Threats and Attacks in Network Security

Threat

Threat is a potential occurrence of an undesired event that can eventually damage and interrupt the operational and functional activities of an organization. A threat can affect the integrity and availability factors of an organization. The impact of threats is high and it can affect the existence of the physical IT assets in an organization. The existence of threats may be accidental, intentional, or due to the impact of some other action.

Attack

An attack is an action taken toward breaching an IT system's security through vulnerabilities. In the context of an attack on a system or network, it also refers to malicious software or commands that can cause an unanticipated behavior of legitimate software or hardware because attackers take advantage of the vulnerabilities.

Vulnerability

Vulnerability is the existence of a weakness, design, or implementation error that, when exploited, leads to an unexpected and undesired event compromising the security of the system. Simply put, a vulnerability is a security loophole that allows an attacker to enter the system by bypassing various user authentications.

Network Security Concerns

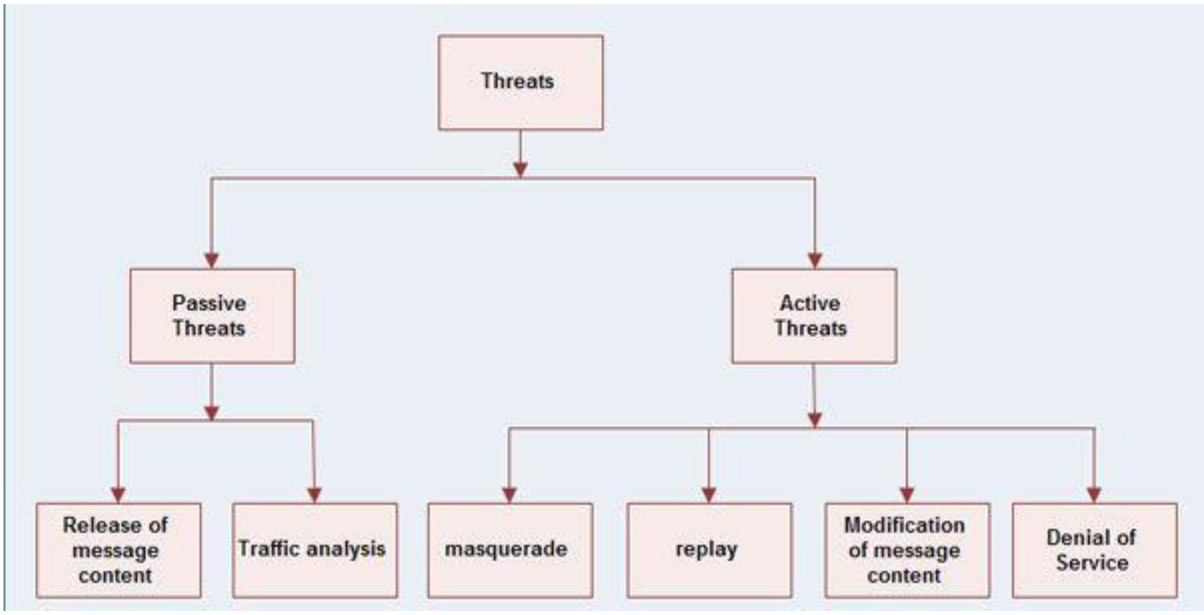
Attacks on networks are increasing at a fast rate. Constant attacks are a major issue in the computing world. Organizations are raising funds for securing network security. Network security concerns affect the availability, confidentiality, and integrity of the information present in an organization. Attackers are exploiting loopholes in security-related technologies. Administrators need to be more vigilant toward newer attacks that can occur in the network. Network administrators need to categorize the type of attacks occurring in the network.

Designing and implementing a network is an easy task, but, maintaining the security of the network is a difficult task. Attackers use various exploitation tools to gain access to the network and its resources.

The organization's network can also be at risk for different types of attacks from the inside. The employees of an organization can, at times, pose a threat to the security of the company's network. Insider threats can be more dangerous than external ones. Attackers perform network attacks to take control of a computer for curiosity and excitement, for publicity and fame, for financial gains, to spy or corporate espionage, get information about the organization, and to disrupt the proper working of an application or service. The organization needs to implement tasks that monitor and identify the attacks in the network on a daily basis. The sharing of information and resources across the computers in a network can attract intruders wanting to gain access to that information. The organization may consider taking certain protective steps to prevent any kind of unauthorized access to its network. Administrators can locate the various areas of continuous attacks, thereby assisting the organization in planning for security.

- Insecure or poor design of network
- End-user carelessness
- Intentional end-user acts

Types of Network Security Threats



There are basically two categories of threats to the network.

1. Passive threats
2. Active threats

1. Passive threats

   a) Release of message contents

   b) Traffic analysis

2. Active threats

   a) Masquerade

   b) Replay

   c) Modification of message contents

   d) Denial of service

• **Passive threats**, sometimes referred to as eavesdropping dropping, involve attempts by an attacker to obtain information relating to communication.

a) Release of message contents

• A telephone conversation, an e-mail message and a transferred file may contain sensitive or confidential information.

• We would like to prevent the opponent from learning the content of these transmissions.

b) Traffic analysis

• It is a kind of attack done on encrypted messages.

• The opponent might be able to observe the pattern of such encrypted message.

• The opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged.

• **Active threats** involve some modification of the data stream or the creation of a false stream.

a) Masquerade

• It takes place when one entity pretends to be a different entity.

• A masquerade attack usually includes one of the other forms of active attack.

• For *e.g.* authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges.

b) Replay

• It involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.

c) Modification of message

• It means that some position of a message is altered, or that messages are delayed or rendered, to produce an unauthorized effect.

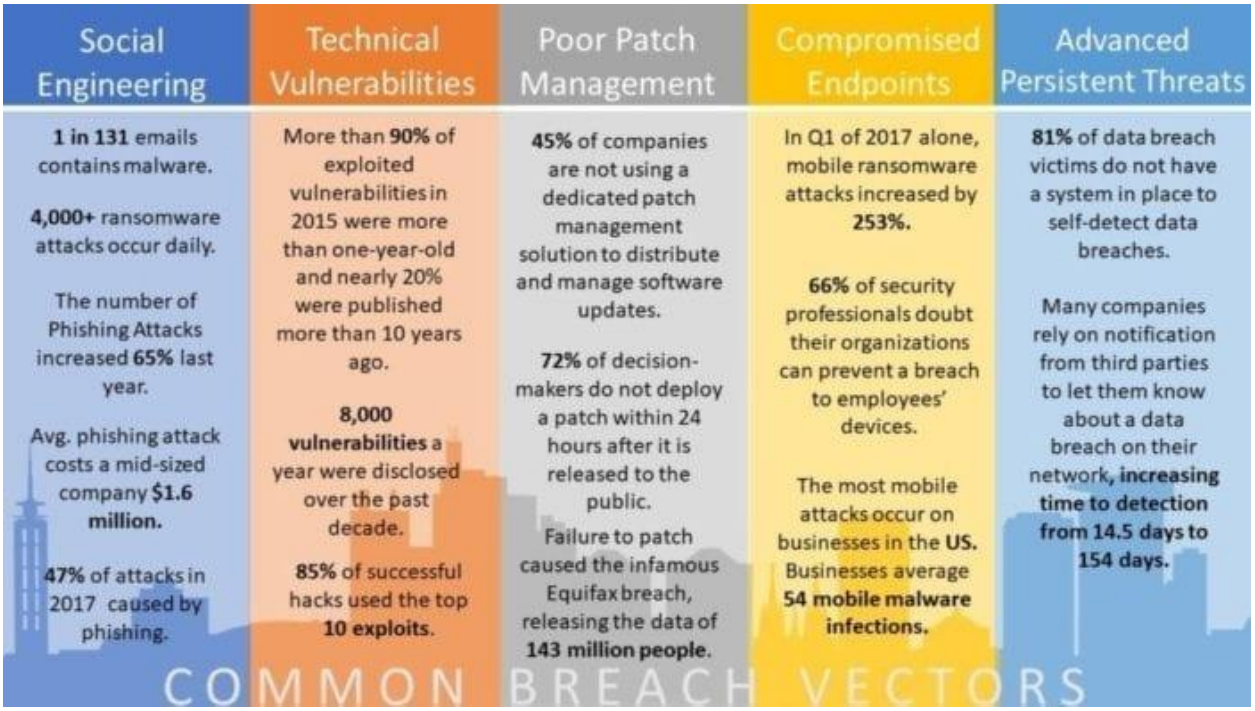
d) Denial of service (DOS)

• A denial of service attack takes place when the availability to a resource is intentionally blocked or degraded by an attacker.

• In this way the normal use or management of communication facilities is inhibited.

• This attack may have a specific target. For *e.g.* an entity may suppress all messages directed to a particular destination.

• Another form of service denial is the disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade performance.



COMMON BREACH VECTORS

Social Engineering	Technical Vulnerabilities	Poor Patch Management	Compromised Endpoints	Advanced Persistent Threats
1 in 131 emails contains malware. **4,000+** ransomware attacks occur daily. The number of Phishing Attacks increased **65%** last year. Avg. phishing attack costs a mid-sized company **$1.6 million.** **47%** of attacks in 2017 caused by phishing.	More than **90%** of exploited vulnerabilities in 2015 were more than one-year-old and nearly 20% were published more than 10 years ago. **8,000 vulnerabilities** a year were disclosed over the past decade. **85%** of successful hacks used the top **10 exploits.**	**45%** of companies are not using a dedicated patch management solution to distribute and manage software updates. **72%** of decision-makers do not deploy a patch within 24 hours after it is released to the public. Failure to patch caused the infamous Equifax breach, releasing the data of **143 million people.**	In Q1 of 2017 alone, mobile ransomware attacks increased by **253%.** **66%** of security professionals doubt their organizations can prevent a breach to employees' devices. The most mobile attacks occur on businesses in the **US.** Businesses average **54 mobile malware infections.**	**81%** of data breach victims do not have a system in place to self-detect data breaches. Many companies rely on notification from third parties to let them know about a data breach on their network, **increasing time to detection from 14.5 days to 154 days.**

Social Engineering
Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information. Phishing or Spear phishing may be the top techniques used by social engineers to get your confidential information. A list of top 10 techniques used by hackers are as follows:

1. Pretexting
2. Phishing
3. Water-holing
4. Diversion theft
5. Spear phishing
6. Baiting

7. Quid Pro Quo
8. Tailgating
9. Honeytrap
10. Rogue

Technical Vulnerabilities

A vulnerability is a weakness of an asset or control that could potentially be exploited by one or more threats. An asset is any tangible or intangible thing or characteristic that has value to an organization, a control is an administrative, managerial, technical, or legal method that can be used to modify or manage risk, and a threat is any potential event that could harm an organization or system.

