Chapter 5

Networks & Security

DE HOGESCHOOL MET HET NETWERK

Elfde-Liniestraat 24, 3500 Hasselt, www.pxl.be

Networks & Security

1. **Introduction**
2. Protocols and vulnerabilities & attacks
3. Security technologies

Security Threats and Vulnerabilities

- Vulnerability is the degree of weakness in a network or a device.
- Some degree of vulnerability is inherent in routers, switches, desktops, servers, and even security devices.
- Typically, the network devices under attack are the endpoints, such as servers and desktop computers.

Security Threats and Vulnerabilities

There are three primary vulnerabilities or weaknesses:

- **Technological Vulnerabilities**
  TCP/IP Protocol weaknesses, Operating System Weaknesses, and Network Equipment weaknesses.
- **Configuration Vulnerabilities**
  unsecured user accounts, system accounts with easily guessed passwords, misconfigured internet services, unsecure default settings, and misconfigured network equipment.
- **Security Policy Vulnerabilities**
  lack of a written security policy, politics, lack of authentication continuity, logical access controls not applied, software and hardware installation and changes not following policy, and a nonexistent disaster recovery plan.

All three of these sources of vulnerabilities can leave a network or device open to various attacks, including malicious code attacks and network attacks.

Classification of network attacks

- **Reconnaissance attacks**
  - gathering information about a target system or network, such as open ports, IP addresses, network topology, or active services, to identify potential vulnerabilities or entry points for an attack.
- **Access attacks**
  - attempts to gain unauthorized access to a system or network, often exploiting identified vulnerabilities or using methods like brute force, password attacks, or social engineering.
- **Denial of service**
  - overwhelm a target system or network with excessive traffic, requests, or other malicious activities, causing service disruptions or making the target unresponsive.
- **Man-in-the-Middle (MITM) Attacks**
  - intercepting and potentially altering the communication between two parties without their knowledge, enabling eavesdropping, data manipulation, or session hijacking.
- **Insider Attacks**
  - perpetrated by individuals who have legitimate access to a network or system, such as employees or contractors, who misuse their access to compromise data or system integrity.
- **Distributed Attacks**
  - involve multiple devices or systems, often compromised and controlled by an attacker, working in concert to target a single victim. An example is a Distributed Denial of Service (DDoS) attack.
- **Malware Attacks**
  - involve the use of malicious software, such as viruses, worms, ransomware, or Trojans, to compromise a target system or network, steal sensitive information, or cause damage.
- **Social Engineering Attacks**
  - rely on manipulating human behavior and trust, using tactics like phishing, pretexting, or baiting, to deceive individuals into revealing sensitive information, granting unauthorized access, or downloading malware.
- **Physical Network Attacks**
  - target the physical components of a network, such as unauthorized access to networking equipment, eavesdropping or tapping, device theft, or jamming wireless communication.

Network attack Mitigations (1/2)

To mitigate network attacks, organizations should implement a multi-layered security strategy that covers various aspects of network security.

1. **Firewall**: Deploy firewalls to filter incoming and outgoing traffic, block malicious IP addresses, and enforce network security policies.
2. **Intrusion Detection and Prevention Systems (IDS/IPS)**: Implement IDS/IPS solutions to monitor network traffic for signs of suspicious activities or potential attacks and take appropriate action to block or mitigate threats.
3. **Regular Patching and Updates**: Keep all software, firmware, and operating systems up-to-date to minimize vulnerabilities that attackers can exploit.
4. **Network Segmentation**: Divide the network into smaller, isolated segments to limit the potential impact of an attack and restrict unauthorized access to sensitive information.
5. **Access Control**: Implement strong access control policies, including role-based access control (RBAC), to ensure that users have the minimum necessary privileges to perform their tasks.
6. **Strong Authentication**: Enforce multi-factor authentication (MFA) for accessing critical systems or sensitive data.
7. **Encryption**: Use encryption for data transmission and storage to protect sensitive information from eavesdropping or theft.

