationships, thereby identifying potential threats and mitigating the risk of infection and spread within the network.

Note: Refer to the demo document for detailed steps:
03_Analyzing_Malware_Reports_Using_VirusTotal

ASSISTED PRACTICE

Assisted Practice: Guidelines

Steps to be followed are:

1. Disable the Google Chrome security settings
2. Disable the Windows Defender
3. Download the malware
4. Download 7-zip
5. Perform VirusTotal analysis
6. Perform hash, IP information, and graph analysis

Physical Attack

Physical Attack

Physical infrastructure attacks are deliberate assaults on critical infrastructure, aiming to disrupt, damage, or destroy physical components.

- These attacks can have severe consequences, affecting essential services that communities rely on.
- These attacks involve using stealthy tactics to breach physical spaces.

Physical Attack

Brute-force physical attack

This is a method of trying many password combinations to gain unauthorized access to a system.

RFID cloning

RFID cloning is copying information from one chip onto another card, like making a fake key for a door that uses RFID cards instead of metal ones.

TECHNOLOGY

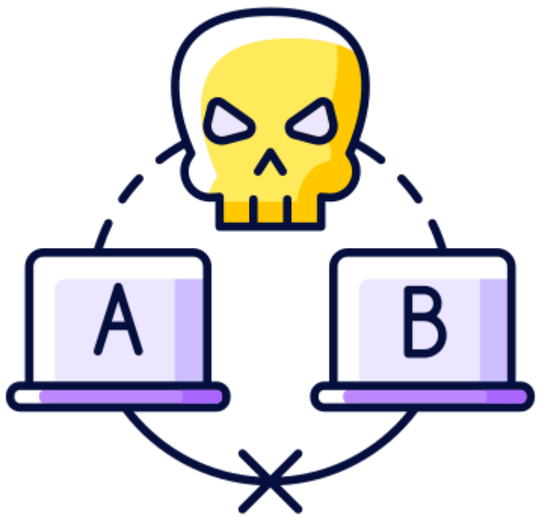
Network Attack

Network Attack

A network attack is an unauthorized and malicious attempt to disrupt, compromise, or gain access to computer systems, data, or communication within a network, often for malicious purposes.

Network attacks that target an organization’s servers, holding confidential information, are called server-side attacks.

Forms of Network Attacks

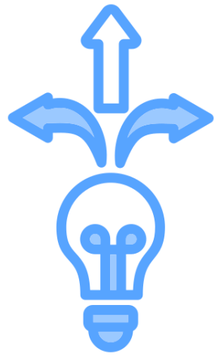


Passive attacks:
Involve monitoring network traffic to gather information without altering it

Active attacks:
Involve modifying network traffic or systems

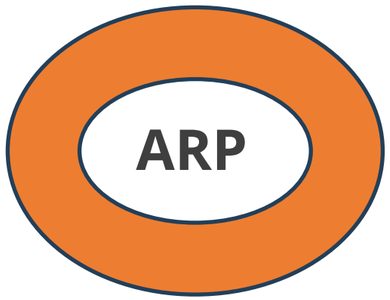
Types of Network Attacks

Pivoting attack

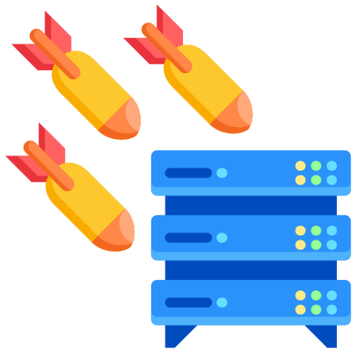


DoS or DDoS attack

ARP poisoning



Smurf attack



Pivoting

It refers to a technique used by attackers or ethical hackers during penetration testing to move laterally within a network.

Pivoting Attack

Using foothold

Once inside the initial system, the attacker leverages its resources to further their reach.

Gaining foothold

The attacker first needs to gain access to a single system within the network.

1

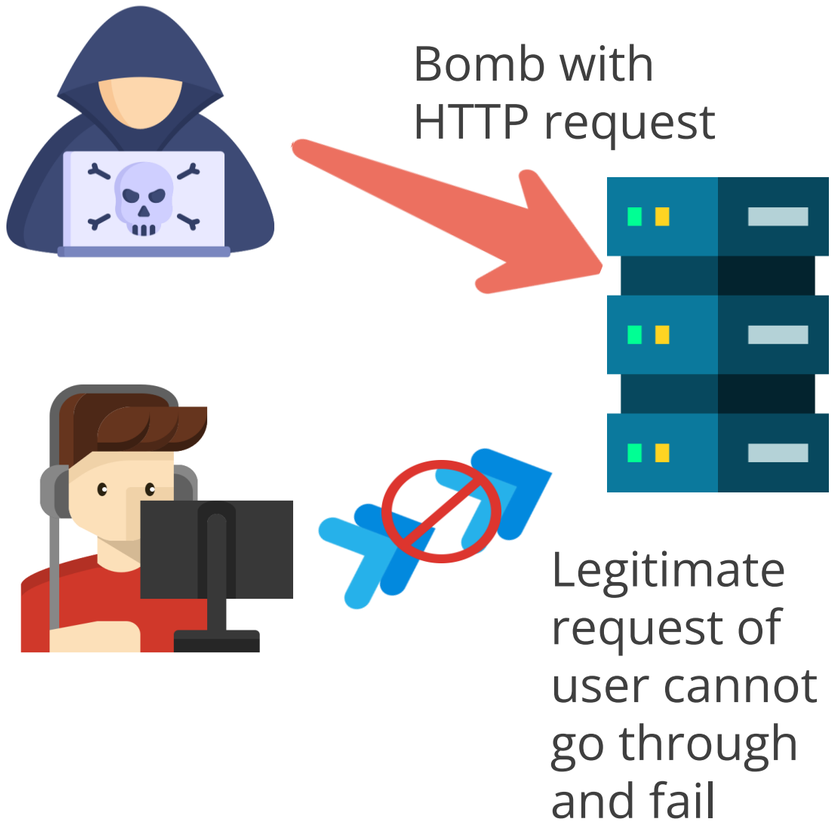
2

3

Moving laterally

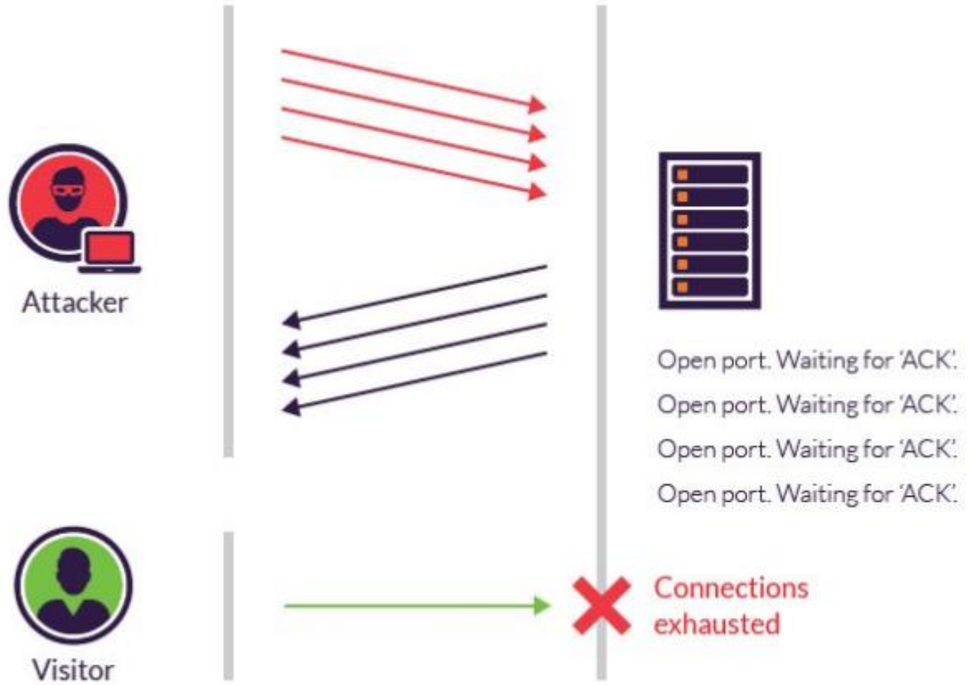
With the compromised system as a pivot point, the attacker can then launch attacks on other machines on the network.

Denial-of-Service Attack



- A denial-of-service attack (DoS attack) is a cyber attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the internet.
- This can be accomplished by crashing the system, taking it offline, or sending an overwhelming number of requests that the machine cannot process.

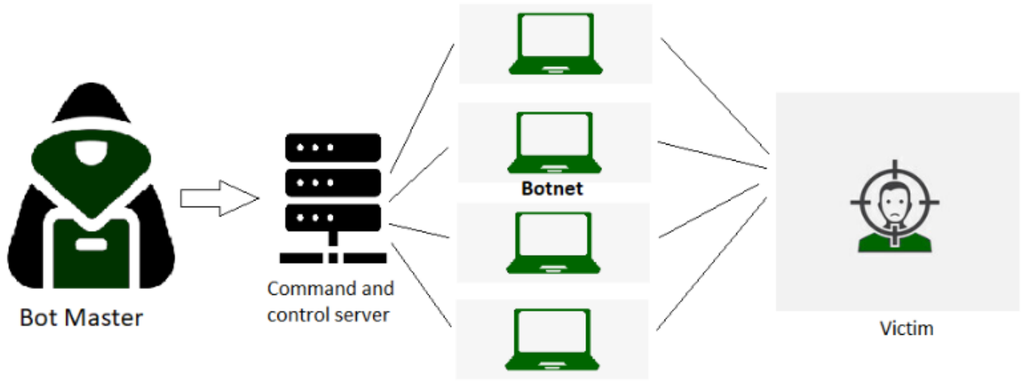
SYN Flood Attack



- A SYN flood (half-open attack) is a type of denial-of-service (DoS) attack that aims to make a server unavailable to legitimate traffic by consuming all available server resources.
- By repeatedly sending initial connection request (SYN) packets, the attacker can overwhelm all available ports on a targeted server machine, causing the targeted device to respond to legitimate traffic sluggishly or not at all.

Distributed Denial-of-Service Attack

In a typical DDoS attack, the hacker begins by exploiting a computer system and making it the DDoS master, which then identifies other vulnerable systems and gains control over them.



Their main aim is to prevent legitimate users from accessing a system or site.

Types of DDoS Attacks

Network or volume centric

These attacks use bots and botnets to flood the network layers with seemingly legitimate traffic, causing network operations to become extremely slow or to not work at all.

Application layer

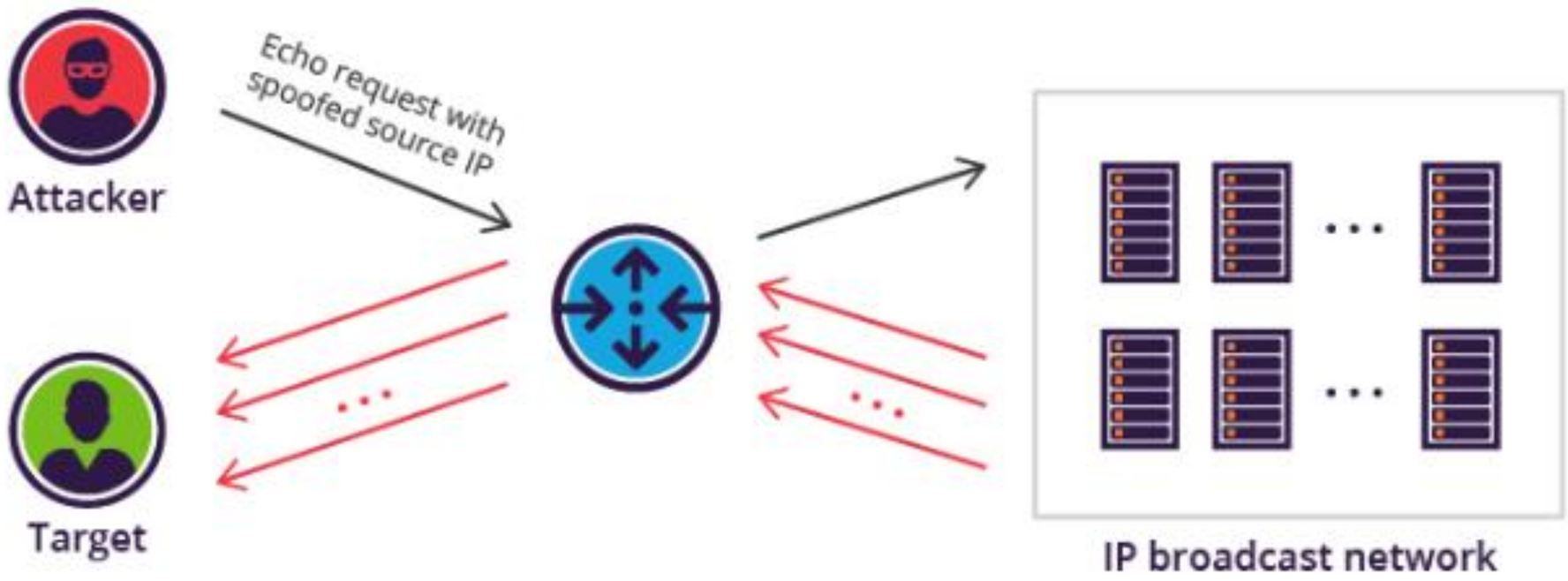
These attacks exhaust resources by consuming too much of the application's resources. They target the layer managing HTTP and SMTP communication.