Poor Patch Management

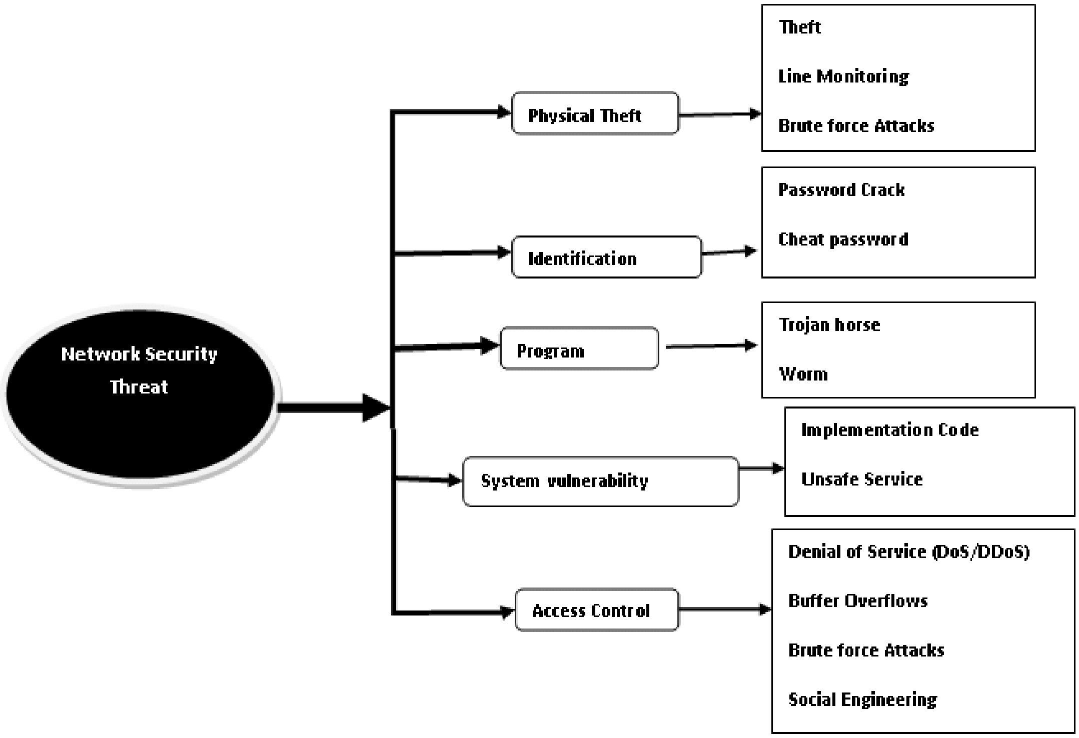
Patch management is a strategy for managing patches or upgrades for software applications and technologies. A patch management plan can help a business or organization handle these changes efficiently. A poor patch management plan can put a company at risk for hackers finding ways through their systems via vulnerabilities. A proper patch management plan will help your organization find missing security patches, support multiple systems and platforms, and handle increased compliance restraints.

Compromised Endpoints

Compromised endpoints have become much more common in the mobile-era that we live in today. BYOD means that employees are connecting their own devices to a corporate network. While this helps an employee's productivity, it may cause problems for an organization's network since corporate policy may not be enforced on the device.

Advanced Persistent Threats

An advanced persistent threat is a set of stealthy and continuous computer hacking processes, often orchestrated by a person or persons targeting a specific entity. An APT usually targets either private organizations, states or both for business or political motives. APT processes require a high degree of covertness over a long period of time.



How to address Common Network Security Threats

1. Security Awareness Training
2. Vulnerability Management
3. Patch Management
4. Endpoint Detection and Response
5. Managed SIEM with Security Monitoring

Types of Network Security Vulnerabilities

A network security breach can occur because of the following vulnerabilities:

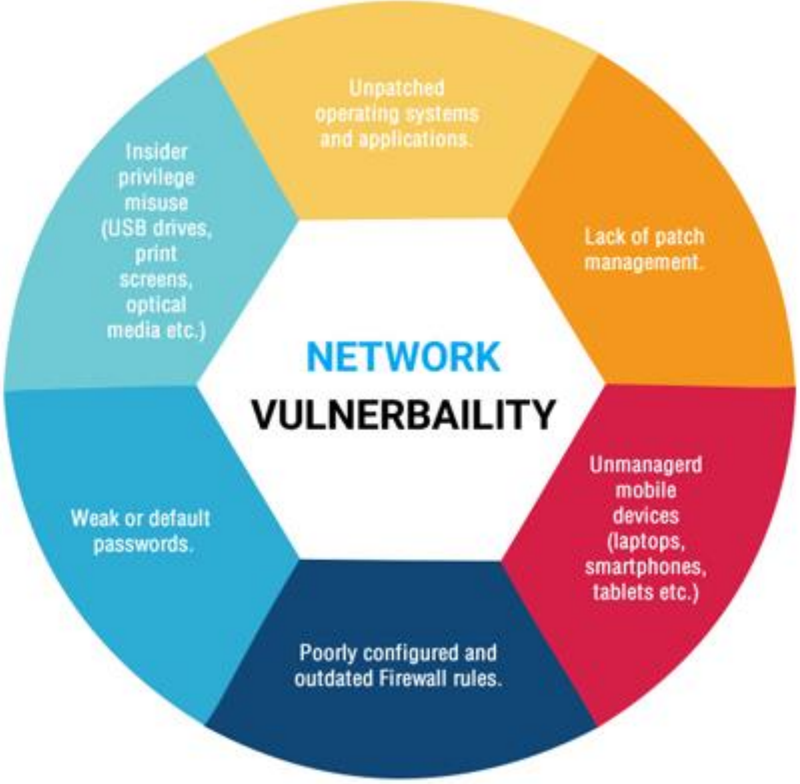
Technological vulnerabilities

A technological vulnerability exists due to the inherent weakness in the operating system, printers, scanners, or other networking equipment. Attackers can detect loopholes in protocols (like SMTP, FTP, and ICMP). Attackers detect the lack of authentication in networking equipment, like switches and routers, leading to an intrusion. Regular security audits by the network administrator or information security officer will help keep track of any irregular activities on the network.

Network Vulnerability

A network vulnerability is a weakness or flaw in software, hardware, or organizational processes, which when compromised by a threat, can result in a security breach**.**

Network vulnerabilities come in many forms but the most common types are:


Unpatched operating systems and applications.
Lack of patch management.
Unmanagerd mobile devices (laptops, smartphones, tablets etc.)
Poorly configured and outdated Firewall rules.
Weak or default passwords.
Insider privilege misuse (USB drives, print screens, optical media etc.)
NETWORK
VULNERBAILITY

1. Malware, short for malicious software, such as Trojans, viruses, and worms that are installed on a user's machine or a host server.
2. Social engineering attacks that fool users into giving up personal information such as a username or password.
3. Outdated or unpatched software that exposes the systems running the application and potentially the entire network.
4. Misconfigured firewalls / operating systems that allow or have default policies enabled.

Vulnerability Type	**Description**
Network device vulnerabilities	Various network devices such as firewall, routers, switches can be vulnerable due to the following reasons: • Lack of authentication • Insecure routing protocols • Lack of password protection • Vulnerabilities in firewall
Operating system vulnerabilities	Operating system can be vulnerable due to the following reasons: • No latest patches updated • Inherently insecure

TCP/IP protocol vulnerabilities	HTTP, SMTP, SNMP, FTP, ICMP are inherently insecure
System account vulnerabilities	Setting weaker passwords to system networks
Default password and settings	Keeping network devices/products with their default settings and passwords
User account vulnerabilities	Insecure transfer of user account details such as username and password over the network
Network device misconfiguration	Misconfiguration of network devices
Internet service misconfiguration	Misconfiguration of internet services. Ex: Enabling JavaScript and misconfiguring IIS, Apache, FTP, Terminal services etc.

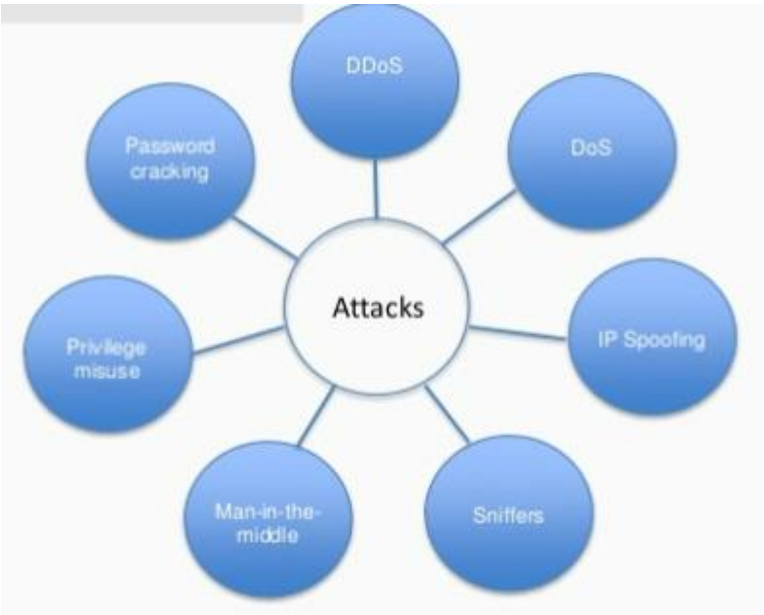
Security policy vulnerabilities

Security policy vulnerabilities exist when there is an improper drafting and enforcement of the security policies in the organization. Lack of appropriate policy enforcement may lead to unauthorized access to network resources. If an administrator fails to regularly monitor and audit the activities, it will be easy for attackers to exploit the system.

Vulnerability Type	**Description**
Security policy unawareness	Lack of awareness in security policies
Unwritten policy	Unwritten policy is difficult to implement and use
Lack of continuity	Lack of continuity in implementing and using security policies

Types of Network Security Attacks

Organizations are facing challenges in maintaining the security of their network, as the number of attacks on networks are growing day by day. Attackers or hackers are finding new ways of getting into networks. The motive behind the attacks differ based on the objective of each attacker. Some attackers want to steal the hardware and software, while others perform actions that reduce the bandwidth of the network resources—and others are after customer data. The network administrator, on the other hand, needs to be highly efficient in identifying these attacks and have knowledge on what each of these different types of attacks are.



There are multiple types of network attacks cut across all platform types and categories of software and most of the common ones are as follows:

- Spoofing
- Hijacking
- Trojans
- DoS and DDoS
- Sniffing
- Mapping
- Social engineering

Spoofing (Identity or IP Address Spoofing)

Any internet connected device sends IP datagrams which are internet data packets into the network. These datagrams carry application layer data and the sender's IP address and if the attacker is able of getting the control over the software running on a network device, it gets easy for them to alter the device's protocols and putting an arbitrary IP address into the data packet's source address field. Spoofers do it so that it becomes difficult to find the actual host who sent the datagram.

Ingress filtering is the countermeasure of spoofing and routers usually perform this. Routers perform ingress filtering to check the IP address of incoming datagrams and try to find out if the source addresses which are to be known, to be reachable via that interface. Router discards the source address of the packets which are not in the valid range.

Hijacking (man-in-the-middle attack)

Hijacking is an attack technique where man-in-the-middle takes advantage of the way headers are constructed in a weakness in the TCP/IP protocol stack. Hijackers perform hijacking by actively monitoring capturing, and controlling your communication transparently when you are communicating with another person. The attacker may re-route a data exchange and while your computers are communicating at low levels of the network layer, they might not be able to find with whom they are exchanging data. Man-in-middle attacks takes the advantage of this technique as the person with whom you communicate will think that it is you (actual user) who has sent a message whereas the fact is, it is the hacker who actively responding on your behalf using your identity. So if you find anything unusual while having conversation with your friend of receiving any message from the unauthorized contact, avoid any kind of communication as this may be either a hacking attempt or hacker.

Trojans

These are malicious programs that seem like legitimate software, but actually they when launched, they perform unintended or malicious activities behind the scenes. Most of the remote control spyware programs are of this type. A Trojan program file will look, operate, and appear to be the same size as the compromised system file.

