4.1 DDoS, DNS poisoning, and domain hijacking

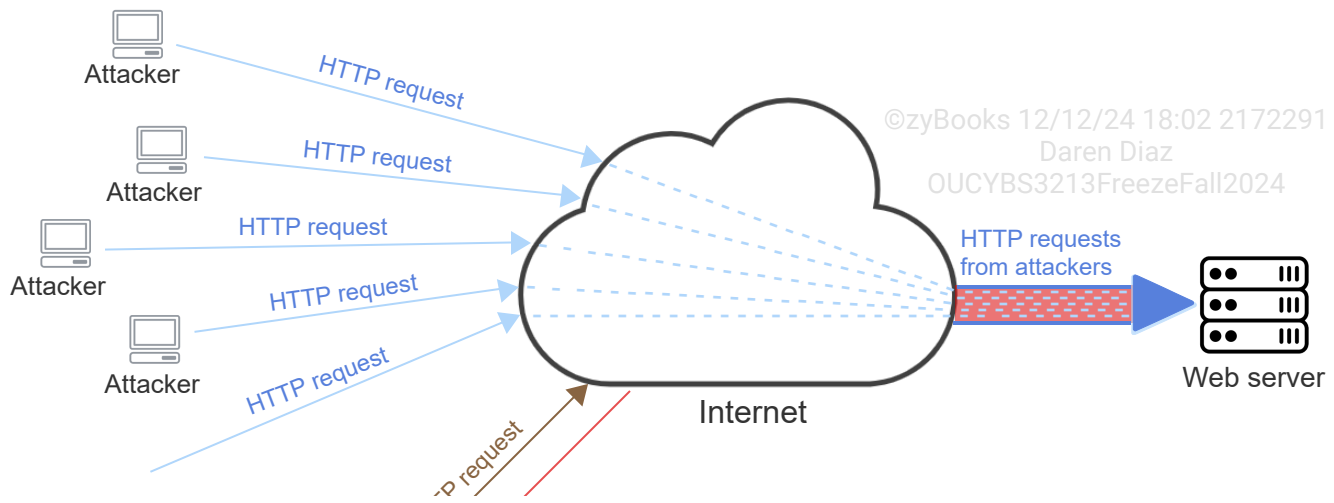
Distributed denial-of-service (DDoS)

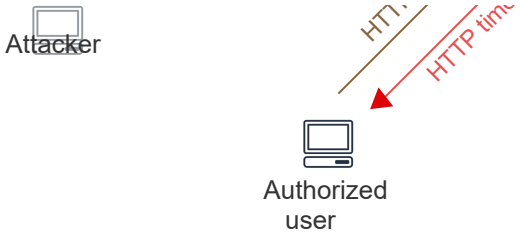
A ***denial-of-service*** (***DoS***) attack is an attack against a network resource that aims to prevent, disrupt, or delay authorized users from accessing the network resource. A ***distributed denial-of-service*** (***DDoS***) attack is a DoS attack that is simultaneously launched from multiple systems.

Three types of DDoS attacks exist:

- A ***network-based DDoS attack***, also known as ***volume-based DDoS attack***, is a DDoS attack that aims to exhaust the target system's network bandwidth. Ex: The UDP and ICMP floods are network-based DDoS attacks.
- A ***protocol-based DDoS attack***, also known as ***state exhaustion DDoS attack***, is a DDoS attack that aims to exhaust the target system's network resources or the resources of a network infrastructure equipment, such as a firewall or a load balancer. A protocol-based DDoS attack exploits the weaknesses of network layer (OSI layer 3) and transport layer (OSI layer 4) protocols to create maliciously configured protocol packets. Ex: A TCP SYN flood is a protocol-based DDoS attack.
- An ***application layer DDoS attack***, also known as an ***OSI layer 7 DDoS attack***, is a DDoS attack that aims to exhaust specific functions or features of a program. Ex: A DDoS attack that floods an Internet web server with HTTP requests is an application layer or layer 7 DDoS attack.

PARTICIPATION ACTIVITY 4.1.1: DDoS attack.





Animation content:

Static image: Five computer icons each labeled "Attacker." Each attacker has an arrow labeled "HTTP request" pointing to a cloud labeled "Internet." Each of the arrows extends as a dashed line. The dashed lines converge across the Internet cloud into an arrow labeled "HTTP requests from attackers" pointing to a server icon labeled "Web server." Another computer icon is labeled "Authorized user." The Authorized user has an arrow labeled "HTTP request" pointing to the Internet cloud. The Internet cloud has an arrow labeled "HTTP timeout" pointing back to the Authorized user.

Animation captions:

1. In an application layer DDoS attack, multiple systems send HTTP requests to an HTTP Server at the same time.
2. The web server's network bandwidth is exhausted by the attacker's HTTP requests.
3. An HTTP request from an authorized user times out because the user does not receive a response from the web server.

A DDoS attack may target operational technology (OT). ***Operational technology (OT)*** is the set of hardware devices and software programs that monitor and control industrial equipment. Ex: OT is used in industrial control systems (ICS) for monitoring and controlling power plants and manufacturing processes. OT is particularly vulnerable to DDoS attacks because legacy hardware and software are often used in OT. OT devices have limited resources and capabilities and are less likely to be secured against modern day attacks.

PARTICIPATION ACTIVITY 4.1.2: DDoS.

How to use this tool

Volume-based DDoS attack **Protocol-based DDoS attack**

Application layer DDoS attack

	A DDoS attack that aims to exhaust the targeted system's network bandwidth.
	A DDoS attack that aims to exhaust the processing capacity of network infrastructure resources.
	A DDoS attack that targets a layer 7 process.

Reset

PARTICIPATION ACTIVITY 4.1.3: DDoS.

Select the DDoS attack type for each of the following scenarios.

1) A DDoS attack that targets a database server.
   - Network
   - Protocol
   - Application

2) A DDoS attack that uses the *ping* utility to overload a network.
   - Network
   - Protocol
   - Application

3) A DDoS attack that overloads the targeted system with DNS response traffic.
   - Network
   - Protocol
   - Application

4) A DDoS attack that targets a web server.
   - Network
   - Protocol

○ Application

DDoS attack methods

A DDoS attack disrupts service availability by overwhelming network components through the exploitation of vulnerabilities in a protocol or application layer. Ex: IP lacks source IP verification and an attacker can manipulate spoofed IP addresses to launch a DDoS attack. DDoS attack methods:

- An ***amplified DDoS attack*** is a DDoS attack method exploiting the response mechanism of certain protocols to amplify (increase) traffic volume towards a target. Ex: A DNS amplification attack requests all records associated with a domain from multiple public DNS servers using the target's IP as the source, thereby flooding the target with overwhelming DNS responses.
- A ***reflected DDoS attack*** is a DDoS attack method exploiting the response mechanism of certain protocols to redirect traffic from third-party services towards a target. Ex: A reflected UDP flood attack sends spoofed UDP requests to multiple public UDP services using the target's IP as the source, thereby flooding the target with overwhelming UDP responses.

Table 4.1.1: DDoS attack methods.

Feature	Amplified	Reflected
Method	Exploits asymmetry in response sizes in IP protocols	Exploits the lack of source IP verification in protocols
Mechanism	Sends small requests that elicit disproportionately large responses due to unauthenticated source IPs	Spoofs the target's IP address, causing servers to send responses to the target instead of the attacker
Traffic origin	Multiple protocol servers	Multiple third-party services
Attack vector	Typically targets UDP-based protocols, including DNS and NTP due to amplification potential	Utilizes various protocols such as SNMP, LDAP, and ICMP, depending on the availability of vulnerable services for reflection

PARTICIPATION ACTIVITY 4.1.4: DDoS attack methods.

1) An amplified DDoS attack exploits the _____ in response sizes in IP protocols like DNS or NTP, which lack source IP verification.

- symmetry
- asymmetry
- uniformity

2) Amplified and reflected DDoS attacks exploit the IP protocol's lack of _____.

- payload encryption
- source IP verification
- destination IP verification

3) In a reflected DDoS attack, the attacker aims to _____ towards the target.

- encrypt data
- redirect traffic
- slow down network connections

4) An effective mitigation strategy for amplified DDoS attacks may involve _____ at the network perimeter.

- encryption of all network traffic
- disabling all network services
- filtering and rate-limiting techniques

DNS

Domain name system (DNS) is a hierarchical and decentralized naming system for identifying and locating the resources connected to a network. A network resource has a domain name and an IP address. ***DNS resolution***, also known as ***DNS lookup*** or ***DNS query***, is the process of translating or resolving a domain name to an IP address. DNS resolution is performed by a DNS nameserver, or simply DNS server. Ex: A DNS server resolves the domain "google.com" to IP address "216.58.210.206".

DNS is broken up into different zones. A ***DNS zone*** is a portion of a DNS namespace that is managed by an administrator or specific organization. An ***authoritative name server*** is a DNS server that manages a domain's configuration, also known as the domain's DNS record. Ex: An authoritative name server for the domain "google.com" is "ns1.google.com".

Domain reputation is a measure of a domain's trustworthiness based on historical data on the domain. Email service providers use domain reputation scores to adjust the priority of delivering emails. If an email domain is associated with spam email, the email domain would have a low domain reputation score. Based on an email domain's low reputation score, a service provider may reduce the priority of delivering emails originated from the domain.