DoS vs. DDoS Attack

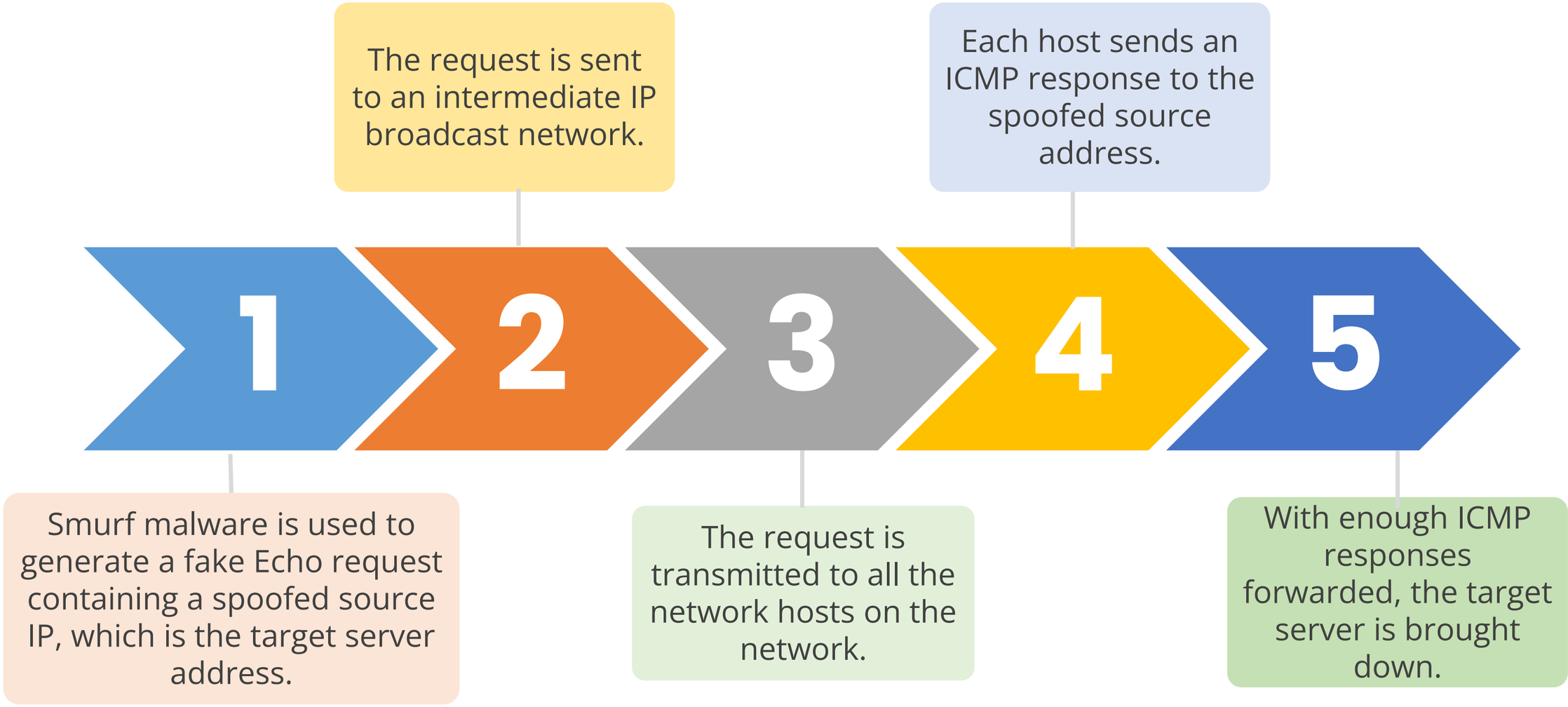
DoS attack	DDoS attack
A hacker uses a single internet connection to either exploit a software vulnerability or flood a target with fake requests.	A hacker launches attacks from multiple connected devices that are distributed across the internet.

Smurf Attack

It is a distributed denial-of-service (DDoS) attack in which an attacker attempts to flood a targeted server with Internet Control Message Protocol (ICMP) packets.

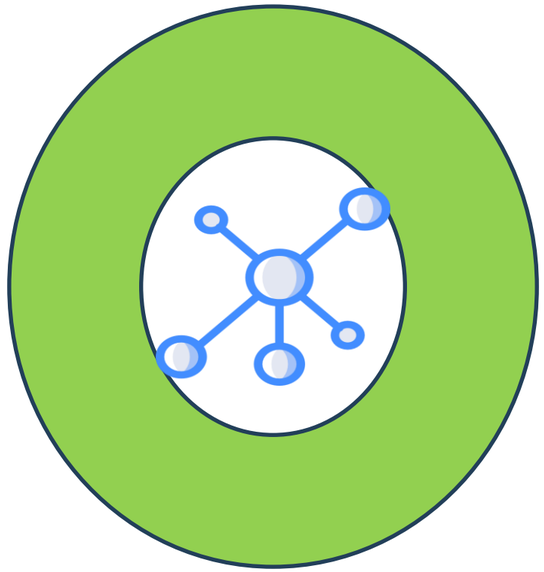


Smurf Attack Flow



What Is ARP?

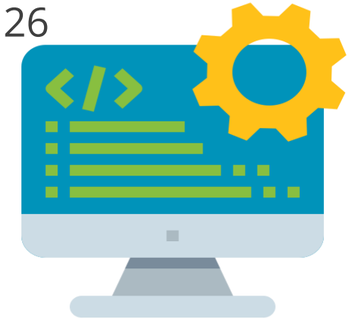
Address Resolution Protocol or ARP is a crucial protocol in networking, especially on Local Area Networks (LANs), like your home or office network.



- ARP helps translate logical IP addresses, which are the addresses used to identify devices on a network, to physical addresses.
- These physical addresses are called Media Access Control (MAC) addresses and are baked into every network interface card (NIC).

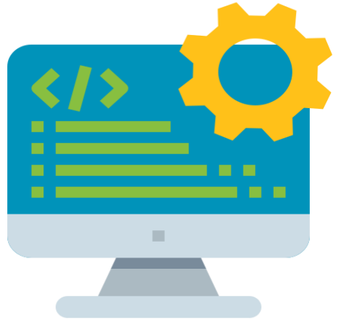
ARP Functioning

IP address 10.0.0.1
MAC address 00-B0-D0-63-C2-26



IP Address	MAC Address
10.0.0.1	**00-B0-D0-63-C2-26**
10.0.0.2	**00-B0-D0-63-C2-27**
10.0.0.3	**00-B0-D0-63-C2-28**
10.0.0.4	??? **00-B0-D0-63-C2-29**

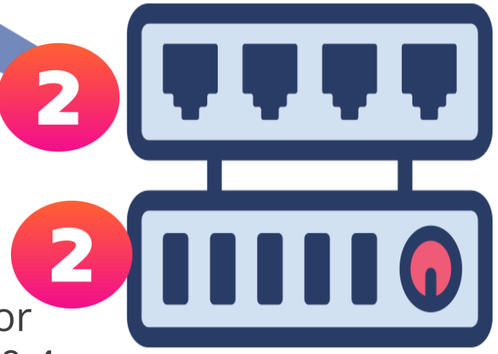
4 IP Address 10.0.0.2
MAC Address 00-B0-D0-63-C2-27



Arp table is updated with 10.0.04 MAC address

2 ARP query looking for MAC address of 10.0.0.4

2 ARP query looking for MAC address of 10.0.0.4

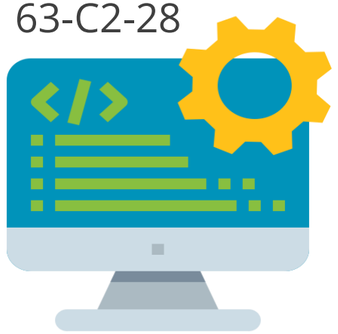


2 ARP query looking for MAC address of 10.0.0.4

IP Address 10.0.0.4
MAC Address 00-B0-D0-63-C2-29

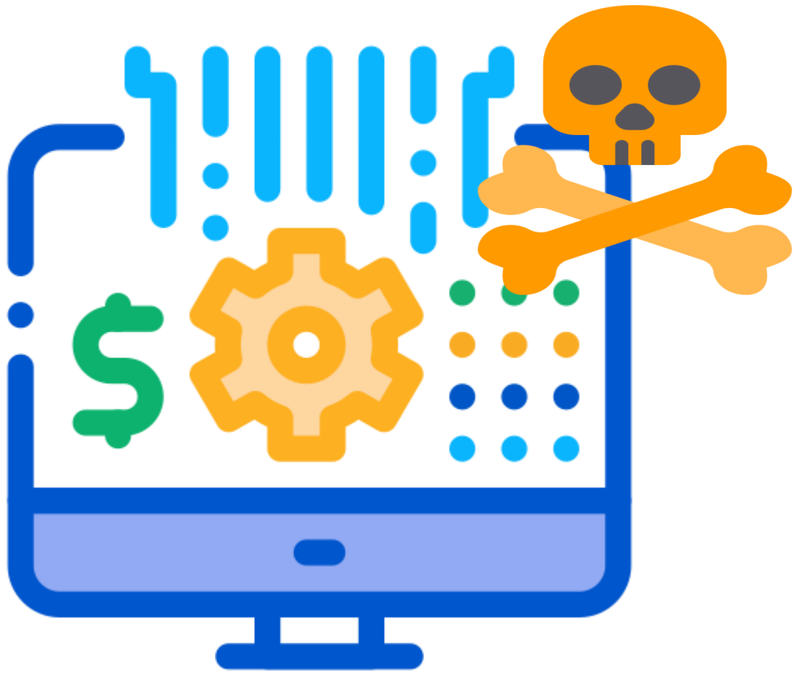
1 ARP request is broadcast to all systems and received by all four systems

IP Address 10.0.0.3
MAC Address 00-B0-D0-63-C2-28



3 Only 10.0.0.4 will respond back with its MAC address

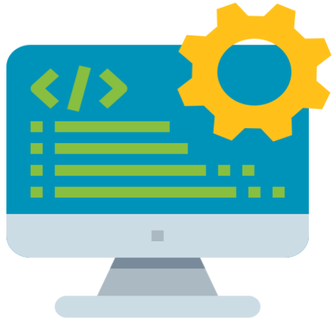
ARP Cache Poisoning



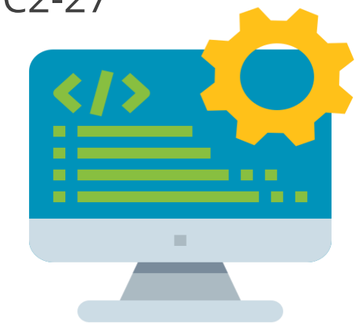
- ARP cache poisoning, also known as ARP spoofing, is a cyber attack that manipulates the Address Resolution Protocol (ARP) for malicious purposes.
- It disrupts normal network traffic by creating a false mapping between IP addresses and Media Access Control (MAC) addresses.

ARP Cache Poisoning

IP Address 10.0.0.1
MAC Address 00-B0-D0-63-C2-26



IP Address 10.0.0.2
MAC Address 00-B0-D0-63-C2-27



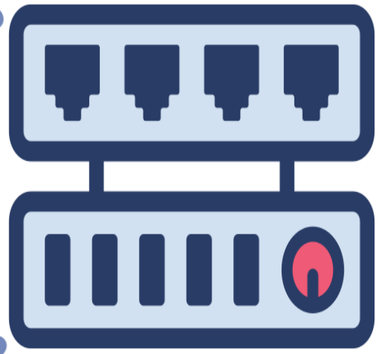
IP Address	MAC Address
10.0.0.1	00-B0-D0-63-C2-26
10.0.0.2	00-B0-D0-63-C2-27
10.0.0.3	00-B0-D0-63-C2-29

4 ARP cache is poisoned with hacker's MAC address

2 ARP query looking for MAC address of 10.0.0.3

2 ARP query looking for MAC address of 10.0.0.3

2 ARP query looking for MAC address of 10.0.0.3



IP Address 10.0.0.4
MAC Address 00-B0-D0-63-C2-29

ARP query looking for MAC address of 10.0.0.3

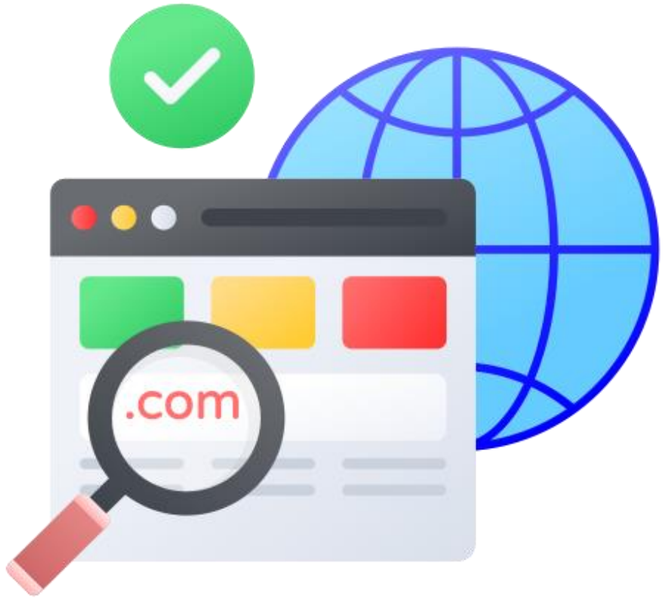
3 Attacker responds with their MAC address, claiming to be 10.0.0.3, and poisons the cache

1 ARP request is broadcast to all systems and received by all four systems

IP Address 10.0.0.3
MAC Address 00-B0-D0-63-C2-28

Domain Name System

Domain Name System (DNS) is a name service that provides a standardized system for naming TCP/IP hosts. It is also a way to search for a host's IP address using the DNS name.



Domain Name System

If DNS is used to look up the name abc.com, the user will get the IP address of the web host: 99.86.47.10.

Who is abc.com?

Abc.com is 99.86.47.10.

DNS Features

DNS uses a hierarchical naming structure.

DNS names are not case-sensitive.

DNS names can be up to 63 characters.

DNS organizes domains into subdomains.

DNS Cache Poisoning

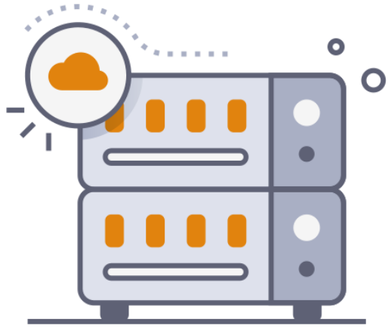
- DNS cache poisoning, also known as DNS spoofing, is a cyberattack that corrupts the data stored in the Domain Name System (DNS) cache.
- Attackers tamper with the cache to provide false information, essentially giving you the wrong address when you look up a website.

DNS Cache Poisoning

1

Website	IP address
www.abc.com	~~11.0.0.2~~ replaced by fake DNS address by hacker 11.0.0.1

2 The user tries to access abc.com



www.fake.com-->11.0.0.1

3 The user's request will be redirected to fake.com instead of abc.com due to cache poisoning

www.abc.com-->11.0.0.2

4 The hacker poisons the DNS cache and replaces the original IP of abc.com with the IP address of the website fake.com

DNS Attack

An attacker disrupts the DNS server with lots of DNS requests, making it inaccessible.

- Attackers flood DNS servers with a massive amount of valid but spoofed DNS request packets.
- This overload of requests can slow down or even crash the DNS server, preventing legitimate users from resolving website names to IP addresses and accessing the internet.

DNS Amplification

An attacker spoofs a DNS server and uses it to propagate false information about bogus websites.

