CYBER SECURITY ESSENTIALS

UNIT 1: Security roles and security controls : information security roles, security control and framework

types, threat actor types and attack Vectors, Threat Intelligence Sources.

Performing security assessments : assess organizational security with network reconnaissance

tools, security concerns with general vulnerability types, vulnerability scanning techniques,

penetration testing concepts

Social engineering and malware : social engineering techniques, indicators of malware-based

attacks

- **Security roles and security controls** : information security roles, security control and framework types, threat actor types and attack Vectors, Threat Intelligence Sources.

Principles of Information Security

- The fundamental principles (tenets) of information security are ***confidentiality, integrity, and availability***.
- Every element of an information security program (and every security control put in place by an entity) should be designed to achieve one or more of these principles.
- Together, they are called the CIA Triad.


CONFIDENTIALITY
CIA
TRIAD
INTEGRITY
AVAILABILITY

- **Confidentiality** measures are designed to protect against unauthorized disclosure of information.
- The objective of the confidentiality principle is to ensure that private information remains private and that it can only be viewed or accessed by individuals who need that information in order to complete their job duties.

- **Integrity** involves protection from unauthorized modifications (e.g., add, delete, or change) of data.
- The principle of integrity is designed to ensure that data can be trusted to be accurate and that it has not been inappropriately modified.

- **Availability** is protecting the functionality of support systems and ensuring data is fully available at the point in time (or period requirements) when it is needed by its users.
- The objective of availability is to ensure that data is available to be used when it is needed to make decisions.

- Effectively executing all three tenets of the Security Triad creates an ideal outcome from an information security perspective.

- WHICH OF THE FOLLOWING IS NOT A PRINCIPLE OF INFORMATION SECURITY?
- a) INTEGRITY
- b) AUTHENTICATION
- c) CONFIDENTIALITY
- d) AVAILABILITY

- *Consider this example:* An organization obtains or creates a piece of sensitive data that will be used in the course of its business operations. Because the data is sensitive, that data should only be able to be seen by the people in the organization that need to see it in order to do their jobs. It should be protected from access by unauthorized individuals. This is an example of the *principle of confidentiality*.

- When the individual that needs that piece of data to perform a job duty is ready to utilize it, it must be readily accessible (i.e. online) in a timely and reliable manner so the job task can be completed on time and the company can continue its processing. This describes the *principle of availability*.

- And finally, the data will be used in calculations that affect business decisions and investments that will be made by the organization. Therefore, the accuracy of the data is critical to ensure the proper calculations and results upon which decisions will be made. The assurance that the data has **not been improperly tampered** with and therefore **can be trusted** when making the calculations and resulting decisions is the *principle of integrity*.

- Information Security Roles and Responsibilities
- Overall responsibility
  - Chief Security Officer (CSO)
  - Chief Information Security Officer (CISO)
- Managerial
- Technical
  - Information Systems Security Officer (ISSO)
- Non-technical
- Due care/liability

- Information Security Business **Units**
- Security Operations Center (SOC)
- DevSecOps
  - Development, security, and operations
- Incident response
  - Cyber incident response team (CIRT)
  - Computer security incident response team (CSIRT)
  - Computer emergency response team (CERT)

- security control and framework types

- **Security Control Categories**
- Technical
  - Controls implemented in operating systems, software, and security appliances
- Operational
  - Controls that depend on a person for implementation
- Managerial
  - Controls that give oversight of the system

- Security Control Functional Types
- Preventive
  - Physically or logically restricts unauthorized access
  - Operates before an attack
- Detective
  - May not prevent or deter access, but it will identify and record any attempted or successful intrusion
  - Operates during an attack
- Corrective
  - Responds to and fixes an incident and may also prevent its reoccurrence
  - Operates after an attack

- Physical
  - Controls such as alarms, gateways, and locks that deter access to premises and hardware
- Deterrent
  - May not physically or logically prevent access, but psychologically discourages an attacker from attempting an intrusion
- Compensating
  - Substitutes for a principal control

- Information Security Standards, Regulations, and Compliance, Authentication, Authorization, and Accounting (AAA)


REGULATIONS
STANDARDS
COMPLIANCE
RULES
LAW
POLICIES

Information Security Standards

- a level of quality
- OR
- a level of quality that you compare something else with

Information Security Regulations

- an official rule that controls how something is done
- OR
- the control of something by using rules

- Regulations are in place to help companies improve their information security strategy by providing guidelines and best practices based on the company's industry and type of data they maintain.
- Non-compliance with these regulations can result in severe fines, or worse, a data breach.

- Most companies are subject to at least one security regulation.
- The difficulty comes in determining which ones apply and interpreting what policies and controls are required to reach compliance.

- Part of that difficulty is because regulations are not written in a way that can be easily **understood** by the average person.
- Often, partnering with a *security professional* is necessary to decode relevant requirements and devise an implementation plan.
- These professionals have **experience** implementing systems, policies, and procedures to satisfy the requirements of various regulations and enhance the security of an organization.

- Many(*security professional)* have obtained credentials, such as the HISP (Holistic Information Security Practitioner), that signifies they have a deeper understanding of the system controls required to reach compliance.

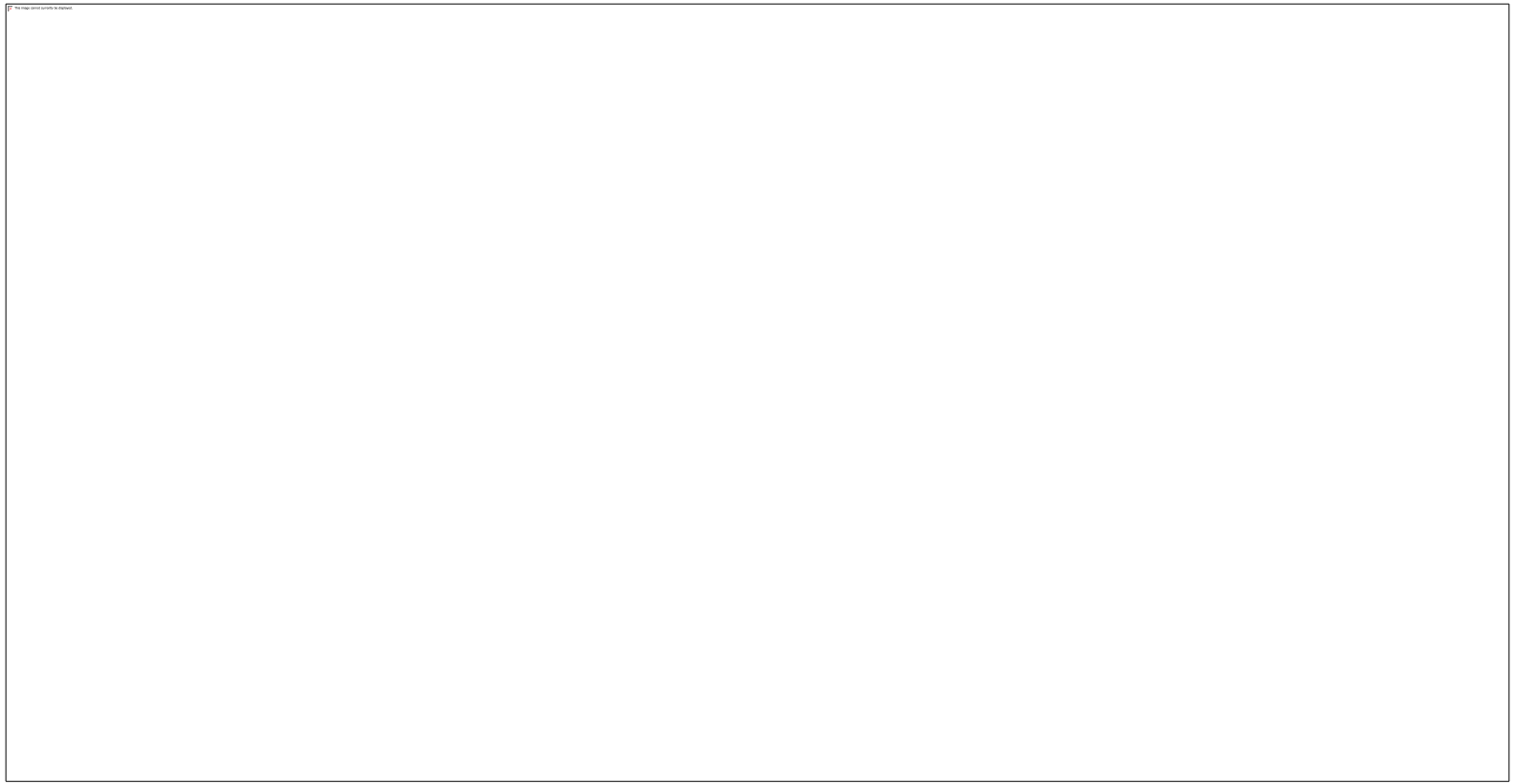
Information Security Compliance

- the act of obeying an order, rule, or request
- OR
- the act or process of doing what you have been asked or ordered to do

- **Information Security Compliance: Which regulations relate to me?**

- Assessing which rules and regulations apply to an organization is no easy feat.
- Often, organizations need to comply with multiple frameworks and regulations, many of which have overlapping qualities.

- This entry is part of a series of information security compliance articles. In subsequent articles we will discuss the specific regulations and cybersecurity frameworks, describing their precise applications. These include, but are not limited to:



- EXAMPLE:
- Think of a local hospital. It does deal with patients and other healthcare-related data.

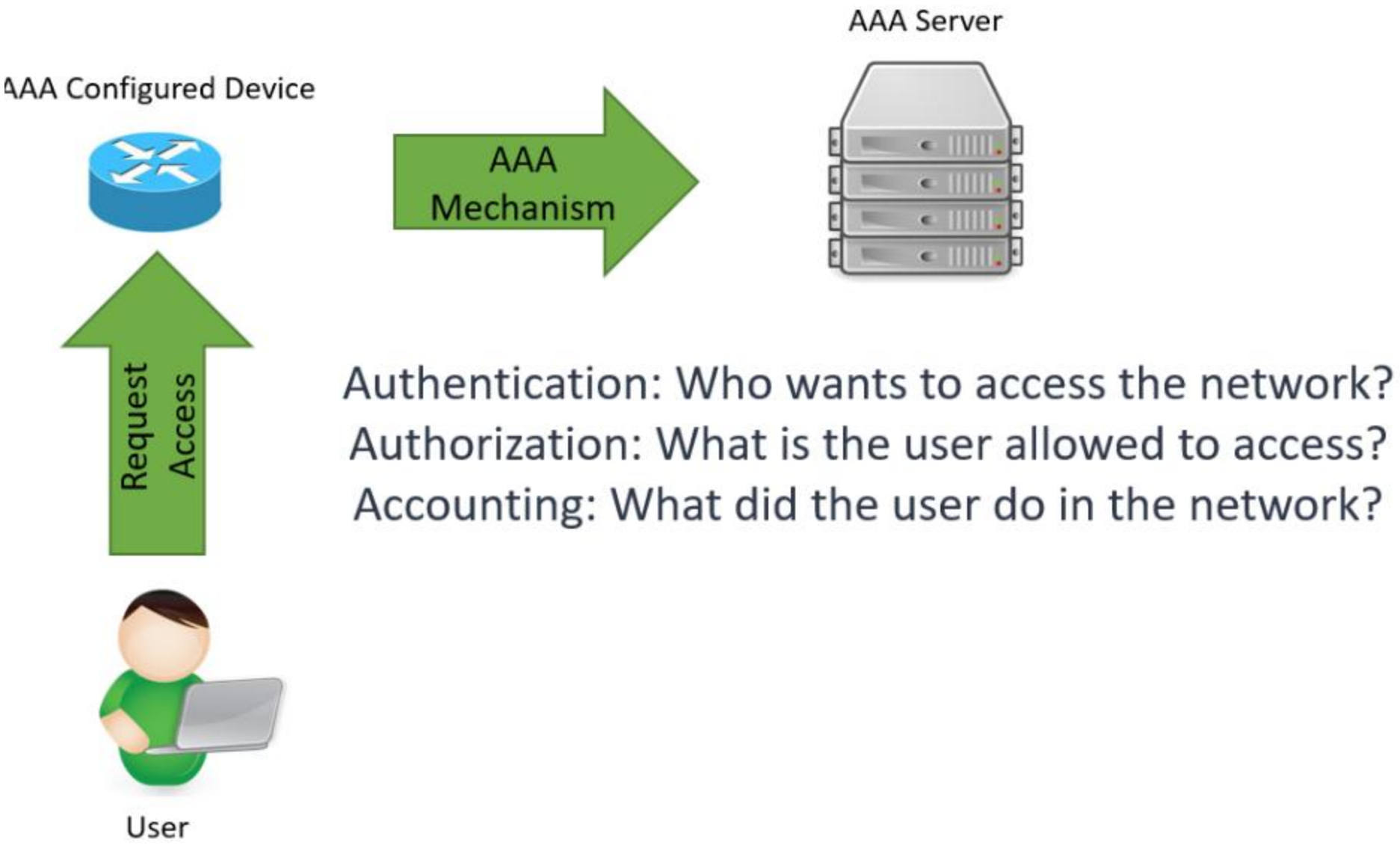
- With the regulation identified, the hospital must look carefully at what sort of protection it must offer patients and place safeguards in effect to prevent a breach of security. On the ground level, it cannot give away information without the express consent of the patient.