PARTICIPATION ACTIVITY | 4.1.5: DNS.

How to use this tool

Domain reputation **DNS resolution** **Domain name system**

Authoritative name server

	A hierarchical and decentralized naming system for identifying and locating the resources connected to a network.
	The process of translating or resolving a domain name to an IP address.
	A DNS server that manages a domain's DNS record.
	A measure of a domain's trustworthiness based on historical information on the domain.

Reset

DNS attacks

Domain hijacking is the act of changing the registration information of a domain without the knowledge or consent of the domain owner. Domain hijacking can be performed through technical means such exploiting a vulnerability in a DNS host system. Non-technical means such as social engineering attacks can be used to modify a domain's registration information or fraudulently transfer domain ownership to a third party.

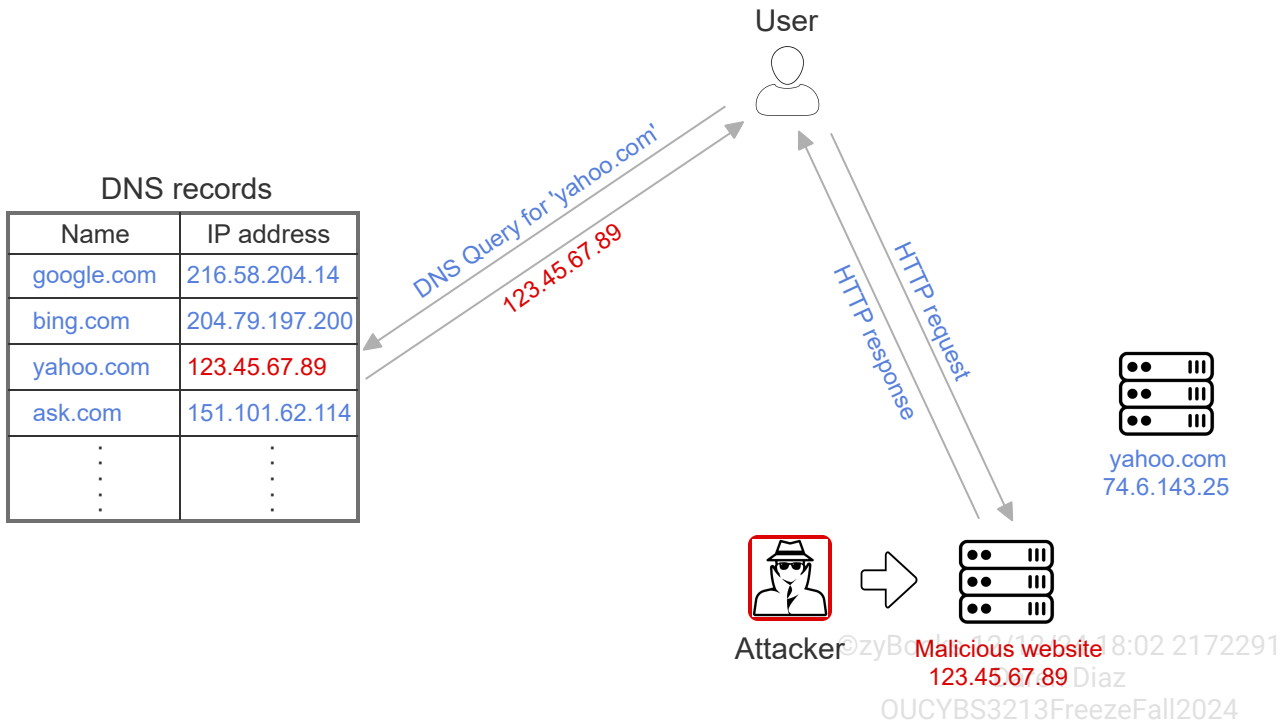
URL redirection is the act of using a URL to divert a user to a malicious website. URL redirection can be performed by sending a potential victim a phishing email that contains a link to a malicious

website. A system's hosts file can also be used in a URL redirection attack. A hosts file is used to resolve a domain name to an IP address prior to querying a DNS server. A host file can be modified to map a domain name to the IP address of a malicious website.

DNS poisoning, also known as ***DNS cache poisoning***, or ***DNS spoofing***, is an attack that aims to redirect a user to a malicious website by modifying the user's DNS query. In a DNS poisoning attack, an attacker replaces an IP address in a DNS record with the IP address of a computer under the attacker's control. A DNS poisoning attack can be performed by various methods such as installing malware on a user's computer, modifying a DNS message in transit, modifying DNS server settings on a router, or modifying DNS records on a DNS server.

A DNS poisoning attack can be used as part of a phishing attack. A user's DNS query for a website can be redirected to a spoofed website that resembles the website that the user intended to access. The spoofed website is used to collect information from the user such as the user's credentials.

PARTICIPATION ACTIVITY 4.1.6: DNS poisoning attack.



Animation content:

Static image: A table labeled "DNS records" with columns "Name" and "IP address." The first row shows the name "google.com" and the IP address "216.58.204.14". The second row shows the name "bing.com" and the IP address "204.79.197.200". The third row shows the name "yahoo.com" and the IP address "123.45.67.89" in red. The fourth row shows the name "ask.com" and the IP address "151.101.62.114". A server icon labeled "yahoo.com, 74.6.143.25". A server icon labeled "Malicious website, 123.45.67.89" in red font. An Attacker icon has an arrow pointing to the Malicious website icon. An icon labeled "User" has an arrow labeled "DNS Query for 'yahoo.com'" pointing toward the "yahoo.com" row of the DNS records table. An arrow labeled "123.45.67.89" points from the "yahoo.com" row to the User. An arrow labeled "HTTP request" points from the User to the Malicious website icon. An arrow labeled "HTTP response" points from the Malicious website icon to the User.
Step 1: A user queries and receives a domain's IP address from DNS. The user sends an HTTP request to the web server hosting the domain.
A table labeled "DNS records" with columns "Name" and "IP address." The first row shows the name "google.com" and the IP address "216.58.204.14". The second row shows the name "bing.com" and the IP address "204.79.197.200". The third row shows the name "yahoo.com" and the IP address "74.6.143.25". The fourth row shows the name "ask.com" and the IP address "151.101.62.114". A server icon labeled "yahoo.com, 74.6.143.25". An icon labeled "User". An arrow labeled "DNS Query for 'yahoo.com'" appears pointing toward the "yahoo.com" row of the DNS records table. An arrow labeled "74.6.143.25" appears pointing from the "yahoo.com" row to the User. An arrow labeled "HTTP request" appears pointing from the User to the "yahoo.com" server icon. An arrow labeled "HTTP response" appears pointing from the "yahoo.com" server icon to the User.
Step 2: An attacker sets up a malicious website on a web server.
An attacker icon appears. An arrow appears pointing from the Attacker icon to a server icon labeled "Malicious website, 123.45.67.89".
Step 3: The attacker launches a DNS poisoning attack and modifies a DNS record with the IP address of the web server hosting the malicious web site.
The IP address for "yahoo.com" is changed to "123.45.67.89" in red font.
Step 4: The next time a user queries the DNS, the DNS returns the IP address of the web server hosting the malicious website. The user sends an HTTP request to the malicious website.
An arrow labeled "DNS Query for 'yahoo.com'" appears pointing from the User icon to the "yahoo.com" row of the DNS records table. An arrow labeled "123.45.67.89" appears pointing from the "yahoo.com" row to the User. An arrow labeled "HTTP request" appears pointing from the User to the Malicious website icon. An arrow labeled "HTTP response" appears pointing from the Malicious website icon to the User.

Animation captions:

1. A user queries and receives a domain's IP address from DNS. The user sends an HTTP request to the web server hosting the domain.
2. An attacker sets up a malicious website on a web server.
3. The attacker launches a DNS poisoning attack and modifies a DNS record with the IP address of the web server hosting the malicious web site.

4. The next time a user queries the DNS, the DNS returns the IP address of the web server hosting the malicious website. The user sends an HTTP request to the malicious website.

PARTICIPATION ACTIVITY 4.1.7: DNS attacks.

How to use this tool

Domain hijacking **DNS poisoning** **URL redirection**

	The act of changing the registration of a domain without the knowledge or consent of the domain owner.
	An attack in which corrupt DNS information is inserted into a DNS server's cache.
	The act of using a URL to divert a user to a malicious website.

Reset

PARTICIPATION ACTIVITY 4.1.8: DNS attacks.

1) What does a DNS lookup return?
   - A domain name
   - An IP address
   - A domain registration information

2) What is modified in a DNS poisoning attack?

   - A domain name
   - An IP address
   - A domain registration information

3) What is modified in domain hijacking?

- A domain name
- A domain IP address
- A domain registration information

DNSSEC

Domain Name System Security Extensions, or ***DNS Security Extensions***, or ***DNSSEC***, is a set of extensions to DNS that provide a DNS resolver cryptographic authentication of DNS data using digital signatures. DNSSEC assigns every DNS zone a public-private key pair. A zone owner uses the zone's private key to digitally sign DNS data in the zone. A DNS resolver uses a zone's public key to validate the authenticity of DNS data in the zone. If a DNS resolver validates the digital signature over the DNS data, the DNS resolver returns the DNS data to a client. If a DNS resolver cannot validate the digital signature over the DNS data, the DNS resolver discards the DNS data and returns an error to the DNS client.