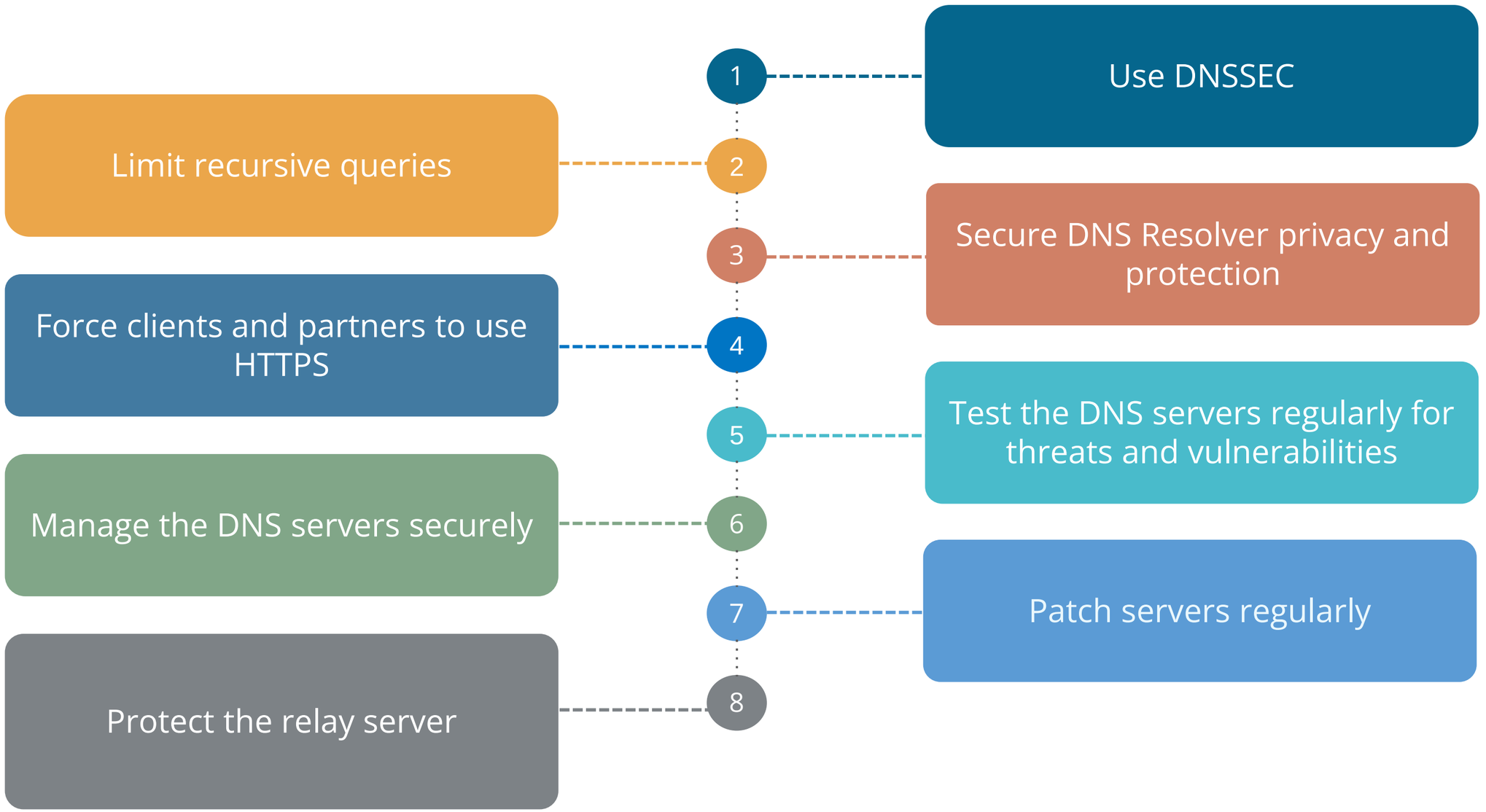
Legitimate users are redirected toward these bogus websites.

Users are then bombed with excessive and useless information.

DNS Commands

Command	Function
ipconfig/displaydns	To view the DNS cache
ipconfig/flushdns	To clear the DNS cache
dnslookup/	To check the DNS record on the DNS server, append the command with the name of the computer you want to check, for example, dnslookup computer 1

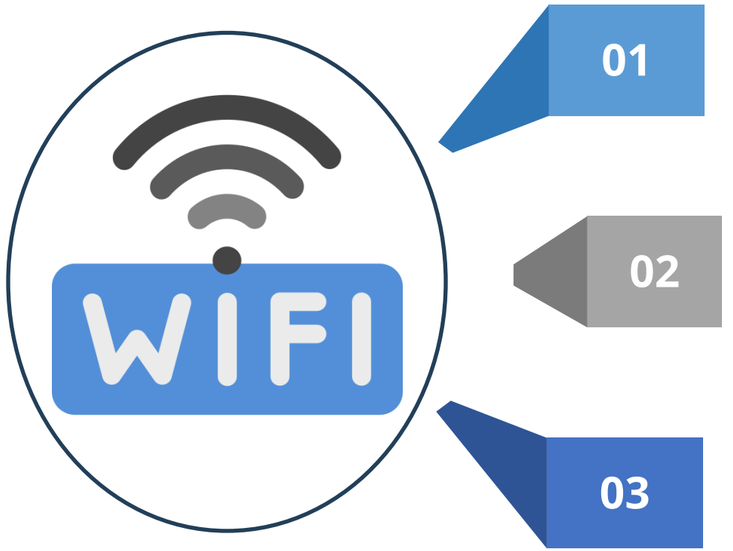
Steps to Protect Against DNS Attacks



Wi-Fi

- A wireless network is a computer network that uses radio waves instead of cables to connect devices to each other.
- This allows you to connect to the internet or other devices on the network without being tethered to a physical location.

Benefits of Wireless Network



01

Mobility: One can move around freely without having to worry about being tangled in cables.

02

Flexibility: One can easily set up a wireless network and expand.

03

Cost-effective: One does not need to spend money on cables or installation fees.

Wireless Attacks

Evil Twin

An evil twin is a fraudulent Wi-Fi access point that appears to be legitimate but is set up to eavesdrop on wireless communications.

Rogue AP

A rogue access point is a wireless access point that has been installed on a secure network without explicit authorization from a local network administrator.

Jamming

Jamming is a form of denial of service that specifically targets the radio spectrum aspect of wireless.

Wireless Attacks

Wi-Fi Protected Setup

- Wi-Fi Protected Setup (WPS) is a network security standard that was created to provide users with an easy method of configuring wireless networks, involving an eight-digit PIN.
- A successful attack can reveal the PIN and, subsequently, the WPA/WPA2 passphrase, allowing unauthorized parties to gain access to the network.

Disassociation

- Disassociation attacks are designed to disconnect a host from the wireless access point and network.
- Disassociation attacks stem from the deauthentication frame that is in the IEEE 802.11 (Wi-Fi) standard.

War Driving

- It is the act of searching for Wi-Fi networks, usually from a moving vehicle, using a laptop or smartphone.
- It involves slowly driving around an area with the goal of locating Wi-Fi signals.

Controls to Secure Wi-Fi

Using encryption

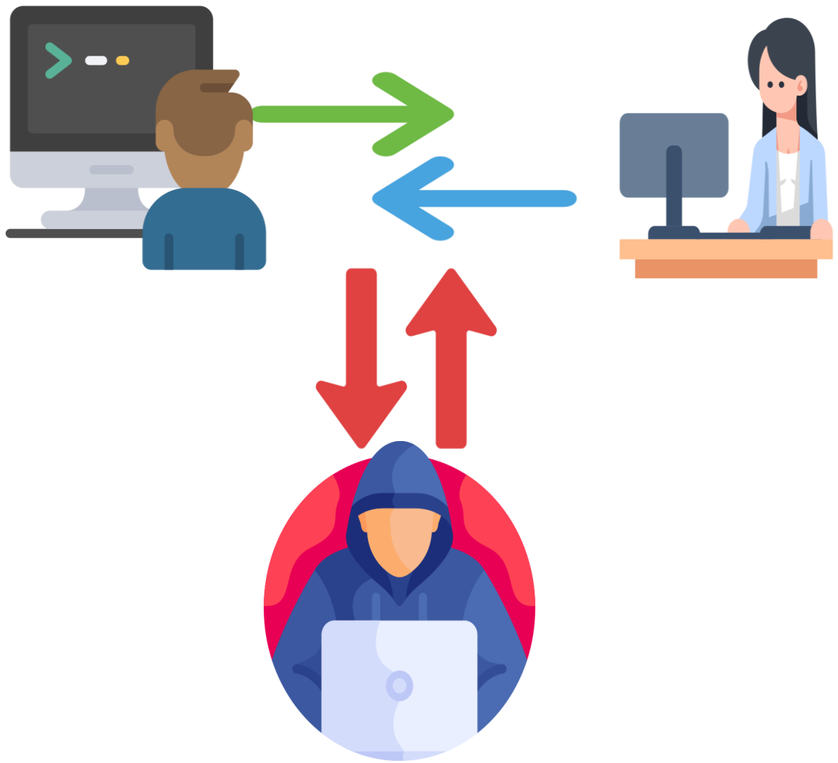
Using WPA2 authentication

Using antivirus, antispyware, and firewall

Turning off SSID Broadcast

Using WPA3 authentication

On-Path Attack

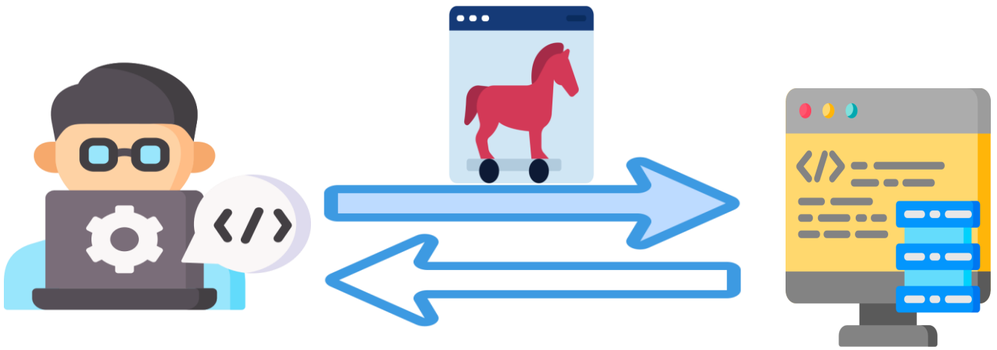


- On-path attacks, often referred to as man-in-the-middle or interception attacks, involve an adversary positioning themselves to intercept the communication between two parties.
- They can intercept, modify, or eavesdrop on data being exchanged.
- This silent intrusion enables cybercriminals to exploit sensitive information, launch further attacks, or even manipulate transactions undetected.

Man-in-the-Middle Attack

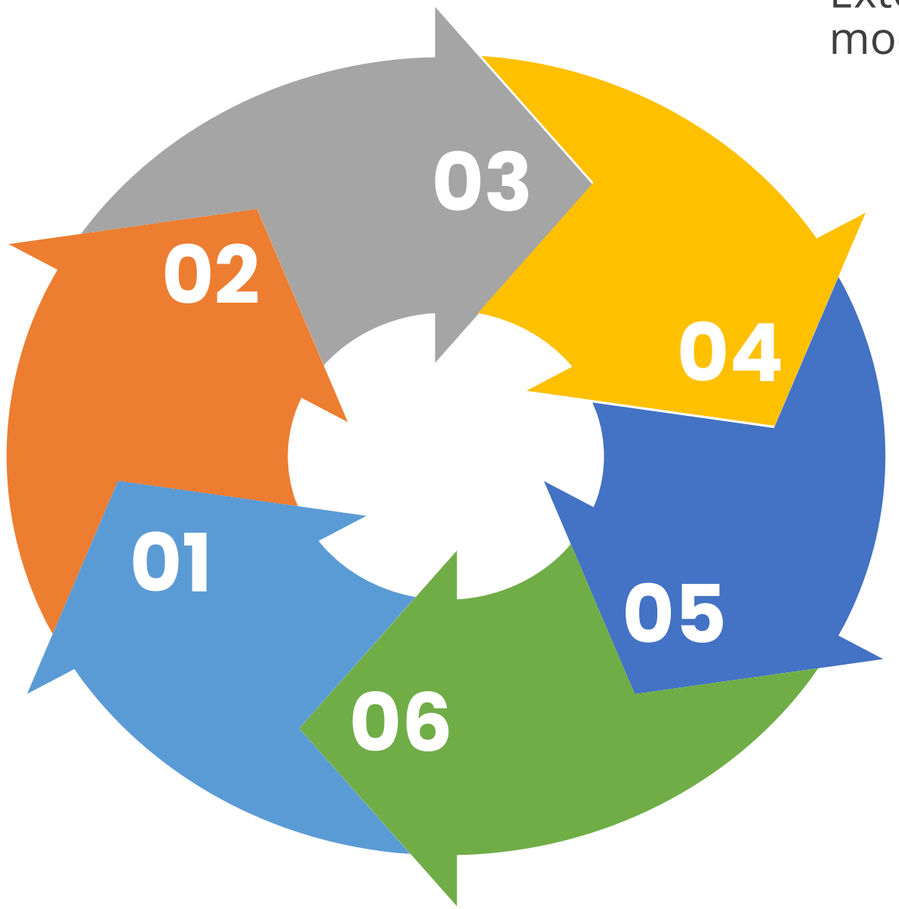
- MITM generally occurs when an attacker is able to place himself in the middle of two other hosts that are communicating.
- It is done by ensuring that all communication going to or from the target host is routed through the attacker's host.
- The attacker can observe all traffic before relaying it and modify or block it.
- To the target host, it appears that communication is occurring normally since all expected replies are received.

Man-in-the-Browser Attack



- The first element is a malware attack that places a Trojan element that can act as a proxy on the target machine.
- This malware changes browser behavior through browser helper objects or extensions.
- When a user connects to their bank, the malware recognizes the target (a financial transaction) and injects itself into the conversation's stream.
- When the user approves a transfer, the malware intercepts the user's keystrokes and modifies them to perform a different transaction.

Man-in-the-Browser Attack: Flow



User opens bank websites and fills out transaction forms

Malicious browser extension gets installed

Computer gets infected by a virus

Extension notes data and modifies transaction

Money gets transferred to the attacker

Extension modifies transaction receipts to remain undetected

Credential Replay Attack

- A credential replay attack, also known as a playback or repeat attack, is a cyberattack where an attacker steals valid authentication data and reuses it to gain unauthorized access to a system or account.
- One should refrain from using telnet or FTP and instead use SSH and secure version of protocols.

Credential Stuffing Attack

- Credential stuffing is a cyberattack that preys on people's tendency to reuse login credentials across multiple accounts.
- Attackers gather usernames and passwords from data breaches on other websites or services.
- Many people reuse the same login information (username or password) for multiple accounts. If someone reuses their login information from a breached site, the attacker might be able to access their accounts on other sites.

