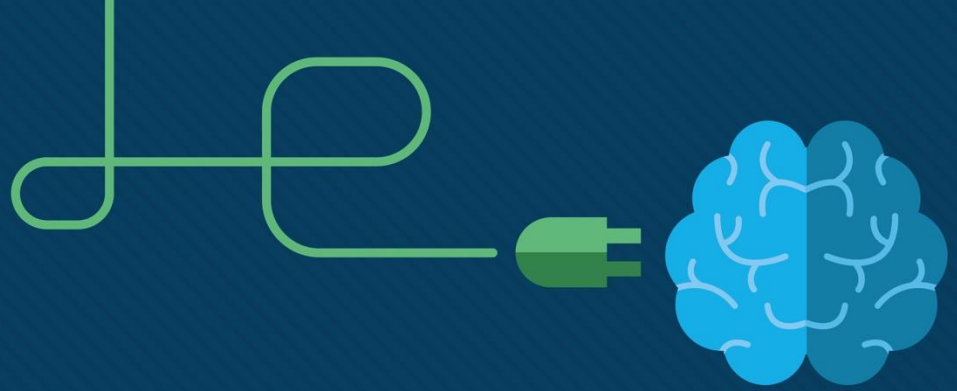


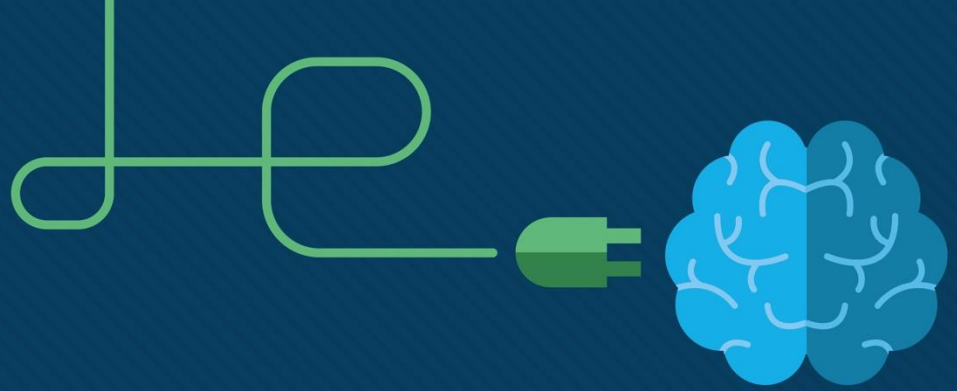
Chapter 7: Network Attacks: A Deeper Look

Instructor Materials

CCNA Cybersecurity Operations v1.1

Chapter 7: Network Attacks: A Deeper Look

CCNA Cybersecurity Operations v1.1
Planning Guide



Chapter 7: Network Attacks: A Deeper Look

CCNA Cybersecurity Operations v1.1

Chapter 7 - Sections & Objectives

- 7.1 Network Monitoring and Tools
  - Explain network traffic monitoring.
    - Explain the importance of network monitoring.
    - Explain how network monitoring is conducted.
- 7.2 Attacking the Foundation
  - Explain how TCP/IP vulnerabilities enable network attacks.
    - Explain how IP vulnerabilities enable network attacks.
    - Explain how TCP and UDP vulnerabilities enable network attacks.
- 7.3 Attacking What We Do
  - Explain how common network applications and services are vulnerable to attack.
    - Explain IP vulnerabilities.
    - Explain how network application vulnerabilities enable network attacks.

7.1 Network Monitoring and Tools

Network Security Topology

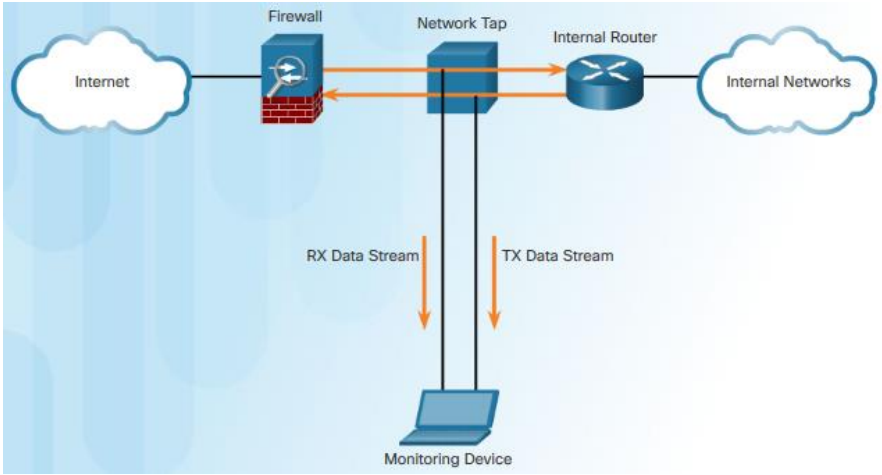
- All networks are targets and need to be secured using a defense-in-depth approach.
- Security analysts must be intimately familiar with normal network behavior because abnormal network behavior typically indicates a problem.

Network Monitoring Methods

- Tools used to help discover normal network behavior include IDS, packet analyzers, SNMP, NetFlow, and others.
- Traffic information capture methods:
  - **Network TAPs** – Network test access points that forward all traffic including physical layer errors to an analysis device.
  - **Port mirroring** – enables a switch to copy frames of one or more ports to a Switch Port Analyzer (SPAN) port connected to an analysis device.

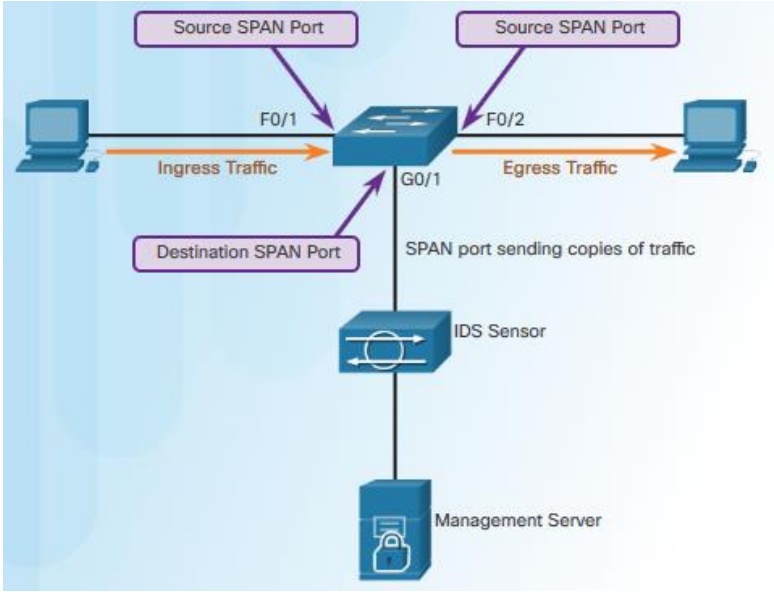
Network Taps

- A network tap is typically 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.
- Taps are also typically fail-safe, which means if it fails or loses power, traffic between the firewall and internal router is not affected.



Traffic Mirroring and SPAN

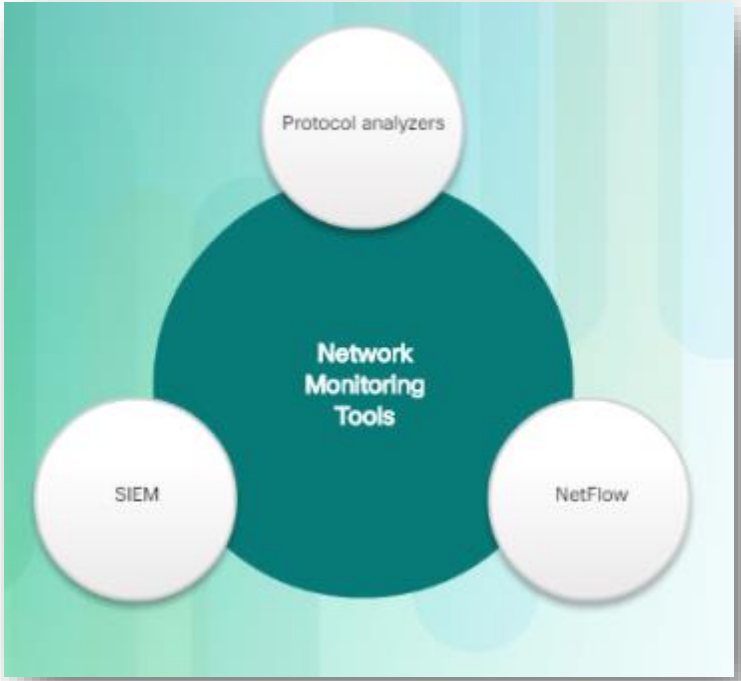
- Port mirroring enables the switch to copy frames of one or more ports to a Switch Port Analyzer (SPAN) port connected to an analysis device.
- In the figure, the switch will forward ingress traffic on F0/1 and egress traffic on F0/2 to the destination SPAN port G0/1 connecting to an IDS.
- The association between source ports and a destination port is called a SPAN session. In a single session, one or multiple ports can be monitored.