To avoid the effects of such attacks, early use of a cryptographic checksum or binary digital signature procedure is the only protection.

Sniffing

Packet sniffing is a way of intercepting data packets travelling to a network. To capture all traffic travelling to and from internet host site, a sniffer program executes its functions at the Ethernet layer in combination with network interface cards (NIC). The sniffer program will collect all communication packets floating by anywhere near the internet host site if any of the Ethernet NIC cards are in promiscuous mode.

A sniffer placed on any inter-network link or backbone device or network aggregation point will therefore be in a state of monitoring the entire lot of traffic. There are multiple sniffers programs on the internet that are free and most of them are passive. Packet sniffers listen all data link layer frames passing by the device's network interface and among them which are more sophisticated ones allow more active intrusion.

It is required to detect network interfaces that are running in promiscuous mode in order to detect packet sniffing. There are two ways of detecting sniffing:

1. Host-based
2. Network-based

Host-based: If the NIC is running in promiscuous mode, several software commands exist that can be run on individual host machines to tell the same.

Network-based: Sniffer programs consume a lot of running processed and log files, but there are solutions which tend to check for the presence of log files and running processes. However, sophisticated intruders almost always are able of hiding tracks by disguising the process and cleaning up the log files.

End-to-end or user-to-user encryption is the best countermeasure against sniffing.

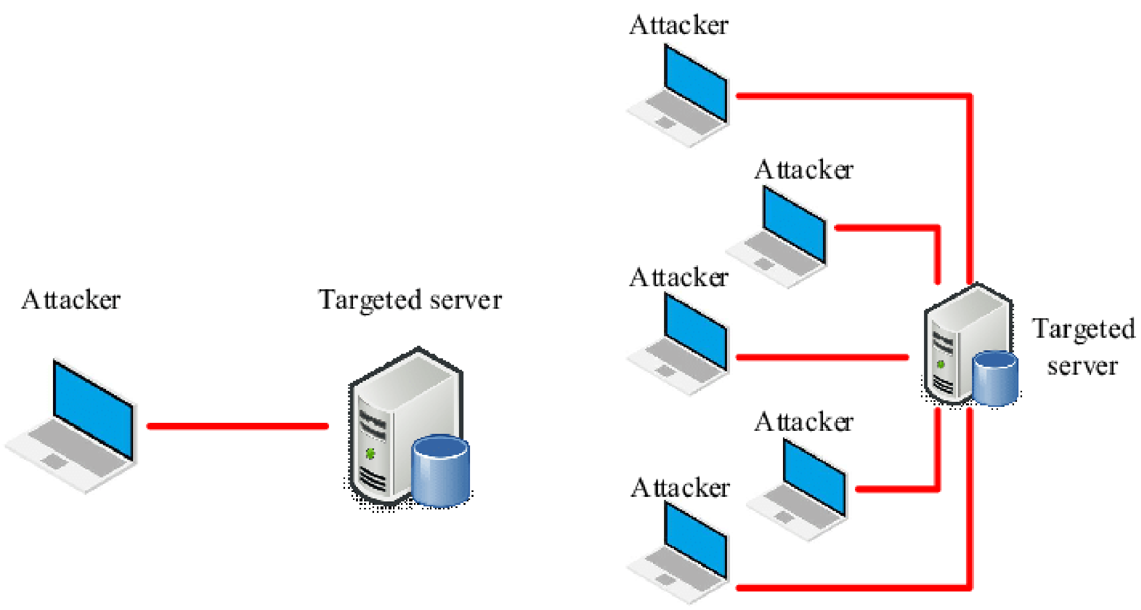
Eavesdropping

Before attacking a network, attackers try to find out some important information like IP address of machines on the network, the operating systems that machines are using connected to a network, and the services that they offer. Using this information, attackers can be more focused on their attacks and it is less likely to cause alarm. The process of gathering all the information is known as mapping.

Strong encryption services that are based on cryptography only are its counter measures. Otherwise, it gets easy for attackers and others to read your data as it traverses the network.

Denial-of-Service attack (DoS) and Distributed-Denial-of-Service (DDoS)

A denial of service attack is a special kind of Internet attack on a network that is carried out at large websites. This attack is designed to perform on the network in order to bring it down to its knees by flooding it with useless traffic. Denial of Service can result if a system (like web server) if flooded with a huge number of illegitimate requests. This act makes the web server unable to respond on legitimate and real requests or tasks.



DoS attack

DDoS attack

A Dos attack can be executed in a number of ways, but its three basic types of attacks are:

- Consumption of computational resources, such as disk space, CPU time, and band width.
- Disruption of configuration details, such as routing information.
- Disruption of physical network components.

DoS attack may bring the following consequences:

- Slow network performance.
- Unavailability of a particular web site.
- Inability to access a particular web site.
- Dramatic increase of spam in your account.

Common forms of denial of service attacks are,

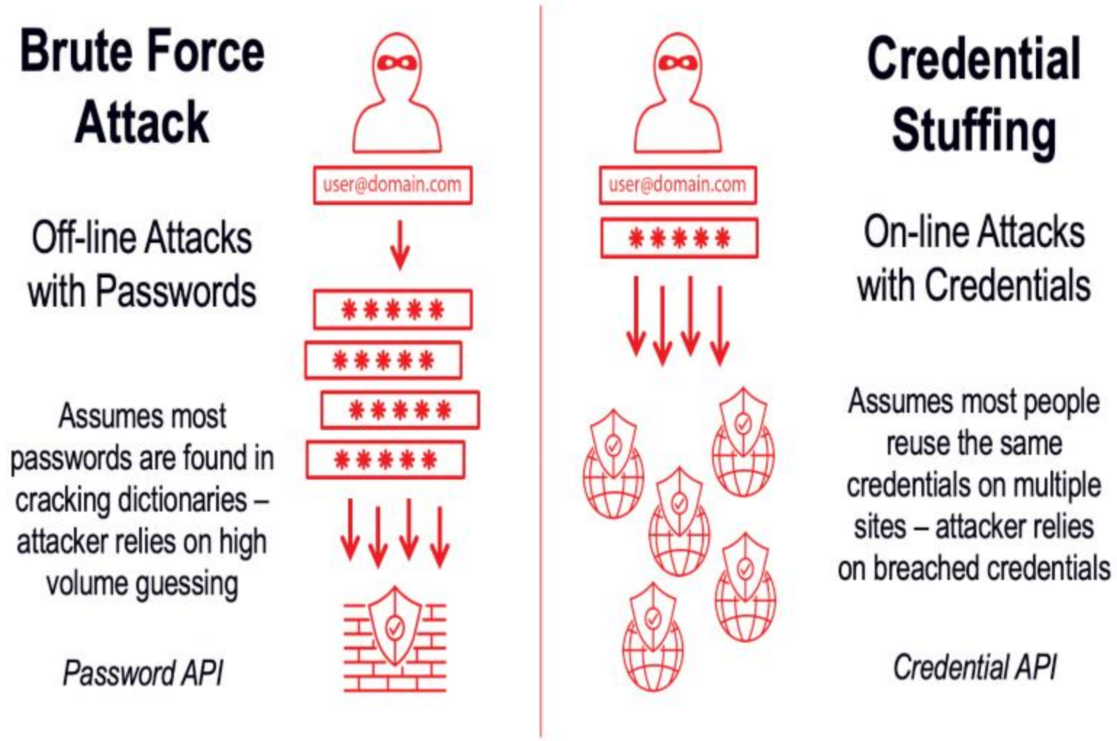
1. Buffer Overflow Attacks simply send more traffic to a network address than the programmer's expectation on size of buffers.
2. In Smurf Attack, the perpetrator sends an IP ping request to a receiving site.
3. SYN floods are a type of attack when a computer tries to make a TCP/IP connection to another computer.

To control DoS attack, only ingress filtering is the only counter measure and that too to a small extent.

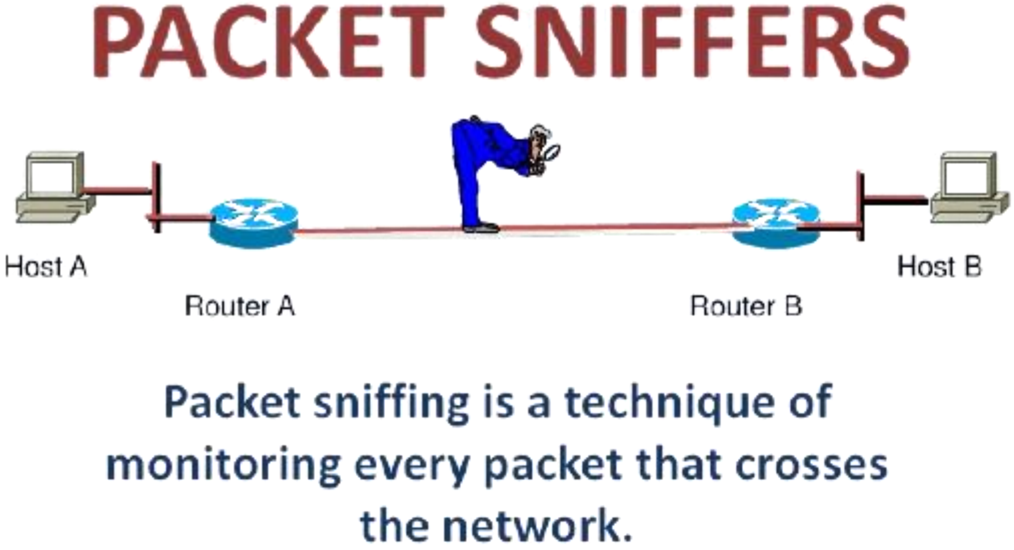
Two Types of DDoS:

1. **Network-centric attack**: Overloads a service by consuming bandwidth
2. **Application-centric attack**: Overloads a service by sending an unrelenting number of packets

Brute Force Attacks: A brute force attack is an attack where cybercriminals use the trial-and-error method to decode a password, username, PIN or find a hidden web page with automated software to check large numbers of possible combinations. Though it is an old attack method, it is still effective and very popular among hackers. In this attack, hackers are not required to trick users into downloading malware or any other related practices involving users for stealing passwords.


Brute Force Attack
Off-line Attacks with Passwords
Assumes most passwords are found in cracking dictionaries – attacker relies on high volume guessing
Password API
user@domain.com
*****
*****
*****
*****
*****
user@domain.com
*****
Credential Stuffing
On-line Attacks with Credentials
Assumes most people reuse the same credentials on multiple sites – attacker relies on breached credentials
Credential API

Packet Sniffer: The packet sniffing attack corresponds to data theft or interception by capturing the network traffic with the help of a sniffer. Sniffer is basically an application that captures network packets. When data is transferred across networks, it is broken down into data packets or small units. These data packets are not encrypted when they reach the receiver and therefore can be read by using sniffing. Just like eavesdropping, the data packets are compromised during the process by a third party. With the help of a sniffer application, the attacker can analyze and gain information from the network, eventually causing the network to crash or become corrupt.



PACKET SNIFFERS

Packet sniffing is a technique of monitoring every packet that crosses the network.