The use of digital signatures in DNSSEC improves DNS security in two ways:

- Data origin authentication
  A DNS client is assured that DNS data originated from the zone owner.
- Data integrity
  A DNS client is assured that DNS data has not been modified in transit.

DNSSEC is designed to protect a DNS client from using malicious DNS data. DNSSEC prevents a man-in-the-middle (MITM) attack by ensuring that DNS data is not forged or modified in transit. Ex: In DNS cache poisoning, an attacker modifies DNS data so that a domain name resolves to the IP address of a malicious website. DNSSEC provides assurance to a DNS client that DNS data is identical to the data published by the zone owner and served on an authoritative DNS server.

PARTICIPATION ACTIVITY 4.1.9: DNSSEC.

1) How does DNSSEC provide authentication of DNS data?
   - By using digital signatures
   - By using authoritative name servers
   - By requiring zone owners to validate DNS queries

2) What is used by a DNS resolver to validate the authenticity of DNS data in

a zone?

- The zone owner's private key
- The zone owner's public key
- The IP address of the DNS authoritative server for the zone

3) A DNS flood attack is a type of DDoS attack in which a DNS server is flooded with DNS queries for a domain to disrupt the DNS server's ability to resolve the domain name to an IP address. How does DNSSEC prevent a DNS flood attack?

- By ensuring that DNS queries are not forged or modified in transit
- By discarding the DNS data that cannot be validated
- DNSSEC cannot prevent a DNS flood attack

CHALLENGE ACTIVITY 4.1.1: Network attacks.

581480.4344582.qx3zqy7

Start

Select the DDoS attack type described in each scenario.

Pick — Send a large number of SYN requests to a server but not acknowledgi server's SYN-ACK responses (SYN flood attack).

Pick — Send a large number of HTTP requests to force a web server to searc un-cached content.

Pick — Send a large number of HTTP requests to randomized URLs.

Pick

Send a large number of UDP packets to random ports on a server (UD flood attack).

1 2

Check Next

4.2 ARP poisoning, MAC flooding, and MAC cloning

Data link layer

The data link layer is the second layer of the seven-layer Open System Interconnection (OSI) model. The ***data link layer***, or ***Layer 2***, facilitates data transfer between two connected devices on the same network. The data link layer is responsible for flow control and the detection and correction of errors that may occur in the physical layer (Layer 1). Ex: Ethernet is a Layer 2 protocol.

Every network device has a media access control (MAC) address at the data link layer. A ***media access control address***, or ***MAC address***, is a unique 48-bit identifier assigned to a network device. A MAC address is typically represented as six groups of two hexadecimal digits, separated by hyphens or colons. Ex: DA-C4-97-C3-3E-DE or 2C:54:91:87:C9:E2.

An ***address resolution protocol (ARP)*** is a protocol used for resolving an internet address (Layer 3) into a MAC address (Layer 2). An ***ARP cache table***, or ***ARP cache***, is a table that maps an internet address to the internet address' corresponding MAC address. To deliver a data packet, an ARP cache table is used to find the MAC address that maps to the data packet's destination IP address.

PARTICIPATION ACTIVITY 4.2.1: Layer 2.

How to use this tool

ARP cache table MAC address ARP

	A 48-bit unique identifier assigned to a network interface controller (NIC) for use as a network address.
	A protocol used for mapping a MAC address to an internet layer or IP address.
	Maintains a record of each IP address and the IP address' corresponding MAC address.

Reset

PARTICIPATION ACTIVITY 4.2.2: Layer 2.

1) The data link layer facilitates data transfer between two devices on which type of network?
   - wide area network (WAN)
   - metropolitan area network (MAN)
   - local area network (LAN)

2) What is stored in an ARP cache table?
   - Internet addresses
   - Internet and MAC addresses
   - MAC addresses

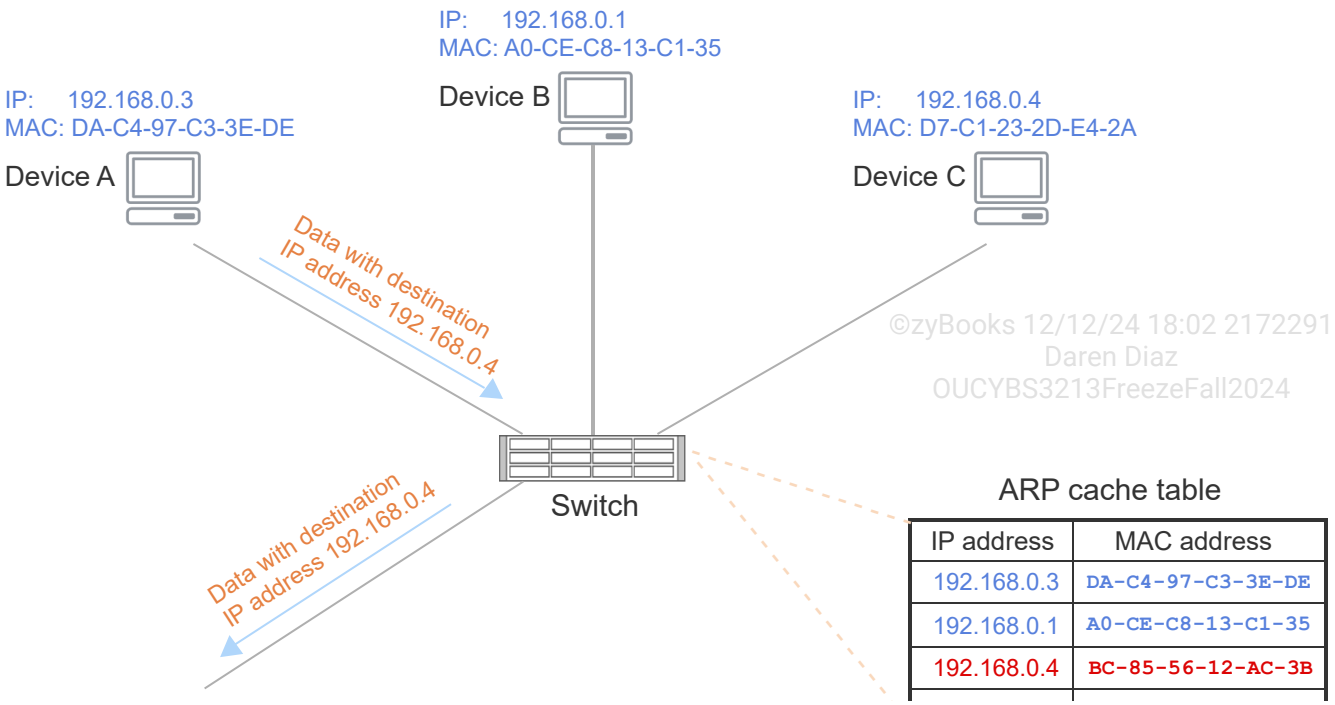
3) What is the purpose of the ARP protocol?
   - resolve a Layer 2 address to a Layer 1 address
   - resolve a Layer 3 address into a Layer 2 address
   - resolve a Layer 3 address into a layer 1 address

Data link layer attacks

The data link layer is subject to three types of attacks:

- ***Address resolution protocol (ARP) poisoning***, also called ***ARP cache poisoning*** or ***ARP spoofing***, is an attack in which an attacker sends spoofed ARP messages on a local area network (LAN) to associate the attacker's MAC address with the IP address of a target host on the LAN. Since the ARP protocol lacks authentication, any device on a LAN can send an ARP message. An ARP spoofing attack can be launched from a compromised host on a LAN or from an attacker's device connected to a LAN. ARP poisoning enables an attacker to receive all the data packets destined for the target host.
- ***Media access control (MAC) flooding*** is an attack in which a large number of invalid MAC addresses are sent to a network switch with the aim of overwriting the switch's MAC table. A ***MAC table*** is a table that maps each network device's MAC address to a physical port on a switch. Since a MAC table has limited storage capacity, a MAC flooding attack causes a switch to overwrite legitimate MAC table entries with invalid MAC addresses. When a switch receives a packet whose destination MAC address is not present in the switch's MAC table, the switch performs unicast flooding. ***Unicast flooding*** is a switch's broadcast of a packet on all the switch's ports. Unicast flooding enables an attacker to gain access to all data packets on a LAN.
- ***MAC cloning***, also known as ***MAC spoofing***, is the act of changing the factory-assigned MAC address of a network device. A MAC address can be changed by a software program without modifying device hardware. MAC cloning enables an attacker to bypass a MAC address-based restricted network or authentication system and hide a rogue device on a network.

PARTICIPATION ACTIVITY 4.2.3: ARP poisoning attack.