Bash Shell Attack

- The Bash shell is a powerful tool found in most Unix-like operating systems that can nonetheless be exploited for malicious purposes.
- Attackers may use Bash scripts to execute unauthorized commands, compromise systems, or manipulate files.
- Common tactics include privilege escalation, file manipulation, and system reconnaissance.

A Bash script can be identified by the .sh file extension.

Cryptographic Attacks

Cryptographic Attack

Cryptography attacks are attempts to bypass the security of cryptographic systems.

- Attackers aim to steal information, tamper with data, or gain unauthorized access to systems protected by encryption.
- These attacks exploit weaknesses in various components of a cryptographic system, including the cryptographic algorithm, encryption keys, cryptography protocols, and key management.

Downgrade Attacks

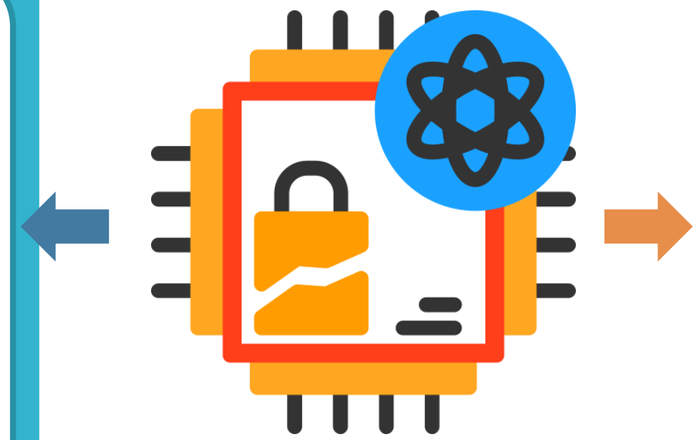
This is a specific type of cryptographic attack where an attacker manipulates a communication to use a weaker encryption standard or protocol than originally intended.

A cryptography downgrade attack is also known as a version rollback attack or bidding-down attack.

Types of Downgrade Attacks

SSL/TLS downgrade attack

- An attacker exploits vulnerabilities in the communication between clients.
- The attacker suggests using an older, less secure encryption method instead of the stronger ones that both parties' support.



SSL stripping attack

- A malicious actor intercepts a secure HTTPS connection and downgrades it to an unsecured HTTP connection, enabling them to eavesdrop on sensitive information exchanged between a user and a website without detection.

Collision Attack

A collision attack occurs when two different inputs produce the same hash value.

- A good hash function should make collisions very unlikely.
- It can be used for digital signature forgery.
- If an attacker can find a collision for a signed message, they could potentially create a new message with the same hash value and forge a valid digital signature.
- Rainbow tables, which are precomputed databases of hash collisions, can be used for cracking password hashes if the hash function used for password storage is vulnerable to collisions.

Birthday Attack

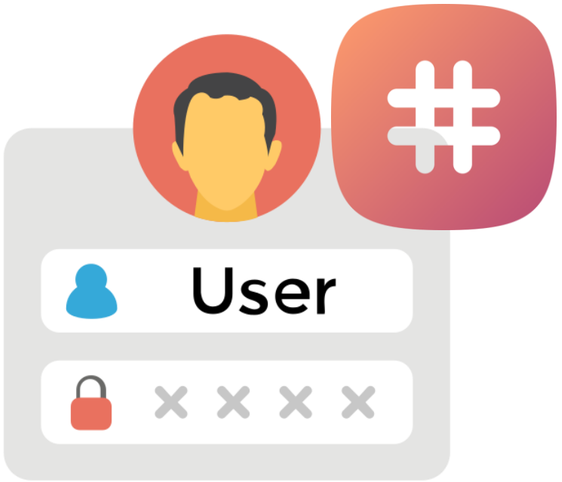
It attempts to exploit the likelihood of two messages generating the same message digest using the same hash function.

- It is based on the statistical probability that with 23 people in a room, there is more than a 50% chance that two people share the same birthday.
- The birthday attack enables a malicious actor to generate different passwords that produce the same hash.
- If the hash is matched, then the attacker knows the password, potentially granting unauthorized access to a user account or system.

Pass-the-Hash Attack

This security concern affects older systems like Windows NT 4.0, where NTLM stored hashed user passwords locally with the MD4 algorithm.

- Attackers could exploit weak hashing using methods like rainbow tables or tools like hashcat to perform hash collision attacks.
- These attacks aim to recover user passwords from their hashed representations.
- The weakness of NTLM is that all of the passwords are stored in the Local Security Authority Subsystem Service (LSASS).



Password Attacks

Secure Your Passwords

Usernames and passwords are the most common methods for identification and authentication.

Issues with passwords

- Vulnerable
- Easily compromised
- Often reused

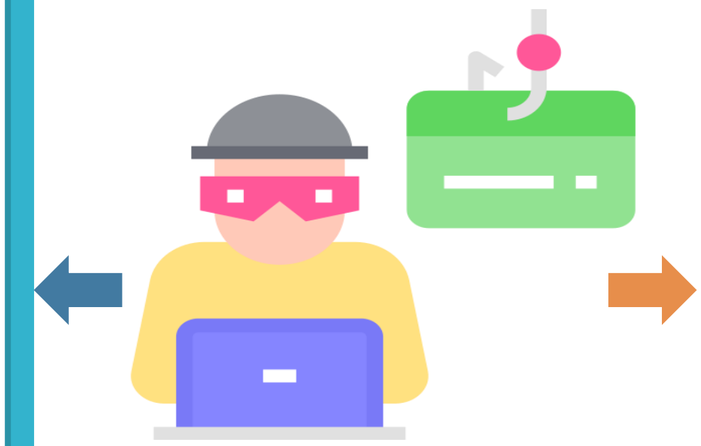
Common password attack methods

- Dictionary attacks (e.g., Crack, John the Ripper)
- Brute-force attacks (e.g., L0phtcrack)
- Hybrid attacks (combining dictionary and brute-force)
- Trojan horse login programs (password-stealing Trojans)
- Social engineering tactics

Types of Password Attacks

Online attacks

- Occurs directly on the login page of a website or service
- Attackers use automated tools to guess passwords repeatedly
- Limited by security measures like multi-factor authentication, login throttling, and CAPTCHA verification



Offline attacks

- Target stolen data storage, not the login system
- Attackers access databases with hashed (scrambled) passwords via security breaches
- Strong, unique passwords and regular password changes prevent this attack

Common Password-Based Attacks

1 Electronic monitoring (replay attack)

- Intercepting network traffic to capture authentication data

2 Access the password file

- Targeting authentication servers to reveal multiple users' passwords

3 Brute-force attack

- Using automated tools to try all possible password combinations

4 Dictionary attack

- Trying thousands of common words to find a matching password

5 Password spraying

- Attempting a single password across many usernames
- Using lists of common or leaked passwords

6 Rainbow table

- Using precomputed password hashes to crack passwords quickly

Application Attacks

Application Attack

It is a category of cyber threats that exploit vulnerabilities in software applications, targeting weaknesses in design, development, and implementation.

These attacks include:

- Compromising data
- Breaching user privacy
- Disrupting functionality

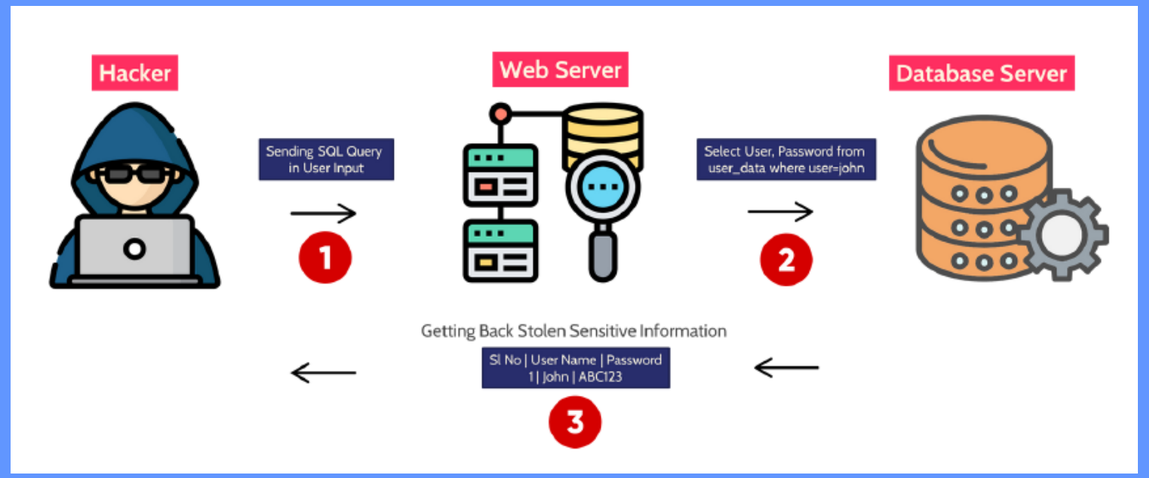
Understanding and addressing these vulnerabilities better protects software applications from malicious attacks.

Injections

These are a type of security vulnerability that arises when an application processes user input unsafely.

These attacks include:

- Exploiting user input
- Sending malicious data
- Forcing the application to perform unintended actions



By understanding and mitigating injection vulnerabilities, we can enhance the security of our applications and protect sensitive information from being compromised.

Replay Attack

These types of cyberthreats occur when an attacker intercepts and retransmits valid data transmissions.

These attacks include:

- Capturing valid data
- Resending intercepted data
- Gaining unauthorized access or permission

Understanding and implementing countermeasures for replay attacks is crucial to maintaining the integrity and security of data transmissions.

Directory Traversal

Directory traversal, also known as path traversal, is a web security vulnerability that attackers can exploit to access files or folders on a web server.

These attacks include:

- Tricking the server into giving unauthorized access
- Executing malicious code
- Exploiting weaknesses in how the web server retrieves documents

Understanding and mitigating directory traversal vulnerabilities is crucial for maintaining the security and integrity of web servers.

Privilege Escalation

It occurs when a malicious user gains a higher level of permissions, access, or privileges than they have been assigned.

These attacks include:

- Exploiting administrative oversights
- Compromising credentials through methods such as keystroke capturing or password cracking

Understanding and preventing privilege escalation is crucial to maintaining the security and integrity of systems and protecting sensitive information.

Privilege Escalation

Privilege escalation can be categorized into two main types:

Horizontal privilege escalation

Occurs when an attacker gains the rights and privileges of another user with similar privileges. This action is referred to as an account takeover.

Vertical privilege escalation

Occurs when an attacker gains access to an account and then elevates its privileges. This is also known as a privilege elevation attack and involves moving from a lower level of privileged access to a higher one.

Source: https://www.beyondtrust.com/blog/entry/privilege-escalation-attack-defense-explained

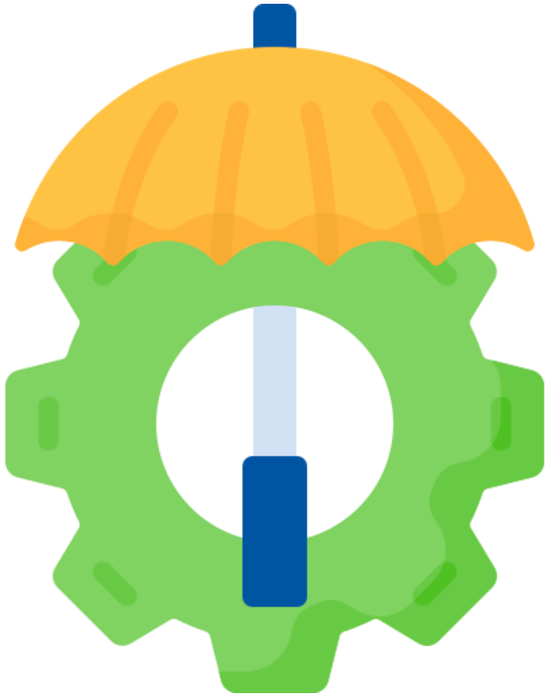
TECHNOLOGY

Mitigation Techniques to Secure the Enterprise

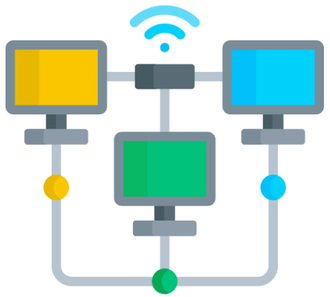
Mitigation Strategies

These are controls that organizations implement to protect themselves from various types of attacks.

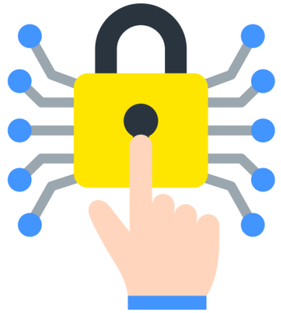
They focus on implementing and understanding practices such as segmentation, access control (including ACLs and permissions), application allowlisting, isolation, patching, encryption, monitoring, and least privilege.