- While the example of the local hospital only had to comply with one regulation, companies often find they must meet the requirements of many regulations.
- In such cases, the best method to approach the situation is to outline all of the regulations that will impact the company first, and then determine which security controls need to be implemented to satisfy all of the requirements effectively.

- There are often overlapping requirements built into different regulations, so by breaking it down into two phases, companies can reduce the amount of time and money they would otherwise spend by reducing the duplicate effort of implementing competing systems.

- AAA


Authentication
user name
******
LOGIN
Who are you?
Validate a system is accessing by the right person
Authorization
Are you allowed to do that?
Check users' permissions to access data


AAA Server
AAA Configured Device
AAA
Mechanism
Request
Access
Authentication: Who wants to access the network?
Authorization: What is the user allowed to access?
Accounting: What did the user do in the network?
User

- **Authentication –**
  The process by which it can be identified that the user, which wants to access the network resources, **VALID OR NOT** by asking some credentials such as username and password.
- As network administrators, we can control how a user is authenticated if someone wants to access the network.
- Some of these methods include using the local database of that device (router) or sending authentication requests to an external server.


Username or email
login

- **Authorization –**
  It provides capabilities to enforce policies on network resources after the user has gained access to the network resources through authentication.
- After the authentication is successful, authorization can be used to determine what resources is the user allowed to access and the operations that can be performed.

- **For example**, if a junior network engineer (who should not access all the resources) wants to access the device then the administrator can create a view that will allow particular commands only to be executed by the user (the commands that are allowed in the method list).
- The administrator can use the authorization method list to specify how the user is authorized to network resources i.e through a local database or ACS server.

- **Accounting –**
  It provides means of monitoring and capturing the **events done** by the user while accessing the network resources. It even monitors **how long** the user has access to the network. The administrator can create an accounting method list to specify **what should be accounted for** and to whom the accounting records should be sent.


AAA Security framework for controlling access
Authentication
Proving and granting access
Authorization
Control what level of access is required
Accounting
Tracking and auditing access and capabilities

- threat actor types and attack Vectors

- Hackers, Script Kiddies, and Hacktivists
  - The “Lone Hacker”
    - White hats versus black hats versus gray hats
    - Authorized versus non-authorized versus semi-authorized
  - Script kiddies
  - Hacker teams and hacktivists

- **Black hat hackers** are **criminals** who break into computer networks with malicious intent. They may also release malware that destroys files, holds computers hostage, or steals passwords, credit card numbers, and other personal information.

- Black hats are motivated by self-serving reasons, such as financial gain, revenge, or simply to spread havoc. Sometimes their motivation might be ideological, by targeting people they strongly disagree with.

- Some black hat organizations even have call centers, which they use to make outbound calls, pretending to work for a well-known technology organization such as Microsoft.
- In this scam, the hacker tries to convince potential victims to allow remote access to their computers or download software. By granting access or downloading the recommended software, the victim inadvertently enables criminals to harvest passwords and banking information or take over the computer and use it to launch attacks on others.

- One of the most famous black hat hackers is Kevin Mitnick, who, at one point, was the most wanted cybercriminal in the world. As a black hat hacker, he hacked into over 40 major corporations, including IBM and Motorola, and even the US National Defense warning system. He was subsequently arrested and served time in jail. Following his release, he became a cybersecurity consultant who uses his hacking knowledge for white hat hacking purposes.

- **White hat hackers** – sometimes also called “ethical hackers” or “good hackers” – are the antithesis of black hats. They exploit computer systems or networks to identify their security flaws so they can make recommendations for improvement.

- White hat hackers use their capabilities to uncover security failings to help safeguard organizations from dangerous hackers.

- White hat hacker tactics and skills include:
- **1. Social engineering**
- White hat hackers commonly use social engineering (“people hacking”) to discover weaknesses in an organization’s “human” defenses. Social engineering is about tricking and manipulating victims into doing something they should not (making wire transfers, sharing login credentials, and so on).
- **2. Penetration testing**
- Penetration testing aims to uncover vulnerabilities and weaknesses in an organization’s defenses and endpoints so they can be rectified.

- **3. Reconnaissance and research**
- This involves researching the organization to discover vulnerabilities within the physical and IT infrastructure. The objective is to gain enough information to identify ways to legally bypass security controls and mechanisms without damaging or breaking anything.
- **4. Programming**
- White hat hackers create honeypots that serve as decoys to lure cybercriminals to distract them or help the white hats gain valuable information about the attackers.

- **honeypots :** It mimics a target for hackers, and uses their intrusion attempts to gain information about cybercriminals and the way they are operating or to distract them from other targets.

- **5. Using a variety of digital and physical tools**
- This includes hardware and devices that allow the penetration testers to install bots and other malware and gain access to the network or servers.

- Somewhere between white and black are **gray hat hackers**. Gray hat hackers enact a blend of both black hat and white hat activities. Gray hat hackers often look for vulnerabilities in a system without the owner's permission or knowledge. If issues are found, they report them to the owner, sometimes requesting a small fee to fix the problem.

- Some gray hat hackers like to believe they are doing something good for companies by hacking their websites and invading their networks without permission. Still, company owners rarely appreciate unauthorized forays into their business information infrastructure.
- Often, a gray hat's real intention is to show off their skills and gain publicity — maybe even appreciation — for what they consider a contribution to cybersecurity.

- **Script Kiddies:** a hacker or cracker who uses pre-written scripts or existing programmes to uncover vulnerabilities in target systems. These users frequently are unaware of the complexity of the scripts they are running and the harm they cause as a result.

- **Hacktivists:** Groups of criminals known as hacktivists collaborate to **launch cyberattacks** in favour of political causes.

- Attack Surface and Vectors
  - Attack surface
    - Points where an attacker can discover/exploit vulnerabilities in a network or application
  - Vectors
    - Direct access
    - Removable media
    - Email
    - Remote and wireless
    - Supply chain
    - Web and social media
    - Cloud

Threat Intelligence Sources

- **Threat Intelligence:** Digital technologies lie at the heart of nearly every industry today.
- The automation and greater connectedness they afford have revolutionized the world's economic and cultural institutions — but they've also brought risk in the form of cyberattacks.
- **Threat intelligence is knowledge that allows you to prevent or mitigate those attacks.**
- Rooted in data, threat intelligence provides context — like who is attacking you, what their motivation and capabilities are, and what indicators of compromise in your systems to look for — that helps you make informed decisions about your security.

- ***Threat intelligence*** *is evidence-based knowledge, including context, mechanisms, indicators, implications and action-oriented advice about an existing or emerging menace or hazard to assets.*

- Threat Intelligence Sources:
  - *Threat Intelligence* Feeds
  - subscription-based threat intelligence platforms

- **Performing security assessments** : assess organizational security with network reconnaissance tools, security concerns with general vulnerability types, vulnerability scanning techniques, penetration testing concepts

- assess organizational security with network reconnaissance tools:
- ipconfig/ifconfig/ip, ping,
- and arp: The **arp** command displays and modifies the Internet-to-adapter address translation tables.

- route and tracert/traceroute
- pathping/mtr
- Pathping: provides statistics for latency and packet loss along a route over a longer measuring period. pathping is a Windows tool; the equivalent on Linux is **mtr**.
- IP Scanners: An IP scanner performs host discovery and identifies how the hosts are connected together in an internetwork.

- and Nmap: The **Nmap Security Scanner** (nmap.org) is one of the most popular open-source IP scanners. Nmap can use diverse methods of host discovery, some of which can operate stealthily and serve to defeat security mechanisms such as firewalls and intrusion detection. The tool is open-source software with packages for most versions of Windows, Linux, and macOS. It can be operated with a command line or via a GUI (Zenmap).
- If a host is detected, Nmap performs a port scan against that host to determine which services it is running.

- Service Discovery: Having identified active IP hosts on the network and gained an idea of the network topology, the next step in network reconnaissance is to work out which operating systems are in use, which network services each host is running, and, if possible, which application software is underpinning those services. This process is described as **service discovery**.
- and Nmap

- Netstat: show the state of TCP/UDP ports on the local machine.

- and nslookup: The **nslookup** command queries internet domain name servers.

- Other Reconnaissance and Discovery Tools:
- theHarvester: **theHarvester** is a tool for gathering open-source intelligence (OSINT) for a particular domain or company name (github.com/laramies/theHarvester). It works by scanning multiple public data sources to gather emails, names, subdomains, IPs, URLs and other relevant data.

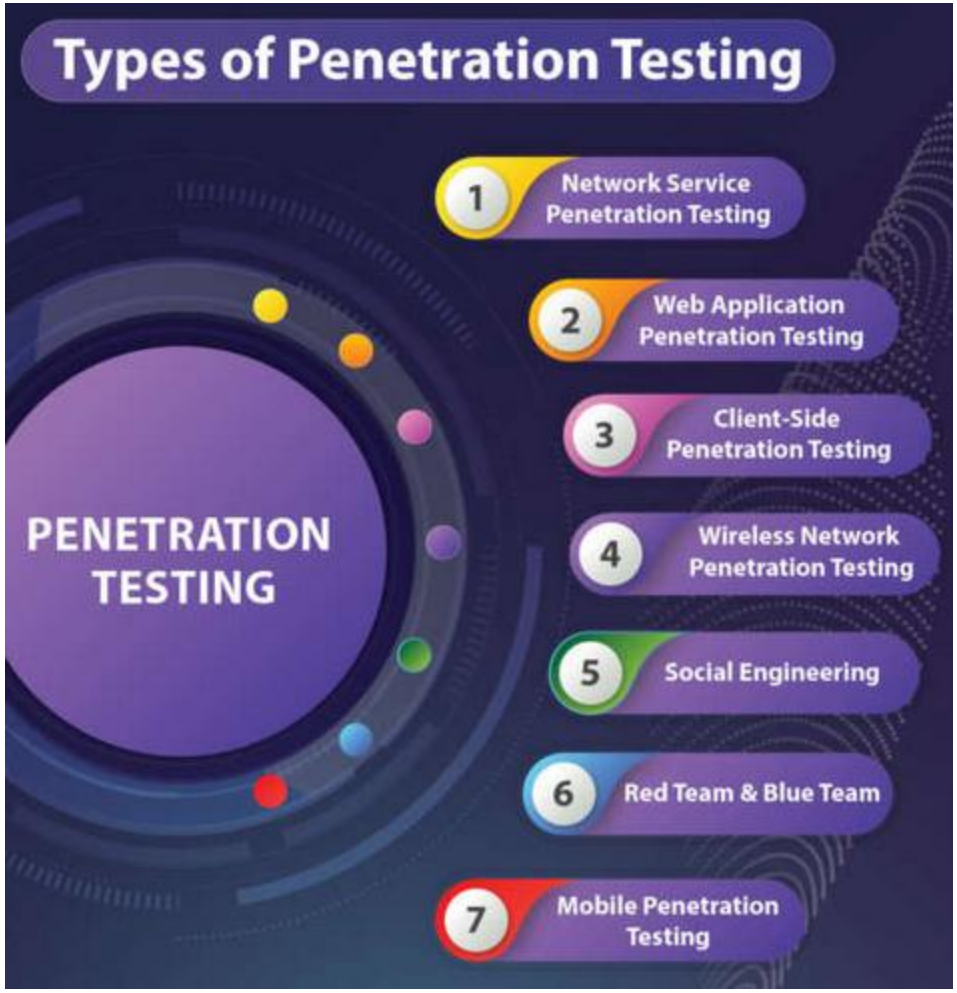
- Dnsenum: dnsenum packages a number of tests into a single query.
- scanless
- curl
- Nessus
- Packet Capture and tcpdump
- Packet Analysis and Wireshark
- Packet Injection and Replay
- hping
- Tcpreplay
- Metasploit
- Sn1Per
- Netcat