Network Security Monitoring Tools

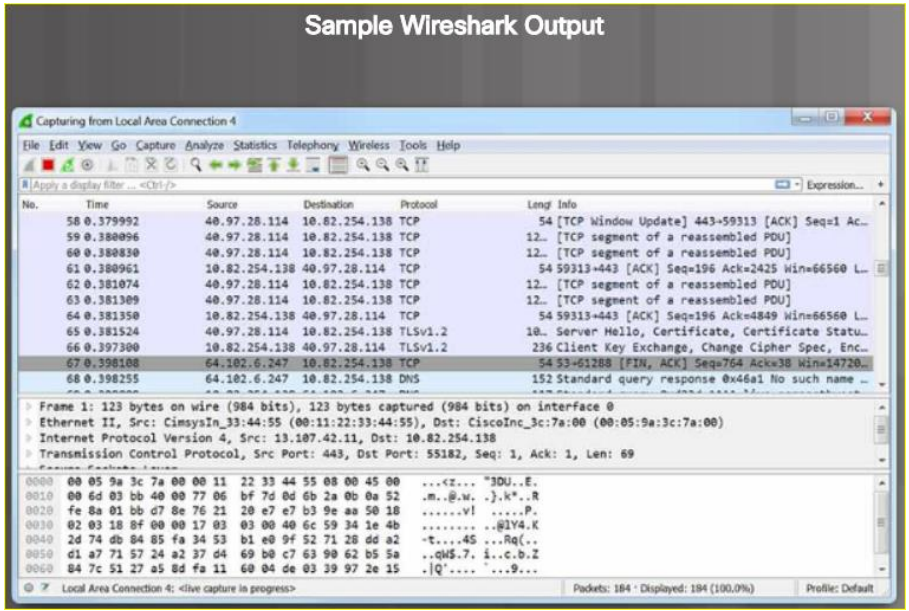
- **Monitoring Tools:**
  - **Protocol Analyzers** – Are programs used to capture traffic. Ex. Wireshark and Tcpdump.
  - **NetFlow** – Provides a complete audit trail of basic information about every IP flow forwarded on a device.
  - **SIEM** – Security Information Event Management systems provide 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.

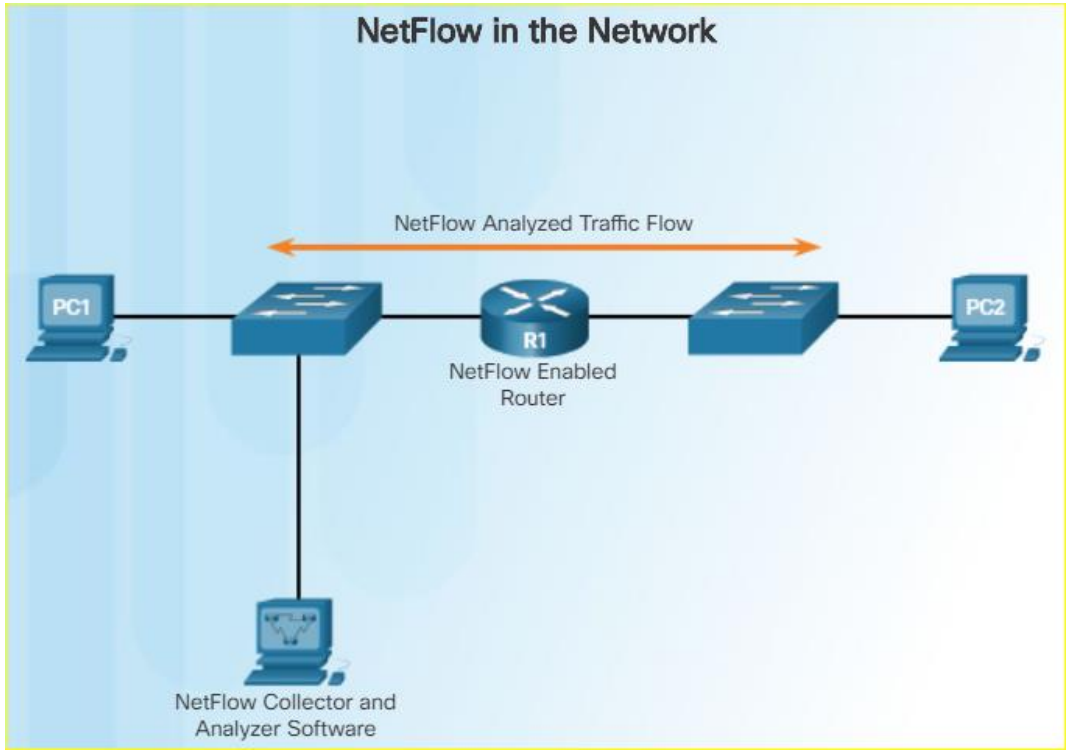


Network Protocol Analyzers

- Analysts can use protocol analyzers such as Wireshark and tcpdump to see network exchanges down to the packet level.
- Network protocol analyzers are also very useful for network troubleshooting, software and protocol development, and education. In security forensics, a security analyst may reconstruct an incident from relevant packet captures.



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.

SIEM

- Security Information Event Management (SIEM) systems provide real time reporting and long-term analysis of security events.
- SIEM includes the following essential functions:
  - **Forensic analysis** – The ability to search logs and event records from sources throughout the organization. It provides more complete information for forensic analysis.
  - **Correlation** – Examines logs and events from different systems or applications, speeding detection of and reaction to security threats.
  - **Aggregation** - Aggregation reduces the volume of event data by consolidating duplicate event records.
  - **Reporting** - Reporting presents the correlated and aggregated event data in real-time monitoring and long-term summaries.

SIEM Systems

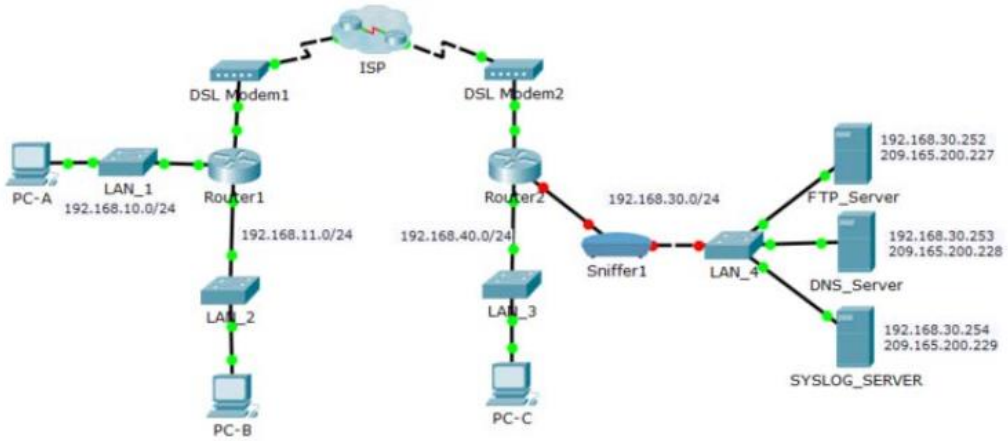
- Splunk is one of the more popular proprietary SIEM systems used by Security Operation Centers.
- As an open source option, this course uses the ELK suite for SIEM functionality. ELK is an acronym for three open source products from Elastic:
- **Elasticsearch** - Document oriented full text search engine
- **Logstash** - Pipeline processing system that connects "inputs" to "outputs" with optional "filters" in between
- **Kibana** - Browser based analytics and search dashboard for Elasticsearch