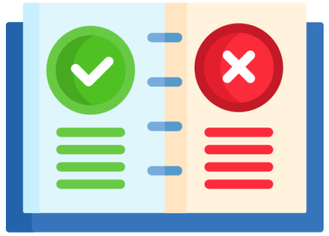
Mitigation Strategies



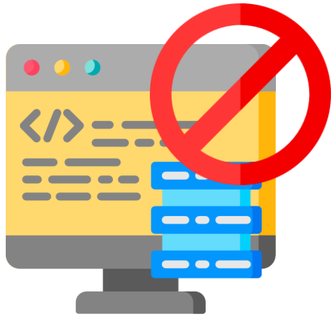
Segmentation



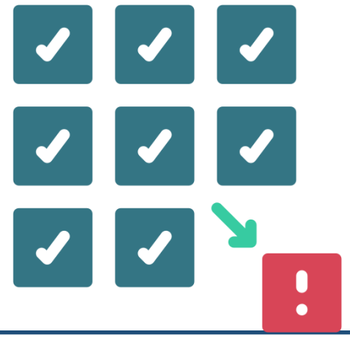
Access control



Application allowlist



Application blocklist



Isolation

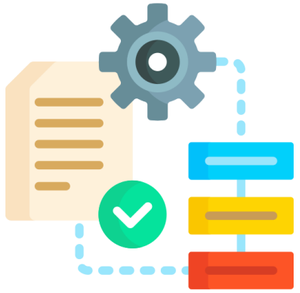
Patching

Mitigation Strategies

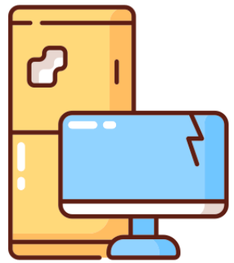
Encryption

Monitoring

Least privilege access



Configuration enforcement

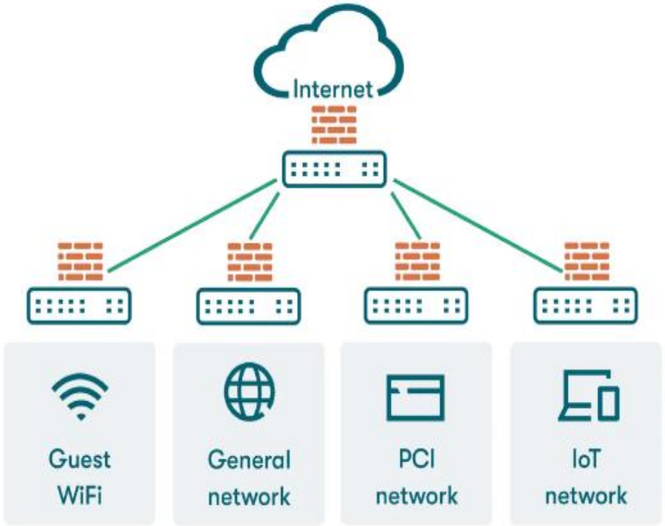


Decommissioning

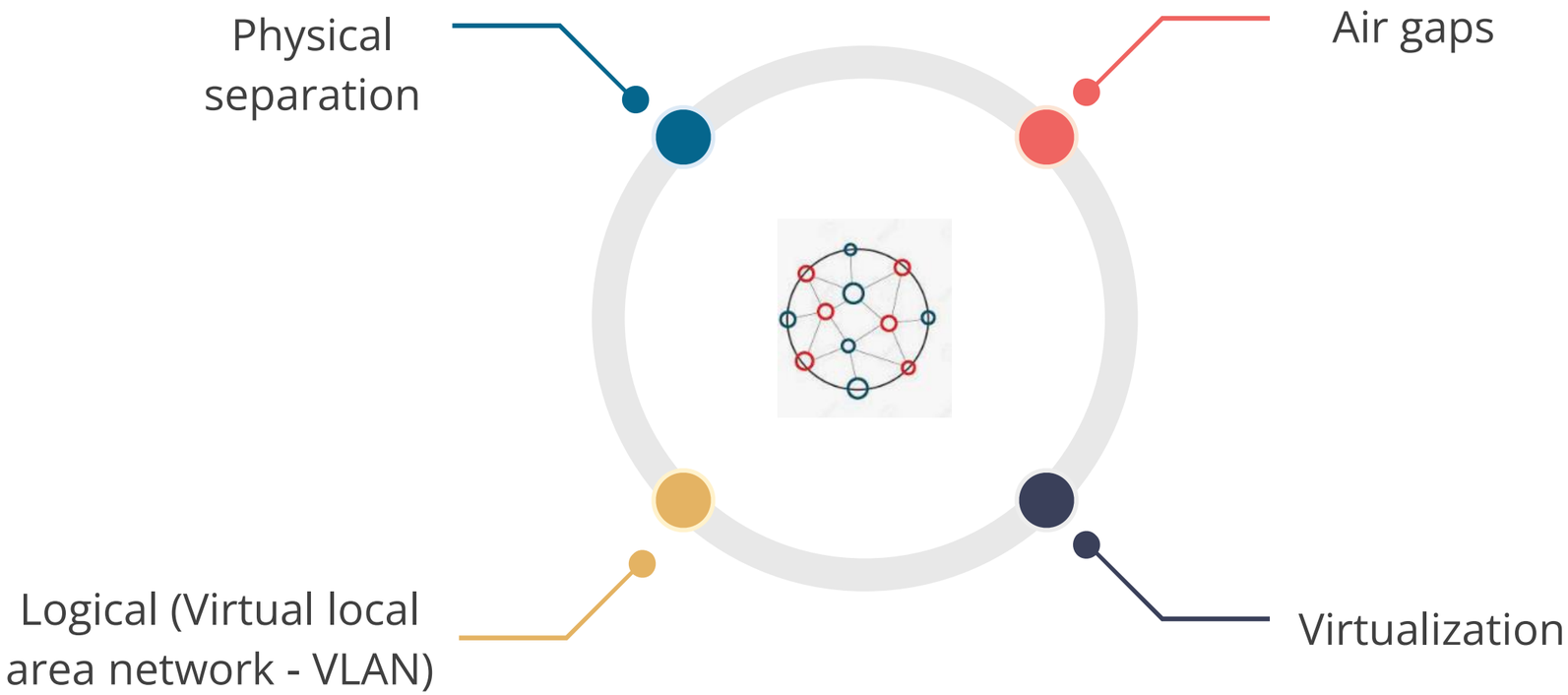
Hardening techniques

Segregation, Segmentation, and Isolation

- Network segregation, segmentation, and isolation are some of the most effective controls an organization can implement to mitigate the effect of a network intrusion.
- Network segmentation and isolation are fundamental security practices that involve dividing a large network into smaller, isolated subnetworks.
- This approach enhances security, improves performance, and simplifies network management.



Types of Segregation or Segmentation



Types of Segregation or Segmentation

Physical separation

- Separate physical equipment handles different classes of traffic, including separate switches, routers, and cables.
- This is the most secure method of separating traffic, but also the most expensive.
- Organizations commonly have separate physical paths in the outermost sections of the network where connections to the Internet are made.

Virtualization

- Virtualization offers server isolation logically while still enabling physical hosting.
- Virtual machines enable the running of multiple servers on a single piece of hardware, maximizing enterprise machine utilization.
- By definition, a virtual machine provides a certain level of isolation from the underlying hardware, operating through a hypervisor layer.

Types of Segregation or Segmentation

Air gaps

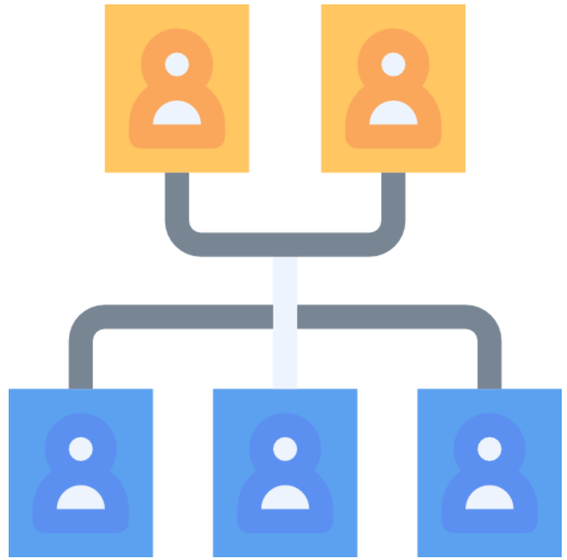
- An air gap is a term used to describe the absence of any data path between two networks, which are only connected physically by a gap between them.
- Physically or logically, there is no direct path between them.
- It refers to isolating a secure network or computer from all other networks, particularly the Internet, to prevent unauthorized access.

VLAN

- VLANs group ports on the same or different switches to confine traffic within specified groups.
- A VLAN isolates broadcast domains on a switch, functioning similarly to a router managing multiple broadcast domains.
- It isolates segments, reduces routing broadcasts, and segregates department functions.
- It can be segmented logically.

Micro-Segmentation

- Micro-segmentation creates security zones and is specifically designed to provide granular security controls within the same data center or cloud environment.
- It isolates workloads from each other and defines individual security controls to secure them.



Benefits of Micro-Segmentation

Reduce network attack surface

By limiting an attacker's movement from one potentially compromised workload to another

Improve breach containment

By blocking unsanctioned activities and drastically improving threat detection and response times with real-time alerts

Strengthen regulatory compliance

By isolating segments that specifically store regulated data, such as PII and PHI

Achieve zero trust

By creating and enforcing granular security policies through micro-segmentation

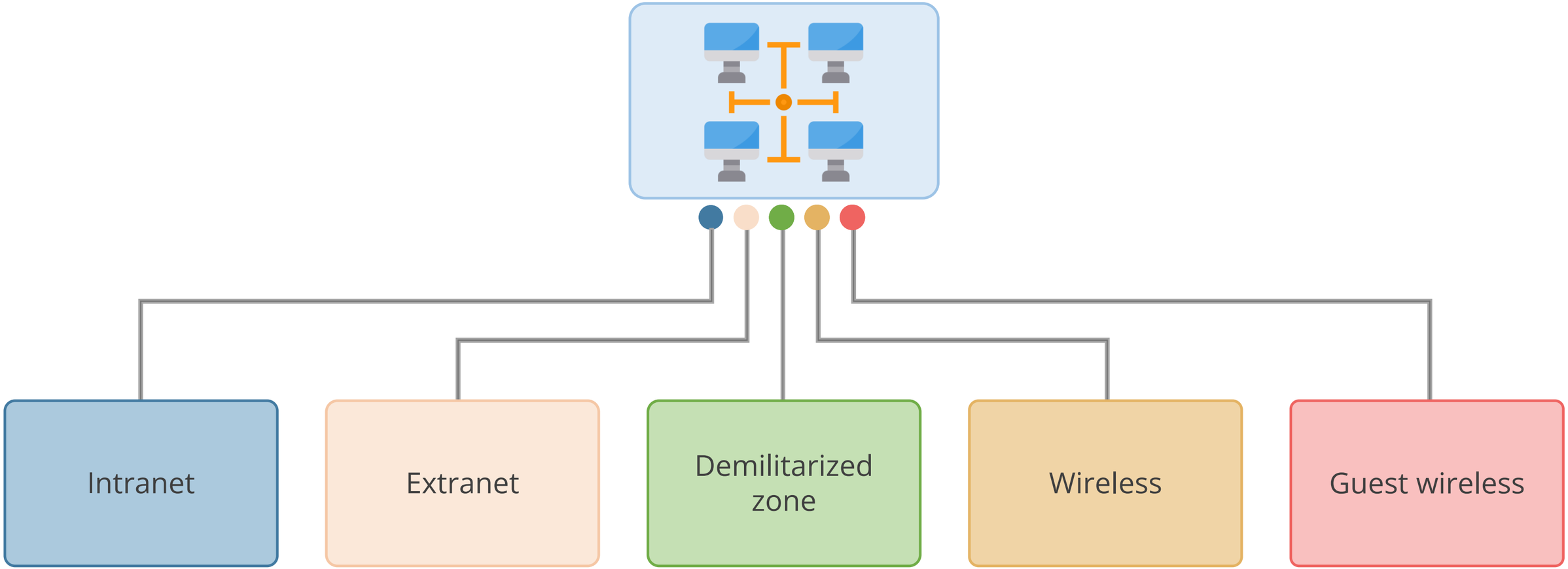
Zones

Each sub-network created through segmentation is called a zone.

- These zones represent groups of devices or functionalities that have similar security needs.
- Network zones are the building blocks of network segmentation.
- They are essentially the individual sub-networks created when a larger network is divided into smaller, more manageable sections.

Types of Network Zones

Dividing a campus network or data center into zones implies that each zone has a different security configuration. The main zones are as follows:



Intranet

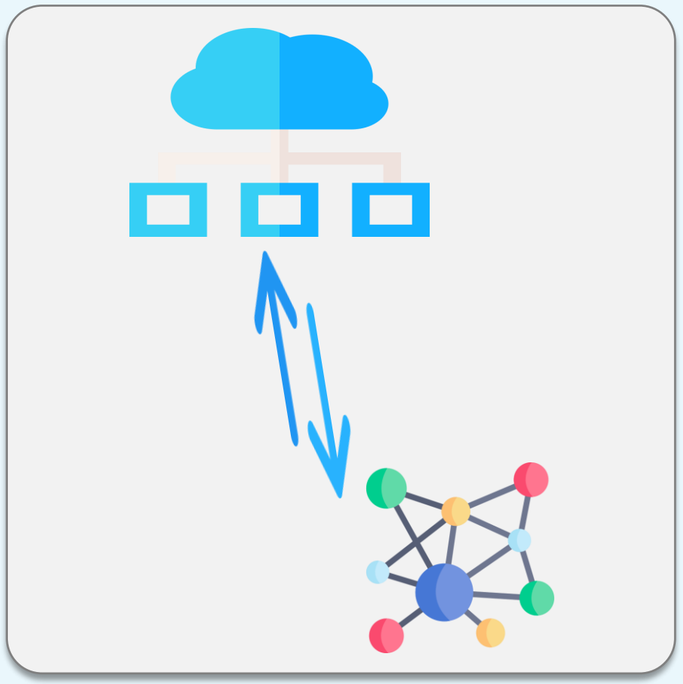
An intranet functions like the internet for users but is entirely contained within and secured by the network's trusted area and managed by system and network administrators.

- Typically referred to as campus or corporate networks, intranets are used every day in companies around the world.
- Content on intranet web servers is not available over the internet to untrusted users.

Extranet

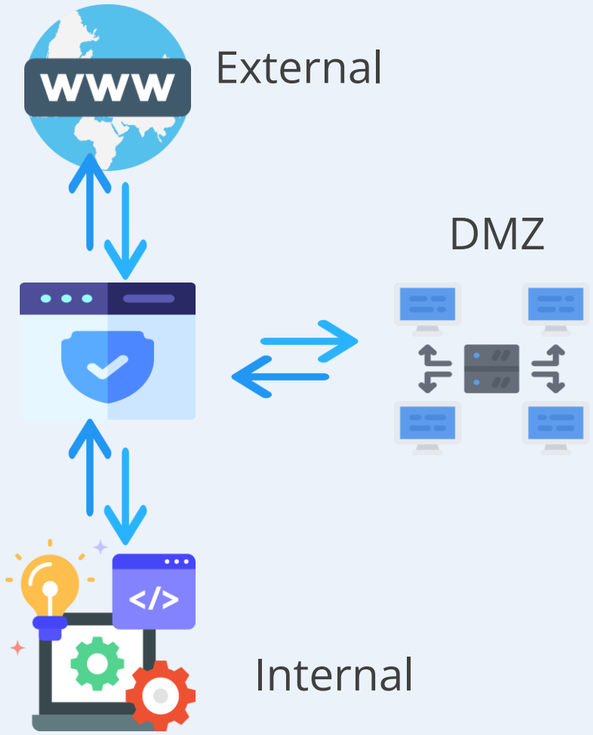
An extranet is an extension of a selected portion of a company's intranet to external partners.

- This allows a business to share information with customers, suppliers, partners, and other trusted groups while using a common set of Internet protocols to facilitate operations.
- Extranets can utilize public networks to extend their reach beyond a company's internal network, typically secured using some form of security like a VPN.