Animation content:

Static image: A switch connected to four computers labeled "Device A", "Device B", "Device C", and "Attacker's device". Each device is labeled with an IP address and a MAC address. Device C's IP address is 192.168.0.4 and MAC address is D7-C1-23-2D-E4-2A. The attacker's device IP address is 192.168.0.2 and MAC address is BC-85-56-12-AC-3B. A table labeled "ARP cache table" has each IP address and the corresponding MAC address. The row with IP address 192.168.0.4 shows corresponding MAC address MC-85-56-12-AC-3B and is highlighted in red. An arrow labeled "Data with destination IP address 192.168.0.4" points from Device A to the switch. A second arrow labeled "Data with destination IP address 192.168.0.4" points from the switch to the Attacker's device.
Step 1: A switch's ARP cache table is updated with the IP and MAC addresses of each device connected to the switch.
A switch and an empty table labeled "ARP cache table" with "IP address" and "MAC address" columns. A computer labeled "Device A" appears with Device A's IP address and MAC address. Copies of Device A's IP address and MAC address appear in the ARP cache table. Device B, Device C, and the Attacker's device each appear with IP addresses and MAC addresses. Each device's IP address and MAC address are added to the ARP cache table.
Step 2: The switch looks up the IP address in the ARP cache table to determine the MAC address that corresponds to a data packet's destination IP address.
An arrow labeled "Data with destination IP address 192.168.0.4" appears pointing from Device A to the switch. The third row of the ARP cache table is highlighted and has the IP address 192.168.0.4 and the MAC address D7-C1-23-2D-E4-2A. A second arrow labeled "Data with destination IP address 192.168.0.4" appears pointing from the switch to Device C.
Step 3: In an ARP poisoning attack, an attacker sends a spoofed ARP message on the network to associate the attacker's MAC address with the IP address of a target host.
The previous arrows disappear. "IP: 192.18.0.4" and "MAC: BC-85-56-12-AC-3B" appear above the connection between the Attacker's device and the switch. The MAC address corresponding to the IP address 192.168.0.4 changes to BC-85-56-12-AC-3B.
Step 4: The data packets with the destination IP address of the target host are delivered to the attacker's device.
An arrow labeled "Data with destination IP address 192.168.0.4" appears pointing from Device A to the switch. A second arrow labeled "Data with destination IP address 192.168.0.4" appears pointing from the switch to the Attacker's device.

Animation captions:

1. A switch's ARP cache table is updated with the IP and MAC addresses of each device connected to the switch.

2. The switch looks up the IP address in the ARP cache table to determine the MAC address that corresponds to a data packet's destination IP address.
3. In an ARP poisoning attack, an attacker sends a spoofed ARP message on the network to associate the attacker's MAC address with the IP address of a target host.
4. The data packets with the destination IP address of the target host are delivered to the attacker's device.

PARTICIPATION ACTIVITY 4.2.4: Layer 2 attacks.

How to use this tool

ARP poisoning **MAC cloning** **MAC flooding**

	The act of changing the factory-assigned MAC address of a network device.
	An attack in which a large number of invalid MAC addresses are sent to a network switch with the aim of overwriting the switch's MAC table.
	An attack in which an attacker sends spoofed ARP messages on a local area network (LAN) to associate the attacker's MAC address with the IP address of a target host on the LAN

Reset

PARTICIPATION ACTIVITY 4.2.5: Layer 2 attacks.

1) Which Layer 2 attack may force a switch to broadcast a packet to all the devices connected to the switch?

- ARP poisoning
- MAC flooding
- MAC cloning

2) Which Layer 2 attack may enable an attacker to modify a file that can only be accessed from a device with a specific MAC address?

- ARP poisoning
- MAC flooding
- MAC cloning

3) Which Layer 2 attack may enable an attacker to receive all the data packets destined for a specific host?

- ARP poisoning
- MAC flooding
- MAC cloning

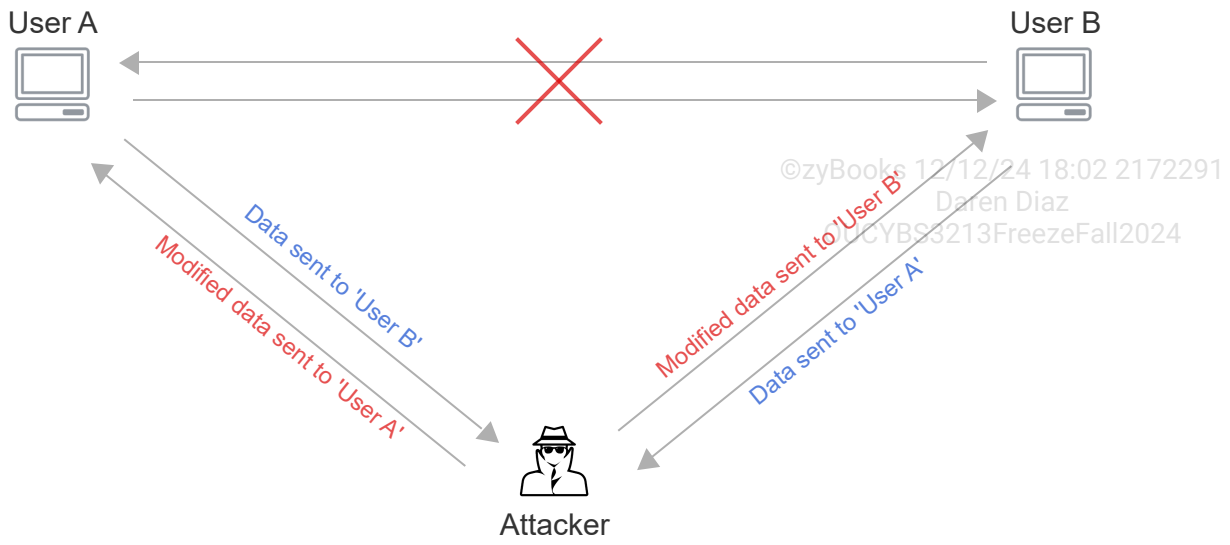
4.3 On-path attacks: Man-In-The-Middle and Man-In-The-Browser

MITM

A ***Man-In-The-Middle (MITM)***, or ***MitM*** attack, is an attack in which an attacker eavesdrops or modifies the communications between two parties. An MITM attack operates at the network layer (Layer 3). In an MITM attack, both parties are in communication with an attacker but each party believes that is communicating directly with the other party. Ex: A DNS poisoning attack that redirects a user to a malicious website by modifying the user's DNS query is a MITM attack.

In a typical MITM attack, an attacker intercepts a message in transit, modifies the message, and sends the modified message to the recipient. An attacker uses an MITM attack to impersonate one or both of the two communicating parties. Data communication over a secure channel prevents an MITM attack. A ***secure channel*** is a communication channel that guarantees data authenticity and data confidentiality.

PARTICIPATION ACTIVITY 4.3.1: Man-In-The-Middle (MITM) attack.



Animation content:

Static image: A computer labeled "User A", a computer labeled "User B", and an icon labeled "Attacker". An arrow points from User A to User B. An arrow points from User B to User A. A red "X" is on both arrows. An arrow labeled "Data sent to User B" points from User A to the Attacker. An arrow labeled "Modified data sent to User B" points from the Attacker to User B. An arrow labeled "Data sent to User A" points from User B to the Attacker. An arrow labeled "Modified data sent to User A" points from the Attacker to User A.

Animation captions:

1. An attacker intercepts communication between two parties and creates a separate connection to each party.
2. The attacker intercepts the data sent from 'User A' to 'User B', modifies the data, and sends the modified data to 'User B'.
3. The attacker intercepts the data sent from 'User B' to 'User A', modifies the data, and sends the modified data to 'User A'.

PARTICIPATION ACTIVITY 4.3.2: Man-In-The-Middle (MITM) attack.

How to use this tool

DNS poisoning | MITM | Secure channel

	An attack in which an attacker eavesdrops or modifies communications between two parties.
	A type of man-in-the-middle attack that modifies a user's DNS query to intercept the user's messages.
	A type of communication channel that guarantees data authenticity and data confidentiality.

Reset

PARTICIPATION ACTIVITY 4.3.3: Man-In-The-Middle (MITM) attack.

1) An attacker that only eavesdrops on a communication channel is not conducting an MITM attack.
   - ○ False
   - ○ True

2) To prevent an MITM attack, both data authenticity and data confidentiality should be guaranteed.
   - ○ False
   - ○ True

3) An ARP poisoning attack which associates an attacker's MAC address with the IP address of a target host on a LAN is an MITM attack.
   - ○ False
   - ○ True