Malware Attacks: The term malware originated from combining two terms, malicious software. It is the application that is created with a motive to harm, hijack or spy on the system infected by a virus or containing vulnerabilities. The malware attack is deployed by cybercriminals who create malicious software with the intention to install on the victim's device without his/her knowledge. The sole purpose of doing this is to gain access to their personal, financial or confidential information. There are three common carriers to spread malware:

1. **Phishing emails:** A **social engineering** practice of sending fraudulent emails to victims in order to trick them into downloading malicious email attachments.
2. **Malicious websites:** Cyber-attackers set up websites that include malicious software that is disguised as legitimate downloads to misguide users.
3. **Malvertising:** With the help of advertising networks, cyber threat actors deploy malicious ads that redirect users to malware-hosting websites.

Access Attacks

After gaining information about the target network, attackers then try to gain access by using various exploitation techniques. These are the attempts made toward gaining access to the system or network. This is called an access attack and it includes gaining unauthorized access, brute force, privilege escalations, man-in-the-middle, etc.

Reconnaissance attacks

The reconnaissance attack refers to a technique in which the attackers gather information about the network and organization, helping them perform attacks easier. Gathering information about a network allows attackers to recognize any potential weaknesses it may have.

Types of reconnaissance attack

1. **Active reconnaissance attacks**

Active reconnaissance attacks mostly include port scans and operating system scans. Here, the attacker uses tools to send packets to the target system. For example, the traceroute tool helps gather all the IP addresses for the routers and firewalls. The attacker also gathers more information regarding the services running on the target system.

2. **Passive reconnaissance attacks**

Passive reconnaissance attacks use the method of gaining information from the traffic. Here, the attackers perform sniffing, which helps them gain all the details regarding the weaknesses in the network. The attackers use various tools to gain information about the target.

Example of Reconnaissance attacks includes

Packet sniffing: Packet sniffing monitors every packet that passes through a network. Through various packet-sniffing tools, attackers capture usernames, passwords, and other user information. The user information is available in plain text, as well as on protocols like Telnet and HTTP. Packet sniffing can map the network and break into the target computer.

Port scanning: Port scanning gives attackers access to any open ports on the target machine. Once the access is possible, the intrusion is done.

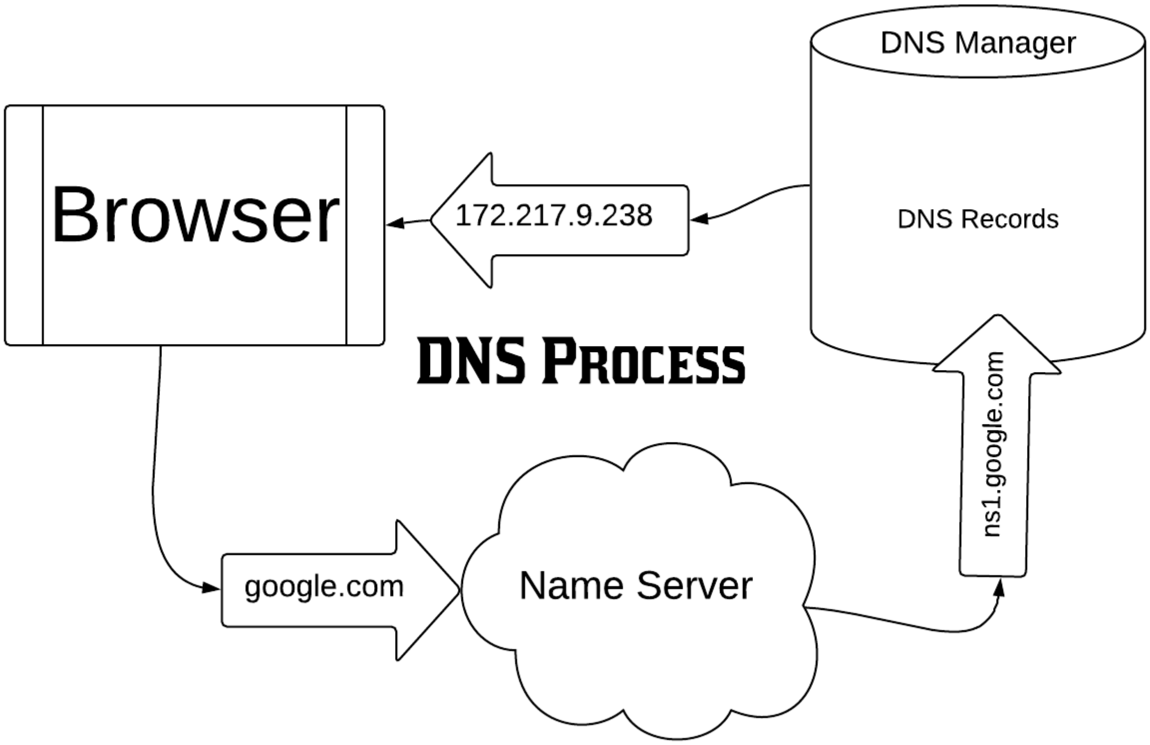
Ping sweeping: Ping sweeping helps to locate the open/live port in a network through an ICMP request. A well-configured ACL can prevent ping sweeping in the network.

DNS Footprinting: DNS footprinting is possible with the help of a DNS query consisting of DNS lookup and WHOIS. The queries provide information about the specific domain and the IP address.

Social Engineering: Social engineering is a technique where targets unknowingly share their credentials or personal information on the network. Attackers use this information to attack the target.

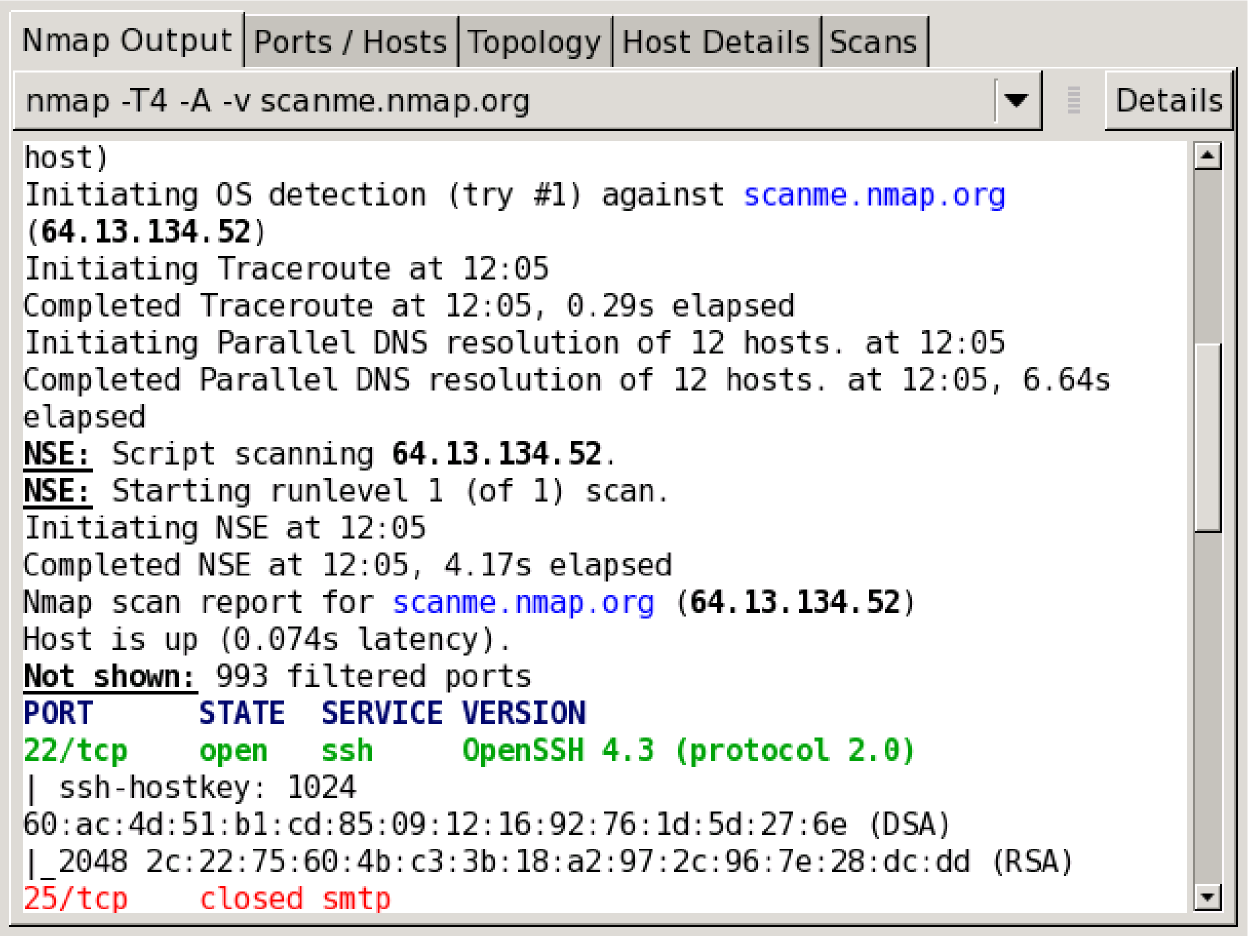
Reconnaissance Attacks: DNS Footprinting

DNS footprinting reveals information about the DNS zone. DNS zone data includes the DNS domain names, computer names, IP addresses, and much more about a particular network. An attacker uses the DNS information to determine key hosts in the network, and then performs social engineering attacks to gather even more information.



Reconnaissance Attacks: Network Information Extraction Using Nmap Scan

Nmap is a network discovery and security-auditing tool and is one of the most popular tools attackers use for network discovery. An attacker mostly uses the Nmap utility to extract all the necessary information from the target. Attackers use Nmap to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. Network administrators also find this tool useful for security-auditing tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.



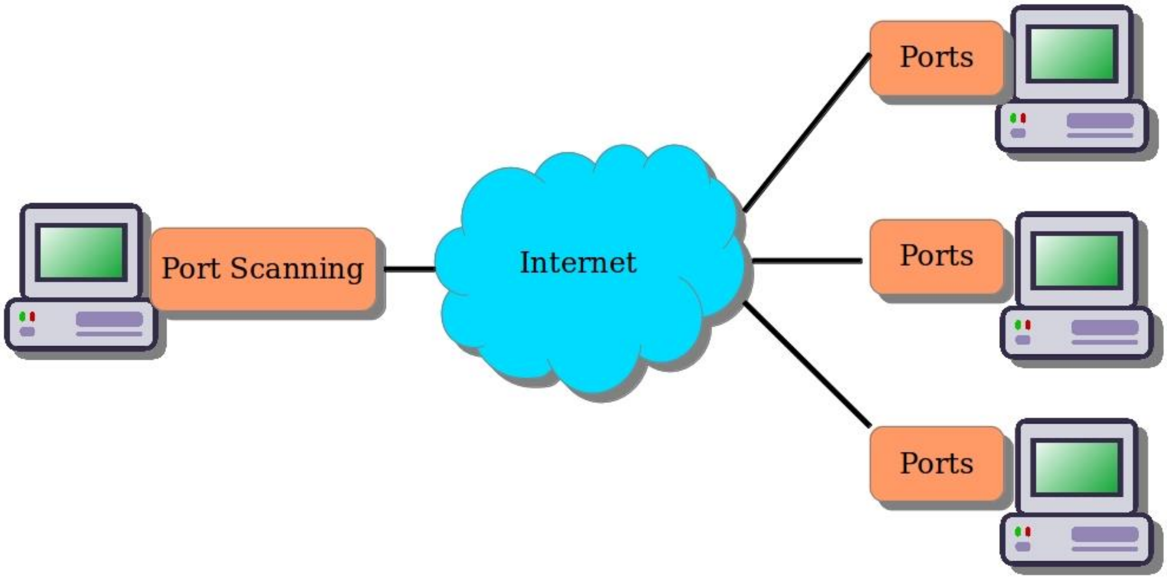
```
nmap -T4 -A -v scanme.nmap.org
```

```
host)
Initiating OS detection (try #1) against scanme.nmap.org
(64.13.134.52)
Initiating Traceroute at 12:05
Completed Traceroute at 12:05, 0.29s elapsed
Initiating Parallel DNS resolution of 12 hosts. at 12:05
Completed Parallel DNS resolution of 12 hosts. at 12:05, 6.64s
elapsed
NSE: Script scanning 64.13.134.52.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 12:05
Completed NSE at 12:05, 4.17s elapsed
Nmap scan report for scanme.nmap.org (64.13.134.52)
Host is up (0.074s latency).
Not shown: 993 filtered ports
PORT      STATE  SERVICE VERSION
22/tcp    open   ssh     OpenSSH 4.3 (protocol 2.0)
| ssh-hostkey: 1024
60:ac:4d:51:b1:cd:85:09:12:16:92:76:1d:5d:27:6e (DSA)
|_2048 2c:22:75:60:4b:c3:3b:18:a2:97:2c:96:7e:28:dc:dd (RSA)
25/tcp    closed smtp
```