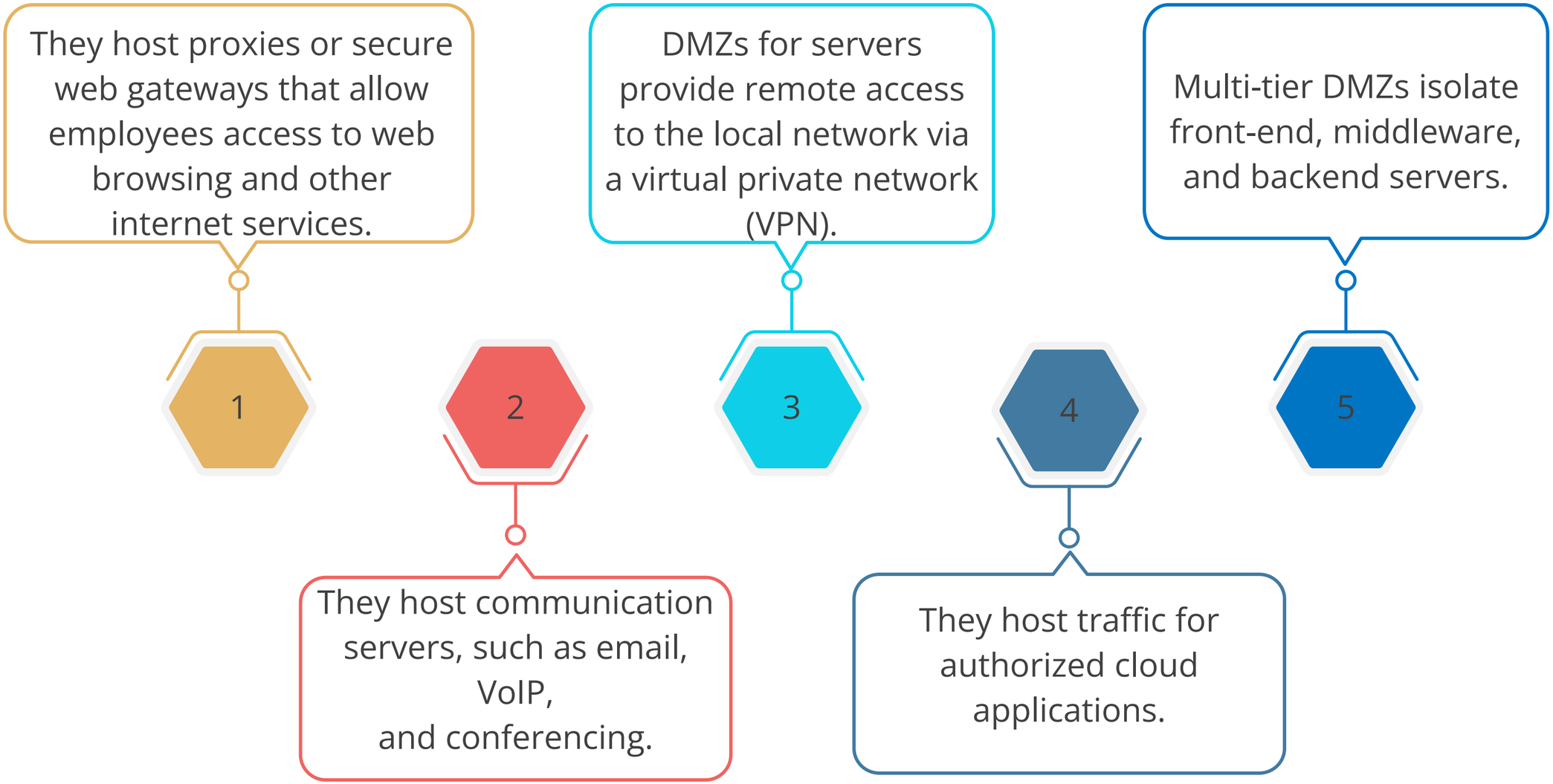
Demilitarized Zones (DMZs)

- In cybersecurity, a DMZ is a physical or logical subnetwork that sits between an internal network and the Internet.
- It isolates your internal network from the public internet, reducing the risk of external threats compromising sensitive data.
- It allows you to expose certain services to the internet, like web servers or email servers, without exposing your entire internal network.



Functions of DMZs

Different types of DMZ are used for different functions.



Wireless Network

Wireless networking involves transmitting packetized data through a physical topology that does not rely on direct physical links.

- Wireless networks should have separate zones.
- Access to the internal zone can be controlled through MAC filtering.
- Wireless access points should be configured to accept connections only from specific MAC addresses.

Guest Wireless Network

- Guest wireless networks should be separated from the internal network using a wireless firewall, as MAC address authentication is not feasible for guests.
- Guest network users should only access the internet gateway for web browsing and email.
- A captive portal can require authentication, payment for usage, or display policies and agreements.

Advantages of Segmentation

Enhanced security

- Segmentation makes it harder for attackers to access sensitive data or critical systems.

Access control

- Access control can be implemented with granularity and more effectively.

Compliance requirement

- It helps in maintaining compliance, as some regulations demand separate segments for sensitive data.

Performance optimization

- Segmentation can lead to improved network performance by reducing broadcast domains and congestion.

Isolation of critical systems

- Organizations often have critical systems that need extra protection.
- Segmentation isolates these systems, safeguarding them.

Scalability and agility

- Segmentation provides scalability and agility, allowing them to adapt to evolving needs without compromising security.

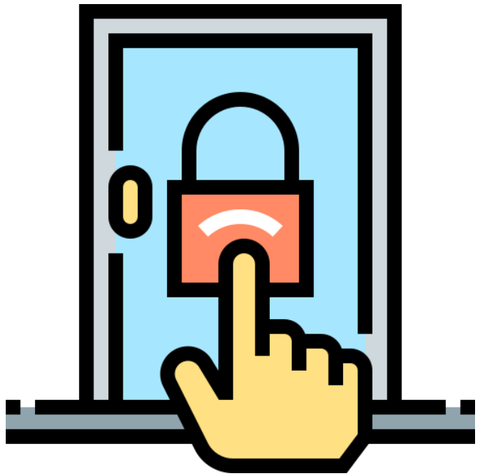
Access Control

- It is the process of allowing or restricting access to an organization’s data, applications, network, or cloud based on its policies.
- It ensures only authorized users access specific resources and is achieved through various means.

Implementing Access Control List

The two controls used for implementing an access control list are:

Access control lists (ACLs)



Access levels

Implementing Access Control Lists

Access control list

- ACLs are vital tools that let administrators define rules to control network traffic.
- ACL rules can grant or deny permissions to specific IP addresses, protocols, or ports, enhancing network access control.

Access levels

- Permissions are defined as rights to perform actions on a system.
- They are typically associated with files, directories, or processes and determine who (or what) can read, write, or execute them.
- Implementing permissions helps ensure that users and systems interact with only the resources necessary for their roles.

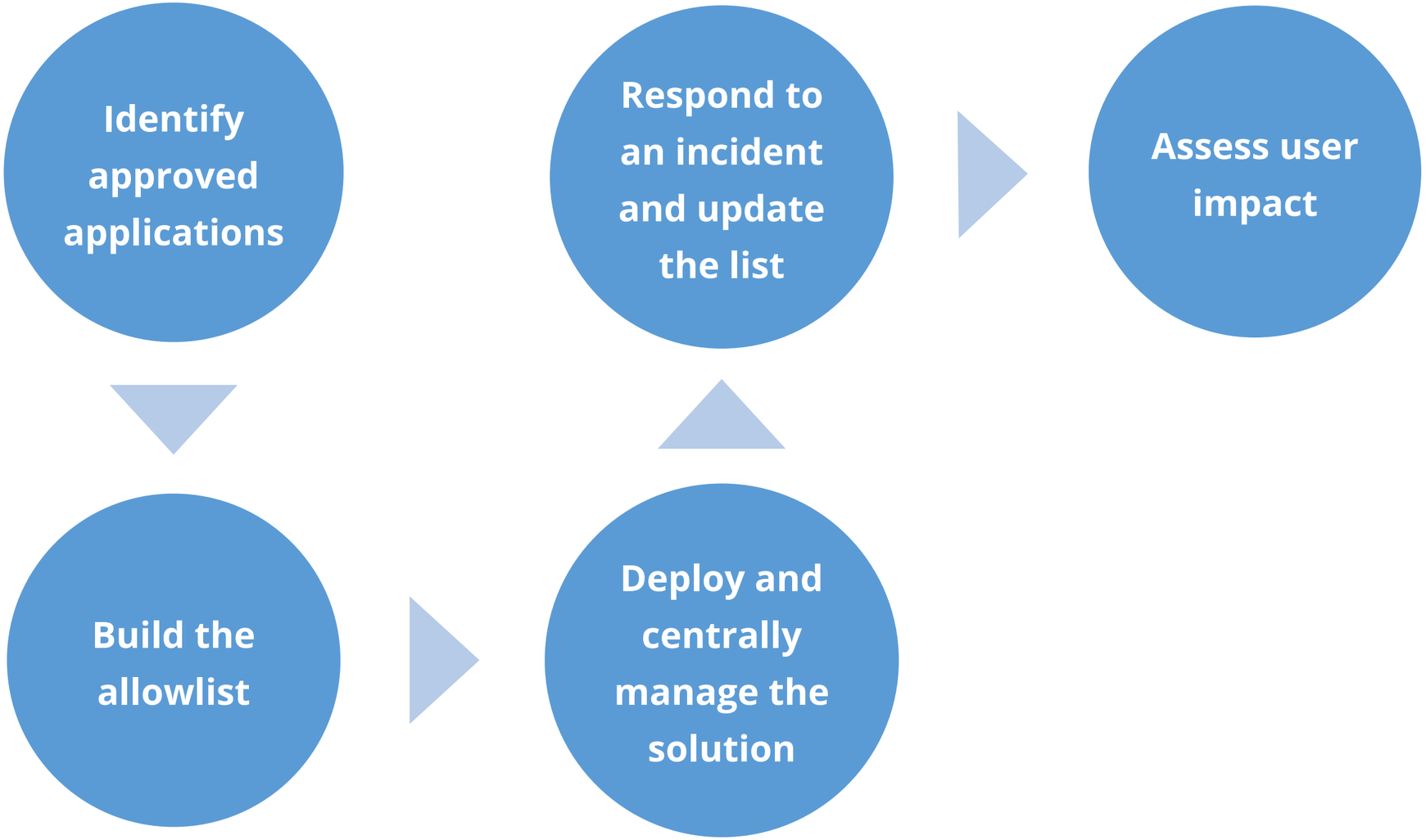
Application Allowlist

- It is a security measure used to restrict what software can run on a device or network.
- It allows only authorized applications to execute, blocking any not on the list.

Application allowlisting is also known as application control or whitelisting.

Application Allowlist

The process of creating, maintaining, and updating an application allowlist is as follows:

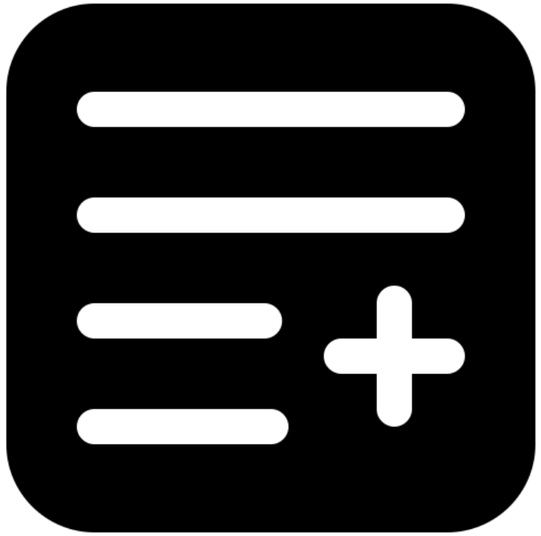


Allowlist Attribute

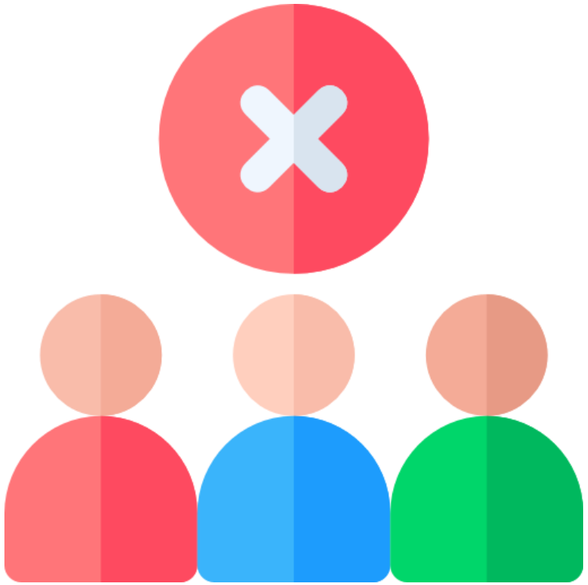
- **Security**: Allows only trusted applications to run, preventing malware and other malicious software
- **Improved management**: Ensures only necessary software is installed and running, improving IT oversight
- **Implementation**: Utilizes security software or operating system settings to enforce application allowlisting

Application Blacklist

- It is a list of software programs that are prohibited from running on a computer system or network.
- It is a cybersecurity measure to block potentially harmful or unwanted applications.



Blacklist Attribute



- **Security focus**: Block known malware, including viruses, worms, and ransomware
- **Productivity boost**: Improve user productivity by limiting access to non-work-related programs
- **Management control**: Ensure compliance with security policies and software licenses

Sandboxing

It is a technique used to safely evaluate the threat in an isolated test environment (sandbox).

- It provides effective protection against zero-day attacks and advanced threats.
- Suspicious email attachments are sent to a virtual sandbox for deep analysis of malicious activity.

Sandboxing Flow

Isolation:
A sandbox creates a segregated environment that mimics a real operating system, allowing suspicious programs to be executed without affecting the real system or network.

1

2

Detonation:
The suspicious code is then detonated within the sandbox, essentially running it and monitoring its behavior closely.

Analyzation:
Security experts can then analyze the code's activity inside the sandbox.

3

4

Threat detection:
By observing the code's behavior, analysts can identify malicious activity, such as attempts to steal data, install malware, or damage the system.

Protection:
If the code is found to be malicious, it can be prevented from entering the real system, thus stopping a cyberattack in its tracks.

5

Benefits of Sandboxing

Proactive defense:

Sandboxing allows for the analysis of unknown or zero-day threats that traditional signature-based security might miss.

Safe analysis:

Security professionals can examine potentially risky code without putting the actual system or network at risk.

Improved detection rates:

Sandboxes can uncover sophisticated malware that might bypass traditional security measures.

Patch Management

Patch management is the process of applying patches to a system at a specified time using a well-defined strategy and plan. Effective patch management ensures that systems remain secure and up-to-date.