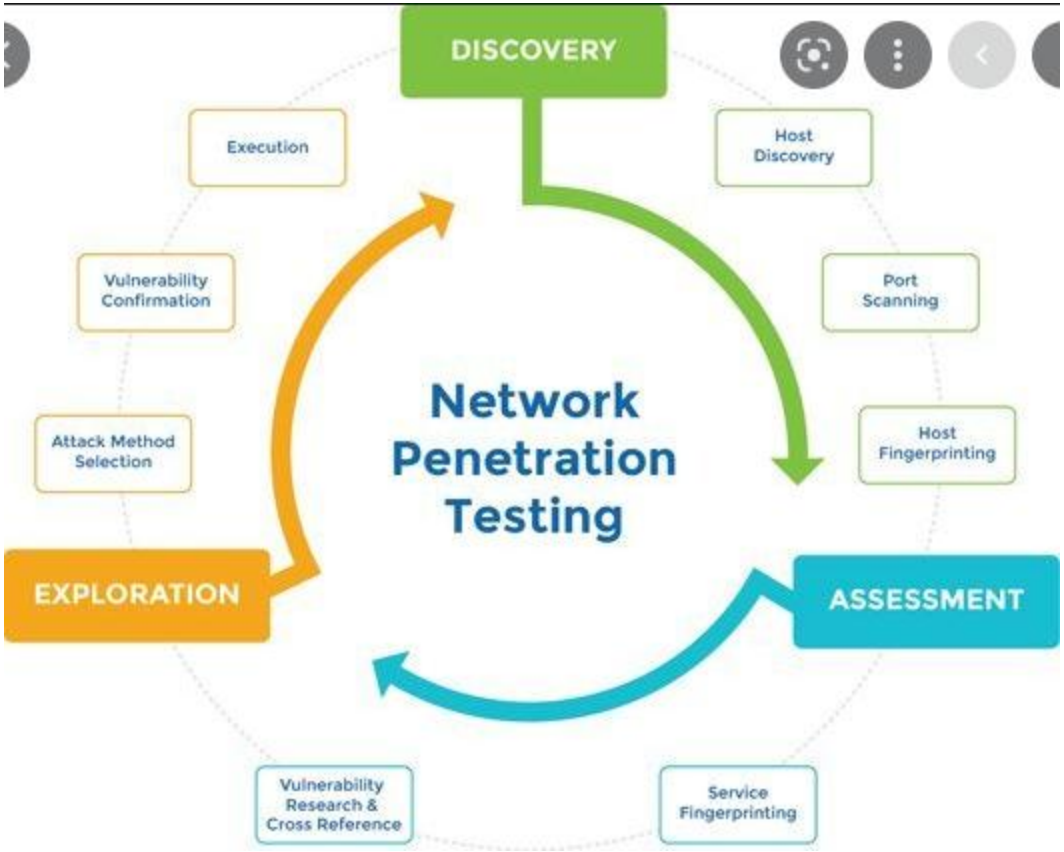
- security concerns with general vulnerability types:
- Software Vulnerabilities and Patch Management
- Zero-day and Legacy Platform Vulnerabilities
- Weak Host Configurations
- Weak Network Configurations

- vulnerability scanning techniques:
- Intrusive versus Non-intrusive Scanning
- Credentialed versus Non-credentialed Scanning
- False Positives, False Negatives, and Log Review
- Threat Hunting

penetration testing concepts

- This service gives you knowledge about current security defects, assesses the efficiency of security measures already in place, and gives you the ability to take further activities to address identified issues and boost security.


Types of Penetration Testing
PENETRATION TESTING
1
Network Service Penetration Testing
2
Web Application Penetration Testing
3
Client-Side Penetration Testing
4
Wireless Network Penetration Testing
5
Social Engineering
6
Red Team & Blue Team
7
Mobile Penetration Testing


DISCOVERY
Host Discovery
Port Scanning
Host Fingerprinting
ASSESSMENT
Service Fingerprinting
Vulnerability Research & Cross Reference
EXPLORATION
Attack Method Selection
Vulnerability Confirmation
Execution
Network Penetration Testing

WEB APPLICATION PENETRATION TESTING STEPS & METHODS

Step 1:
INFORMATION GATHERING

Step 2:
RESEARCH & EXPLOITATION

Step 3:
REPORTING & RECOMMENDATIONS

Step 4:
REMEDIATION & SUPPORT

- Pen Test Attack Life Cycle

- The penetration testing process typically goes through five phases:
  - Planning and reconnaissance,
  - scanning,
  - gaining system access,
  - persistent access,
  - and the final analysis/report.

- **Social engineering and malware** : social engineering techniques, indicators of malware-based attacks

social engineering techniques

- ***What is social engineering?***

- Social engineering involves both face-to-face and written interaction.

- Instead of using technical hacking, social engineering uses human nature to trick people into risking their own or their company's security.

- Social engineering tricks people into paying money to criminals, sending information they shouldn't transmit, installing software they shouldn't download, visiting websites they shouldn't visit, and other blunders that compromise their security or that of their organisations.

- Social engineering is frequently referred to as

"human hacking"

since it *targets human weaknesses* rather than flaws in technical or digital systems.

Any student have been subjected to social engineering attempt and what the experience was like.

- Social Engineering Principles:
  - **Reciprocity -** An attacker's act of friendliness compels the victim to reciprocate by providing sensitive information demands.
  - **Commitment and Consistency -** Even if they know it shouldn't be done, an employee still complies with an attacker's request for login credentials because they first consented to provide it.
  - **Social Proof -** Individuals frequently replicate what other people do.

- **Authority -** An intruder assumes the identity of an authoritative figure, either from the target organisation or from society at large, such as a police officer, attorney, etc.
- **Liking -** People are easily influenced by those they like.
- **and Scarcity -** An attacker claims to urgently want a set of credentials in order to access company software and finish a sales call that is about to expire.

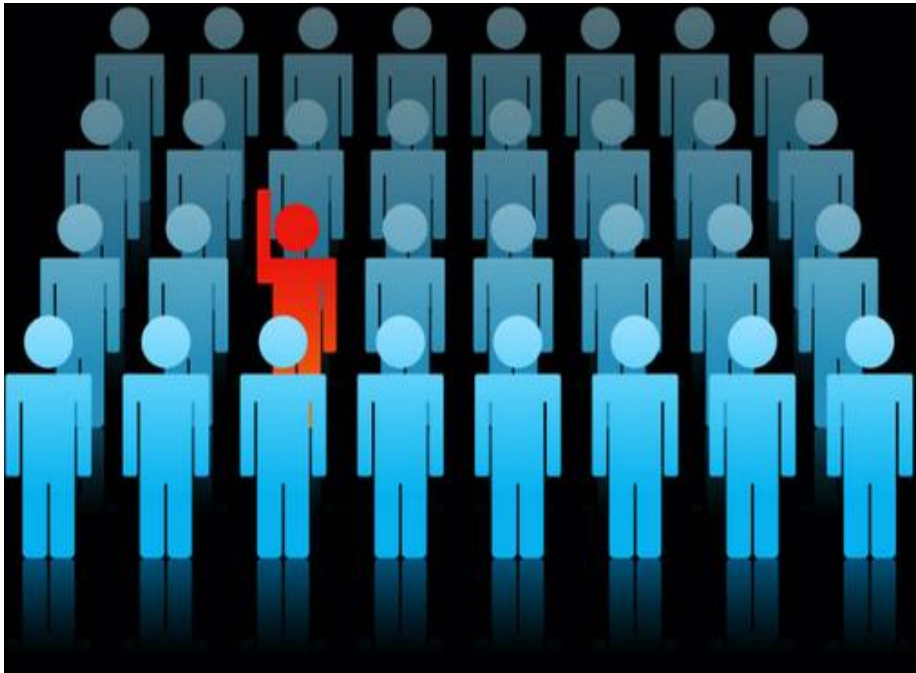
- indicators of malware-based attacks

- Analyze probable indicators to identify the kind of attack given a scenario.

There are four main kinds of network threats:

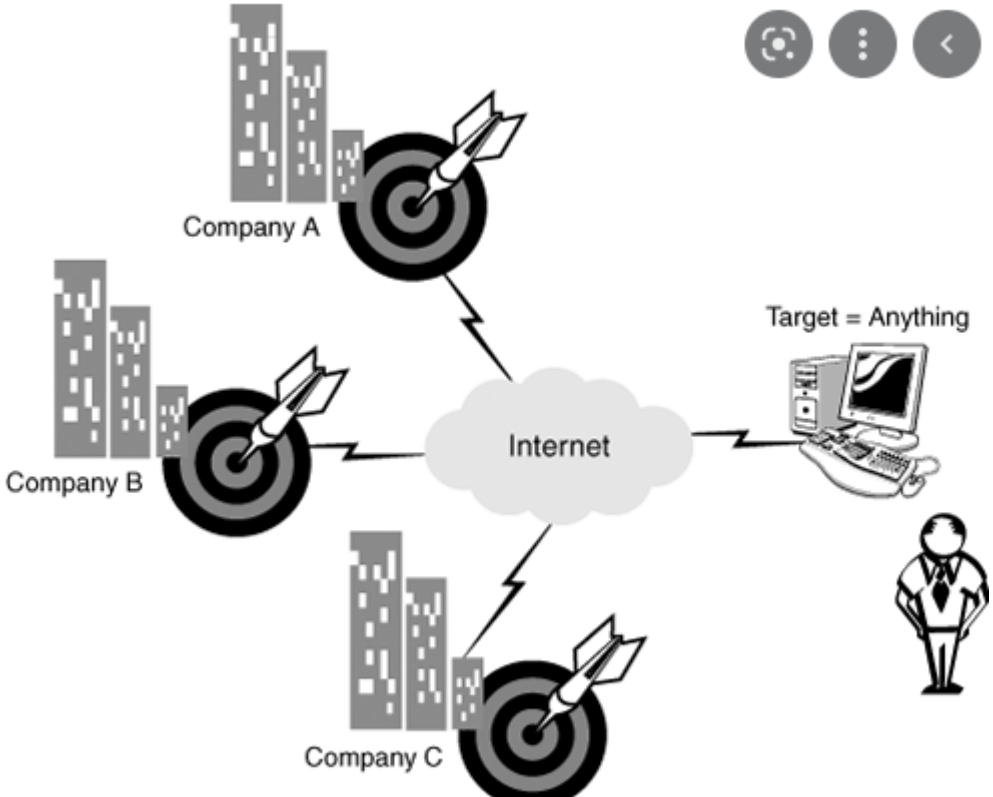
- **External threats:** Threats made by outside organizations or individuals, attempting to get into your network.