Packet Tracer – Logging Network Activity

Networking Academy

Packet Tracer - Logging Network Activity

Topology



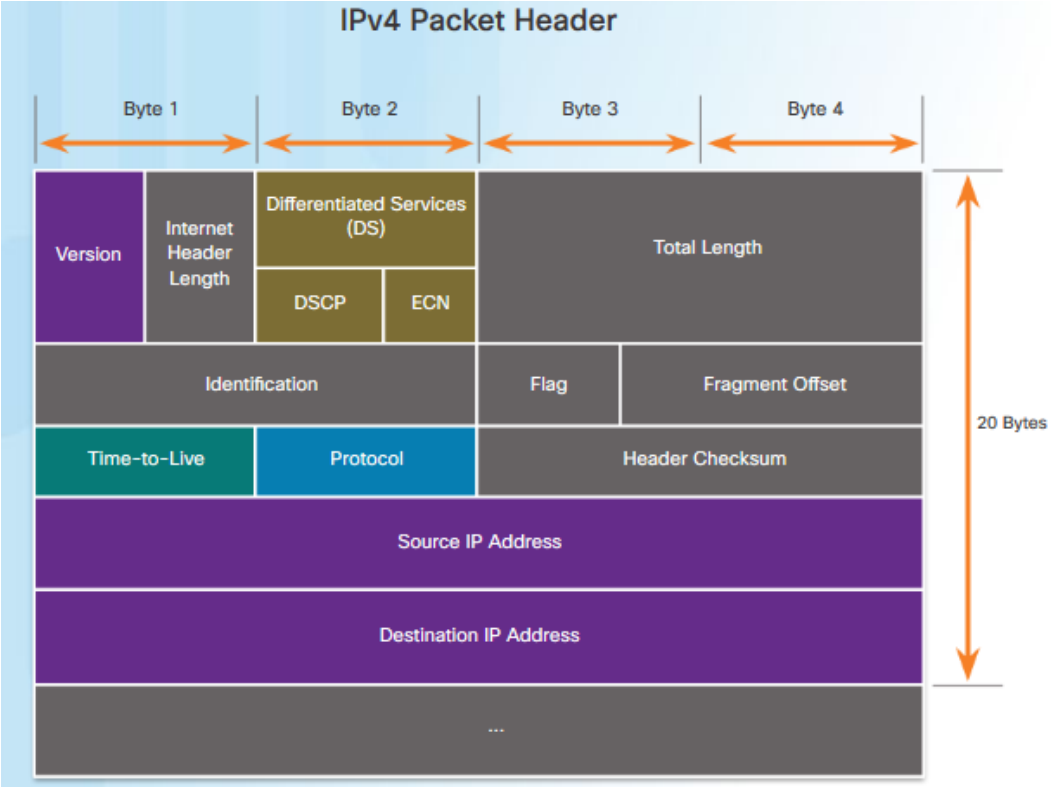
7.2 Attacking the Foundation

IPv4 and IPv6

- It is important for security analysts to understand the different fields in both the IPv4 and IPv6 headers because threat actors can tamper with packet information.

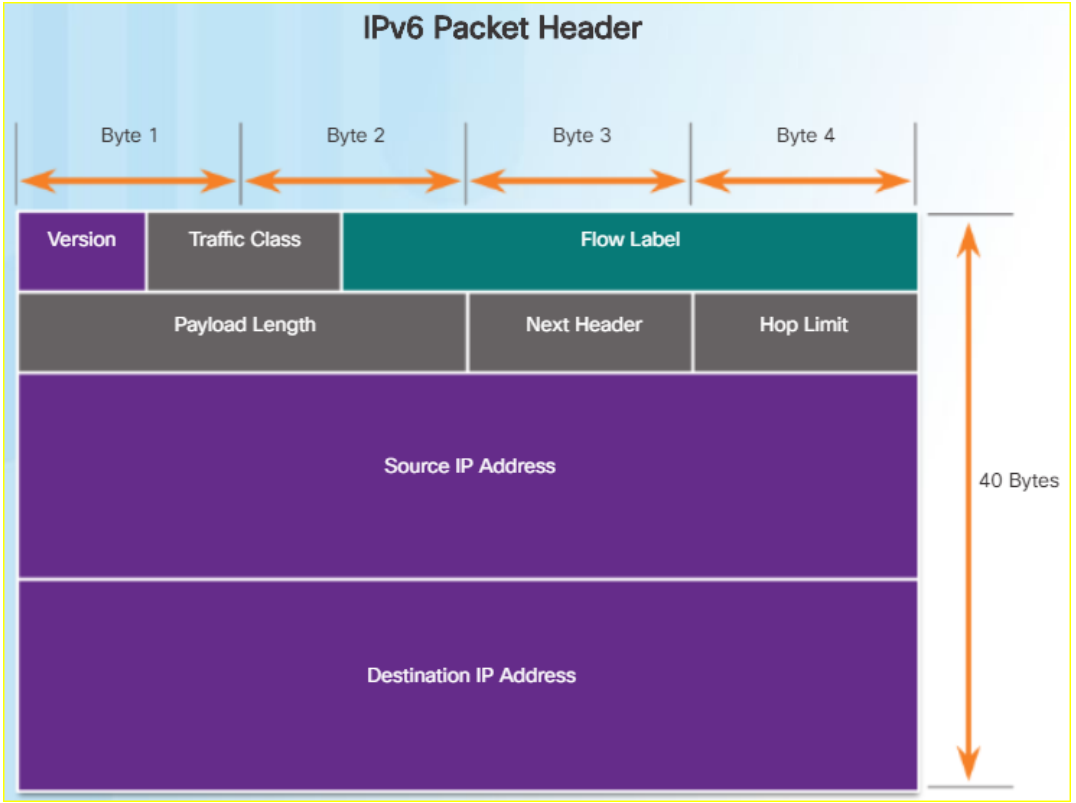
The IPv4 Packet Header

- There are 10 fields in the IPv4 packet header:
  - Version
  - Internet Header length
  - Differentiated Services or DiffServ (DS)
  - Total length
  - Identification, Flag, and Fragment offset
  - Time-to-Live (TTL)
  - Protocol
  - Header checksum
  - Source IPv4 Address
  - Destination IPv4 Address
  - Options and Padding