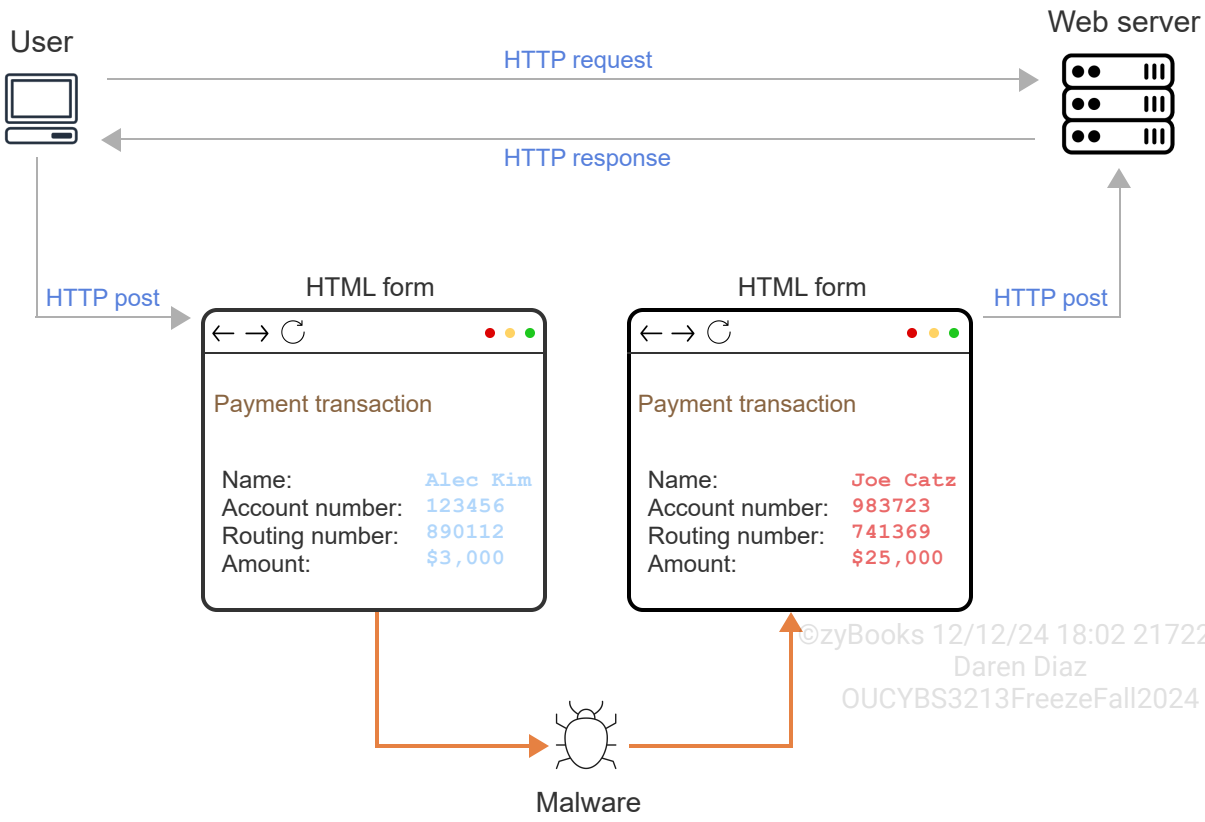
MITB

A ***Man-In-The-Browser (MITB)***, or ***MitB*** attack, is a type of MITM attack that uses malware to intercept or modify messages exchanged between a web browser and a web server. An MITB attack operates at the application layer (Layer 7). An MITB attack is most often used to steal financial information by modifying a user's communications with an Internet banking website.

In an MITB attack, a web browser vulnerability is exploited by a Trojan horse via a browser extension or user script. The extension is activated when a user visits a targeted website. The extension modifies the user's input on a specific HTML form before sending the HTML form data to the targeted website. Similarly, the extension selectively modifies data returned from the targeted website before presenting the data to the user.

An MITB attack is difficult to remove because malware is embedded in an extension and may not be detected by anti-malware software. Since a malware-infected extension also provides added browser functionality and only activates when a user visits a targeted website, the malware may remain undetected on a system for an extended period.

PARTICIPATION ACTIVITY 4.3.4: Man-In-The-Browser (MITB) attack.



Animation content:

Static image: A computer icon labeled "User" and a server icon labeled "Web server". An arrow labeled "HTTP request" points from the User to the Web server. An arrow labeled "HTTP response" points from the Web server to the User. An arrow labeled "HTTP post" points from the User to a web browser window labeled "HTML form". The browser window shows a payment transaction with name "Alec Kim", account number 123456, routing number 890112, and amount $3,000. An arrow points from the browser window to a bug icon labeled "Malware". An arrow points from the Malware bug to a second browser window labeled "HTML form". The second browser window shows the payment transaction information has been changed. The name is now "Joe Catz", the account number is now 983723, the routing number is now 741369, and the amount is now $25,000. An arrow labeled "HTTP post" points from the second HTML form to the Web server.

Animation captions:

1. A malware-infected browser extension is activated when a user accesses an HTML form at a targeted web server.
2. The malware intercepts and modifies the data entered in a HTML form before sending the data to a web server.
3. The HTML form with malware-modified data is sent to the targeted web server.

PARTICIPATION ACTIVITY 4.3.5: Man-In-The-Middle (MITM) attack.

1) In an MITB attack a target host is first infected with malware.
   - False
   - True

2) An attacker that intercepts a user's communication with a web server by eavesdropping on a wireless channel is conducting an MITB attack.
   - False
   - True

3) An MITB attack is only used to capture messages sent from a user to an Internet banking website.
   - False
   - True

4.4 POPS, IMAPS, and S/MIME

Post office protocol (POP)

Post office protocol (POP) is an Internet standard protocol used by an email client to retrieve an email from a mail server. POP does not support the sending of an email. ***POP3***, or POP version 3, is the latest version of POP. POP is an application layer protocol (Layer 7). POP uses TCP port 110.

A mailbox or folder is created for an email account on a POP server. When an email is received by a POP server, the email is saved to the email recipient's mailbox. An email account owner uses a POP client, such as Microsoft Outlook, to connect to a POP server and download the account owner's email. By default, an email is removed from a POP server after the email is downloaded by a POP client.

POP is not a secure protocol because data is transmitted in cleartext. ***POP secure***, also known as ***POPS***, or ***POP3S***, uses SSL/TLS to secure communications between a POP client and a POP server. POP3S provides data privacy and integrity. POP3S uses TCP port 995.

PARTICIPATION ACTIVITY | 4.4.1: POP.

How to use this tool

POP server **POPS** **POP** **POP client**

	A protocol used by an email client to retrieve an email from a mail server.
	Uses SSL/TLS to secure communications between a PAP client and a POP server.
	Receives and stores emails in a user's mailbox.
	Retrieves an email from a POP server.

Reset

PARTICIPATION ACTIVITY 4.4.2: POP.

1) What is POP used for?
   - Send an email
   - Retrieving an email
   - Configure a mail server

2) Which ports are used by POP?
   - TCP port 443
   - TCP port 110
   - TCP ports 22

3) What is the difference between POP and POPS?
   - POP provides data privacy
   - POP provides data integrity
   - POPS provides data privacy and integrity

4) Which port is used by POP3S?
   - TCP port 80
   - UDP port 1812
   - TCP port 995

IMAP

Internet message access protocol (IMAP) is an Internet standard protocol used by an email client to retrieve an email from a mail server. ***IMAP4***, or IMAP version 4, is the latest version of IMAP. IMAP is an application layer protocol (Layer 7). IMAP uses TCP port 143.

IMAP allows for the management of a mailbox by multiple email clients. By default, an email remains on an IMAP server after the email is downloaded by an IMAP client. An email is removed from an IMAP server only if a user explicitly deletes the email on the IMAP server.

IMAP is not a secure protocol because data is transmitted in cleartext. ***IMAP secure***, or ***IMAPS***, uses SSL/TLS to secure communications between an IMAP client and an IMAP server. IMAPS provides data privacy and integrity. IMAPS uses TCP port 993.

Table 4.4.1: POP and IMAP comparison.

Feature	POP	IMAP
Typical usage	Access from single device	Access from multiple devices
Email retrieval	Entire email or headers only	Any email subpart
Port	TCP 110 (POPS uses TCP 995)	TCP 143 (IMAPS uses TCP 993)
Email folders on server	No	Yes
Email search on server	No	Yes

PARTICIPATION ACTIVITY 4.4.3: IMAP.

1) Which protocol supports the creation of folders on a mail server?
   - POP
   - IMAP

2) Which protocol is typically used for accessing email from a single device?
   - POP
   - IMAP

3) Which protocol supports the searching of emails on a mail server?
   - POP
   - IMAP

4) In which protocol a retrieved email is removed from the mail server by default?
   - POP

- IMAP

S/MIME

Multipurpose Internet Mail Extensions (MIME) is an Internet standard that extends the format of an email message to support non-ASCII character sets and multimedia attachments.
Secure/Multipurpose Internet Mail Extensions (S/MIME) is an Internet standard for signing and encrypting MIME data. S/MIME provides authentication, integrity, non-repudiation of origin, and confidentiality security services for electronic messaging applications.

S/MIME requires an X.509 certificate for each email client. S/MIME can use RSA, DSA and ECDSA digital signature algorithms for message signing, and AES and 3DES for message encryption. S/MIME is a widely accepted protocol for sending a digitally signed and encrypted message. S/MIME is supported by most email service providers, but the complexities associated with certificate management and validation have prevented the widespread adoption of the protocol.

PARTICIPATION ACTIVITY 4.4.4: S/MIME.

1) How does S/MIME improve the security of MIME data?
   - By signing MIME data
   - By encrypting MIME data
   - By signing and encrypting MIME data

2) Which one of the following algorithms is not used by S/MIME?
   - DSA
   - AES
   - DES

3) What is the purpose of using X.509 certificates in S/MIME?
   - To increase email storage capacity
   - To validate the identity of the email sender
   - To provide a unique IP address to each email

CHALLENGE ACTIVITY 4.4.1: POPS, IMAPS and S/MIME.

581480.4344582.qx3zqy7

Start

Select the email protocol with the stated feature.