Network attack Mitigations (2/2)

8. **Security Awareness Training**: Educate employees about common attack vectors, such as phishing or social engineering, and train them to recognize and report suspicious activities.
9. **Regular Security Audits**: Conduct periodic security audits to assess the effectiveness of security measures and identify potential weaknesses in the network.
10. **Backup and Disaster Recovery**: Implement a robust backup and disaster recovery plan to ensure business continuity in the event of an attack or data loss.
11. **Endpoint Security**: Deploy antivirus, anti-malware, and other endpoint security solutions on all devices connected to the network.
12. **Secure Configuration**: Configure devices, systems, and software with security best practices in mind, disabling unnecessary services, and applying the principle of least privilege.
13. **Network Monitoring**: Continuously monitor network traffic for anomalies or potential threats, and respond quickly to any detected issues.
14. **Incident Response Plan**: Develop and maintain a well-defined incident response plan to handle security breaches or attacks, ensuring prompt detection, containment, and remediation.

Networks & Security

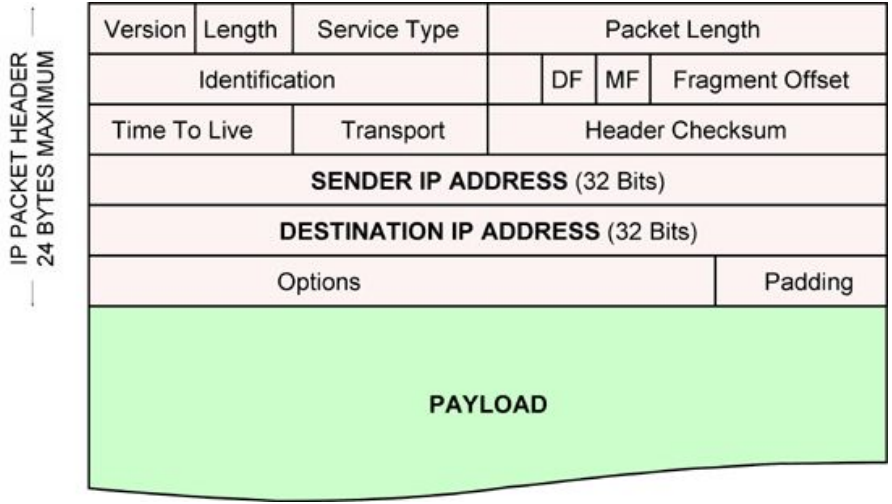
1. Introduction
2. **Protocols and vulnerabilities & attacks**
    1. **The Internet Protocol**
    2. **TCP & UDP**
    3. **DNS**
    4. **DHCP**
    5. **HTTP(s)**
    6. **OSI Layer 2**
    7. **Other protocols**
3. Security technologies

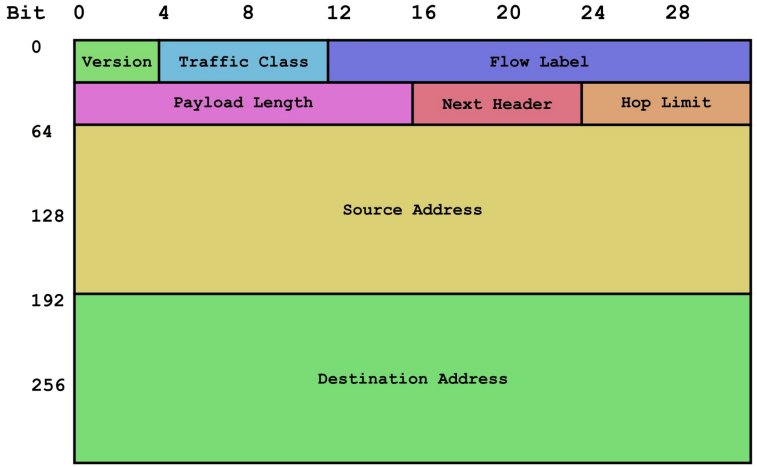
1. The Internet Protocol (IP)

- IP is Layer 3 **connectionless** protocol.
- IP delivers packet from source to destination over network.
- IP does not validate source IP address, allowing spoofing by threat actors.
- Threat actors can tamper with IP header fields for attacks.
- Understanding IPv4 and IPv6 header fields is important for security analysts.