The types of patches are:

Hotfixes

Small updates with a specific purpose that alter the behavior of installed applications in a limited manner

Service packs

Tested and cumulative sets of all hotfixes, security updates, and critical updates

Updates

Address non-critical, non-security-related bugs and provide fixes for specific problems

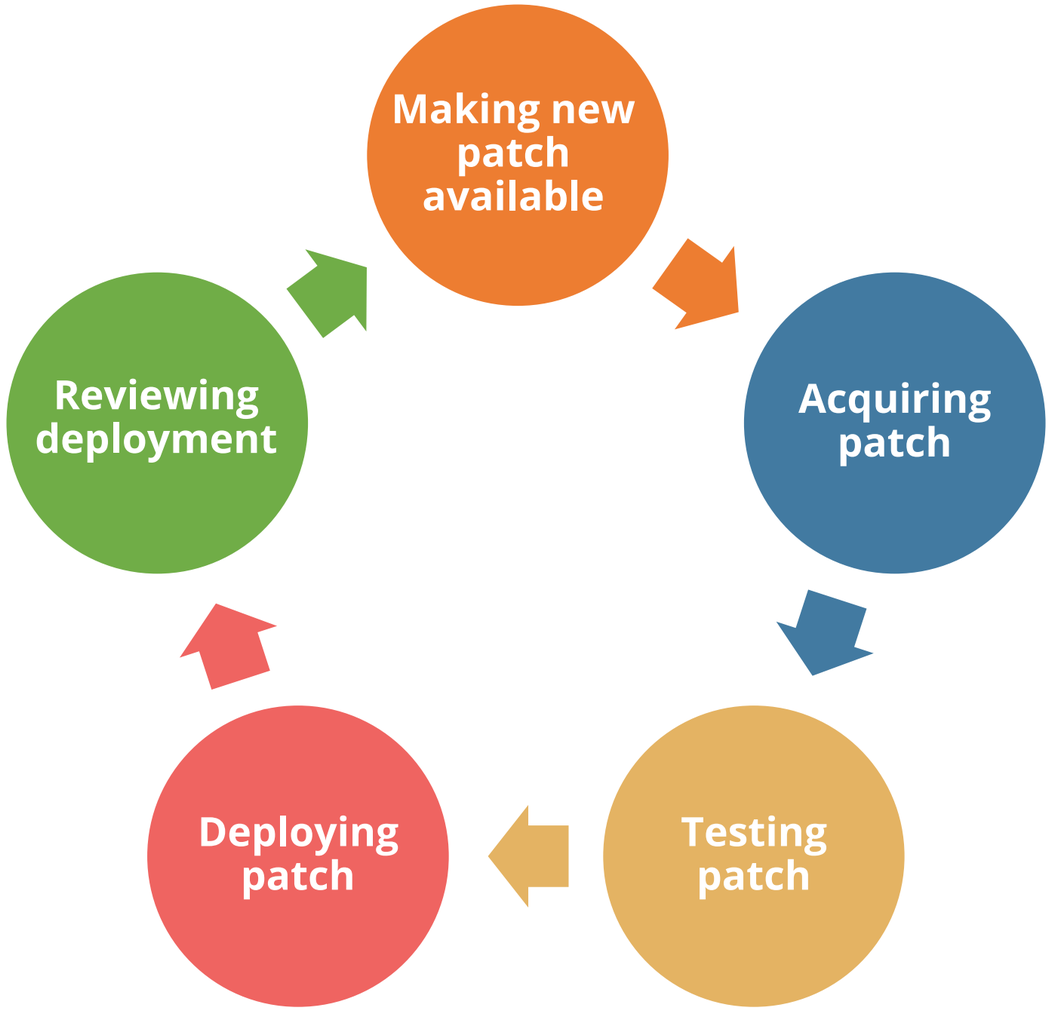
Patch Management Activities

Patch management involves several key activities to ensure systems are secure and up-to-date:

1. Scheduling and prioritizing patches
2. Testing patches
3. Managing changes
4. Installing and deploying patches
5. Auditing and assessing
6. Ensuring compliance

Patch Management Cycle

The following are the phases of an effective patch management cycle:



Encryption

Encryption is a cornerstone of data security that involves the conversion of data from plaintext into an unreadable format (ciphertext) that can only be deciphered with the appropriate decryption key.

Importance of encryption:

Implements data protection: By implementing encryption, enterprises ensure that even if data is intercepted, it will remain indecipherable to unauthorized parties.

Safeguards confidentiality and integrity: Encryption safeguards the confidentiality and integrity of sensitive information.

Implementing robust encryption protocols is essential for protecting data from unauthorized access and ensuring its security.

Encryption as a Mitigation Strategy

Security controls for stored data and data on the network are described below:

Data at rest

- Implementing security controls such as encryption, hashing, compressing, strong passwords, labeling, marking, storage, and documentation
- Using encryption tools like self-encrypting USB drives and file and media encryption software

Data in transit

- Applying security controls with cryptographic functions such as encryption and hashing
- Implementing end-to-end encryption to encrypt data while keeping routing information visible
- Using link encryption to encrypt both data and routing information

Link Encryption vs. End-to-End Encryption

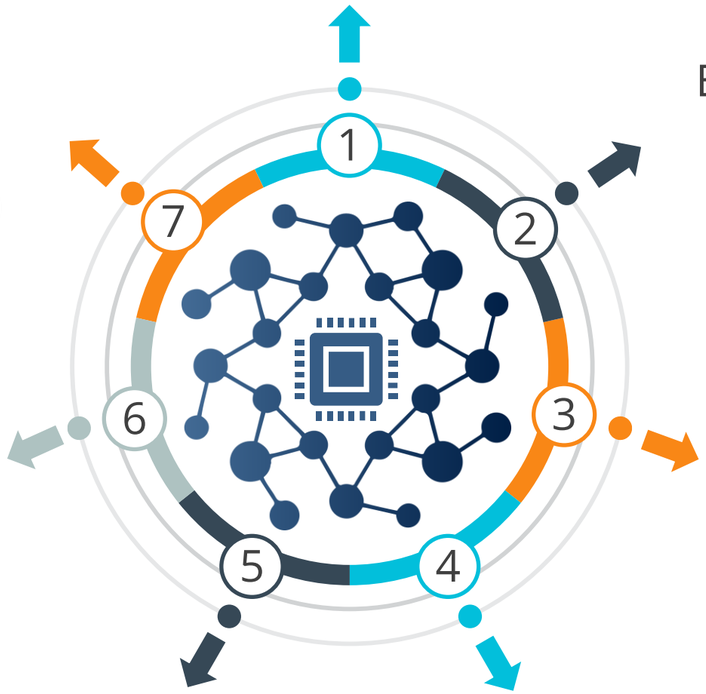
Link encryption

- Performed by the service provider, not the user
- Encrypting all data along a communication path
- Encrypting user information, headers, trailers, addresses, and routing data
- Decrypting and re-encrypting data packets at each node
- Example: A telephone circuit where user information, headers, trailers, addresses, and routing data are all encrypted

End-to-end encryption

- Performed by the end user
- Keeping data encrypted while it is in transit to the remote end
- Encrypting all data except the headers, addresses, routing, and trailer information
- Not needing to decrypt and re-encrypt packets at each hop because the headers and trailers are not encrypted
- Example: WhatsApp, enabling attackers to learn more about a captured packet and where it is headed

Data in Transit: Best Practices



1. Using Secure Socket Layer (SSL) or Transport Layer Security (TLS)
2. Encrypting messages before transmitting emails
3. Using Pretty Good Privacy (PGP) and Secure or Multipurpose Internet Mail Extensions (S/MIME) for email encryption
4. Using end-to-end encryption for intranet communication
5. Using Internet Protocol Security (IPSec) for secure Virtual Private Network (VPN) connectivity
6. Using Secure Shell (SSH) for the administration of network devices
7. Securing wireless networking with Wi-Fi Protected Access 2 (WPA 2)

Homomorphic Encryption

It is a powerful technique in cybersecurity that allows encrypted data to be processed securely.

- Converts data into ciphertext that can be analyzed and worked with as if in its original form
- Enables complex mathematical operations on encrypted data without compromising security
- Allows computations on encrypted data, enhancing the security of user data handled by third parties

Homomorphic encryption is a crucial advancement in data security, providing a balance between data utility and privacy.

Confidential Computing

It employs cryptography to protect data in use when it is processed in a cloud environment.

Trusted Execution Environment (TEE)

A TEE is used to decrypt data only when an authorized program attempts to access it.

Secure enclave

The TEE acts as a secure enclave, enforcing access controls to ensure only authorized applications can call for the protected data.

Malware protection

If a malware application attempts to access data in the TEE, it is denied access because it cannot view the keys needed to decrypt the data.

Distributed workloads

Confidential computing supports distributed workloads, such as edge computing, and can be deployed on edge devices to counteract failures of physical access controls.

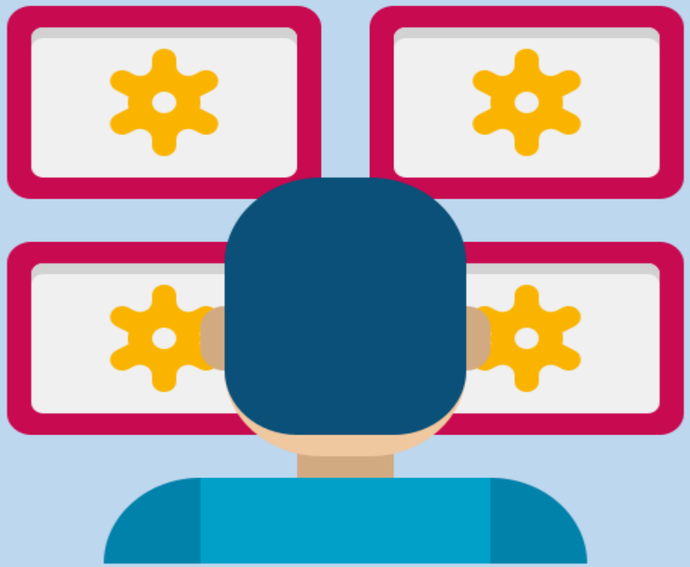
Monitoring

Monitoring is essential for maintaining the security and integrity of network and system activities.

Purpose: Keeping a watchful eye on network and system activities, constantly scanning for any anomalies or suspicious behavior.

Detection: Ensuring that any deviations from the norm are swiftly detected and addressed.

Logs and Alerts: Analyzing logs, traffic patterns, and system behavior to aid in threat detection and alert the security operations center.



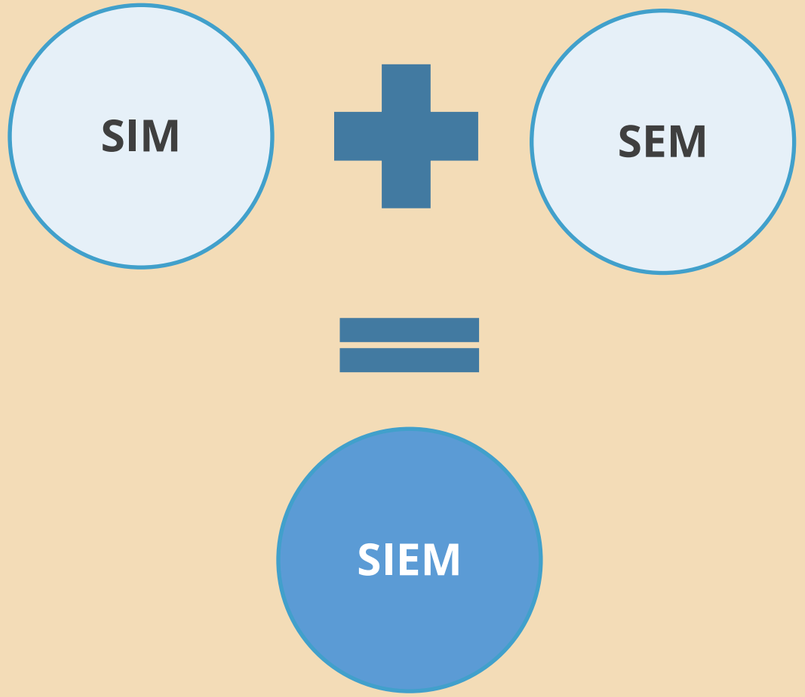
Security Information and Event Management

It is a comprehensive term encompassing software products and services designed to enhance cybersecurity.

The primary functions of SIEM technology include:

Combining Security Information Management (SIM) and Security Event Management (SEM): Merging software products and services that integrate SIM and SEM

Providing real-time analysis: Offering real-time analysis of security alerts generated by network hardware and applications



Security Information and Event Management

SIEM is composed of two primary components, each with distinct roles in cybersecurity. These components are:

Security Event Management (SEM):

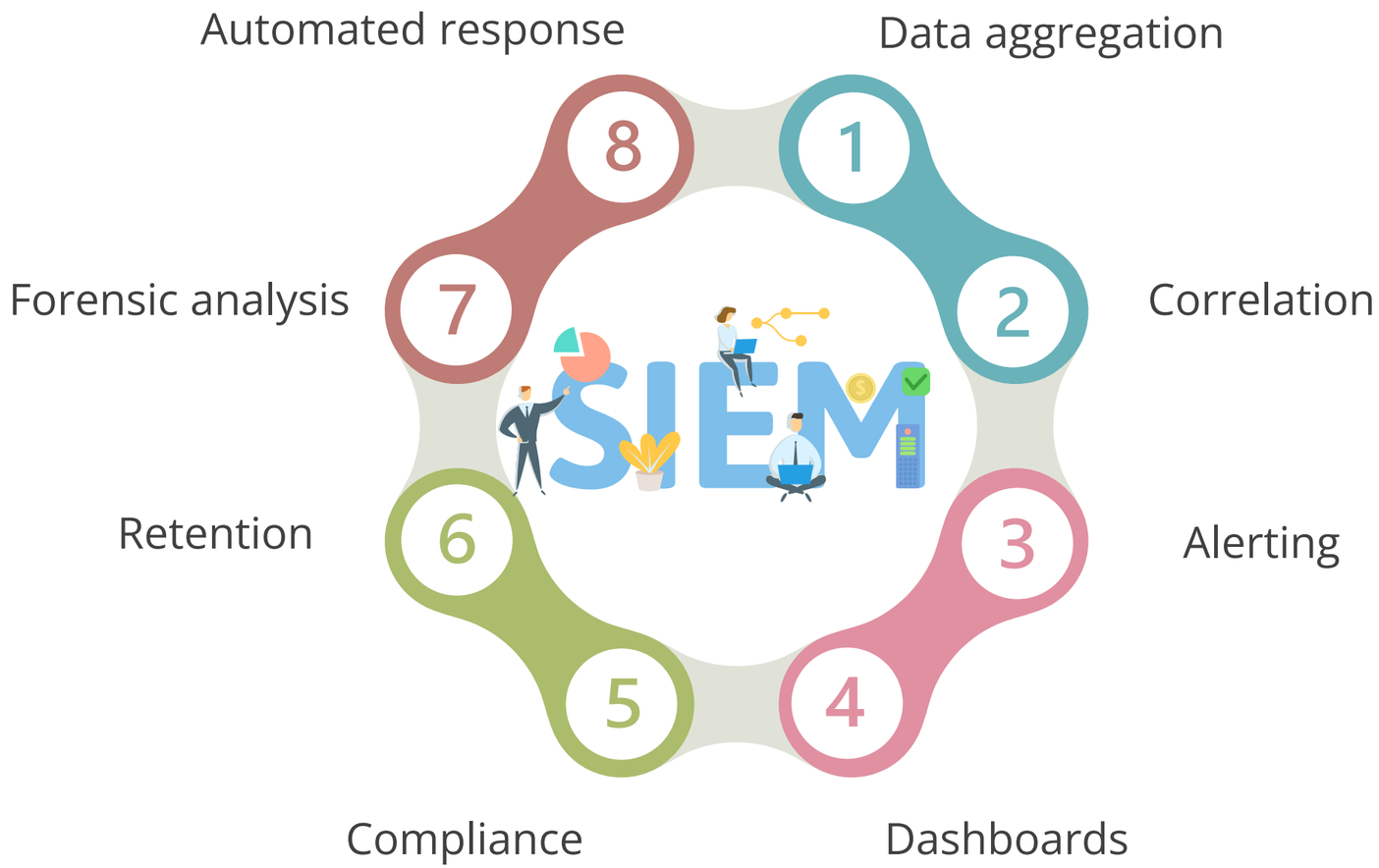
Manages real-time monitoring, event correlation, notifications, and console views