Pick — Uses TCP port 110

Pick — Provides data integrity

Pick — Transmits data in cleartext

1 2 3

Check Next

4.5 SSH, FTPS, and SFTP

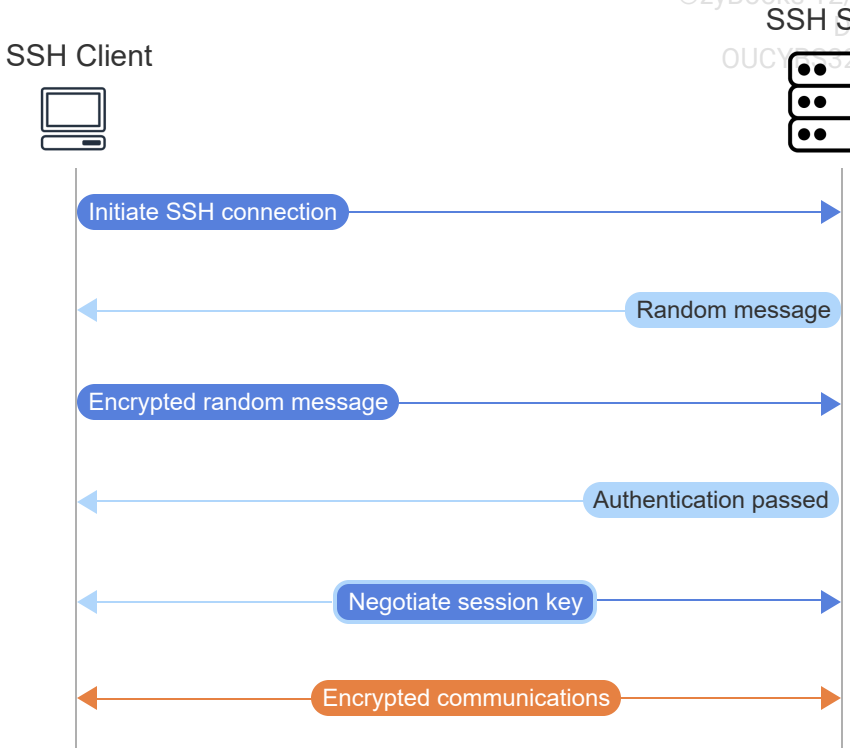
SSH

Secure shell protocol (SSH) is a cryptographic network protocol for securely operating a network service over an insecure network. SSH provides a secure channel by connecting an SSH client to an SSH server using a client-server model. SSH was designed as a replacement for Telnet and for unsecured remote shell protocols that send information (including passwords) in plaintext. SSH uses TCP port 22 by default.

SSH provides data confidentiality by using encryption and data integrity by using message authentication codes (MAC). Since SSH supports protocol tunneling, any network service can be secured with SSH. ***Protocol tunneling*** is the encapsulation of a protocol's packets within the packets of another protocol. SSH is used in SSH file transfer protocol (SFTP) and the secure copy protocol (SCP).

SSH can be used for public key authentication to provision access without requiring a user password for each login. The SSH authentication protocol facilitates automated, passwordless logins and single sign-on (SSO). In SSH authentication, a user's public key is stored on an SSH server and the user's private key is used to authenticate the user.

PARTICIPATION ACTIVITY | 4.5.1: SSH authentication.



Animation content:

Static image: A computer icon labeled "SSH Client" and a server icon labeled "SSH Server". Messages are shown passing between the SSH Client and the SSH Server. The first message is labeled "Initiate SSH connection" and goes from the SSH Client to the SSH Server. The second message is labeled "Random message" and goes from the SSH Server to the SSH Client. The third message is labeled "Encrypted random message" and goes from the SSH Client to the SSH Server. The fourth message is labeled "Authentication passed" and goes from the SSH Server to the SSH Client. The fifth message is labeled "Negotiate session key" and goes in both directions between the SSH Client and the SSH Server. The final message is labeled "Encrypted communications" and goes in both directions between the SSH Client and the SSH Server.

Animation captions:

1. An SSH client initiates a connection to an SSH server.
2. The SSH server sends a random message to the SSH client.

3. The SSH client encrypts the random message with the SSH client's private key and sends the encrypted random message to the SSH server.
4. The SSH server authenticates the SSH client if the SSH server can decrypt the random message with the SSH client's public key stored on the SSH server.
5. The SSH server and the SSH client negotiate a session key using an algorithm, such as Diffie-Hellman, and begin encrypted communications.

PARTICIPATION ACTIVITY 4.5.2: SSH.

1) Which port is used by the SSH protocol?
   - TCP port 80
   - TCP port 49
   - TCP port 22

2) How does SSH provide data confidentiality?
   - By using encryption
   - By using message authentication codes
   - By using digital signatures

3) How does an SSH server authenticate a user?
   - The SSH protocol cannot be used for authentication.
   - By using a user's public key to decrypt a random message that the user encrypted with the user's private key.
   - By using a user's private key to decrypt a random message that the user encrypted with the user's private key.

4) How does SSH provide data integrity?
   - By using encryption
   - By using message authentication codes

- By using digital signatures

FTPS and SFTP

FTPS, also known as ***FTP over SSL*** or ***FTP Secure***, is an extension to the file transfer protocol (FTP) that uses SSL/TLS to provide communication security. FTPS supports all the SSL/TLS cryptographic protocols, including the use of client and server certificates for authentication, AES and 3DES ciphers for encryption, and SHA1 and MD5 hash functions for data integrity. FTPS supports X.509 self-signed or trusted public key certificates. FTPS uses TCP port 989 for the data channel and TCP port 990 for the control channel.

SSH file transfer protocol (SFTP), also known as ***SSH-FTP*** or ***Secure FTP***, is an extension of the SSH protocol that enables secure file transfer capabilities between networked hosts. SFTP provides remote file system management functionality that enables an application to list the contents of a remote directory, delete a remote file, and resume an interrupted file transfer. SFTP uses TCP port 22.

Table 4.5.1: File transfer protocols.

Protocol	Security mechanism	Port
`FTP`	None	TCP 20 (data channel) TCP 21 (control channel)
`FTPS`	FTP over SSL/TLS	TCP 989 (data channel) TCP 990 (control channel)
`SFTP`	SSH	TCP 22

Both FTPS and SFTP are used to securely transfer files between networked hosts. FTPS uses SSL/TLS to create an authenticated and secure communication link between two hosts. SFTP uses SSH protocol extensions for authentication and encryption of an FTP session between networked hosts. FTPS and SFTP are not compatible with each other, meaning that an SFTP client cannot connect to an FTPS server and an FTPS client cannot connect to an SFTP server.

PARTICIPATION ACTIVITY 4.5.3: FTPS and SFTP.

1) Which protocol uses TCP ports 989 and 990?

- FTP
- FTPS
- SFTP

2) Which protocol is an extension of the SSH protocol?

- FTP
- FTPS
- SFTP

3) Which protocol uses SSL/TLS?

- FTP
- FTPS
- SFTP

4) Which protocol provides remote file system management functionality?

- FTP
- FTPS
- SFTP

CHALLENGE ACTIVITY 4.5.1: SSH, FTPS and SFTP.

581480.4344582.qx3zqy7

Start

Select the secure FTP protocol with the stated feature.

Pick — Supports self-signed X.509 public key certificates

Pick — Is an extension of the SSH protocol

Pick — Requires two ports to be open on the firewall

Pick Supports the deletion of a remote file

1 2

Check Next

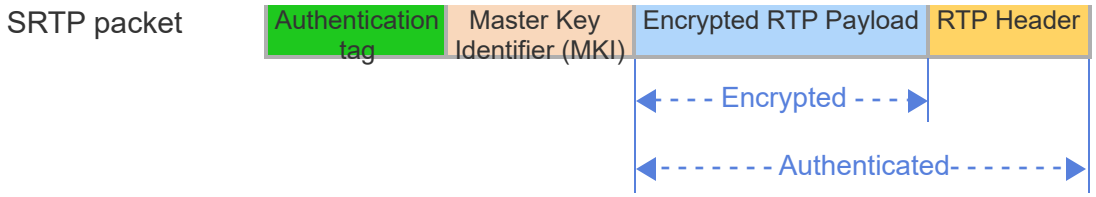
4.6 SRTP, LDAPS, and HTTPS

SRTP

Secure real-time transport protocol (SRTP) is a protocol for secure delivery of voice and video services over an IP network. SRTP is an extension to real-time transport protocol (RTP). SRTP is used in Voice over Internet Protocol (VoIP), video teleconferencing applications, streaming video, and devices that have push-to-talk functionality. SRTP provides confidentiality, authentication, and integrity for data in both unicast (one to one) and multicast (one to many) applications. SRTP uses the advanced encryption algorithm (AES) in counter mode for encryption and the HMAC-SHA1 or HMAC-MD5 to ensure data integrity and authenticity.

SRTP defends against a replay attack by using a sequence number for each packet. A receiver maintains the sequence number of each previously received packet and accepts a new packet only if the packet has not been previously received. SRTP uses UDP port 5004 by default.

PARTICIPATION ACTIVITY 4.6.1: RTP and SRTP packets.