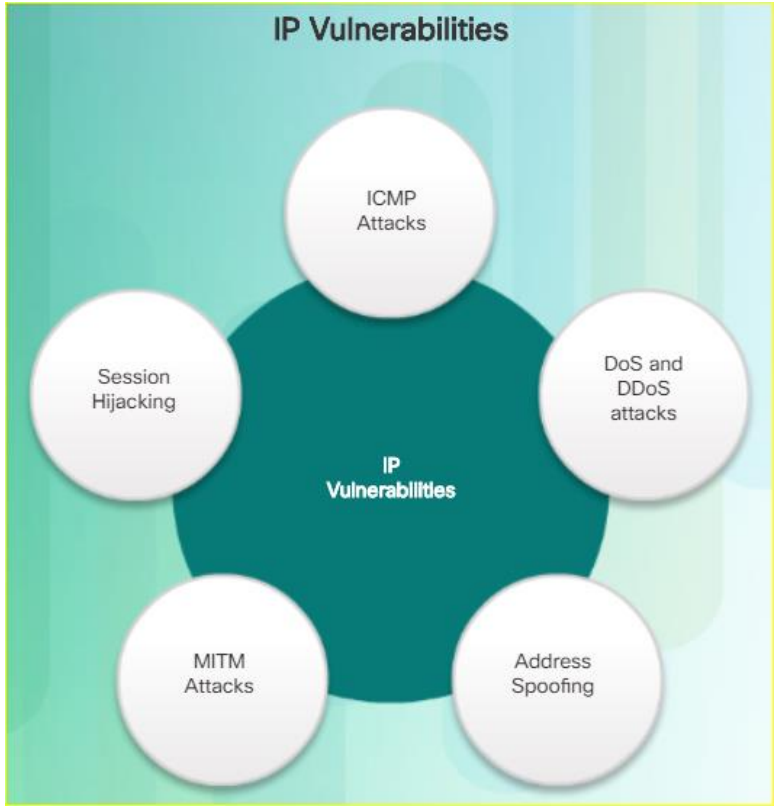


The IPv6 Packet Header

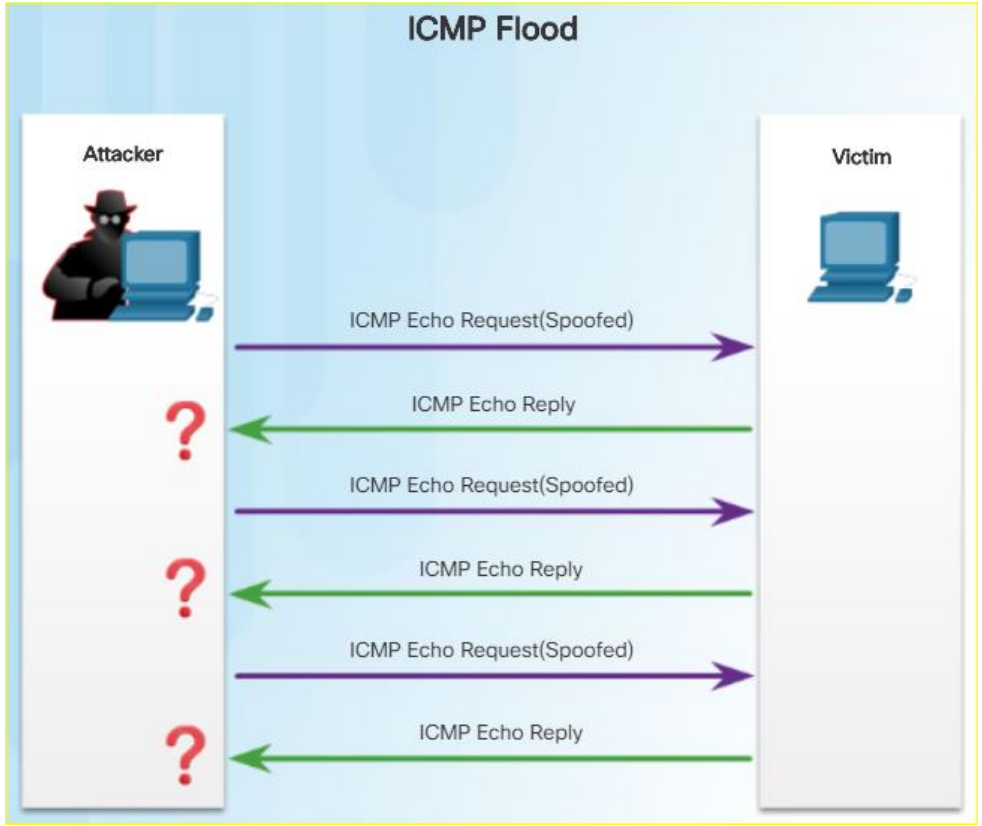
- There are 8 fields in the IPv4 packet header:
  - Version
  - Traffic Class
  - Flow Label
  - Payload Length
  - Next Header
  - Hop Limit
  - Source IPv6 Address
  - Destination IPv6 Address



IP Vulnerabilities



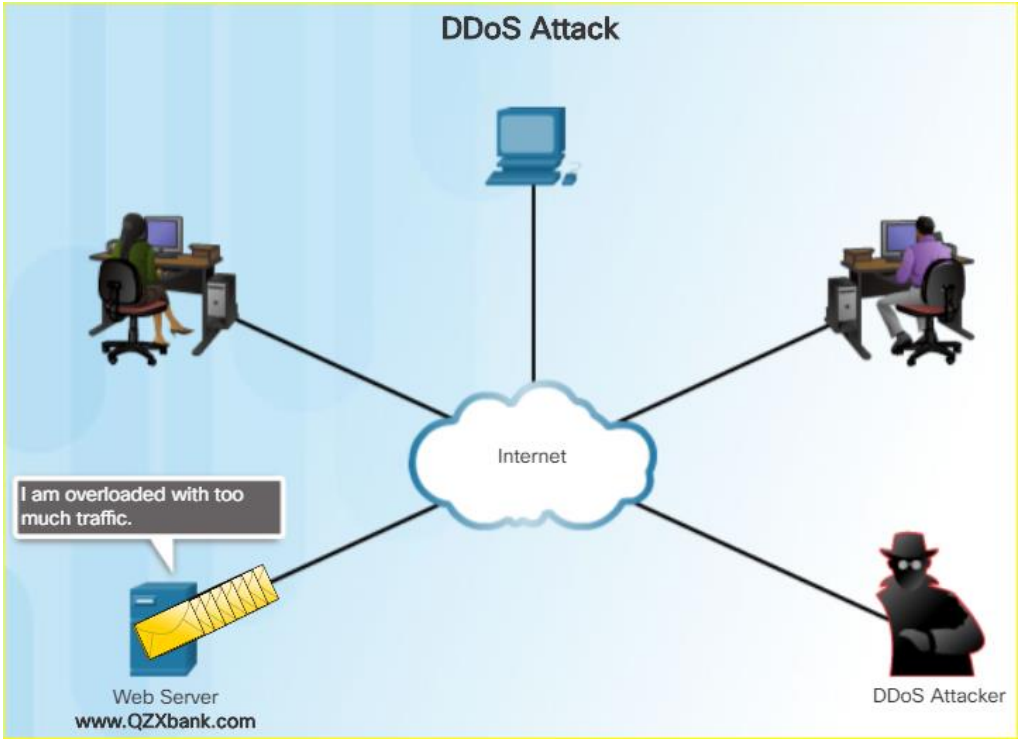
ICMP Attacks



- 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.
- Common ICMP messages of interest to threat actors include:
  - **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.

DoS Attacks

- The goal of a Denial of Service (DoS) attack is to prevent legitimate users from gaining access to websites, email, online accounts, and other services.
- There are two major sources of DoS attacks:
  - **Maliciously Formatted Packets** – Threat actors craft a maliciously formatted packet and forward it to a susceptible host, causing the host to crash or become extremely slow.
  - **Overwhelming Quantity of Traffic** – Threat actors overwhelm a target network, host, or application, causing them to crash or become extremely slow.
- A distributed DoS (DDoS) attack combines multiple DoS attacks.

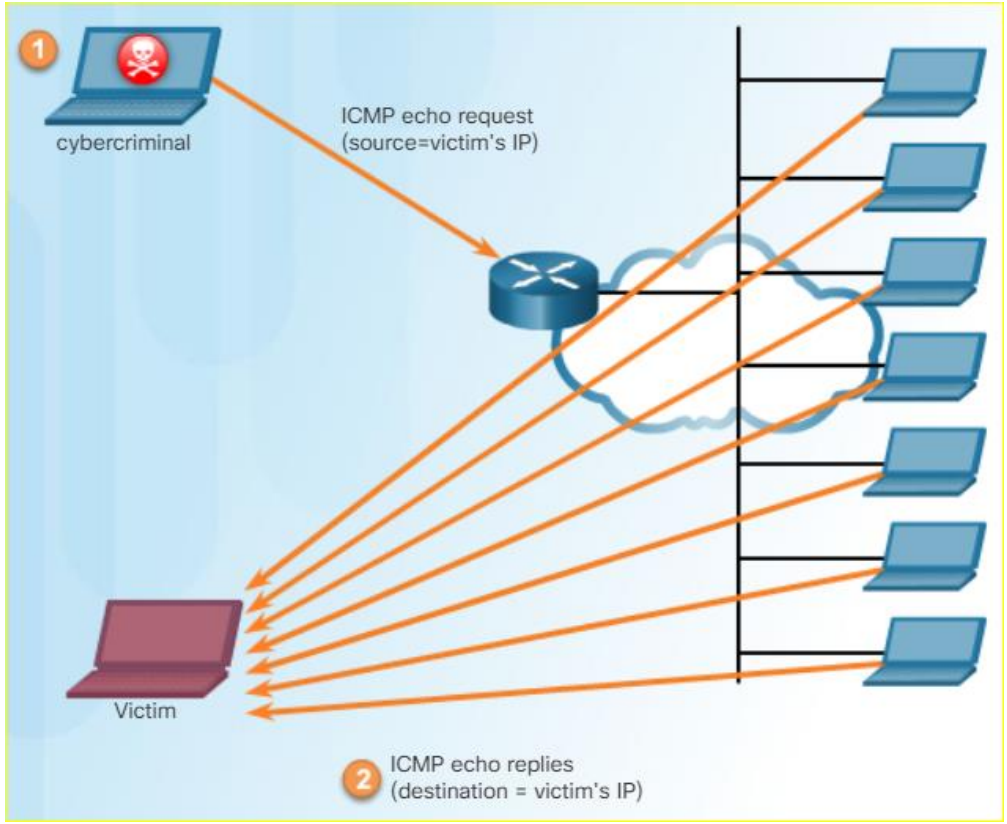


Amplification and Reflection Attacks

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

1. **Amplification** - The threat actor forwards ICMP echo request messages that contain the source IP address of the victim to a large number of hosts.

2. **Reflection** - These hosts all reply to the spoofed IP address of the victim to overwhelm it.