Reconnaissance Attacks: Port Scanning

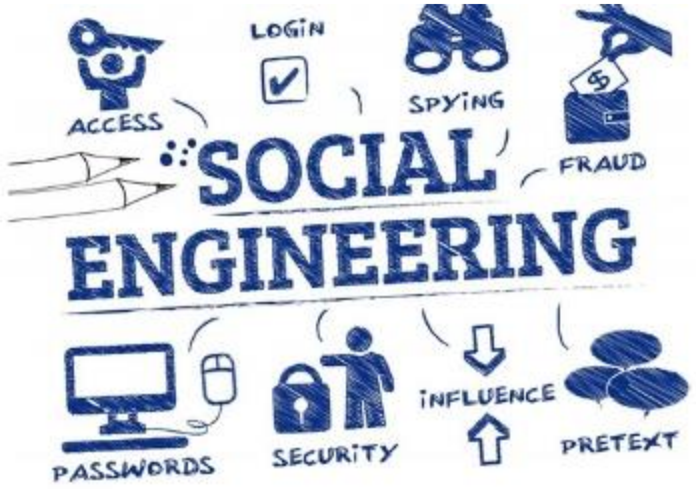
Port scanning is the process of checking what services are running on the target computer by sending a sequence of messages in an attempt to break in. Port scanning involves connecting to or probing TCP and UDP ports on the target system to determine if the services are running or are in a listening state. The listening state provides information about the operating system and the applications currently in use. Sometimes, active services that are listening may allow unauthorized users access to misconfigured systems or software that is running with vulnerabilities. Port-scanning techniques help to identify and list all the open ports on a targeted server or host. Attackers use various port-scanning utilities tools (such as NMAP, Netscan Tools Pro, SuperScan, and PRTG Network Monitor) to detect open ports on the target. These tools help an attacker probe a server or host on the target network for open ports. Open ports are the doorways through which malware get on a system.

Port Scanning (nmap)



Reconnaissance Attacks: Social Engineering Attacks

Social engineering is the art and science of convincing (tricking) people to provide personal or business information. This is one way an intruder chooses to step into an organization. Intruders gain unauthorized access through developing trust relationships with employees. Social engineering refers to the method of influencing and persuading people to reveal sensitive information in order to perform some malicious action. With the help of social engineering tricks, attackers can obtain confidential information, authorization details, and access details of people by deceiving and manipulating them. They can find out who is on vacation or going on vacation, where they work, the security measures in place, or simply listen to the employees talk about their work day. Attackers can easily breach the security of an organization using social engineering tricks. All security measures adopted by the organization are in vain when employees get “social engineered” by strangers. Some examples of social engineering include unwittingly answering the questions of strangers, replying to spam email, and bragging in front of co-workers. Even answering questions on a phone call can lead to social engineering. Employees must be trained properly to recognize these tricks and taught how to counter them when necessary.



Access Attacks: Password Attacks

Password attacks are performed to gain unauthorized access or to get control over a target computer system. Attackers perform password attacks to steal secrets, make slight modifications to websites, steal credit card details, get privileges, etc. Generally, passwords are used to authenticate users with a system. Attackers try to gain these user passwords with different techniques and authenticate with the system to enjoy the privileges the normal user has. Attackers perform different techniques to crack the passwords of servers and routers and get access to the targeted resource.

Password-Attack Techniques:

An attacker may use different types of techniques to crack passwords. Those are:

Dictionary Attack

A dictionary attack is an attempt to crack a user's password by making a guess. Attackers can guess passwords using a manual or an automated approach. This attack tries to match words that occur often or commonly used words in day-to-day life. The most common passwords found are: password, root, administrator, admin, demo, test, guest, qwerty, pet names, date of birth, children names, addresses, and hobbies.

Hybrid Attack

It works like a dictionary attack, but adds numbers and symbols to the words and tries to crack the password. These attacks generalize common things people do to make their passwords hard to guess. The hybrid attacking tool starts guessing a dictionary term and creates other guesses by appending or prepending the characters to the dictionary term. It appends or prepends with dates, numbers, and alphanumeric characters to break the password.

Birthday Attack

Birthday attacks use techniques that solve a class of cryptographic hash functions. The birthday attack falls under brute-force attacks. The logic of a birthday attack depends on the birthday problem that is explained as follows: A probability problem states that if there are 23 people in a room, the probability of at least two people having the same date of birth is more than 0.5. Attackers try to get the birth date of the target employee to crack the password. It is because some users create passwords with their birth date. Attackers use different methodologies (such as probability analysis) to get birth dates.

Rainbow Table Attack

Rainbow table is a huge set of hashes (encoded codes) that are pre-matched to possible plain-text passwords. Rainbow tables are used by password-cracking software to breach network security. All computer systems that require authentication store user accounts and passwords in the database in an encrypted form. If the attacker gains access to the password database, the password-cracking software compares the rainbow table's list of hashes with hashed passwords in the database. The rainbow table maps plain-text passwords with hashes that are exploited by attackers to access the network as a valid user.

Access Attacks: Network Sniffing

Sniffing involves capturing, decoding, inspecting, and interpreting the information inside a packet on a TCP/IP network. The purpose is to steal information, usually user IDs, passwords, network details, credit card numbers, etc. Sniffing is generally referred to as a "passive" type of attack, where the attacker can be silent/invisible on the network. This makes it difficult to detect; it is a dangerous type of attack. The TCP/IP packet contains vital information required for two network interfaces to communicate with each other. It contains fields such as source and destination IP addresses ports, sequence numbers, and the protocol type. There are three ways to sniff a network:

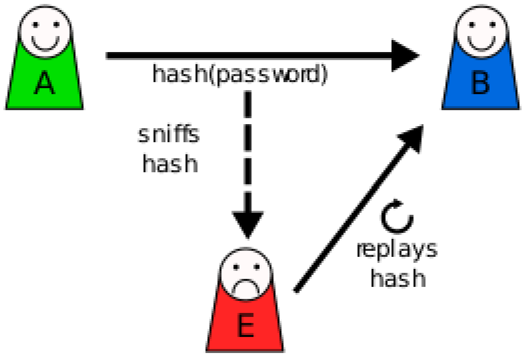
Internal sniff

A person (who may be an employee of the firm) who is already hooked up to the internal LAN can run tools to directly capture network traffic

External sniff

A hacker outside the target network can intercept packets at the firewall level and steal the information. Wireless sniff

Access Attacks: Replay Attack



The replay attack is an extension of the MITM attack in which the attacker replays the information gained from the communication between two parties. The attacker gains the token used for validating the users accessing the webserver by eavesdropping—and later replays the token to the server after modifications or deletions (thereby gaining access to the session). The attacker then sends the server response to the user. In the replay attack, the attacker eavesdrops on the confidential information such as credentials or session ID or any key that the attacker can later use with the receiver in the pretext of the sender. It is one form of a MiTM attack.

Access Attacks: Privilege Escalation

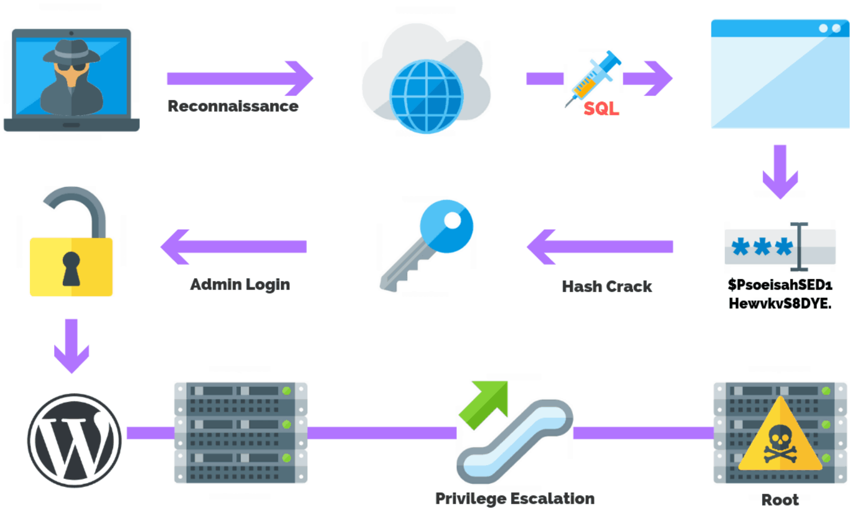
In a privilege-escalation attack, the attacker gains access to the network and the associated data and applications by taking advantage of defects in the design, software application, poorly configured operating systems, etc. Once an attacker has gained access to a remote system with a valid username and password, they will attempt to increase their privileges. The attacker uses a method of escalating the user account to another account with increased privileges, such as administrator privileges. An attacker does privilege escalation to perform unauthorized access and privileged operations on the network or system. An admin account can access more and do more in a network than a regular user. Basically, privilege escalation takes place in two forms. There is vertical privilege escalation and horizontal privilege escalation.

Horizontal Privilege Escalation

In horizontal privilege escalation, the unauthorized user tries to access the resources, functions, and other privileges that belong to the authorized user who has similar access permissions. For instance, online banking user Y can easily access user Z’s bank account.