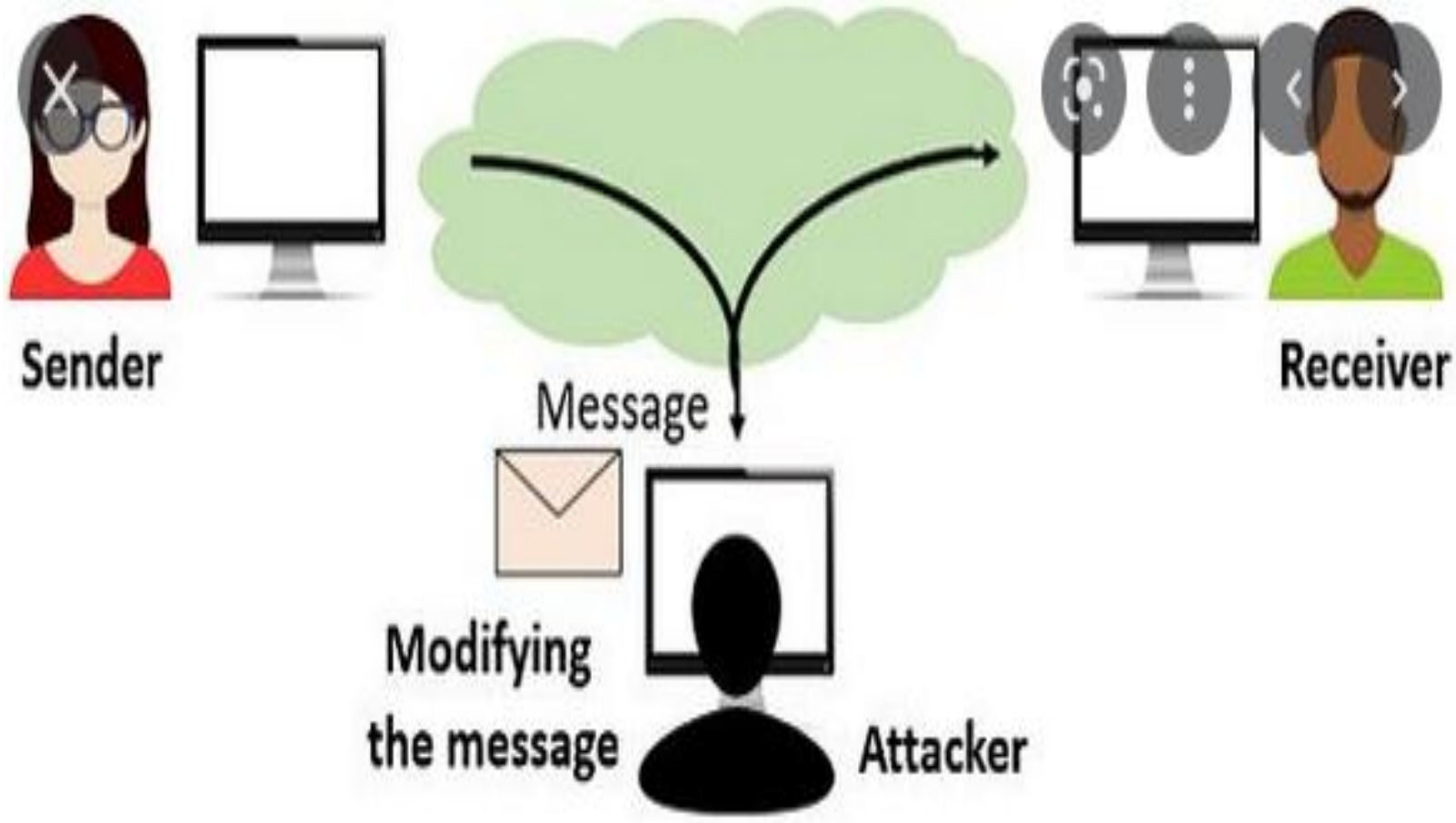
- **Internal threats:** These are threats from malicious insiders, such as disgruntled or improperly vetted employees who are working for someone else.



- **Structured threats**: **Organized** attacks by attackers who know what they're doing and have a clear aim or goal in mind.

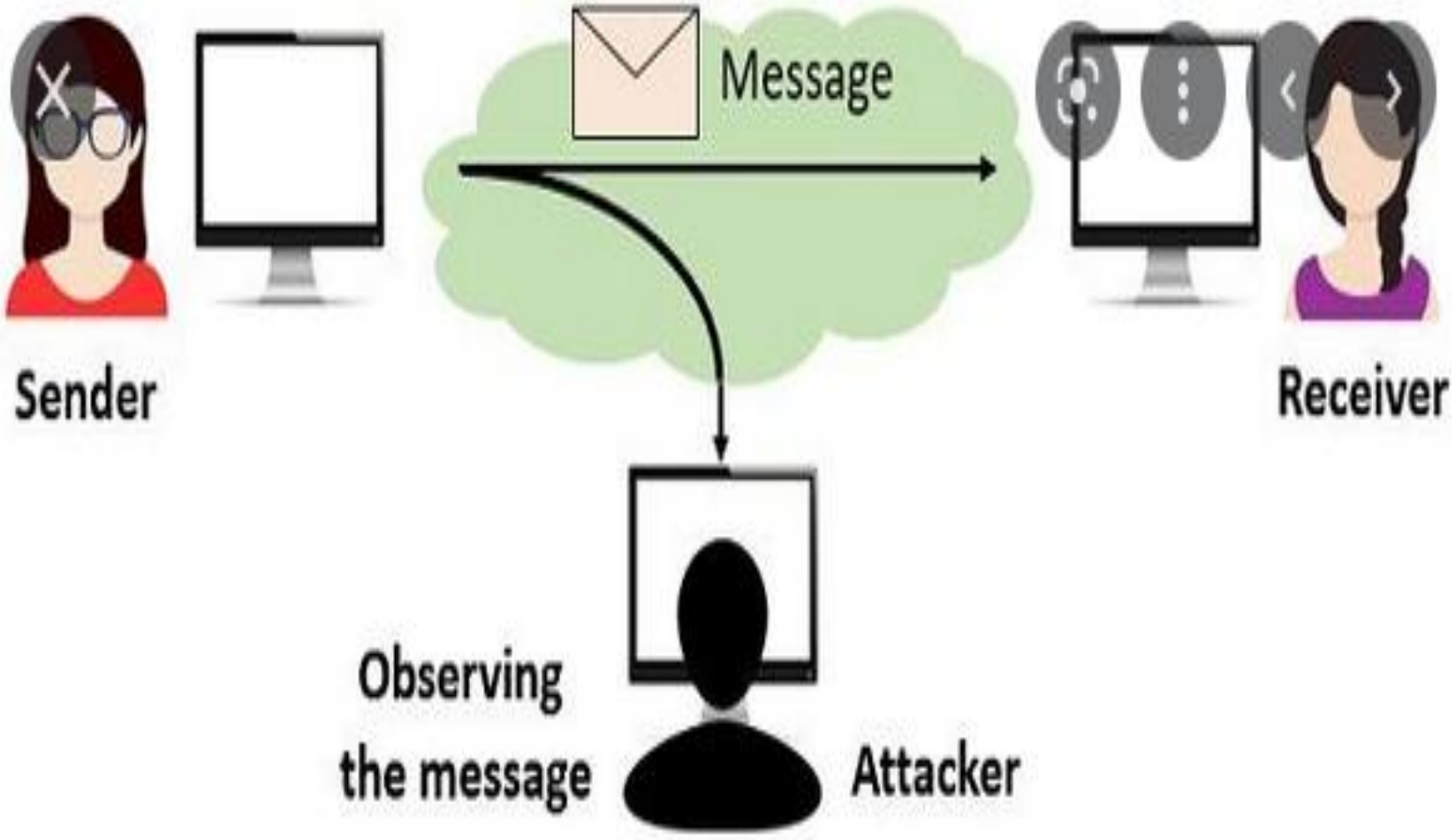
- **Unstructured attacks:** Disorganized attacks, often by amateurs with no concrete goal in mind.





Active Attack

593 × 270

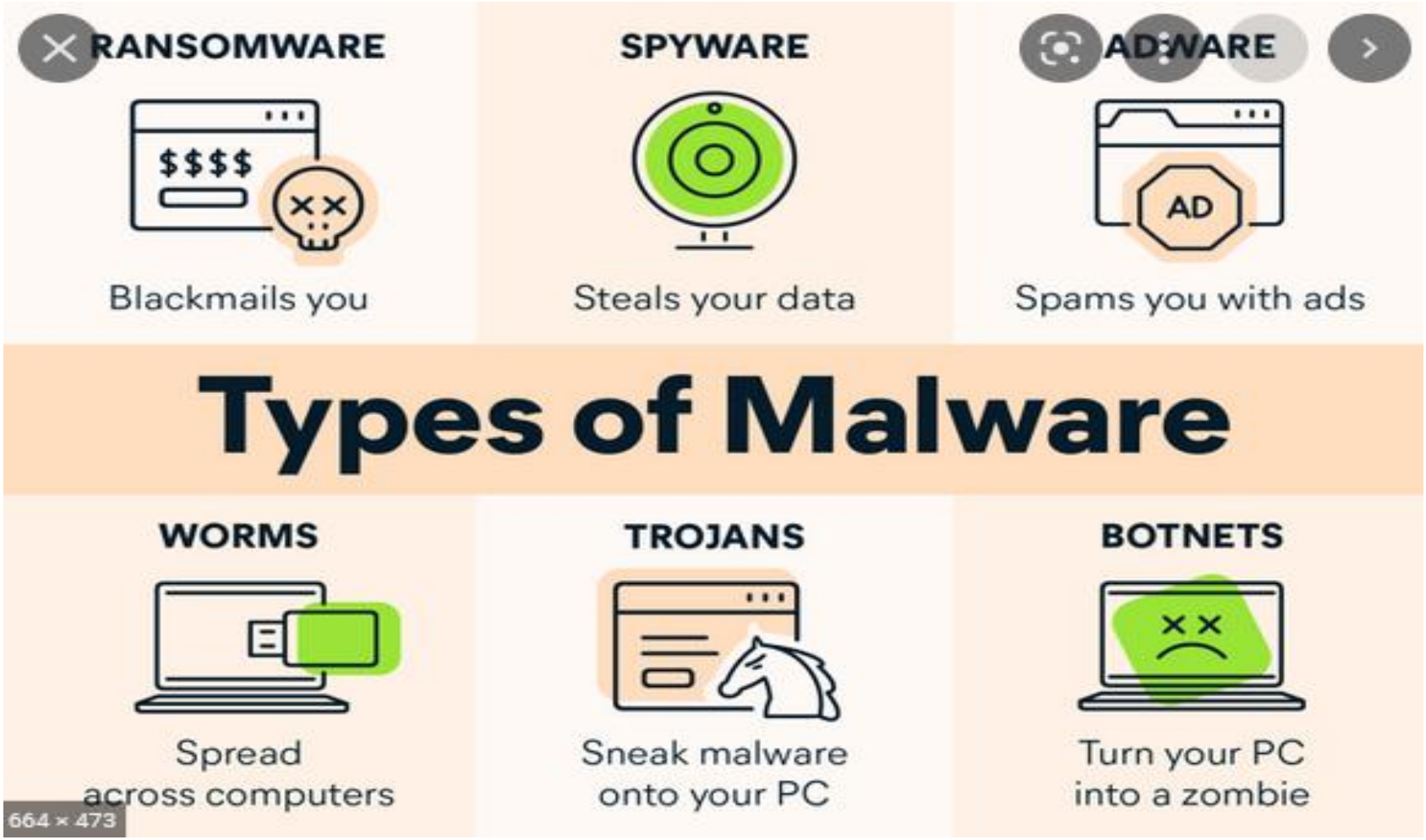


Passive Attack

Some common types of cyber security attacks

1. Malware
2. Phishing
3. Man-in-the-Middle (MitM) Attacks
4. Denial-of-Service (DOS) Attack
5. SQL Injections
6. Zero-day Exploit
7. Password Attack
8. Cross-site Scripting
9. Rootkits
10. Internet of Things (IoT) Attacks

1. Malware


RANSOMWARE
$$$$
Blackmails you
SPYWARE
Steals your data
ADWARE
AD
Spams you with ads
Types of Malware
WORMS
Spread across computers
TROJANS
Sneak malware onto your PC
BOTNETS
Turn your PC into a zombie
664 × 473

- **Viruses**—these infect applications attaching themselves to the initialization sequence. The virus replicates itself, infecting other code in the computer system. Viruses can also attach themselves to executable code or associate themselves with a file by creating a virus file with the same name but with an .exe extension, thus creating a decoy which carries the virus.