DDoS Attacks

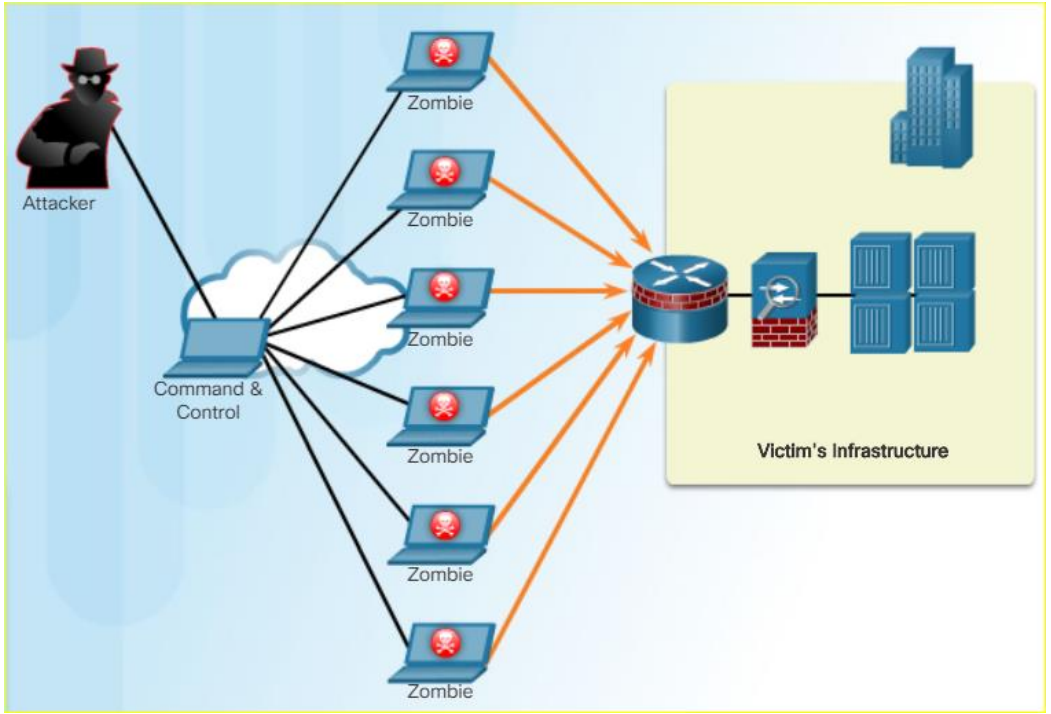
- A DDoS attack is larger in magnitude than a DoS attack because it originates from multiple, coordinated sources. DDoS attacks introduced new terms such as botnet, handler systems, and zombie computers.

A DDoS attack could proceed as follows:

1. The threat actor (botmaster) builds or purchases the use of a botnet of zombie hosts. The command-and-control (CnC) server communicates with zombies over a covert channel using IRC, P2P, DNS, HTTP, or HTTPS.

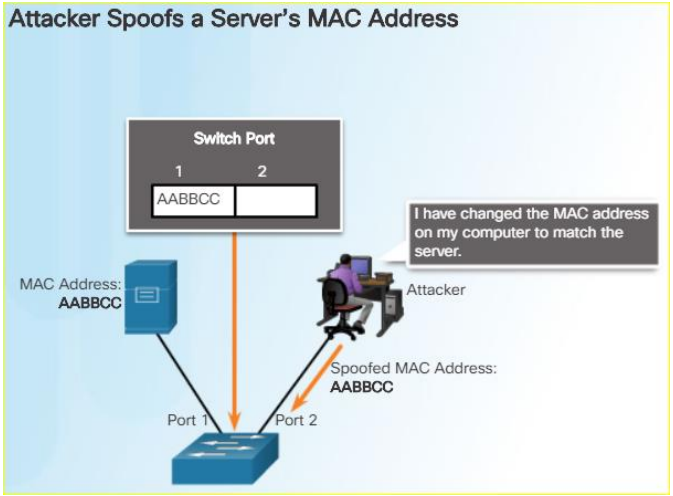
2. Zombie computers continue to scan and infect more targets to create more zombies.

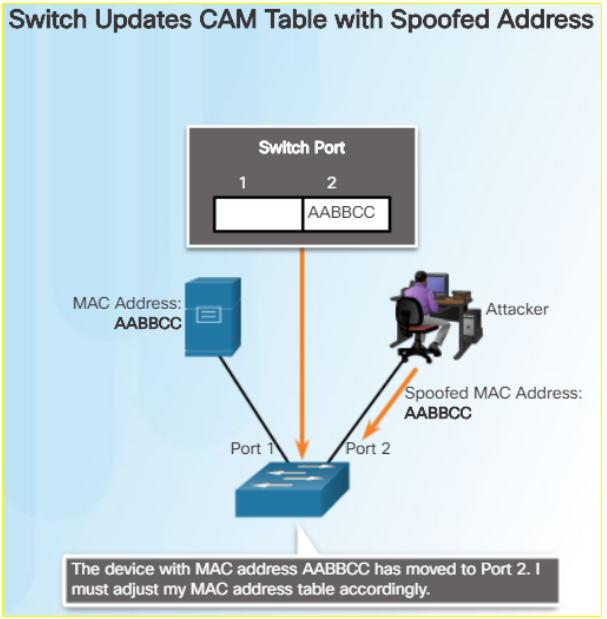
3. When ready, the botmaster uses the handler systems to make the botnet of zombies carry out the DDoS attack on the chosen target.



Address Spoofing Attacks

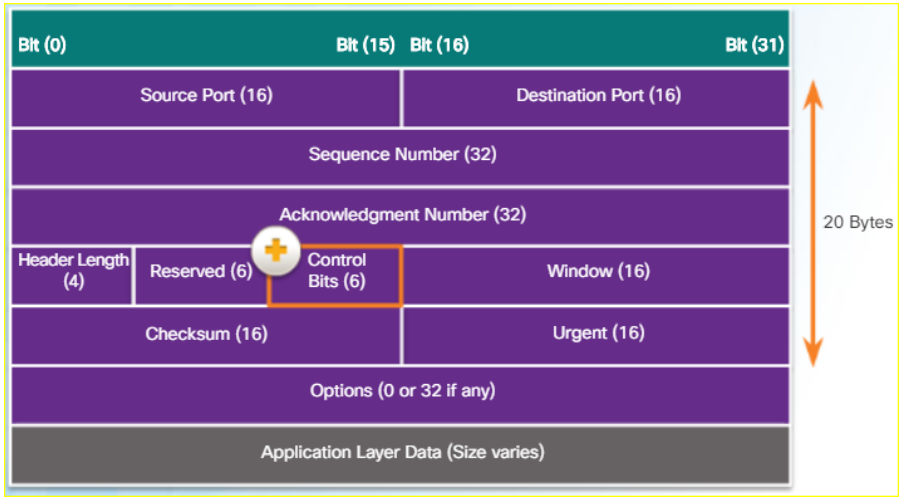
- IP address spoofing attacks occur when a threat actor creates packets with false source IP address information to either hide the identity of the sender or to pose as another legitimate user. The attacker can then gain access to otherwise inaccessible data or circumvent security configurations.