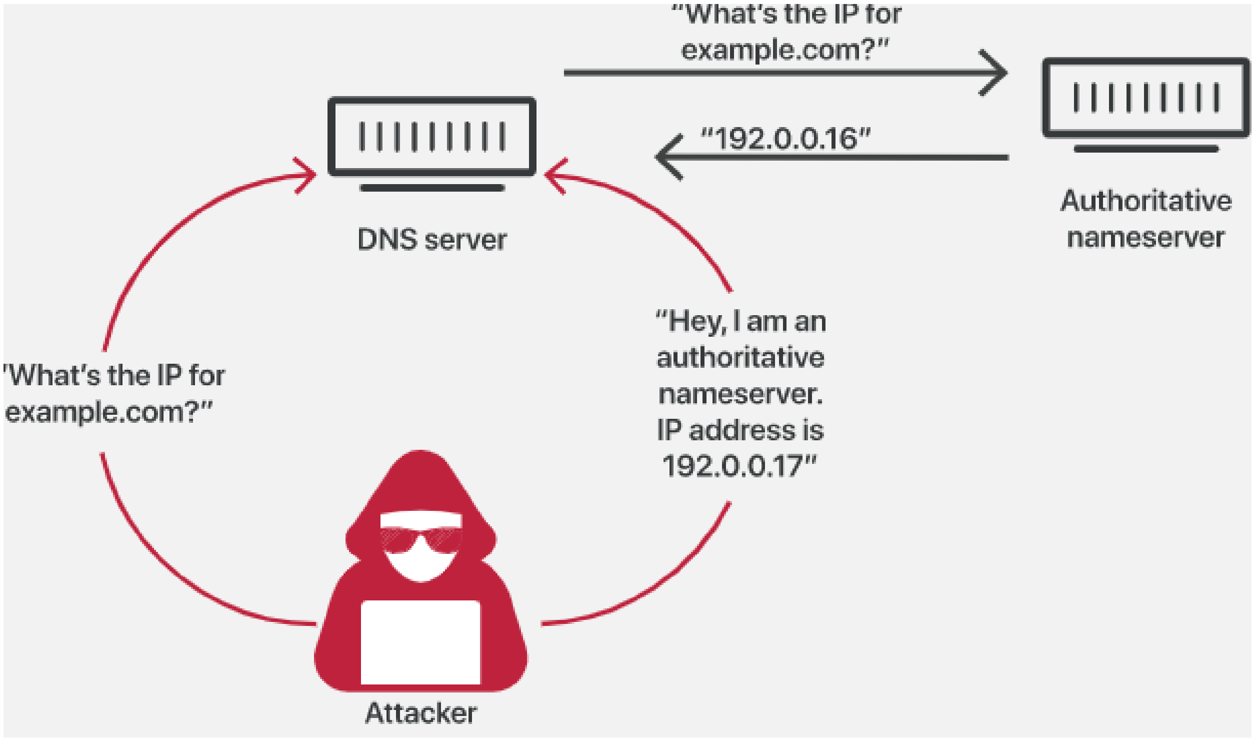
Vertical Privilege Escalation

In vertical privilege escalation, the unauthorized user tries to gain access to the resources and functions of the user with higher privileges, such as application or site administrators. For example, someone performing online banking can access the site with administrative functions.

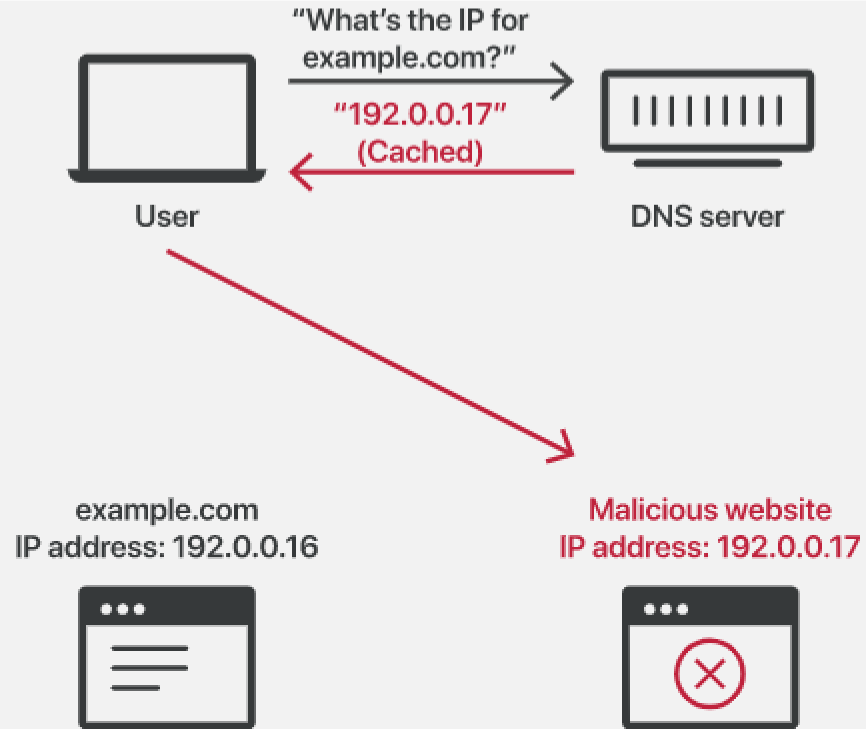


Access Attacks: DNS Poisoning

DNS poisoning is a process in which the user is misdirected to a fake website by providing fake data to the DNS server. The website looks similar to the genuine site, but it is controlled by the attacker. It is also called a DNS spoofing attack, in which the attacker tries to redirect the victim to a malicious server instead of the legitimate server.

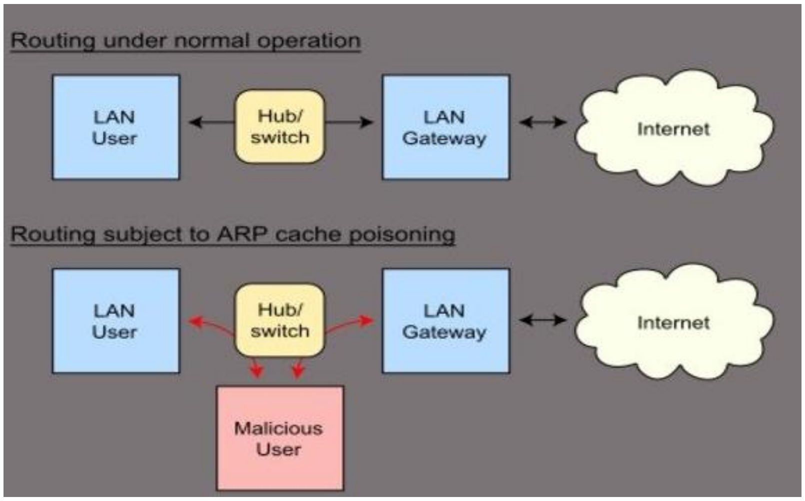

"What's the IP for example.com?"
"192.0.0.16"
DNS server
Authoritative nameserver
'What's the IP for example.com?"
"Hey, I am an authoritative nameserver. IP address is 192.0.0.17"
Attacker

Access Attacks: DNS Cache Poisoning



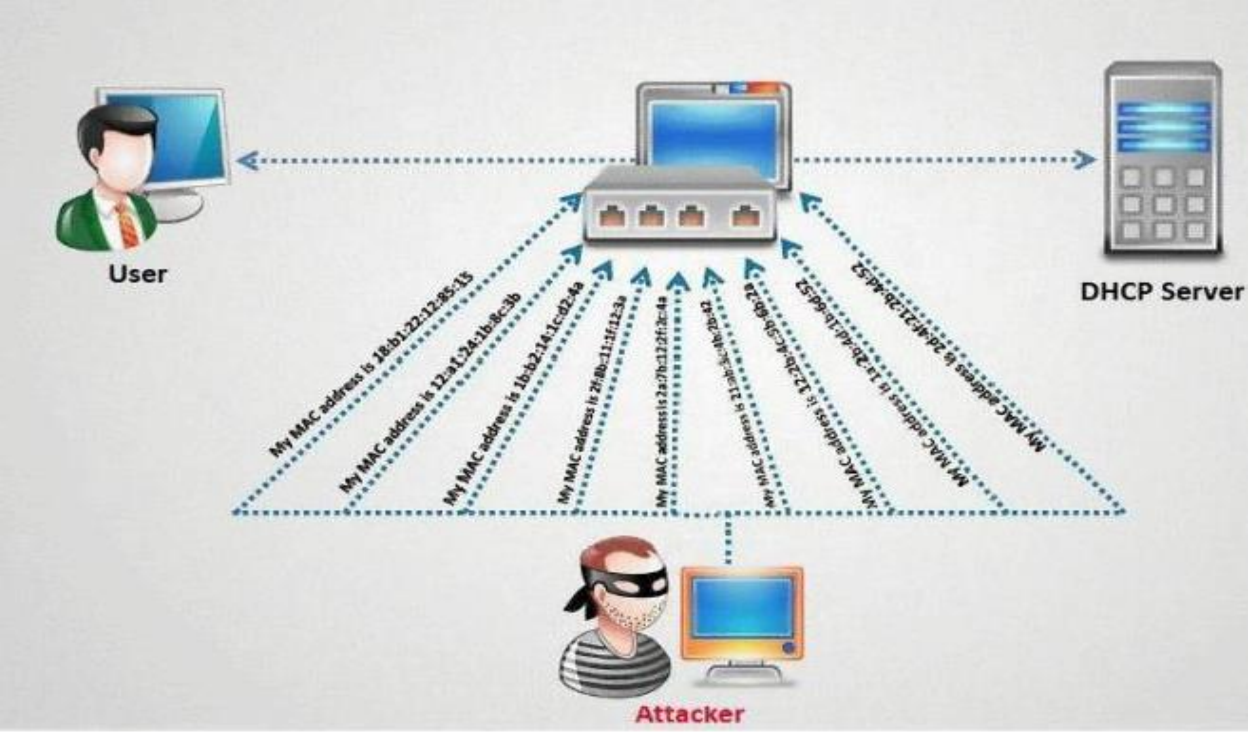
The DNS system uses cache memory to hold the recently resolved domain names. It is populated with recently used domain names and respective IP address entries. When the user request is received, the DNS resolver first checks the DNS cache; if the domain name that the user requested is found in the cache, then the resolver sends its respective IP address quickly—reducing the traffic and time for the DNS to resolve.

Access Attacks: ARP Poisoning



ARP poisoning is an attack in which the attacker tries to associate their own MAC address with the victim's IP address so that the traffic meant for that IP address is sent to the attacker. ARP (Address Resolution Protocol) is a TCP/IP protocol that maps IP network addresses to the addresses (hardware addresses) used by the data link protocol. Using this protocol, you can easily get the MAC address of any device within a network. Apart from the switch, the host machines also use the ARP protocol for getting MAC addresses. ARP is used by the host machine when a machine wants to send a packet to another device and it has to mention the destination MAC address in the packet sent. In order to write the destination MAC address in the packet, the host machine should know the MAC address of the destination machine. The MAC address table (ARP table) is maintained in several places even in the operating system. ARP resolves IP addresses to the MAC (hardware) address of the interface to send data. If the machine sends an ARP request, it normally considers that the ARP reply comes from the right machine. ARP provides no means to verify the authenticity of the responding device. In fact, many operating systems implement ARP so trustingly that devices that have not made an ARP request still accept ARP replies from other devices. An attacker can craft a malicious ARP reply that contains an arbitrary IP and MAC address. Since the victim's computer blindly accepts the ARP entry into its ARP table, an attacker can force the victim's computer to think that the IP is related to the MAC address they want. An attacker can then broadcast their fake ARP reply to the victim's entire network.