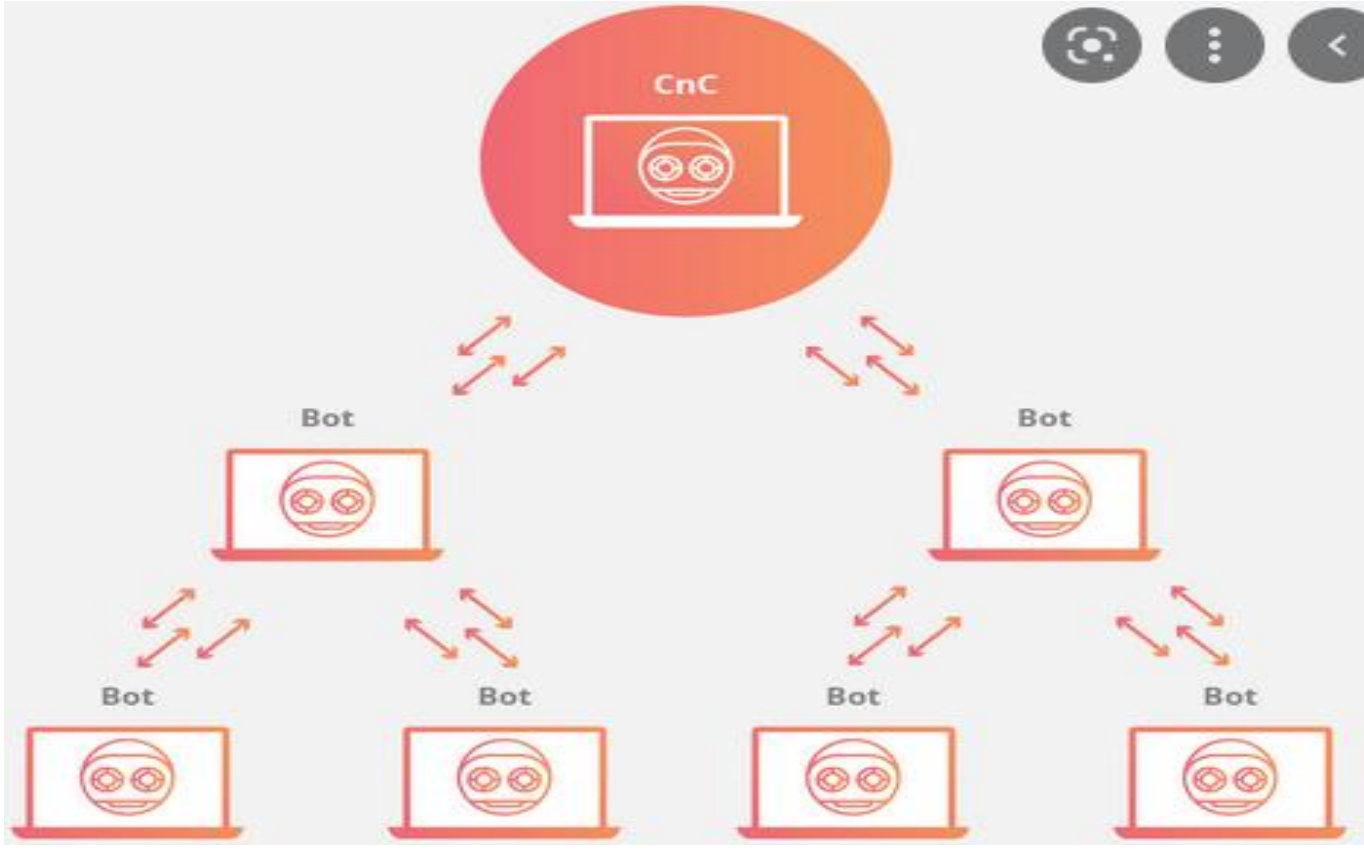
- **Trojans**–a program hiding inside a useful program with malicious purposes. Unlike viruses, a trojan doesn't replicate itself and it is commonly used to establish a backdoor to be exploited by attackers.

- **Worms**—unlike viruses, they don't attack the host, being self-contained programs that propagate across networks and computers. Worms are often installed through email attachments, sending a copy of themselves to every contact in the infected computer email list. They are commonly used to overload an email server and achieve a denial-of-service attack.

- **Ransomware**—a type of malware that denies access to the victim data, threatening to publish or delete it unless a ransom is paid. Advanced ransomware uses cryptoviral extortion, encrypting the victim's data so that it is impossible to decrypt without the decryption key.

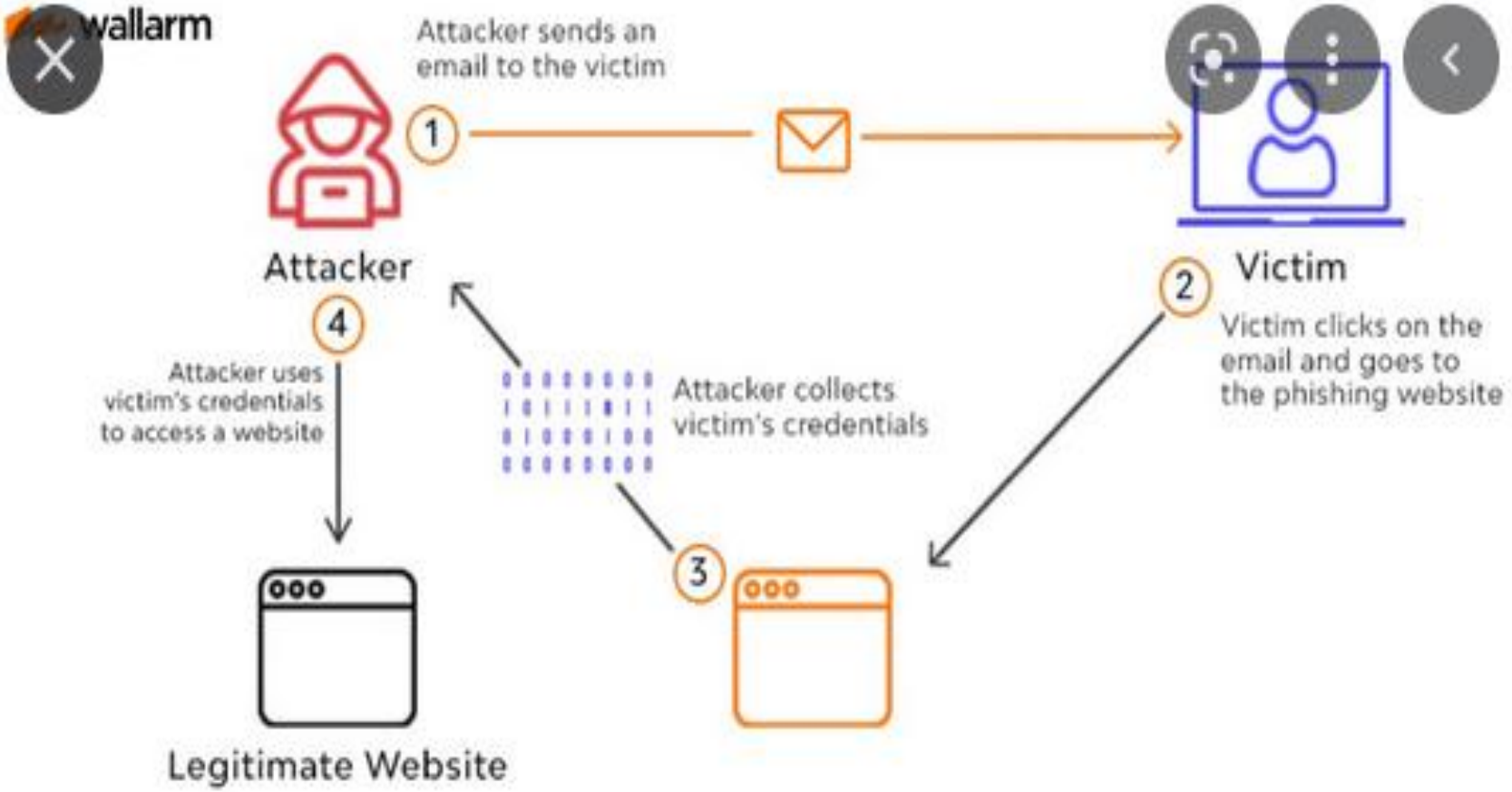
- **Spyware**—a type of program installed to collect information about users, their systems or browsing habits, sending the data to a remote user. The attacker can then use the information for blackmailing purposes or download and install other malicious programs from the web.

- A botnet is a network of infected computers that can be controlled remotely and forced to send spam, spread malware, or stage DDoS attacks — without the consent of the device owners.



- A botnet is a group of computers linked together with malware and controlled by the botnet creator, known as a *bot herder*. Bot herders infect computers to form botnets, which they control as a group to initiate wide-scale cyberattacks, send spam, and conduct phishing campaigns.