Animation content:

Static image: A representation of an RTP packet with a blue section labeled "RTP Payload" and a yellow section labeled "RTP Header". A representation of an SRTP packet with a green section labeled "Authentication tag", a tan section labeled "Master Key Identifier (MKI)", a blue section labeled "Encrypted RTP Payload", and a yellow section labeled "RTP Header". Arrows spanning the Encrypted RTP Payload section indicate that the section is encrypted. Arrows spanning the Encrypted RTP Payload and RTP Header sections indicate that the sections are authenticated.

Animation captions:

1. SRTP encrypts the RTP Payload of an RTP packet with an SRTP session key. SRTP does not encrypt the RTP Header.
2. The Master Key Identifier (MKI) identifies the master key from which the SRTP session key was derived.
3. The Authentication tag contains the message authentication code for the encrypted RTP Payload and the RTP Header.

PARTICIPATION ACTIVITY 4.6.2: SRTP.

1) Which type of applications uses SRTP for improved security?

- Email and voice
- Video and database
- Voice and video

2) Which security services are provided by SRTP?

- Integrity, non-repudiation and authentication

- Integrity, confidentiality and non-repudiation
- Integrity, authentication and confidentiality

3) How does SRTP defend against a replay attack?

- By dropping packets that are received out of order
- By maintaining the sequence numbers of each received packet
- By dropping packets that are not correctly formatted

4) Which cryptographic algorithms are used by SRTP?

- 3DES and HMAC-SHA1
- AES and HMAC-SHA1
- DES and HMAC-MD5

LDAPS

Lightweight directory access protocol (LDAP) is a protocol for accessing and maintaining distributed directory information services over an IP network. A directory service enables the sharing of information about a user, system, service, or application in a network. LDAP is commonly used to provide a central location for storing usernames and passwords. Different applications and services use LDAP to validate a user. Ex: LDAP is used by Active Directory in Windows Server 2019.

LDAP traffic is not secure because data is transmitted in cleartext. ***LDAPS***, or ***LDAP Secure***, or ***LDAP over SSL***, uses SSL/TLS to protect LDAP transmissions. In LDAPS, a client and a server establish an SSL/TLS connection before transmitting an LDAP message. An LDAPS connection is closed when the underlying SSL/TLS connection is terminated. LDAPS uses TCP port 636 by default.

Applications that use LDAP might be vulnerable to LDAP injection attacks. An ***LDAP injection attack*** is an attack in which an attacker exploits input validation vulnerabilities to construct and execute an unauthorized LDAP query. An LDAP injection attack may result in the modification of LDAP content or the granting of permissions to an unauthorized query.

PARTICIPATION ACTIVITY 4.6.3: LDAPS.

How to use this tool

LDAP **LDAP injection attack** **LDAPS**

	A protocol for accessing and maintaining distributed directory information services over an IP network.
	A protocol for accessing and maintaining distributed directory information services securely over an IP network that uses SSL/TLS.
	An attack in which an attacker exploits input validation vulnerabilities to construct and execute an LDAP query.

Reset

PARTICIPATION ACTIVITY 4.6.4: LDAPS.

1) Which port is used by the LDAPS protocol?
   - TCP port 80
   - TCP port 22
   - TCP port 636

2) What is the main application of LDAPS?
   - Validating user credentials
   - Securely sharing information about a user
   - Securely sending an email message

3) What is exploited in an LDAP injection attack?

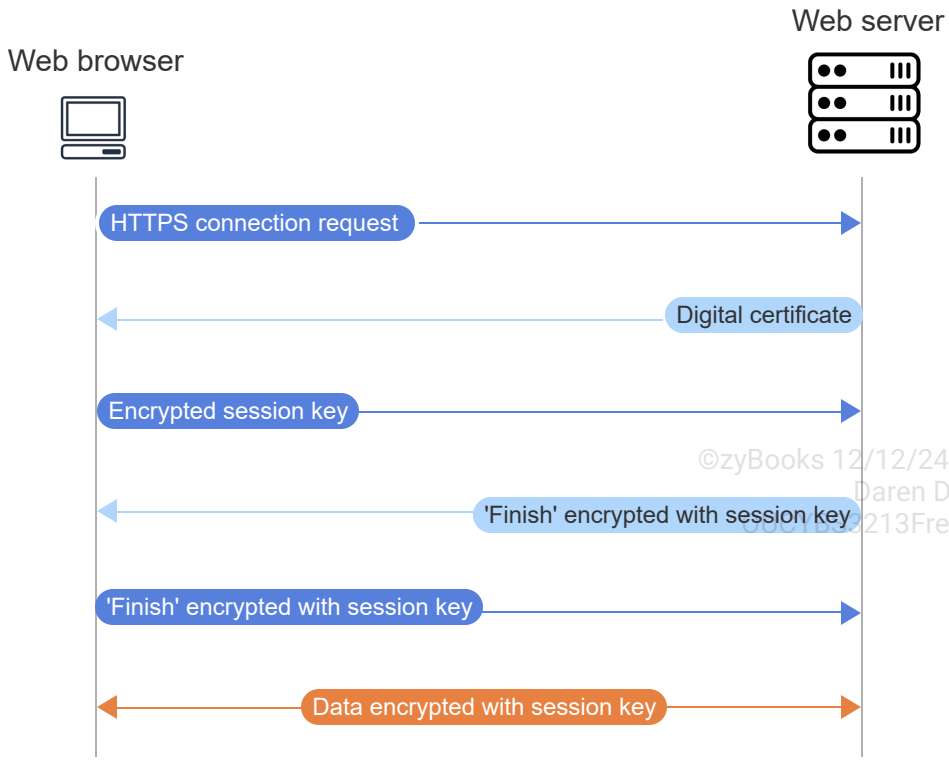
- Weak passwords
- Unencrypted data
- Input validation vulnerabilities

HTTPS

Hypertext transfer protocol secure (HTTPS), also known as ***HTTP over SSL*** or ***HTTP over TLS***, is an extension of the hypertext transfer protocol (HTTP) that uses SSL/TLS to establish an authenticated and encrypted connection between a client and a server. HTTPS is used for secure data exchange between a web browser and a web server. HTTPS is an application layer protocol (Layer 7). HTTPS uses TCP port 443 by default.

HTTPS relies on the cryptographic services provided by the SSL/TLS protocol to secure HTTP data. SSL/TLS uses digital certificates for authentication, encryption for data confidentiality, and message authentication codes (MACs) for data integrity. HTTPS supports mutual authentication. HTTPS protects against a man-in-the-middle attack (MITM) and the eavesdropping and tampering of data exchanged between a web browser and web server.

PARTICIPATION ACTIVITY 4.6.5: HTTPS SSL/TLS handshake.



Animation content:

Static image: A computer icon labeled "Web browser" and a server icon labeled "Web server". Messages are shown passing between the Web browser and Web server. The first message is labeled "HTTPS connection request" and goes from the Web browser to the Web server. The second message is labeled "Digital certificate" and goes from the Web server to the Web browser. The third message is labeled "Encryption session key" and goes from the Web browser to the Web server. The fourth message is labeled "'Finish' encrypted with session key" and goes from the Web server to the Web browser. The fifth message is labeled "'Finish' encrypted with session key" and goes from the Web browser to the Web server. The final message is labeled "Data encrypted with session key" and goes in both directions between the Web browser and the Web server.

Animation captions:

1. A web browser (HTTPS client) requests an HTTPS session from a web server.
2. The web server sends the web server's digital certificate to the web browser.
3. The web browser creates a session key (symmetric key) and encrypts the session key with the web server's public key obtained from the web server's digital certificate.
4. The web server decrypts the session key with the web server's private key, encrypts 'Finish' with the session key and sends the encrypted message to web browser.
5. The web browser encrypts 'Finish' with the session key and sends the encrypted message to the web server. The HTTPS session data is encrypted with the session key.

PARTICIPATION ACTIVITY 4.6.6: HTTPS.

1) Which port is used by the HTTPS protocol?
   - TCP port 80
   - TCP ports 22
   - TCP port 443

2) How does a web browser authenticate a web server?
   - By using the web server's digital certificate
   - By using the web browser's digital certificate

- By using message authentication codes (MACs)

3) Which protocol does HTTPS use to establish an authenticated and encrypted connection between two parties?

- HTTP
- SSH
- SSL/TLS

4) How does HTTPS ensure the confidentiality of HTTP data?

- By using a digital certificate to authenticate a web server
- By using message authentication codes to ensure the integrity of HTTP data
- By encrypting HTTP data

4.7 SNMPv3

SNMPv3

Simple network management protocol (SNMP) is a network protocol for monitoring and managing networked devices in an IP network. SNMP is an application layer protocol (Layer 7). SNMP uses UDP ports 161 and 162.

A ***managed device***, or ***network element***, is a network node that implements an SNMP interface that allows access to the network node's information. A managed device can be any type of device, including a switch, router, cable modem, printer, IP telephone, and computer host. An ***SNMP manager*** is a system that monitors and controls a network element's activities using SNMP. An ***SNMP agent*** is the software that runs on a network element and collects and maintains information on the network element.

An SNMP manager may request information from a network element or set a configuration parameter on a network element. An SNMP agent listens for and executes an SNMP command sent by an SNMP manager. An ***SNMP trap*** is an alert message sent from an SNMP agent to an SNMP manager to notify the SNMP manager of an event at a network element.

PARTICIPATION ACTIVITY 4.7.1: SNMPv3.