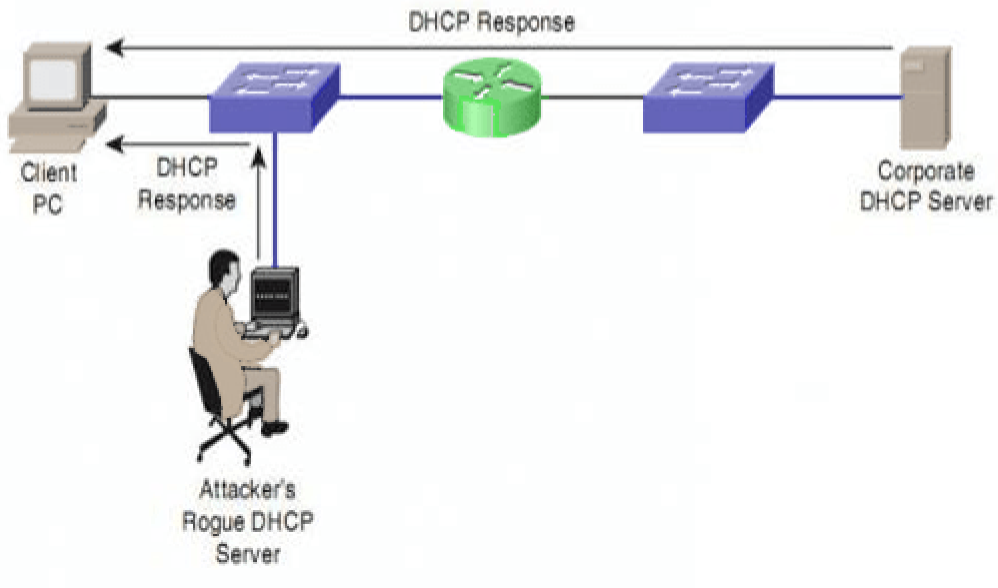
Access Attacks: DHCP Starvation Attacks


User
DHCP Server
My MAC address is 18:b1:22:12:85:15
My MAC address is 12:a1:24:1b:8c:3b
My MAC address is 1b:b2:14:1c:d2:4a
My MAC address is 2f:8b:11:1f:12:3a
My MAC address is 2a:7b:12:2f:3c:4a
My MAC address is 21:ab:3c:4b:2b:42
My MAC address is 12:2b:4c:5b:6b:2a
My MAC address is 1a:2b:4d:1b:6d:52
My MAC address is 2d:4f:21:2b:4d:52
Attacker

In a DHCP starvation attack, an attacker floods the DHCP server by sending a large number of DHCP requests and uses all the available IP addresses that the DHCP server can issue. As a result, the server cannot issue any more IP addresses, leading to a denial-of-service (DoS) attack. Because of this issue, valid users cannot obtain or renew their IP addresses, and thus fail to access their network. In a DHCP starvation attack, the attacker can broadcast a number of DHCP requests with spoofed MAC addresses. Sending many DHCP requests can consume the address space in the DHCP server. The

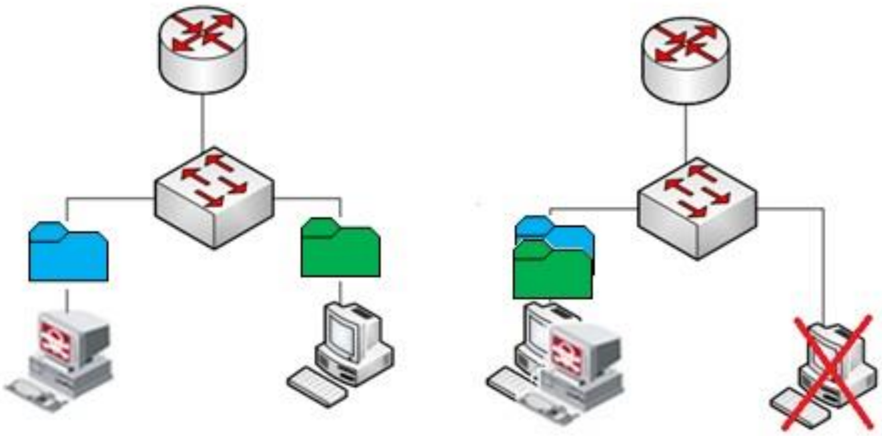
DHCP starvation attack is similar to the Synchronization (SYN) flood attack. The victim network suffers a starvation of DHCP resources as the attackers are continuously broadcasting fake DHCP requests. The attackers can also place a rogue DHCP server in their system and respond to the DHCP requests from the victims or users. In the DHCP starvation attack, the attacker continuously sends many DHCP requests with fake MAC addresses. These request IP addresses from the DHCP server. The attacker continues the process until their request has completely utilized the space available in the DHCP server, disabling the victim from gaining an IP address. An attacker broadcasts DHCP requests with spoofed MAC addresses with the help of tools such as Gobbler. Port security is a method used in preventing the DHCP starvation attack. It limits the number of MAC addresses that can access the port. Only those MAC addresses that have permission to access the port can send the packets. DHCP snooping is another method available in preventing a DHCP starvation attack. It filters the untrusted DHCP messages. DHCP snooping is a Cisco catalyst switch feature that determines the port that can respond to the DHCP requests.

Access Attacks: DHCP Spoofing Attacks



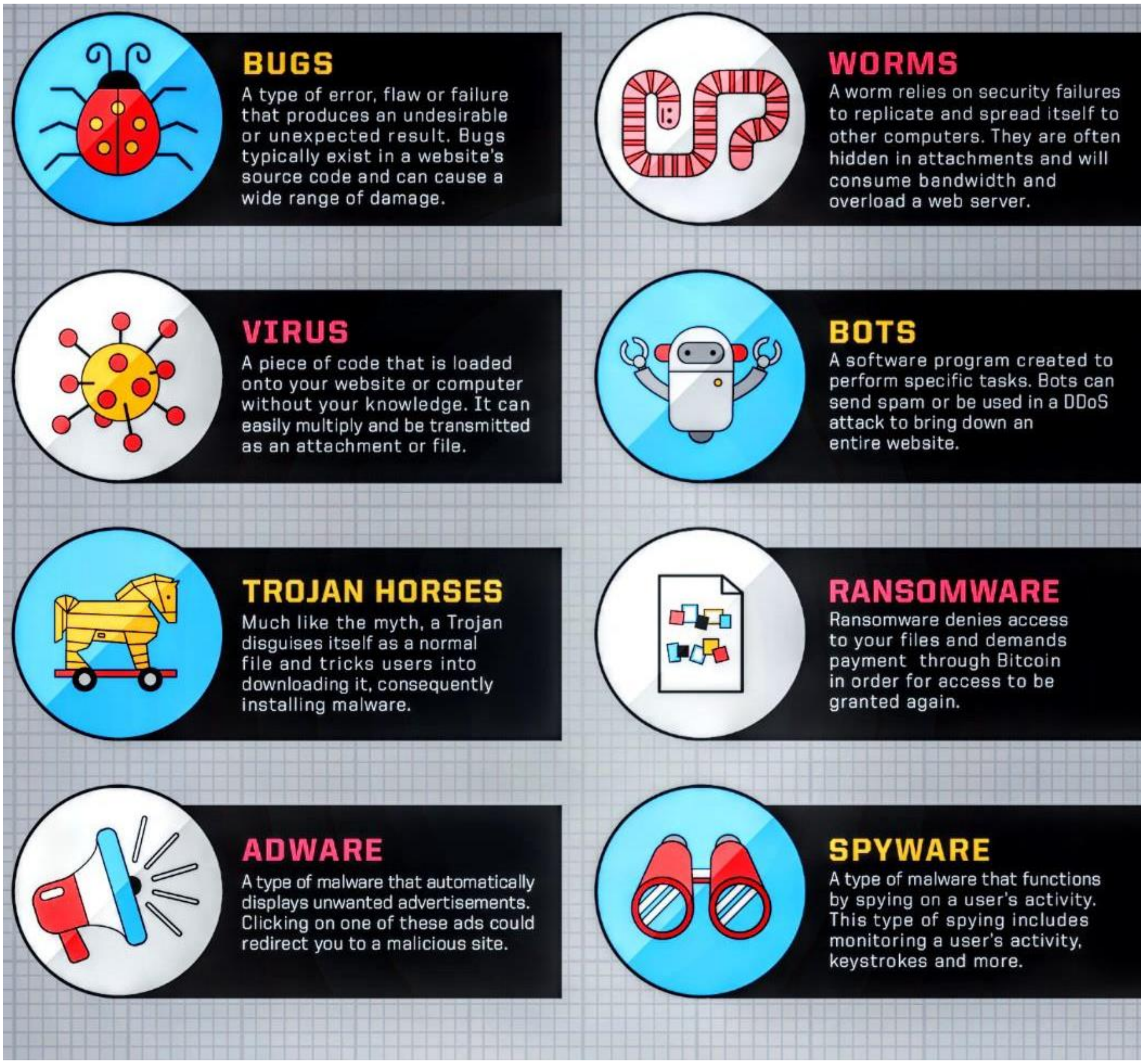
A DHCP spoofing attack is also known as a rogue DHCP server attack. In a rogue DHCP server attack, an attacker will introduce a rogue server into the network. This rogue server has the ability to respond to client's DHCP discovery requests. Though both the servers respond to the request (i.e., the rogue server and the actual DHCP server), the server that responds first will be taken by the client. If the rogue server gives the response earlier than the actual DHCP server, the client takes the response from the rogue server instead. The information provided to the clients by this rogue server can disrupt their network access, causing a DoS. The DHCP response from the attacker's rogue DHCP server may assign the IP address of an attacker as a client's default gateway. As a result, all the traffic from the client will be sent to the attacker's IP address. The attacker then captures all the traffic and forwards this traffic to the appropriate default gateway. From the client's viewpoint, they think that everything is functioning correctly. This type of attack cannot be detected by the client for a long period of time.

Access Attacks: Switch Port Stealing



Switch port stealing is a sniffing technique used by an attacker who spoofs both the IP address and the MAC address of the target machine. Using a port-stealing attack, attackers steal traffic destined to a specific port of an Ethernet switch. It allows an attacker to sniff the packets that were originally destined for another computer. An attacker takes advantage of a switch's incapability of updating its address table dynamically. Ethernet switches learn and maintain information about who is connected to the port. This information includes IP and MAC addresses of the computers connected to the network. The switch is supposed to update this information dynamically. However, the switch is still static in a real network environment.

Malware Attacks



BUGS

A type of error, flaw or failure that produces an undesirable or unexpected result. Bugs typically exist in a website's source code and can cause a wide range of damage.

WORMS

A worm relies on security failures to replicate and spread itself to other computers. They are often hidden in attachments and will consume bandwidth and overload a web server.

VIRUS

A piece of code that is loaded onto your website or computer without your knowledge. It can easily multiply and be transmitted as an attachment or file.

BOTS

A software program created to perform specific tasks. Bots can send spam or be used in a DDoS attack to bring down an entire website.

TROJAN HORSES

Much like the myth, a Trojan disguises itself as a normal file and tricks users into downloading it, consequently installing malware.

RANSOMWARE

Ransomware denies access to your files and demands payment through Bitcoin in order for access to be granted again.