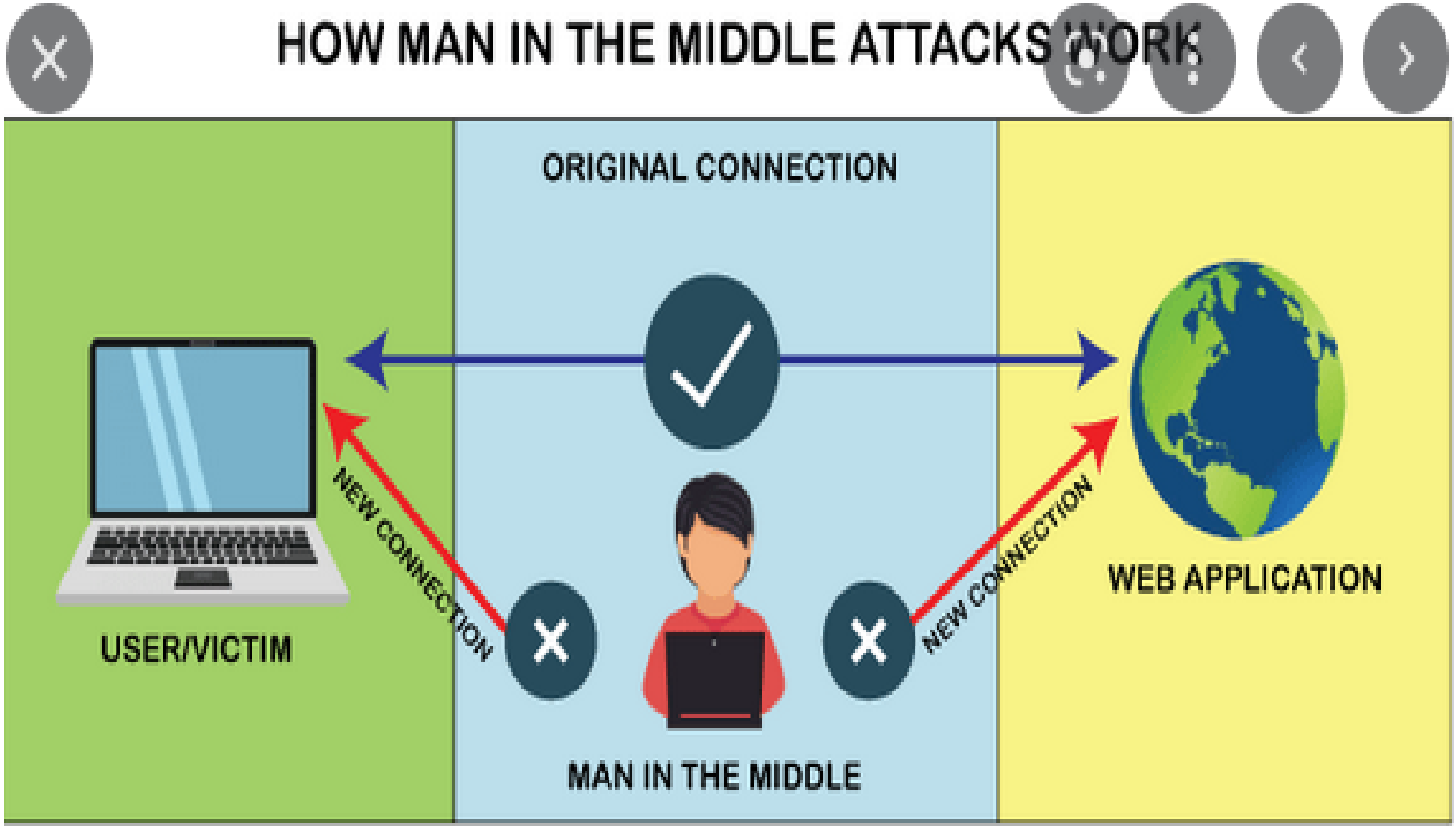
2. Phishing


wallarm
Attacker sends an email to the victim
1
Attacker
Victim
2
Victim clicks on the email and goes to the phishing website
4
Attacker uses victim's credentials to access a website
Attacker collects victim's credentials
3
Legitimate Website

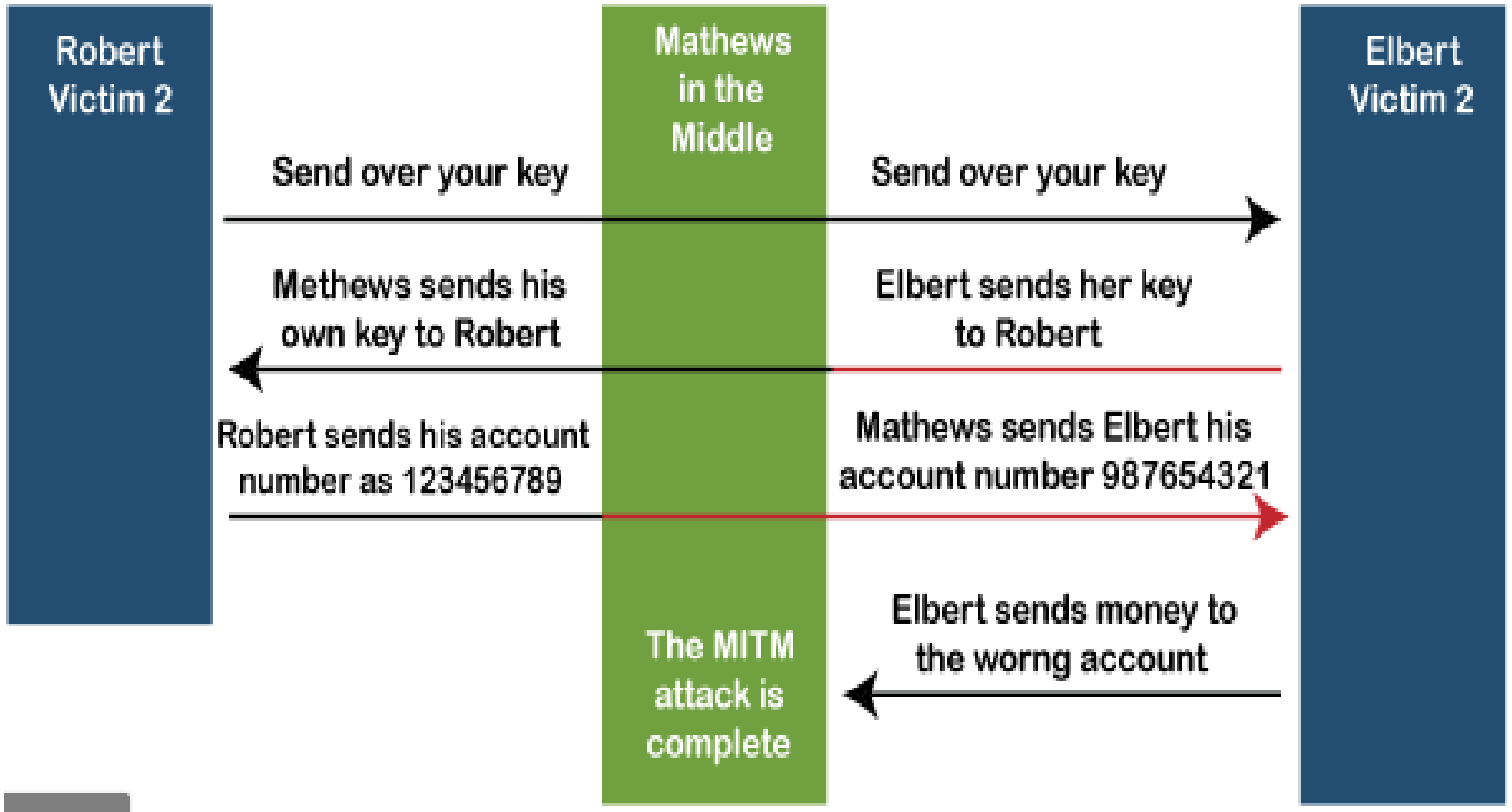
There are several different types of phishing attacks, including:

- **Spear Phishing**–targeted attacks directed at specific companies and/or individuals.
- **Whaling**–attacks targeting senior executives and stakeholders within an organization.
- **Pharming**–leverages DNS cache poisoning to capture user credentials through a fake login landing page.

3. Man-in-the-Middle (MitM) Attacks

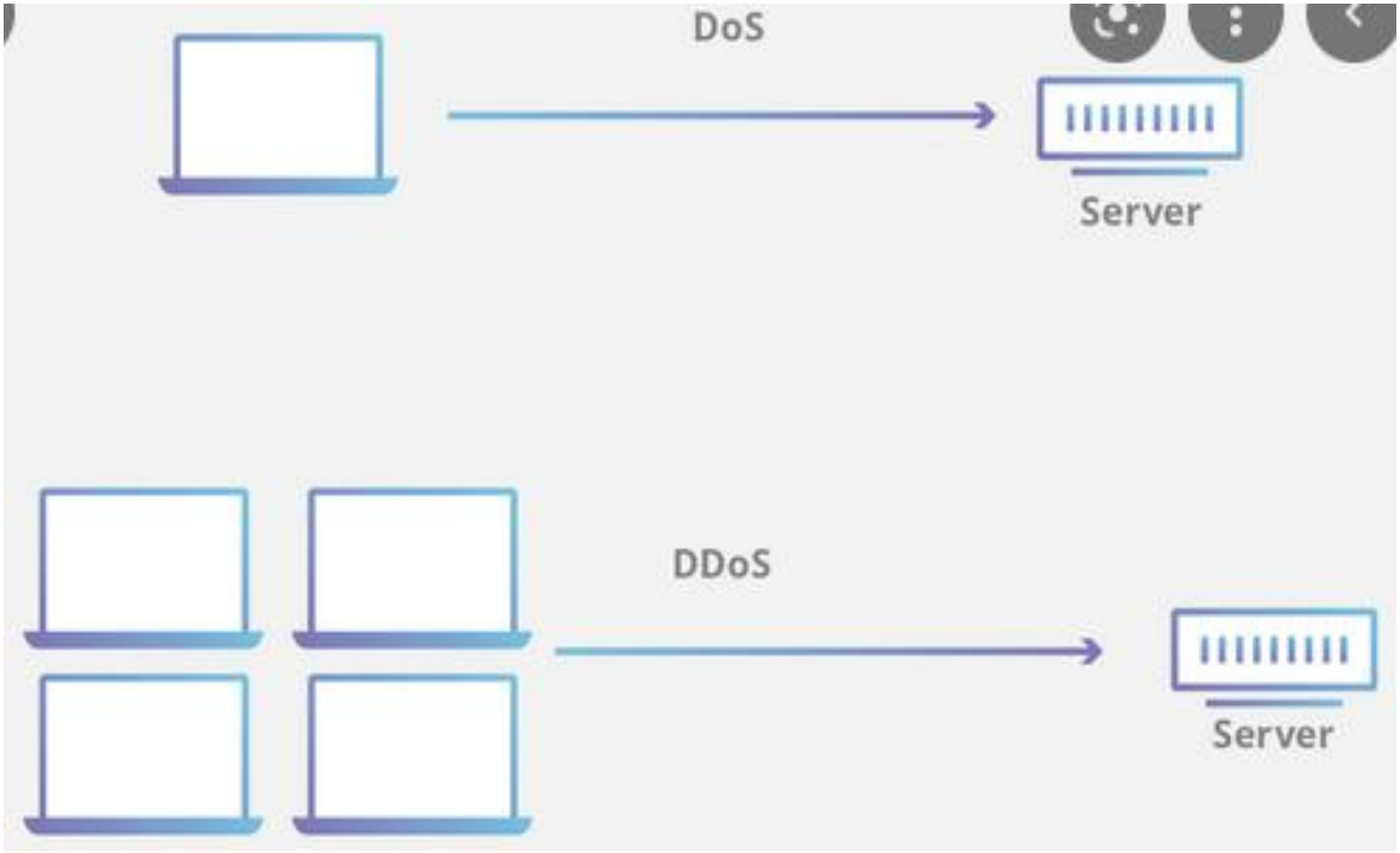


Man-in-the-Middle Attack Example

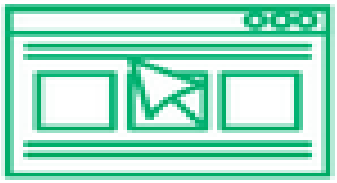


602 × 323

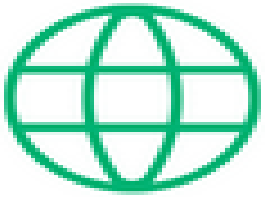
4. Denial-of-Service (DOS) Attack



Common types of DDoS attacks



The **application layer attack**, or "layer 7 DDoS attack", is an attempt to exhaust the resources of your website.