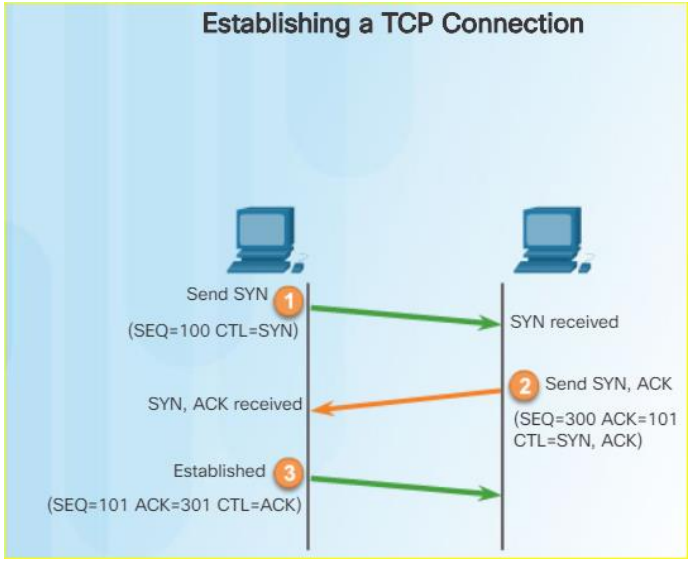




TCP and UDP Vulnerabilities

TCP

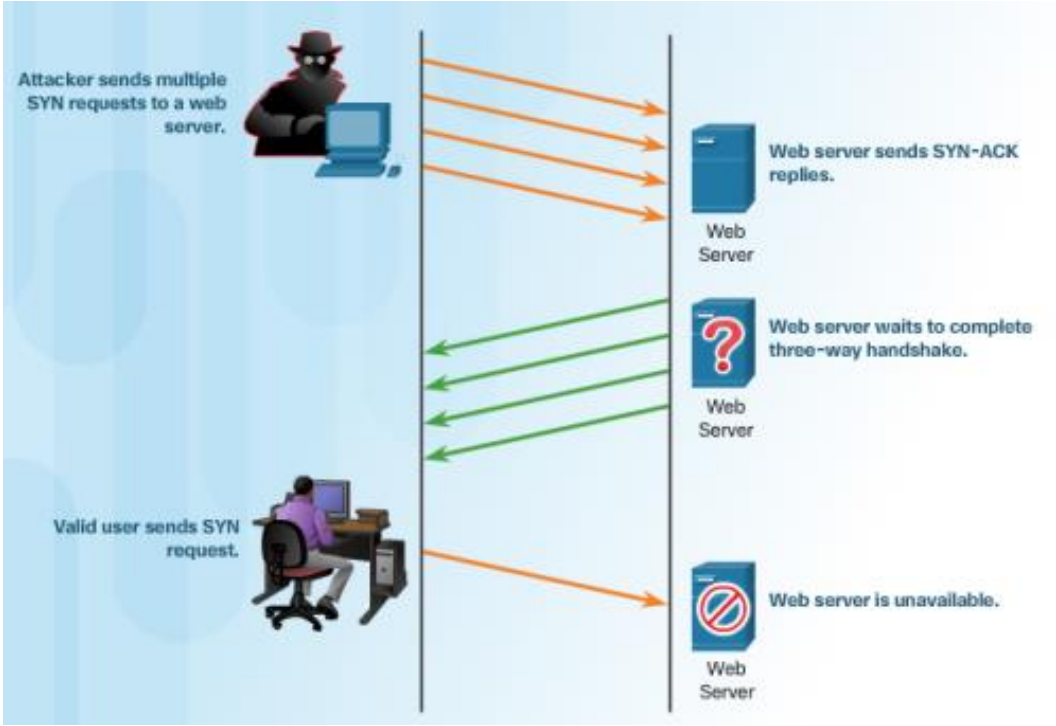




- TCP segment information appears immediately after the IP header.
- TCP provides the following services:
  - **Reliable delivery**
  - **Flow control**
  - **Stateful communication**

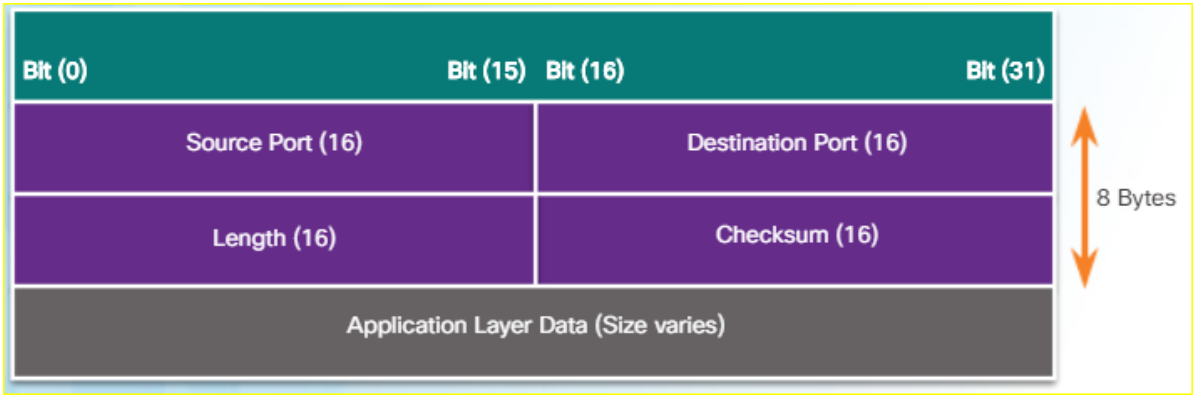
TCP Attacks

- Although the TCP protocol is a connection-oriented and reliable protocol, there are still vulnerabilities that can be exploited.
- TCP attacks target expected protocol behaviors:
  - TCP SYN flood attack
  - TCP reset attack
  - TCP session hijacking



UDP and UDP Attacks

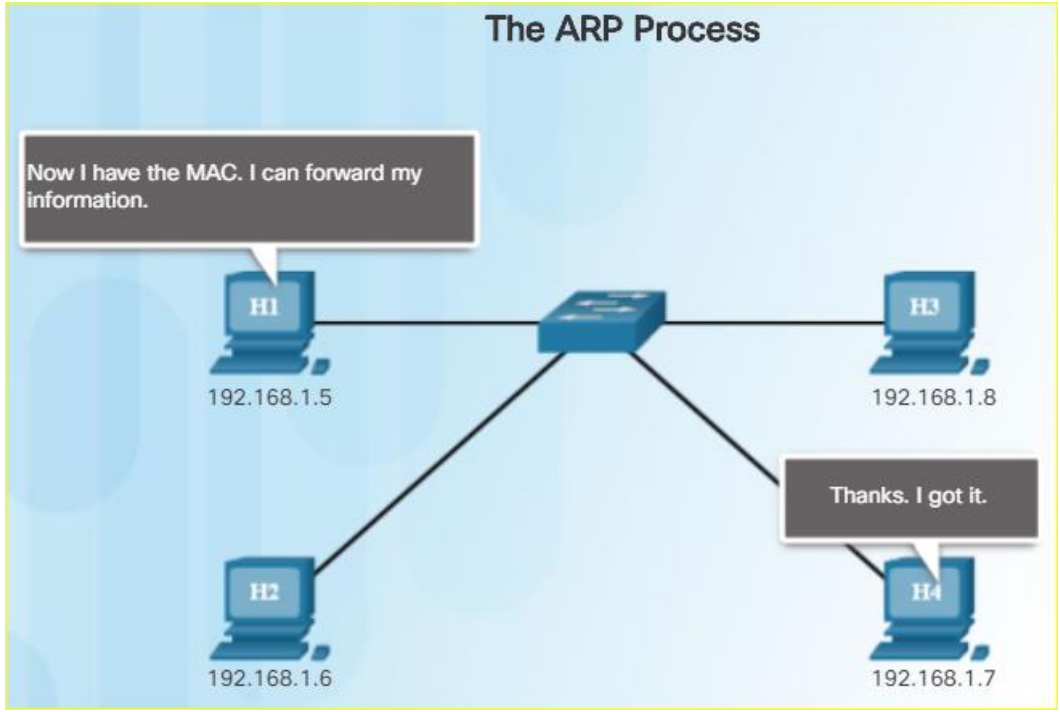
- UDP is a simple protocol that provides the basic transport layer functions. UDP is commonly used by DNS, TFTP, NFS, and SNMP. It is also used with real-time applications such as media streaming or VoIP. UDP is a connectionless transport layer protocol.
- By default, UDP is not protected by any encryption. The lack of encryption allows anyone to look at the traffic, change it, and send it on to its destination.
- UDP protocol attacks target the lack of protocol behaviors (UDP):
  - UDP checksum attack
  - UDP flood attack
  - UDP DoS attacks