1. The Internet Protocol (IP)

- IPv4 and Ipv6 packets





-

1. The Internet Protocol (IP) - ICMP

- developed for diagnostics and reporting errors.
- Devices generate ICMP messages for network errors or outages.
- Ping command is user-generated ICMP *echo request* for connectivity verification.

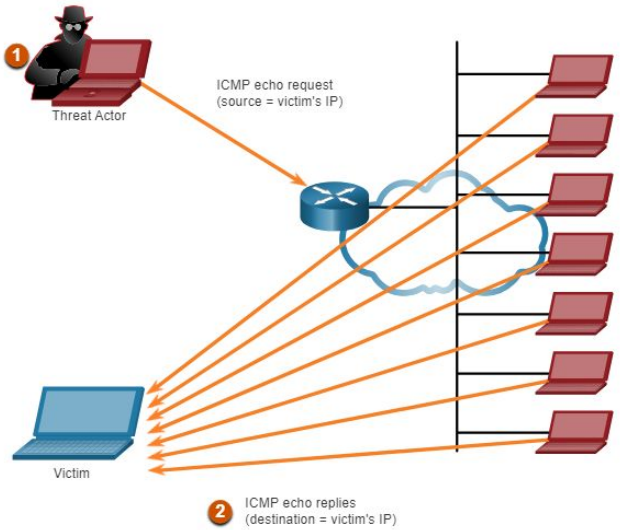
1. The Internet Protocol (IP) - ICMP attacks

- Weakness ICMP
  - Discover (enumeration, reconnaissance, scanning attacks), generate DoS, alter host routing tables
- Countermeasure
  - Networks should have strict ICMP access control list (ACL) filtering on the network edge to avoid ICMP probing from the internet.

1. The Internet Protocol (IP) - ICMP reflection amplification attacks

- **Amplification Attack:** An attacker sends small packets to a service with a fake source IP (the victim's), which sends a larger response to the victim. This increases the data sent to the victim.
- **Reflection Attack:** The attacker sends traffic to a reflector with the victim's spoofed IP. The reflector responds to the victim, flooding their network.

They can be combined in a "**reflection amplification attack**" where an attacker sends an `ICMP Echo Request` (ping) to a network with the spoofed source IP of the victim, and all devices respond to the victim with an `ICMP Echo Reply` (pong), flooding their network.



1. The Internet Protocol (IP) - vulnerabilities and attacks

- IP Spoofing
  - Attacker sends packets with forged IP to bypass controls, launch DoS, or manipulate data.

- IP Source Routing
  - Sender specifies packet route through network, which attackers can exploit to bypass security, eavesdrop, or launch man-in-the-middle attacks.

1. The Internet Protocol (IP) - vulnerabilities and attacks

- ICMP attacks
  - ICMP used for error reporting and diagnostics, but can be exploited for DoS, reconnaissance, or traffic redirection.

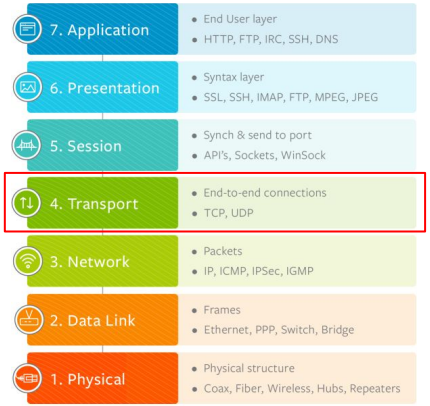
- IP Tunneling
  - Technique to encapsulate IP packets within another, which can be used legitimately or exploited to bypass security, hide malicious traffic, or create covert channels.

1. The Internet Protocol (IP) - vulnerabilities and attacks

- Lack of Encryption
  - IP protocol lacks built-in encryption, making data interception possible. Higher-layer security protocols like TLS/SSL or IPsec can mitigate this.

- IPv6 Transition issues
  - Potential vulnerabilities from misconfigurations or incompatibilities during the transition from IPv4 to IPv6 can be exploited by attackers for security bypass or attacks.