How to use this tool

SNMP agent **SNMP** **SNMP trap** **SNMP manager**

	A system that controls and monitors the activities of a network element using SNMP.
	The software that runs on a network element and collects and maintains information on the network element.
	A networking protocol for monitoring and management of networked devices in an IP network.
	An alert message sent from an SNMP agent to an SNMP manager to notify the SNMP manager of an event at a network element.

Reset

PARTICIPATION ACTIVITY 4.7.2: SNMP.

1) Which ports are used by the SNMP?

- TCP port 80 and TCP port 443
- TCP ports 22 and UDP port 1812
- UDP port 161 and UDP port 162

2) An SNMP _____ monitors and controls the activities of a network element.

- manager
- agent
- trap

3) An SNMP _____ is an alert message.

- manager
- agent
- trap

4) An SNMP _____ collects and maintains information on a network element.

- manager
- agent
- trap

SNMP security

SNMPv3 is the latest version of SNMP. SNMPv3 features security improvements over the previous versions. SNMPv3 supports authentication, encryption, and integrity of an SNMP message. Three security levels exist in SNMPv3:

- ***NoAuthNoPriv***, or ***No Authentication and No Privacy***, is an SNMP security level in which an SNMP message is not authenticated and not encrypted. NoAuthNoPriv should only be used in a closed, secure network.
- ***AuthNoPriv***, or ***Authentication and No Privacy***, is an SNMP security level in which an SNMP message must be authenticated but not encrypted during transmission. SNMPv3 supports HMAC-MD5 and HMAC-SHA for authentication and integrity.
- ***AuthPriv***, or ***Authentication and Privacy***, is an SNMP security level in which an SNMP message must be authenticated and encrypted during transmission. SNMPv3 supports HMAC-MD5 and HMAC-SHA for authentication and integrity, and DES for privacy.

PARTICIPATION ACTIVITY 4.7.3: SNMP.

1) Which symmetric cipher is used by SNMPv3 to provide privacy?

- AES
- DES
- HMAC

2) Which cryptographic method is used by SNMPv3 to provide message authentication?

- MAC
- AES
- HMAC

3) Which cryptographic method is used by SNMPv3 to provide message integrity?

- MAC
- AES
- HMAC

Hardening network devices

Implementing secure protocols like SNMPv3 and hardening switches, routers, and other networking devices is vital for network security. Hardening network devices includes disabling unused services, implementing access control lists, and regularly updating device firmware. Hardening network devices reduce attack surfaces, prevent unauthorized access, and ensure compliance with established security standards.

4.8 IPSec

IPSec

Internet Protocol Security (IPSec) is a protocol suite for securing data communications over an IP network. IPSec ensures the authenticity, integrity, and confidentiality of an IP packet. IPSec is a network layer protocol (Layer 3).

The IPSec protocol suite consists of two main protocols:

- ***Authentication Header (AH)*** is an IPSec protocol that provides authentication and integrity for an IP packet and protection against a replay attack. AH ensures data integrity by using a message digest and data authenticity by using a shared secret key to create the message digest. AH protects against a replay attack by using a sequence number in an AH header. AH authenticates an entire IP packet (IP header and IP payload).

- ***Encapsulating Security Protocol (ESP)*** is an IPSec protocol that provides authentication, integrity, and confidentiality for an IP packet and protection against a replay attack. ESP provides encryption by using a shared key between a data sender and a data receiver. ESP uses the same AH algorithms for providing integrity and authentication. ESP only authenticates an IP payload.

PARTICIPATION ACTIVITY 4.8.1: IPSec.

How to use this tool

Authentication header **Encapsulating Security Protocol** **IPSec**

	A protocol suite for securing data communications over an IP network.
	An IPSec protocol that provides authentication and integrity for an IP packet.
	An IPSec protocol that provides authentication, integrity, and confidentiality for an IP packet

Reset

PARTICIPATION ACTIVITY 4.8.2: IPSec.

1) Which IPSec protocol provides protection against a replay attack?
   - AH
   - ESP
   - AH and ESP

2) Which IPSec protocol provides data confidentiality?
   - AH
   - ESP
   - AH and ESP

3) Which IPSec protocol provides authentication and integrity of an IP packet?

- AH
- ESP
- AH and ESP

4) Which IPSec protocol authenticates an entire IP packet?

- AH
- ESP
- AH and ESP

5) Which IPSec protocol only authenticates an IP payload?

- AH
- ESP
- AH and ESP

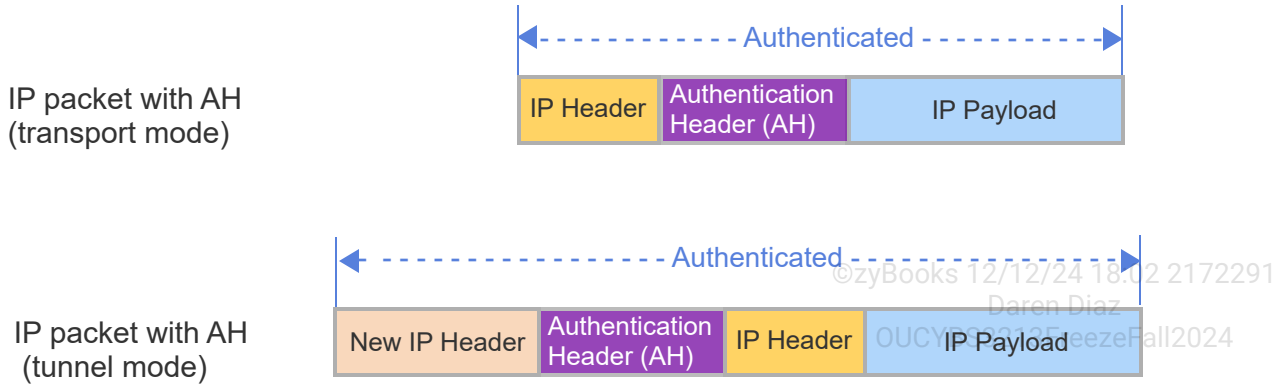
IPSec modes

The IPSec AH and IPSec ESP protocols can be used in two modes:

- ***Transport mode*** is an IPSec mode in which only an IP payload is authenticated and encrypted, not the IP header. Transport mode is used for end-to-end communications such as communications between a host and a gateway, or a client and a server.
- ***Tunnel mode*** is an IPSec mode in which an IP packet (IP header and IP payload) is authenticated, encrypted, and encapsulated in a tunneling protocol. IPSec is commonly encapsulated in Layer 2 Tunneling Protocol (L2TP). Tunnel mode is used in communications between two gateways, a host and a gateway, or two hosts.

PARTICIPATION ACTIVITY 4.8.3: IPSec AH protocol.

Original IP packet



Animation content:

Static image: Representations of three IP packets. The first is labeled "Original IP packet" and has a yellow section labeled "IP Header" and a blue section labeled "IP Payload". The second is labeled "IP packet with AH (transport mode)" and has a yellow section labeled "IP Header", a purple section labeled "Authentication Header (AH)", and a blue section labeled "IP Payload". Arrows span the entire representation showing that the IP packet is authenticated. The third IP packet is labeled "IP packet with AH (tunnel mode)" and has a tan section labeled "New IP Header", a purple section labeled "Authentication Header (AH)", a yellow section labeled "IP Header", and a blue section labeled "IP Payload". Arrows span the entire representation showing that the IP packet is authenticated.

Animation captions:

1. In transport mode, an IP payload is authenticated and encrypted. The Authentication Header (AH) is inserted after the IP Payload.
2. The IP Header is inserted after the Authentication Header (AH). The entire IP packet is authenticated.
3. In tunnel mode, an IP packet (IP Payload and IP Header) is authenticated and encrypted. The Authentication Header (AH) is inserted after the IP Packet.
4. A new IP Header is inserted after the AH and the original IP packet (IP Header and IP Payload). The new IP packet is authenticated.

PARTICIPATION ACTIVITY 4.8.4: IPSec.

1) In which IPSec mode an IP header is not authenticated?

- Transport
- Tunnel

- Transport and tunnel

2) In which IPSec mode an entire IP packet is encapsulated in another protocol?
   - Transport
   - Tunnel
   - Transport and tunnel

3) In which IPSec mode an IP payload is encrypted?
   - Transport
   - Tunnel
   - Transport and tunnel

4) Which IPSec mode is used in communications between a server and a client?
   - Transport
   - Tunnel
   - Transport and tunnel

5) Which IPSec mode is used in communications between two gateways?
   - Transport
   - Tunnel
   - Transport and tunnel

6) In which IPSec mode an IP payload is authenticated?
   - Transport
   - Tunnel
   - Transport and tunnel

4.9 LAB: Network enumeration (Walkthrough)

IT-Labs are not printable at this time.

4.10 LAB: Denial-of-Service (DoS) attacks (Walkthrough)

IT-Labs are not printable at this time.

4.11 LAB: Secure shell (SSH) (Walkthrough)

IT-Labs are not printable at this time.

4.12 LAB: HTTPS (Walkthrough)

IT-Labs are not printable at this time.

4.13 LAB: Security audit through network scanning (Scenario)

IT-Labs are not printable at this time.

©zyBooks 12/12/24 18:02 2172291
Daren Diaz
OUCYBS3213FreezeFall2024