7.3 Attacking What We Do

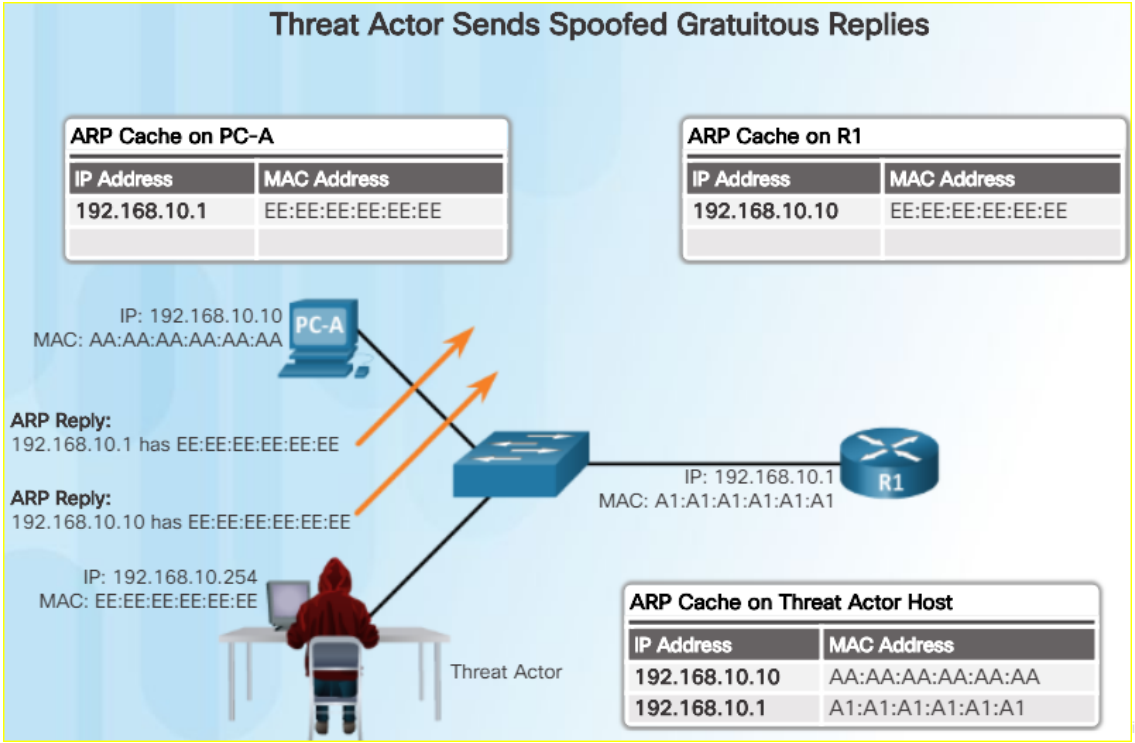
ARP Vulnerabilities

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



ARP Cache Poisoning

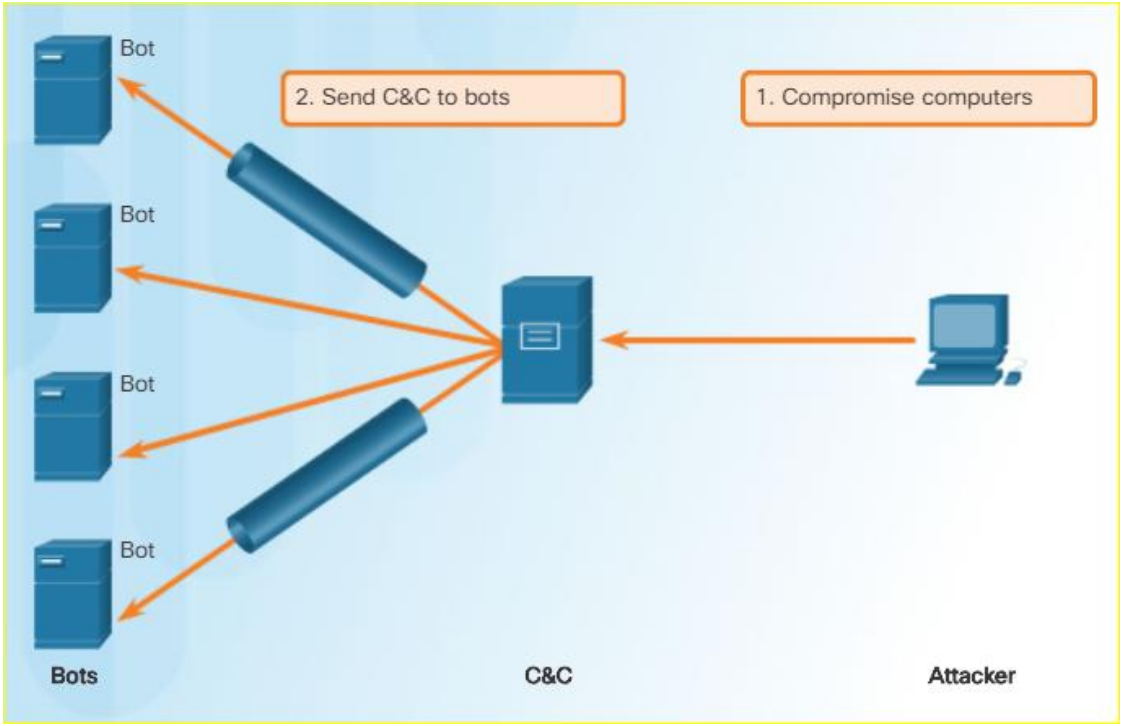
- ARP cache poisoning attacks deliberately poison the cache of another computer with spoofed IP address to MAC address mappings.



DNS Attacks

- DNS servers resolve names to IP addresses and are a major target of attackers. Some DNS exploits are:
  - **DNS Open Resolvers** (public name servers)
  - **DNS Stealth Attacks**
  - **DNS Shadowing Attacks** – hijacked domains are used to create subdomains which are used to resolve to malicious web sites
  - **DNS Tunneling Attacks** - hides malicious instructions inside DNS queries and responses

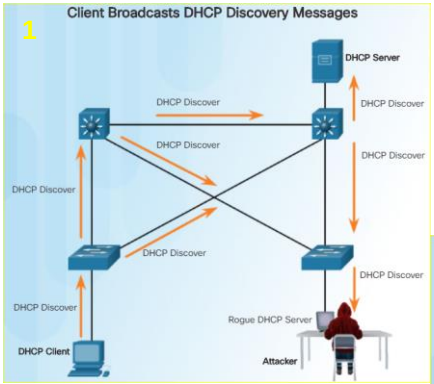
DNS Tunneling

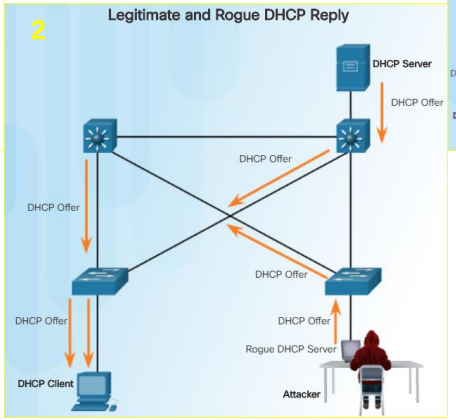


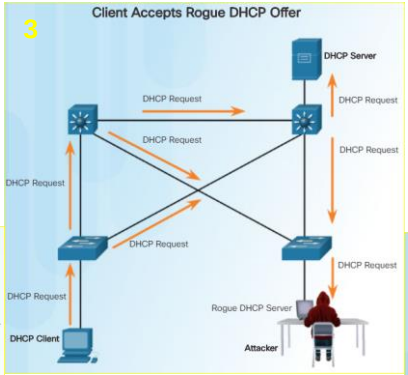
- Threat actors who use DNS tunneling place non-DNS traffic within DNS traffic. This method often circumvents security solutions. For the threat actor to use DNS tunneling, the different types of DNS records such as TXT, MX, SRV, NULL, A, or CNAME are altered.

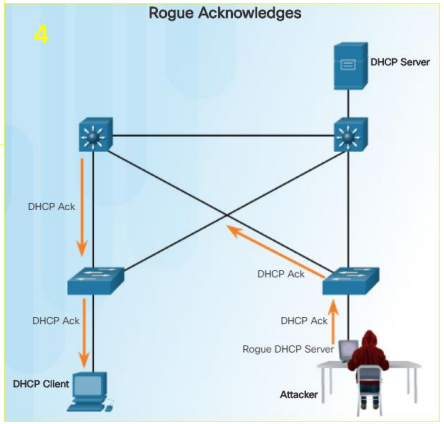
DHCP

- A DHCP attack could result in every host on the network communicating with malicious DNS servers and gateways. A DHCP spoofing attack creates a rogue DHCP server to serve falsified information.









Lab – Exploring DNS Traffic

Networking Academy

Lab – Exploring DNS Traffic

Objectives

Part 1: Capture DNS Traffic

Part 2: Explore DNS Query Traffic

Part 3: Explore DNS Response Traffic

Background / Scenario

Wireshark is an open source packet capture and analysis tool. Wireshark gives a detailed breakdown of the network protocol stack. Wireshark allows you to filter traffic for network troubleshooting, investigate security issues, and analyze network protocols. Because Wireshark allows you to view the packet details, it can be used as a reconnaissance tool for an attacker.

In this lab, you will install Wireshark on a Windows system and use Wireshark to filter for DNS packets and view the details of both DNS query and response packets.

Required Resources

- 1 Windows PC with Internet access and Wireshark installed

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.