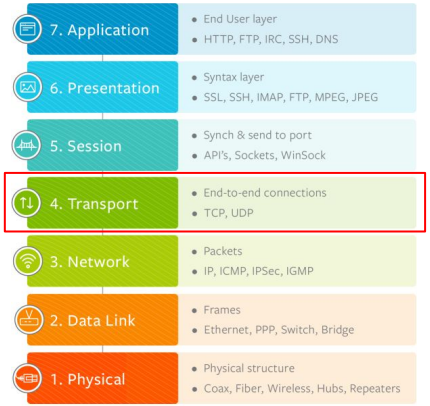
2. Transmission Control Protocol (TCP) & User Datagram Protocol (UDP)



TCP

- TCP establishes a connection for reliable communication.
- Error checking mechanisms detect and correct transmission errors.
- Retransmission ensures data integrity and completeness.
- Flow control prevents congestion and maintains optimal transmission rate.
- TCP ensures ordered delivery of packets.
- TCP is ideal for guaranteed data delivery applications such as web browsing, file transfer, and email.

2. Transmission Control Protocol (TCP) & User Datagram Protocol (UDP)

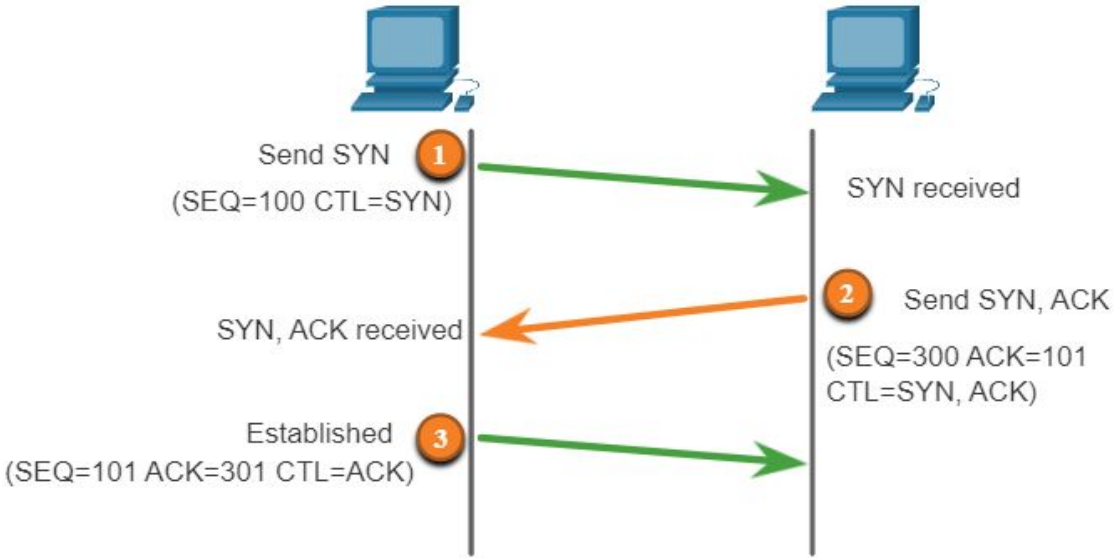


UDP

- UDP is connectionless and allows for faster data transmission.
- Minimal error checking is performed, with no correction or retransmission.
- UDP has lower overhead and is efficient for some applications and network conditions.
- No flow control can lead to packet loss and network congestion.
- UDP does not guarantee ordered delivery, leaving it to the application layer.
- UDP is suitable for low latency applications such as streaming media, online gaming, and real-time data transmission.