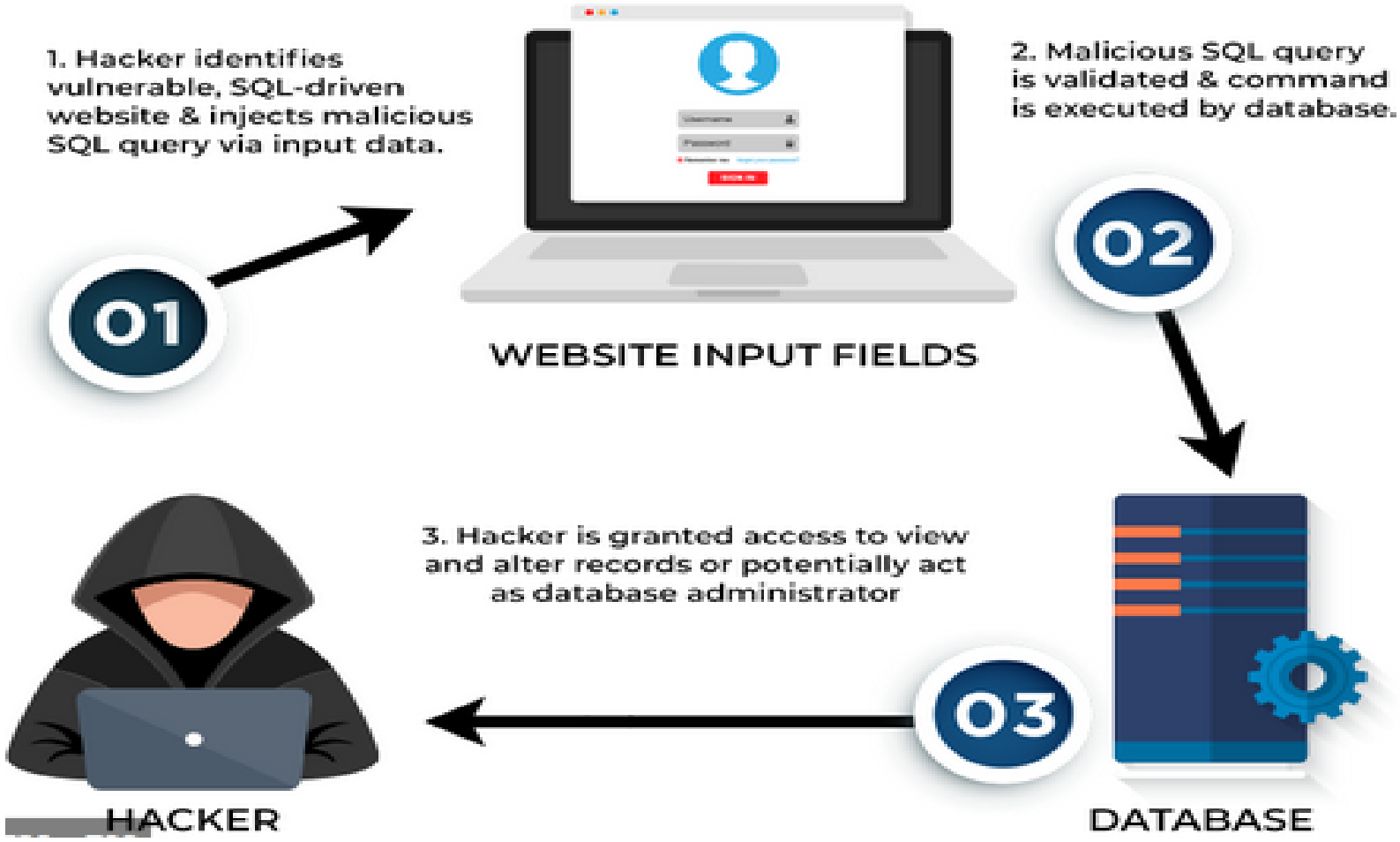


A **protocol attack** is a little more sophisticated, as it specifically targets weaknesses in servers by sending connection requests from different IP addresses.

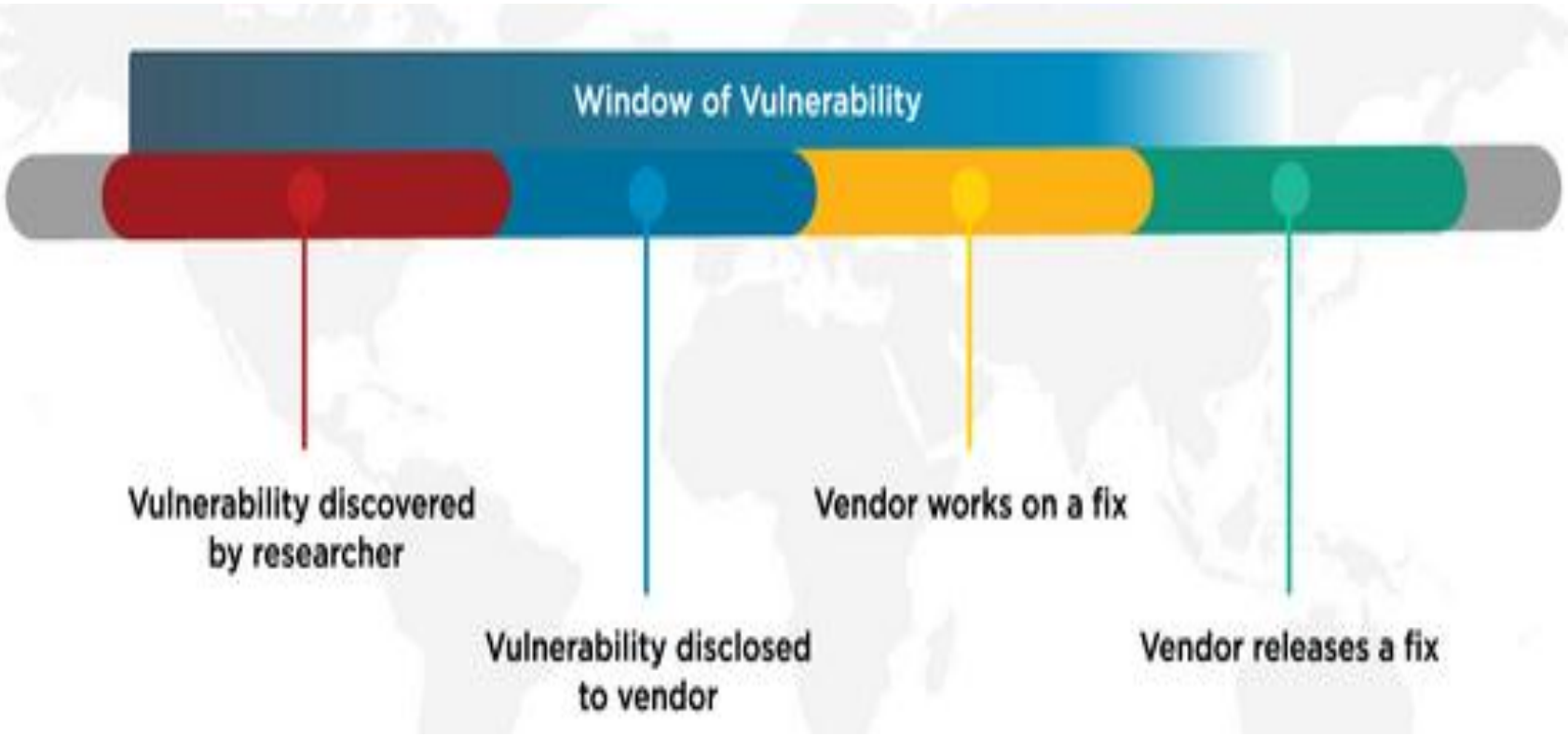
Finally, a **volumetric attack** is a different version of the "overwhelming traffic" sort of attack.

5. SQL Injections

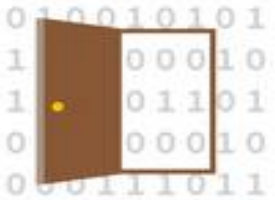
FUNCTIONING OF AN SQL INJECTION



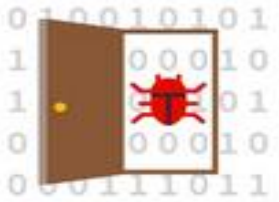
6. Zero-day Exploit



‘Zero-Day’ Defined



A **zero-day vulnerability** is a security software flaw that’s unknown to someone interested in mitigating the flaw.

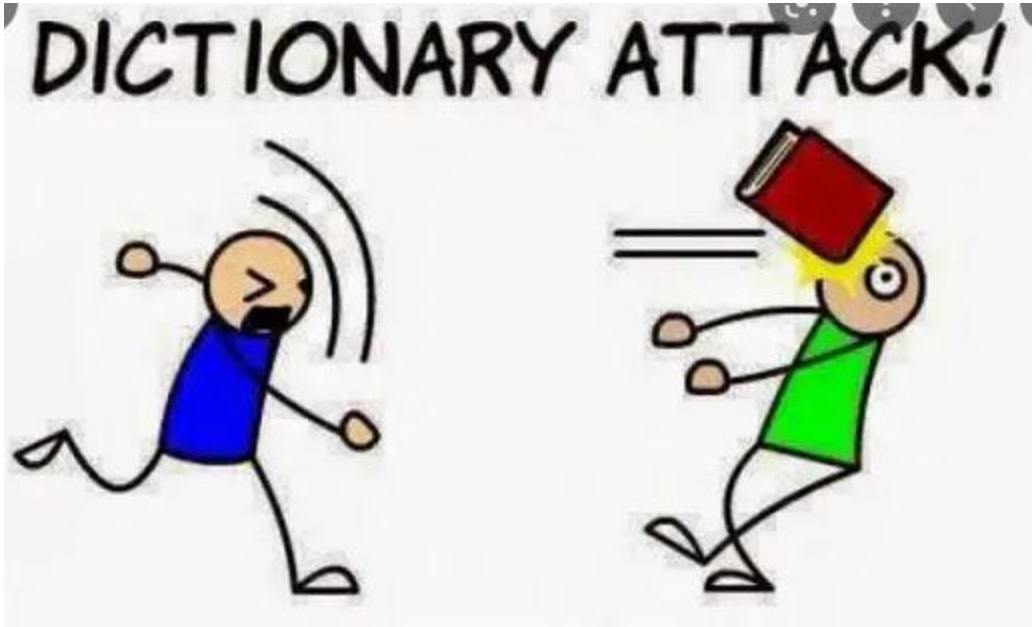


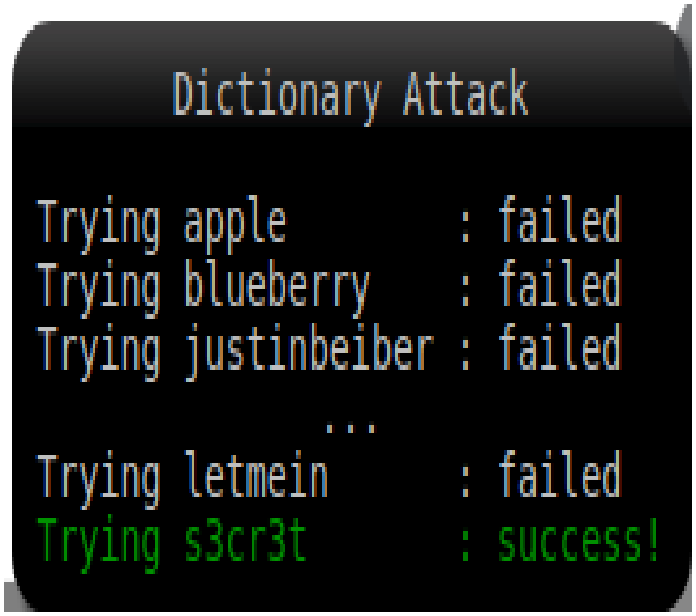
A **zero-day exploit** is when hackers take advantage of a zero-day vulnerability for malicious reasons.

A **zero-day attack** is when hackers leverage their zero-day exploit to commit a cyberattack.