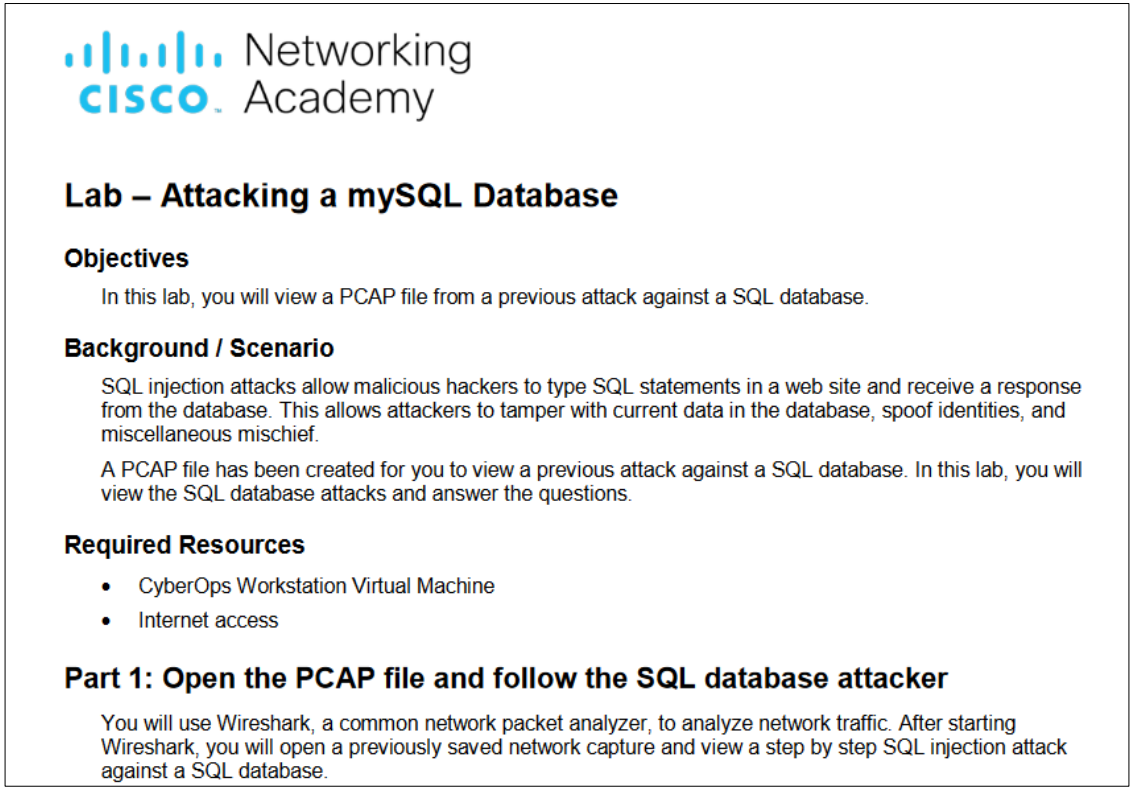
Email

- Email messages are accessed from many different devices that are often not protected by the company's firewall.
  - **Attachment-based attacks** – email with malicious executable files attached.
  - **Email spoofing** – phishing attack where the message appears to come from a legitimate source.
  - **Spam email** – unsolicited email with advertisements or malicious content.
  - **Open mail relay server** – massive amount of spam and worms can be sent by misconfigured email servers.
  - **Homoglyphs** – phishing scheme where text characters (hyperlinks) look similar to real text and links.

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.

Lab – Attacking a mySQL Database



Networking Academy

Lab – Attacking a mySQL Database

Objectives

In this lab, you will view a PCAP file from a previous attack against a SQL database.

Background / Scenario

SQL injection attacks allow malicious hackers to type SQL statements in a web site and receive a response from the database. This allows attackers to tamper with current data in the database, spoof identities, and miscellaneous mischief.

A PCAP file has been created for you to view a previous attack against a SQL database. In this lab, you will view the SQL database attacks and answer the questions.

Required Resources

- CyberOps Workstation Virtual Machine
- Internet access

Part 1: Open the PCAP file and follow the SQL database attacker

You will use Wireshark, a common network packet analyzer, to analyze network traffic. After starting Wireshark, you will open a previously saved network capture and view a step by step SQL injection attack against a SQL database.

Lab – Reading Server Logs

Networking Academy

Lab – Reading Server Logs

Objectives

Part 1: Reading Log Files with Cat, More, and Less

Part 2: Log Files and Syslog

Part 3: Log Files and Journalctl

Background / Scenario

Log files are an important tool for troubleshooting and monitoring. Different application generates different log files, each one containing its own set of fields and information. While the field structure may change between log files, the tools used to read them are mostly the same. In this lab, you will learn about common tools used to read log file and practice using them.

Required Resources

- CyberOps Workstation Virtual Machine
- Internet access

Part 1: Reading Log Files with Cat, More, Less, and Tail

Log files are files used to record specific events triggered by applications, services or the operating system itself. Usually stored as plain-text, log files are an indispensable resource for troubleshooting.

7.4 Chapter Summary

Summary

- All networks are targets and need to be secured using a defense-in-depth approach.
- Tools used to help discover normal network behavior include IDS, packet analyzers, SNMP, NetFlow, and others.
- A network tap forwards all traffic including physical layer errors to an analysis device.
- 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.
- Analysts can use protocol analyzers such as Wireshark and tcpdump to see network exchanges down to the packet level.
- NetFlow can be used for network and security monitoring, network planning, and traffic analysis; however, it does not capture the content.
- Security Information Event Management (SIEM) systems provide real time reporting and long-term analysis of security events.
- Splunk and ELK are two proprietary SIEM systems used by Security Operation Centers.

Summary (Cont.)

- Security analysts must understand the different fields in both the IPv4 and IPv6 headers because threat actors can tamper with packet information.
- There are 10 fields in the IPv4 packet header: Version, Internet header length, Differentiated Services or DiffServ (DS), Total length, Identification, Flag, and Fragment offset, Time-to-Live (TTL), Protocol, Header checksum, Source IPv4 Address, Destination IPv4 Address, Options and Padding.
- There are 8 fields in the IPv4 packet header: Version, Traffic Class, Flow Label, Payload Length, Next Header, Hop Limit, Source IPv6 Address, Destination IPv6 Address
- IP vulnerabilities include ICMP attacks, DoS and DDoS attacks, address spoofing, MITM attacks, and session hijacking.
- 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.

Summary (Cont.)

- The goal of a Denial of Service (DoS) attack is to prevent legitimate users from gaining access to websites, email, online accounts, and other services.
- Threat actors often use amplification and reflection techniques to create DoS attacks.
- A DDoS attack is larger than a DoS attack because it originates from multiple sources. DDoS attacks introduced terms such as botnet, handler systems, and zombie computers.
- 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.
- TCP provides the following services: reliable delivery, flow control, stateful communication.
- Although the TCP protocol is a connection-oriented and reliable protocol, there are still vulnerabilities that can be exploited.
- UDP is a simple protocol that provides the basic transport layer functions. UDP is commonly used by DNS, TFTP, NFS, and SNMP. It is also used with real-time applications such as media streaming or VoIP. UDP is a connectionless transport layer protocol.

Summary (Cont.)

- Hosts broadcast an ARP Request to other hosts on the segment to determine the MAC address of a host with a particular IP address.
- ARP cache poisoning attacks deliberately poison the cache of another computer with spoofed IP address to MAC address mappings.
- DNS servers resolve names to IP addresses and are a major target of attackers.
- Threat actors who use DNS tunneling place non-DNS traffic within DNS traffic.
- A DHCP spoofing attack creates a rogue DHCP server to serve falsified information.
- Browsing the Web (http and https) is possibly the largest vector of attack. Security analysts should have in depth knowledge of how web attacks work.
- Email messages are accessed from many different devices that are often not protected by the company's firewall.
- Web applications commonly connect to a relational database. Because relational databases often contain sensitive data, databases are a frequent target for attacks.

New Terms

- amplification and reflection technique
- ARP cache poisoning
- Blind spoofing
- Cross-Site Scripting (XSS)
- DNS tunneling
- domain generation algorithms
- domain shadowing
- double IP flux
- fast flux
- Homoglyphs
- HTTP 302 cushioning
- iFrame
- network tap
- Non-blind spoofing
- OS fingerprinting
- port mirroring
- session hijacking
- SQL Injection
- Switch Port Analyzer (SPAN)

Cybersecurity Operations Certification

This chapter covers the following areas in the Cybersecurity Operations Certification:

From 210-250 SECFND - Understanding Cisco Cybersecurity Fundamentals:

- **Domain 1: Network Concepts**
  - 1.2 Describe the operation of the following protocols: IP, TCP, UDP, ICMP.
  - 1.3 Describe the operation of the following network services: ARP, DNS, DHCP.
  - 1.11 Compare and contrast the characteristics of data obtained from taps or traffic mirroring and Netflow in the analysis of network traffic.

Cybersecurity Operations Certification (Cont.)

This chapter covers the following areas in the Cybersecurity Operations Certification:

From 210-250 SECOPS - Understanding Cisco Cybersecurity Fundamentals:

- **Domain 2: Network Intrusion Analysis**
  - 2.2 Describe the fields in the following protocol headers as they relate to intrusion analysis: IPv4, IPv6, UDP

Cybersecurity Operations Certification (Cont.)

This chapter covers the following areas in the Cybersecurity Operations Certification:

From 210-250 SECFND - Understanding Cisco Cybersecurity Fundamentals:

- **Domain 6: Attack Methods**
  - 6.2 Describe the following network attacks: DoS, DDoS, MiTM
  - 6.3 Describe the following web application attacks: SQL Injection, Command Injections, Cross Site Scripting.
  - 6.5 Describe the following end-point based attacks: Buffer Overflows, Command and Control (C2), Malware, Rootkit, Port Scanning, Host Profiling .


CISCO