2. TCP & UDP

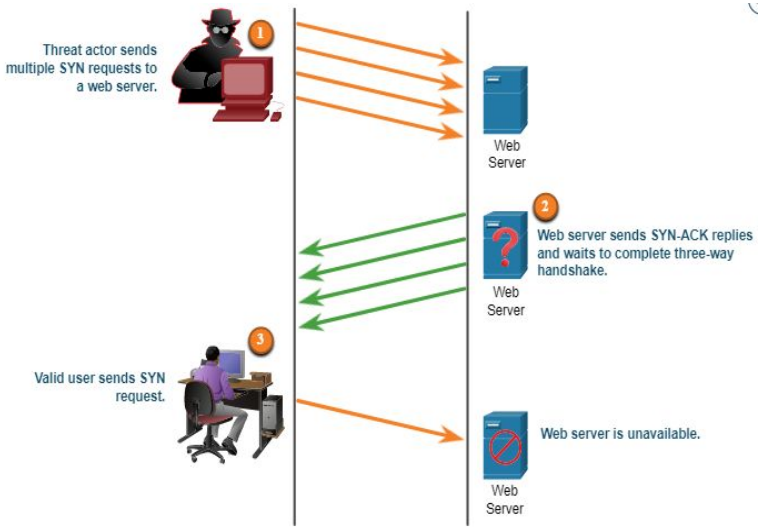
TCP 3-way handshake



2. TCP & UDP - TCP attacks

TCP SYN Flood attack

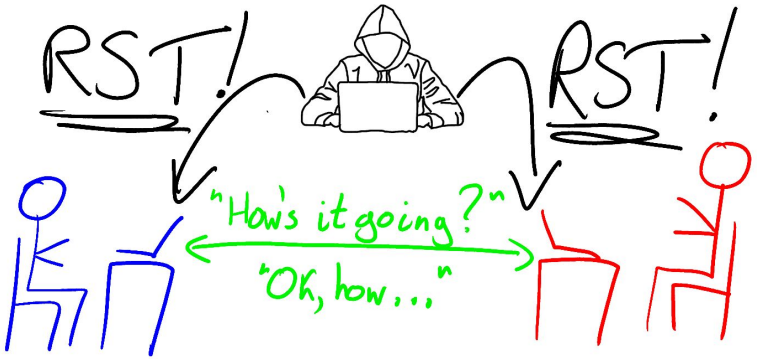
- TCP SYN Flood attack exploits handshake with many connection requests.
- Attacker spoofs IP addresses to complicate connection establishment.
- Target server allocates resources for each attempt, but no ACK packets arrive.
- Attack overwhelms server resources, causing denial of service (DoS).



2. TCP & UDP - TCP attacks

TCP reset Attack

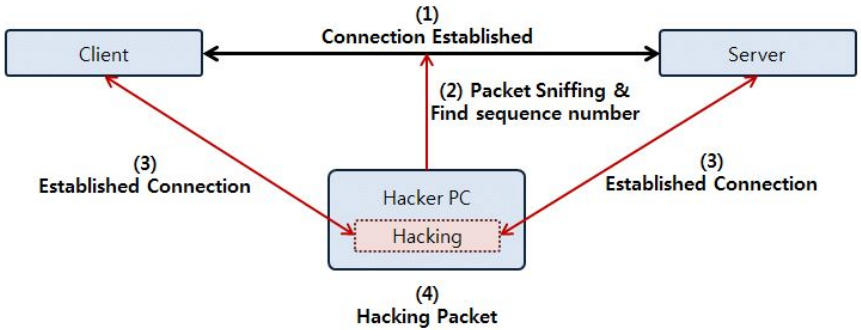
- Attacker sends forged TCP RST packet to terminate connection.
- Spoofing includes valid sequence number.
- Devices interpret packet as legitimate signal to terminate, causing abrupt disconnection.
- Attack can cause service disruption, data loss, or create opportunities for further attacks.