Security Information Management (SIM):

Provides long-term storage, analysis, and reporting of log data

SIEM Functionality

SIEM systems provide a range of critical functionalities to enhance cybersecurity. These functionalities include:



Security Orchestration, Automation, and Response (SOAR)

It is a stack of compatible software programs that enable organizations to:

Collect and aggregate data: Gather vast amounts of security data and alerts from a wide range of sources

Automate responses: Build automated processes to respond to low-level security events

Standardize procedures: Standardize threat detection and remediation procedures

SOAR Components

SOAR (Security Orchestration, Automation, and Response) comprises several key components that work together to enhance cybersecurity operations:

Security orchestration

- Integrates internal and external tools through custom integrations and APIs
- Connects systems like vulnerability scanners, endpoint protection, and firewalls

Security automation

- Ingests and analyzes data to create automated processes, replacing manual tasks
- Uses AI and machine learning to prioritize threats and automate responses

Security response

- Provides a unified view for planning, managing, and reporting security actions
- Facilitates collaboration and threat intelligence sharing
- Includes post-incident activities like case management and reporting

Need for SOAR in SIEM

Security Orchestration, Automation, and Response (SOAR) is essential for enhancing the capabilities of SIEM tools. The key reasons for the necessity of SOAR include:

Regular tuning	Differentiating between anomalous and normal activity
Consistent fine-tuning	Preventing overwhelming security teams with alerts
Dedicated staff	Managing rules to avoid confusing normal and suspicious activities
Data ingestion	Handling external data feeds beyond traditional logs

Configuration Enforcement

It ensures that digital systems and assets adhere to secure, predefined settings to minimize vulnerabilities. Key techniques include:

Standardization

Vulnerability mitigation

Compliance adherence

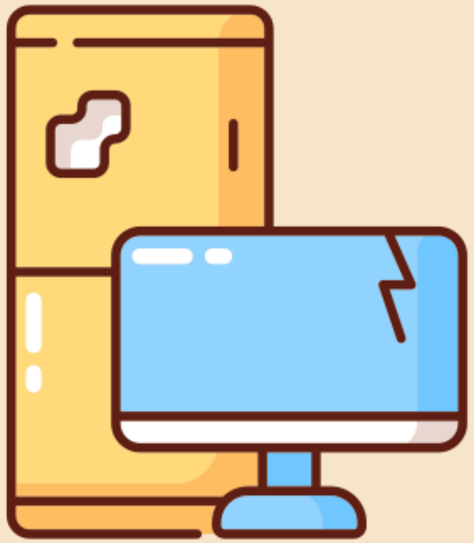
Automation

Decommissioning

It is the process of retiring assets that are no longer needed within an organization’s infrastructure. Important aspects to consider are:

Retiring assets: Involves removing legacy devices running obsolete operating systems or outdated hardware

Data sanitization: Ensures that any sensitive data stored on these devices is properly sanitized to prevent data breaches



Documentation

It is crucial in the decommissioning process to ensure a comprehensive and accountable record of all retired assets. Key steps include:

1

Updated asset register:

Keep an updated inventory of all assets, including decommissioned items

2

Detailed records:

Document dates, reasons, and responsible parties for the decommissioning process

3

Compliance and auditing:

Maintain records for compliance and auditing purposes

Decommissioning Process

Effective decommissioning involves proper sanitization methods to securely dispose of paper and media assets.

Paper sanitization

- **Best method:** Burning
- **Second-best:** Pulping (soaking in water and mechanically processing)
- **Least effective:** Shredding (use a cross-cut shredder for better results)

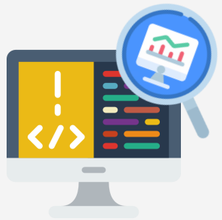
Media sanitization

- **Best method:** Shredding (e.g., metal hard drives)
- **Second-best:** Pulverizing with a sledgehammer
- **Least secure:** Degaussing (erasing magnetic fields)

Hardening

Hardening strengthens a system or network to reduce security risks and safeguard against cyber threats. Key techniques include:

Encryption



Endpoint detection and response

Disabling ports and protocols

Host-based IPS

Host-based firewall

Different Types of Hardening Techniques

System hardening

Secure the operating system by disabling unnecessary services, closing unused ports, enabling security features, and enforcing strong password policies

Network hardening

Secure the network with firewalls, intrusion detection and prevention systems, and network segmentation

Application hardening

Secure applications by removing unnecessary features, configuring security settings, and keeping applications up-to-date with security patches

Database hardening

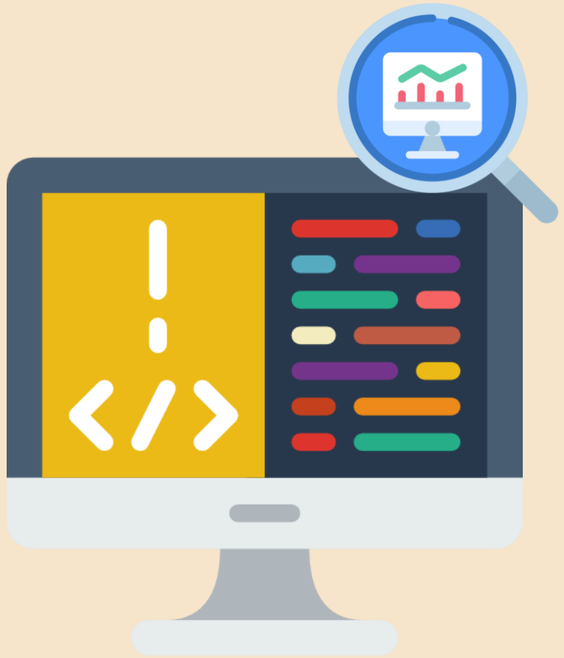
Secure databases with access control, data encryption, and regular backups

End Point Detection and Response

Endpoint Detection and Response (EDR) is a cybersecurity solution designed to monitor endpoints for malicious activity and respond to threats in real time.

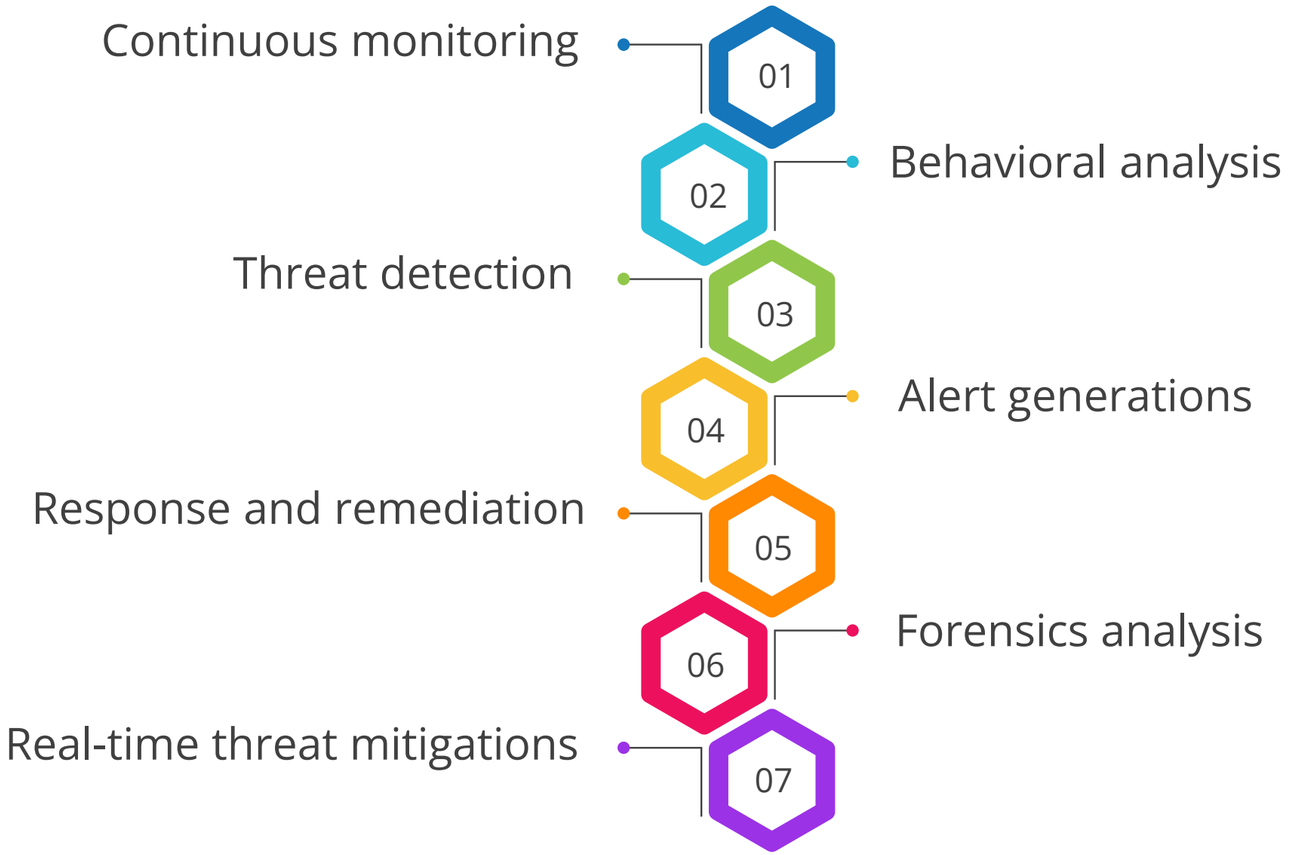
Real-time monitoring: Uses AI and ML technologies to detect and respond to threats

Comprehensive coverage: Monitors and protects infrastructure and network endpoints, including computers, servers, and mobile devices



Functions of EDR

It provides a comprehensive suite of functionalities to enhance cybersecurity. Key functions include:

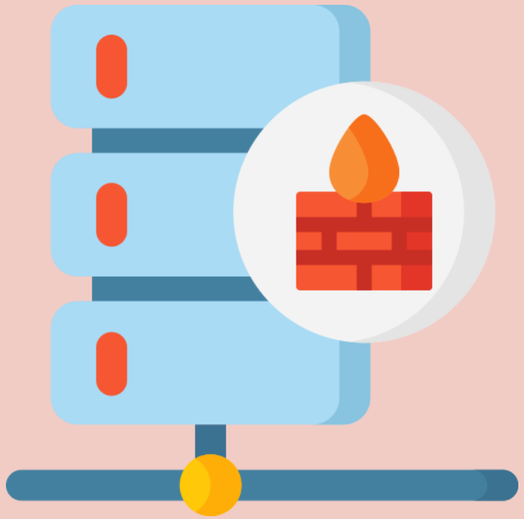


Host-Based Firewall

Host-based firewalls are software firewalls that run on individual devices to enhance security. Important aspects include:

Monitoring and control: Monitor and control incoming and outgoing network traffic at the device level to prevent unauthorized access and malicious activities

Remote protection: Protect laptops when users are working away from home



Host-Based Intrusion Prevention System

HIPS is a security solution designed to protect individual computer systems or hosts from unauthorized access, malicious activities, and cyber threats. Important aspects include:

Host-level operation: Monitors and analyzes the activities and behaviors of applications and processes running on a computer

Comprehensive protection: Guards against unauthorized access and malicious activities

Disabling Unused Ports

Disabling unused ports and protocols is a proactive measure to reduce the attack surface of a network. Key benefits include:

Reduced attack surface: Minimizes the avenues through which malicious actors can infiltrate by closing off unused or unnecessary communication pathways

Implementing Public Key Infrastructure

Duration: 10 Min.

Problem Statement:

As a system administrator, you are required to demonstrate the configuration and management of a Public Key Infrastructure (PKI). This involves installing and configuring Active Directory Certificate Services (ADCS) on Windows Server 2022. The goal is to establish a secure and efficient PKI environment for issuing, managing, and validating digital certificates within the organization.

Note: Refer to the demo document for detailed steps:
04_Implementing_Public_Key_Infrastructure

ASSISTED PRACTICE

Assisted Practice: Guidelines

Steps to be followed are:

1. Install certificate services
2. Configure active directory certificate services

Generating a Web Server Certificate

Duration: 10 Min.

Problem Statement:

As a system administrator, you are tasked with demonstrating the process of generating and managing web server certificates using Public Key Infrastructure (PKI). This includes installing Internet Information Services (IIS) on Windows Server 2022 and configuring it to serve a secure web page. The objective is to ensure the secure transmission of data between the server and clients by utilizing SSL/TLS certificates.

Note: Refer to the demo document for detailed steps:
05_Generating_a_Web_Server_Certificate

ASSISTED PRACTICE

Assisted Practice: Guidelines

Steps to be followed are:

1. Install Internet Information Services (IIS)
2. Create a secure website

Key Takeaways

- Understanding various threat actors and their motivations is essential for anticipating and countering security breaches effectively.
- Recognizing common threat vectors and attack surfaces enhances defensive strategies and helps prevent unauthorized access and data breaches.
- Identifying different types of vulnerabilities within systems is crucial for recognizing potential security weaknesses and implementing appropriate mitigation measures.
- Analyzing indicators of malicious activity allows for swift responses to security incidents, thereby minimizing potential damage and maintaining system integrity.
- Implementing effective mitigation techniques ensures robust security for enterprise operations.