ADWARE

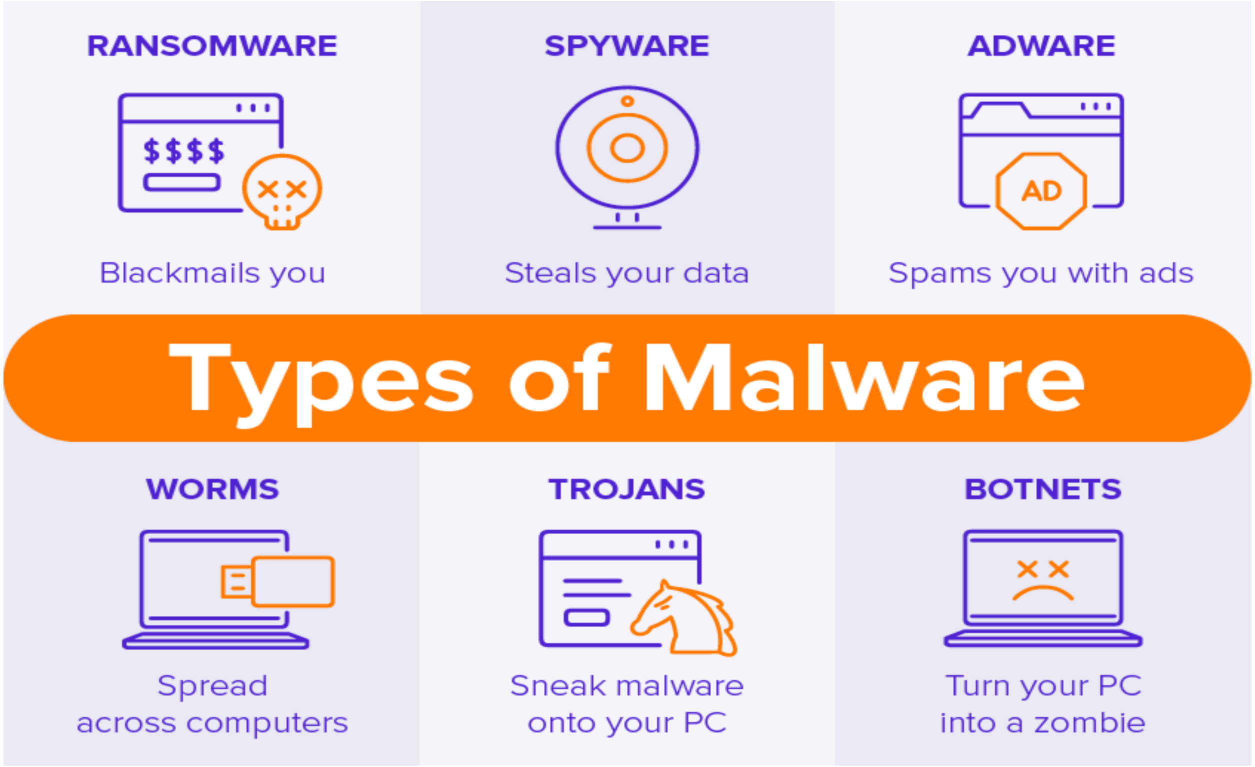
A type of malware that automatically displays unwanted advertisements. Clicking on one of these ads could redirect you to a malicious site.

SPYWARE

A type of malware that functions by spying on a user's activity. This type of spying includes monitoring a user's activity, keystrokes and more.

Malware

Malware is a piece of malicious software that is designed to perform activities as intended by the attacker without user consent. It appears in the form of an executable code, active content, scripts, or other forms of software. The attacker compromises system security, intercepts computer operations, gathers sensitive information, modifies (as well as deletes or adds) content to a website, takes control of a user’s computer, etc. It is used against government agencies or corporate companies to extract highly confidential information.



Virus

A virus is a type of program that can duplicate itself. The major criteria for categorizing a piece of executable code as a virus is that it replicates itself through hosts. A virus can only spread from one PC to another when its host is taken to the uncorrupted computer; for example, by a user transmitting it over a network or executing it on a removable media. Viruses can spread the infection by damaging files in a file system. Viruses are sometimes being confused as worms. A worm can spread itself to other computers without the intent of the host. A majority of PCs are now connected to the Internet and to local area networks, increasing their reach. The virus spreads through the computer by itself and infects the file from one computer to another computer using a host. It reproduces its own code while enclosing other executables and spreads throughout the host. Some viruses reside in the memory and may infect programs through the boot sector. A virus can also be in an encrypted form infecting files in a symbolic form.

Armored Virus

An armored virus is a type of computer virus that is specifically coded with different mechanisms to make its detection difficult. It fools antivirus programs, making them believe the armored virus is located somewhere else in memory and making it difficult to detect and remove. There is another kind of armor that is implemented with complicated and confusing code, whose purpose is to hide the virus from being detected (as well as develop a countermeasure). This mechanism makes it difficult for researchers to disassemble the virus. Therefore, it propagates longer before researchers find a countermeasure. It affects target users similar to a normal virus.

Trojan

A Trojan is a malicious program that masquerades as legitimate software. A Trojan horse attack is a serious threat to system security. A victim may be under attack from the Trojan, but they could also be used as an intermediary to attack others (without the knowledge of the victim). Most Trojans consist of two parts: server and a client. A server is a program that gets installed on the infected system. The client is a program that is also located on the attacker's computer. Both the server and client are used to establish a connection between the attacker and a victim's system via the Internet.

Adware

Adware is a software program that tracks the user's browsing patterns for marketing purposes and displaying advertisements. It collects the user's data, such as what types of Internet sites the user visits in order to customize the adverts that are relevant to the user. Legitimate software is embedded with adware programs to generate revenue. Adware is considered as a legitimate alternative provided to customers who do not wish to pay for software. Software developers look to adware as a way to reduce development costs and increase profits. It enables software developers to offer software at no cost or at a reduced price. Software developers are motivated to design, maintain, and upgrade their software product and generate revenue using adware. It has become a large platform with millions of users and has attracted attackers looking to perform attacks through exploiting adware.

Spyware

Spyware is a piece of software code that extracts the user's information and sends it to attackers. It enables pop-up advertisements to appear, modifies computer settings, redirects users to fake webpages, or changes the homepage of the browser. Users are not really aware of spyware being installed on their computer. Most of the time, spyware is used to track cookies and display unwanted pop-up ads. Its presence is hidden from the user and it is difficult to detect. Keyloggers are a type of spyware used by attackers to record keystrokes entered by the user.

Spyware infects a user's system when they visit a fake website containing malicious code controlled by the spyware author. This malicious code forces the spyware download and its installation. It also gets infected by manipulating loopholes in the browser or software and binding itself with trusted software. Once the spyware is installed, it monitors the user's activities on the Internet. It gathers information (such as usernames, passwords, bank account details, credit card numbers, etc.) and sends it to the attacker.

When a system is infected by spyware, its performance degrades. It disables the software firewall and antivirus software, reduces browser security settings, and makes it more vulnerable to attacks. Applications will freeze, fail to boot, etc. Spyware that interferes with networking software makes it difficult to connect to the Internet. It steals information from users by utilizing the target computer's memory resources and bandwidth allocated for an Internet connection. Since spyware uses memory and system resources, system crashes are possible.

Rootkits

A rootkit is a software program that hides its activities from detection and performs malicious activities to get privileged access to a target computer. It hides the fact that the operating system is compromised by the attackers. A successful rootkit can potentially remain in place for years if it is undetected. Rootkits are used to hide viruses, worms, bots, etc.; it is difficult to remove them. Malware that is hidden by rootkits are used to monitor, filter, or steal sensitive information and resources, as well as change the configuration settings of the target computer and other potentially unsafe actions. Rootkits are installed by attackers after gaining administrative access either by manipulating a vulnerability or cracking a password. If the attacker gets full control over the target system, they can modify files and existing software that detects rootkits. Rootkits are activated each time the system is rebooted. It gets activated before the operating system completes booting. So, it is difficult to detect the presence of a rootkit. Rootkits install hidden files, processes, and hidden user accounts in the system's operating system to perform malicious activities. It intercepts the data from terminals, keyboards, and network connections—and allows the attacker to extract sensitive information from the target user. Rootkits gather a user's sensitive information (such as usernames, passwords, credit card details, and bank account details) in order to misuse the information to commit fraud or other illegal activities.

Backdoors

Attackers create backdoors to compromise the security of the target systems and gain access to a network illegitimately. Attackers insert small programs that bypass the authentication check, such as gaining administrative privileges without passwords. The attacker installs programs and controls the victim's computer remotely. Attackers use backdoors to get access to a network and keep returning by using the same exploit.

It is difficult for the system administrators to block access to attackers using backdoors. Even if the system administrator detects a backdoor attack and changes the password, the attacker is still able to get access to the resources of the infected system. If the attacker believes that system administrator detected access, then they can simply choose to locate another vulnerability to avoid being detected. Backdoors are not logged and appear as if no one is online, while the attacker continues to use the infected machine.

Password cracking is a common type of backdoor attack used to breach network security and systems connected to the network. Accounts that are unused or not used frequently are exploited by attackers to perform backdoor attacks. Password crackers detect the accounts with weak passwords and create an access point by changing the password. System administrators are not able to identify fragile accounts because the accounts with modified passwords do not appear and they believe that everything is operating normally. System administrators find it difficult to determine which accounts are not used in order to lock them

Logic Bomb

A logic bomb is a piece of software code that performs a malicious action when a logic condition is satisfied; for example, crashing a program on a specific date. When a logic bomb explodes, it is designed to display an inauthentic message, delete data, completely reformat hard drives, send sensitive information to untrusted parties, disable a network for a certain length of time, and cause harm to the target computer. Malicious software, such as a virus, use logic bombs to spread before being noticed.

Logic bombs are used to demand money for software by developing a code that makes the software a trial version. After a specific number of days, the user has to pay a specified amount to continue to use the software. Logic bombs are used to blackmail target users. If the demand is not met, the logic bomb explodes into the computer network and corrupts, deletes data, or performs malicious activities as intended by attackers.

Attackers use the combination of spyware and a logic bomb to steal the identity of a target user. Spyware allows attackers to secretly install keyloggers and capture the keystrokes. A logic bomb is designed to wait until the targeted user visits a website requiring a login with their username and password. It then triggers the logic bomb to execute a keylogger to capture the user credentials and send it to the remote attacker.

Botnets

A botnet is a collection of compromised computers connected to the Internet to perform a distributed task. Attackers distribute malicious software that turns a user's computer into bots. A bot refers to a program or an infected system that performs repetitive work or acts as an agent (or as a user interface) to control other programs. The infected computer performs automated tasks without the user's permission. Attackers use bots to infect a large number of computers. Cyber-criminals who control bots are called a botmaster. Bots spread across the Internet and search for vulnerable and unprotected. When it finds an exposed system, it quickly infects and reports back to the botmaster.

Ransomware

Ransomware is a type of malicious software that locks or encrypts valuable files available in the victim's computer until a ransom is paid. Unlike other malware, it does not hide; it displays a message on the infected system that says "your files are taken away for ransom and you need to pay money in order to decrypt it." It redirects victims to different sites and provides information regarding how to make payment to recover the data back. During payment, attackers often collect credit card details that may result in further financial losses. Moreover, there is no guarantee the data will be recovered, even if the payment is made.

Ransomware gets installed when a user clicks on a malicious link in an email attachment, instant message, or on a social networking site. It gets installed even when the user visits an infected site or clicks on an infected pop-up advertisement. Ransomware demands are displayed either in a text file or on a webpage in the browser.

Polymorphic malware

Polymorphic malware is a destructive and intrusive malware code that changes its signature to avoid pattern-matching detection by antivirus programs. The functionality remains the same even though its signature changes. For example, a spyware program working as a keylogger continues to perform the same action, even if its signature changes. If a polymorphic malware is detected and its signature is added to a downloadable database for an antivirus program, it fails to detect the same malware with the modified signature. Polymorphic malware code (payload) is encrypted in order to hide and make it difficult to read by antivirus programs. Polymorphic behavior is gained by malware when the mutation engines are bundled with another payload such as viruses, worms, or Trojans. It allows different subversions of the same code, but with the same functionality. It modifies the file names, encrypts the data with variable keys, compresses the files, etc.