2. TCP & UDP - TCP attacks

TCP session Hijacking

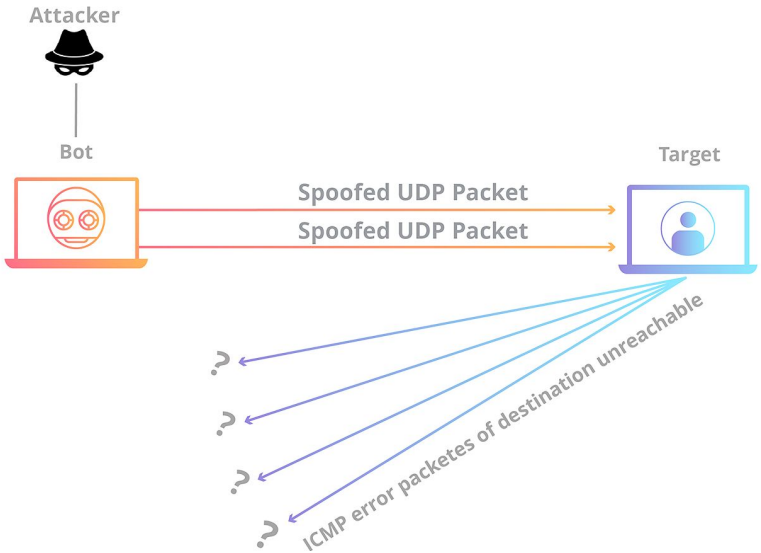
- Also known as TCP sequence prediction attack.
- Attacker intercepts and takes control of established TCP session.
- Predicts valid sequence numbers to inject malicious data/commands.
- Can lead to unauthorized access, data manipulation, or service disruption.
- Mitigation techniques include strong encryption, secure communication protocols (e.g., TLS/SSL), and security measures like intrusion detection systems.



2. TCP & UDP - UDP attacks

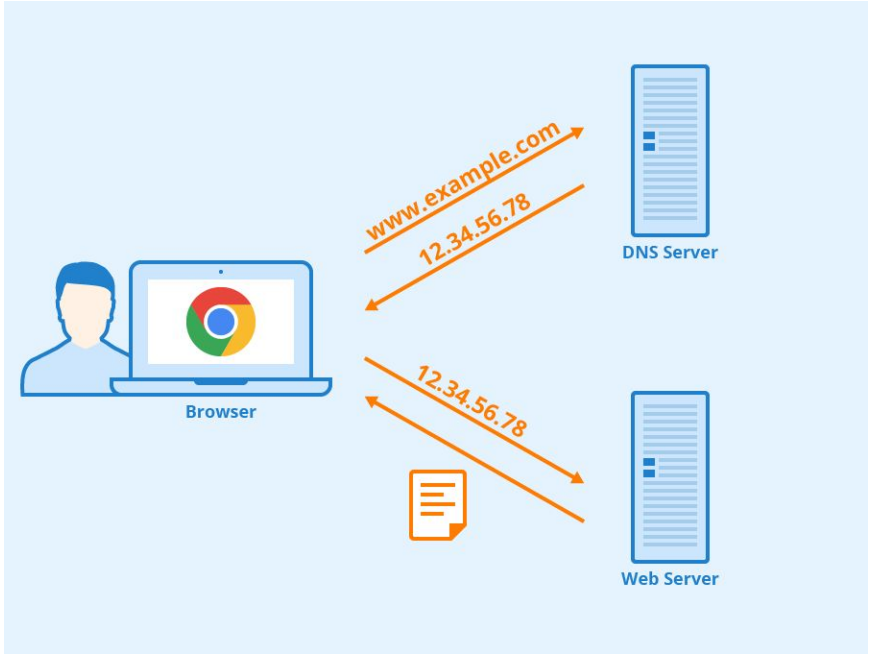
UDP flood attack

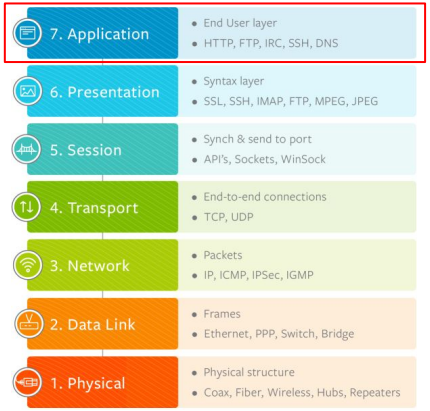
- Tools send UDP packets from spoofed host to server.
- Program searches for closed ports, causing server to reply with ICMP message.
- Traffic on segment from many closed ports uses up bandwidth.
- UDP flood attack consumes network resources.
- Result is similar to DoS attack.



3. DNS

DNS, or the Domain Name System, translates human readable domain names (example.com) to machine readable IP addresses (192.0.2.44).