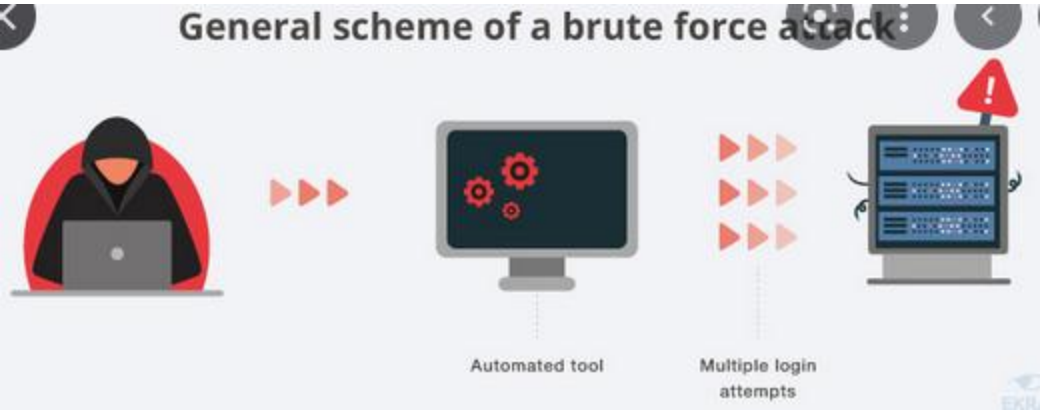
7. Password Attack

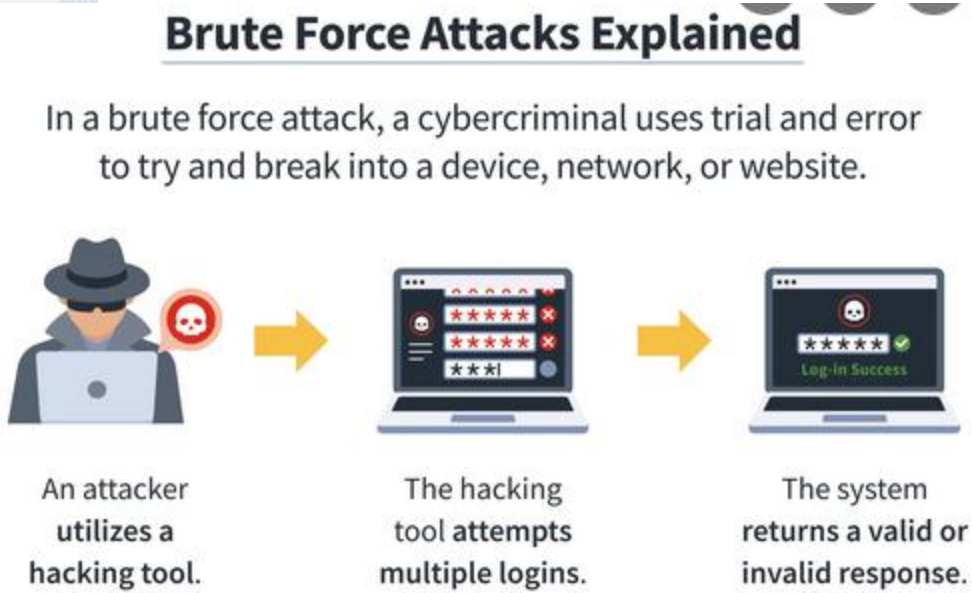
- **Dictionary attack**



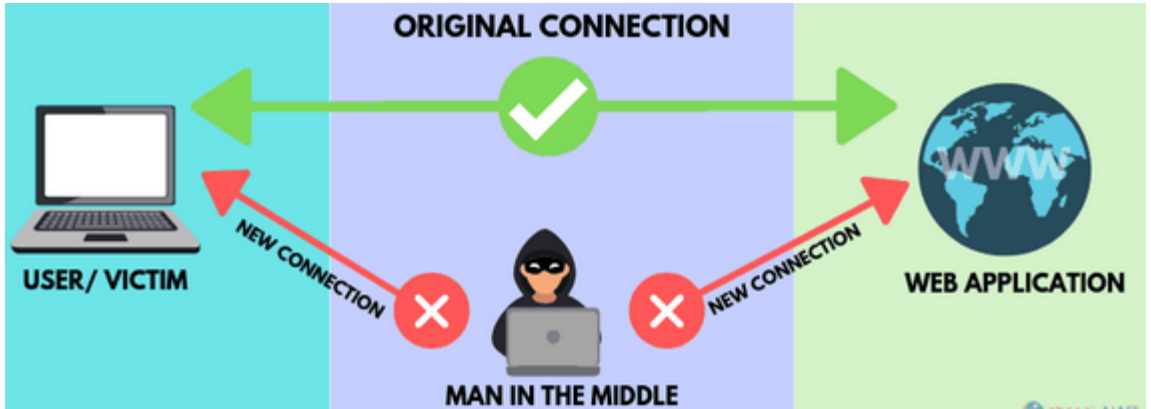


- **Brute force**

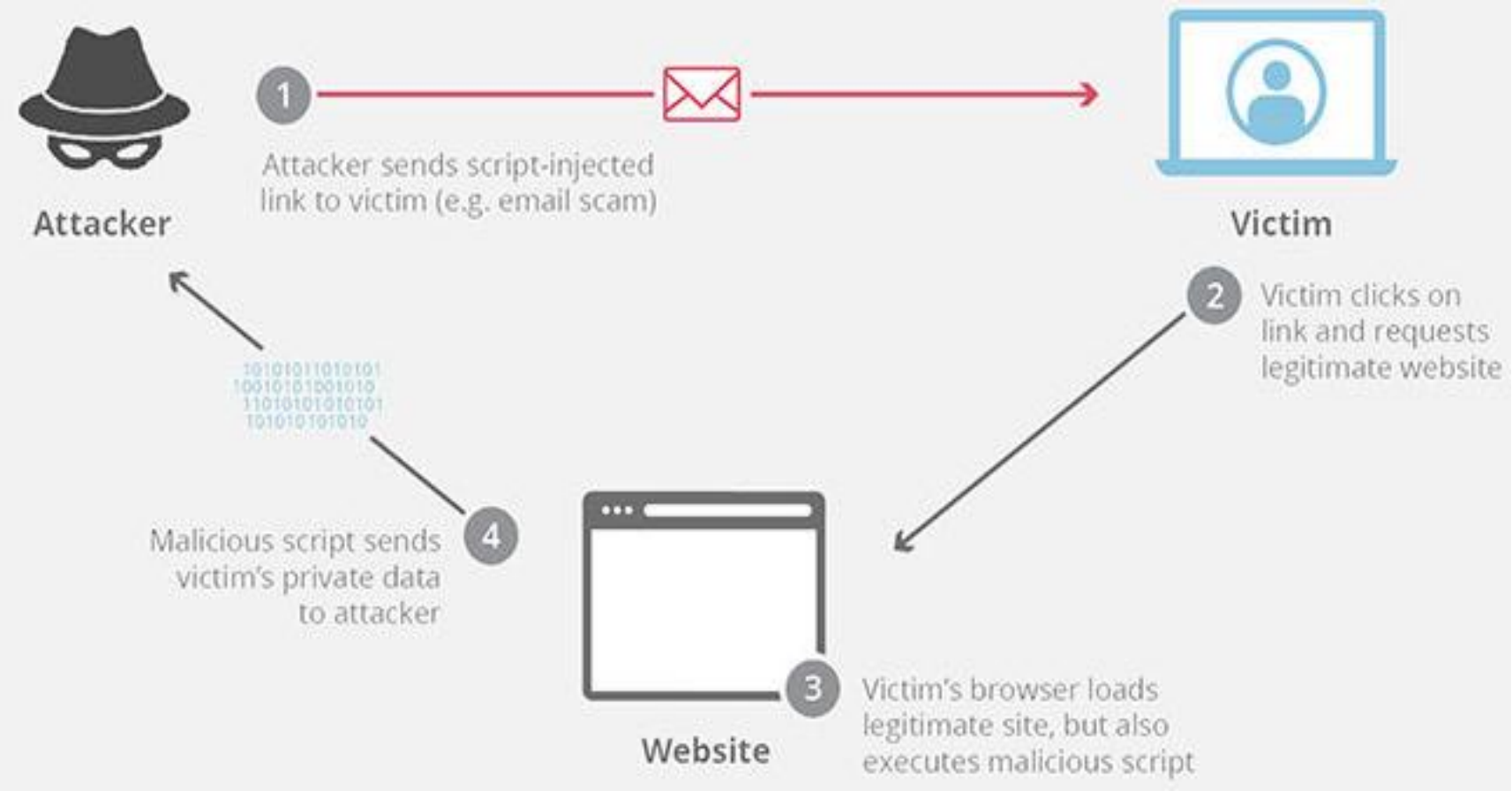

General scheme of a brute force attack
Automated tool
Multiple login attempts


Brute Force Attacks Explained
In a brute force attack, a cybercriminal uses trial and error to try and break into a device, network, or website.
Log-in Success
An attacker utilizes a hacking tool.
The hacking tool attempts multiple logins.
The system returns a valid or invalid response.

- **Man In The Middle**



8. Cross-site Scripting

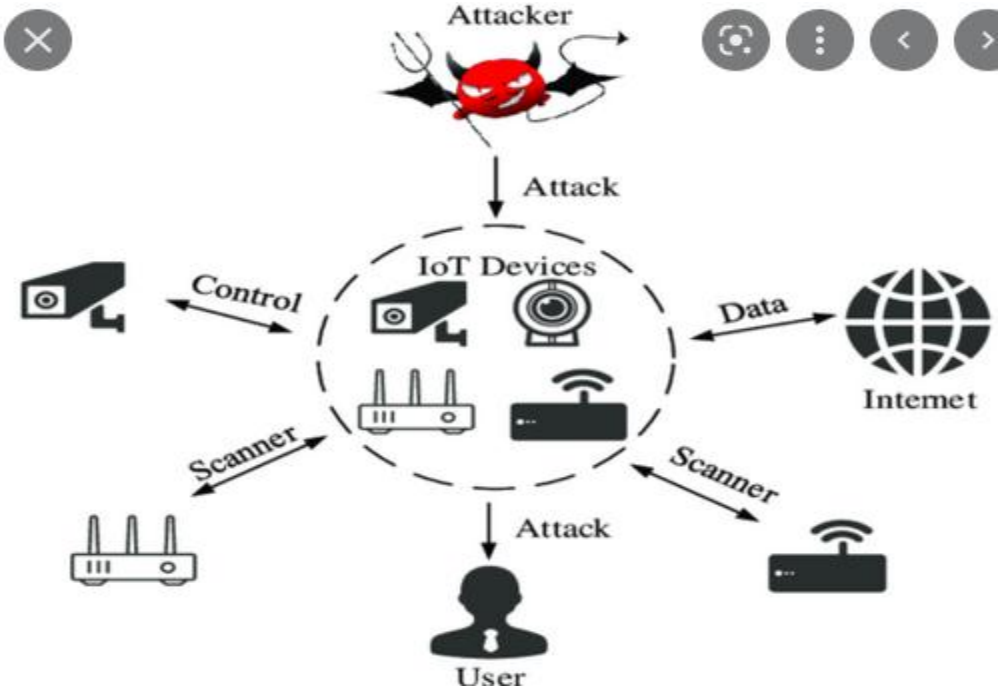


9. Rootkits

- Rootkits are installed inside legitimate software, where they can gain remote control and administration-level access over a system. The attacker then uses the rootkit to steal passwords, keys, credentials, and retrieve critical data.

10. Internet of Things (IoT) Attacks

- IoT attacks are becoming more popular due to the rapid growth of IoT devices and (in general) low priority given to embedded security in these devices and their operating systems.



- ***ADDITIONAL READING IS STRONGLY RECOMMENDED***

References

- https://www.ibm.com/topics/social-engineering
- https://www.kaspersky.co.in/resource-center/threats/how-to-avoid-social-engineering-attacks
- https://us.norton.com/internetsecurity-emerging-threats-what-is-social-engineering.html
- https://www.upguard.com/blog/social-engineering
- https://www.barracuda.com/glossary/social-engineering
- https://crashtest-security.com/penetration-test-steps/