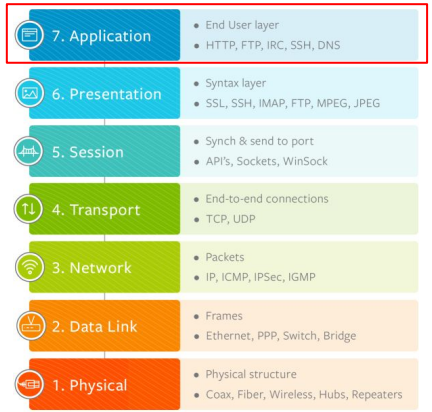


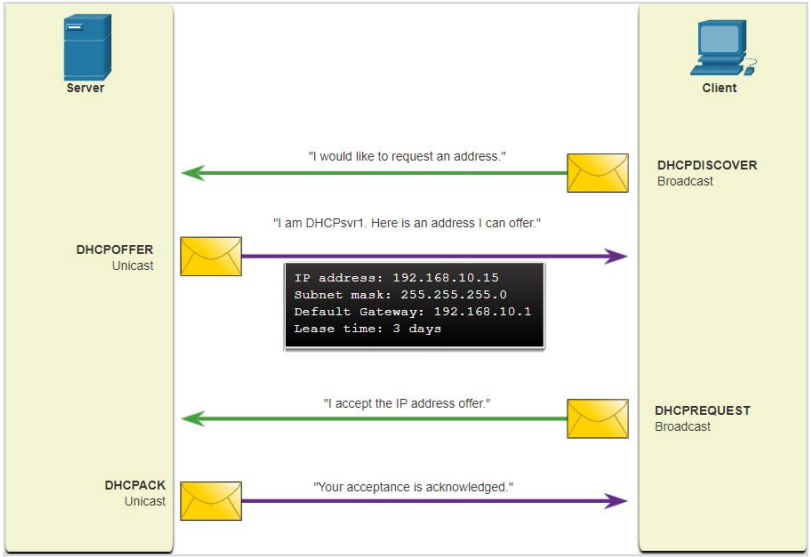
3. DNS attacks

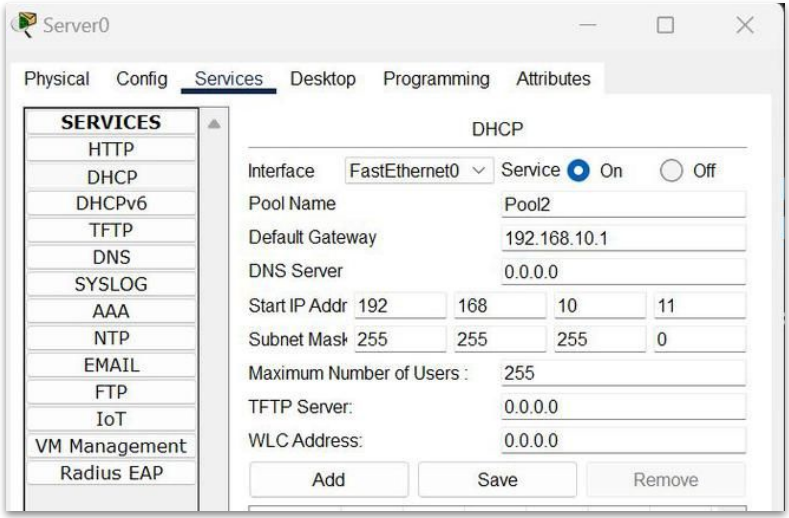
- DNS Cache Poisoning
  - Attackers send falsified RR (Record Resource) info to DNS resolver, redirecting clients to malicious sites.
- DNS Amplification and Reflection
  - Attackers flood target with response traffic from DNS servers due to many queries with target's IP as source.
- DNS Resource Utilization
  - Attackers flood servers with traffic, disrupting services for legitimate users.
- DNS Tunneling
  - Attackers hide non-DNS traffic within DNS traffic to bypass security and establish covert communication.

4. Dynamic Host Configuration Protocol (DHCP)

- a network management protocol used to automate the process of configuring devices on IP networks.
- operates using a four-step process called DORA, consisting of Discover, Offer, Request, and Acknowledge.



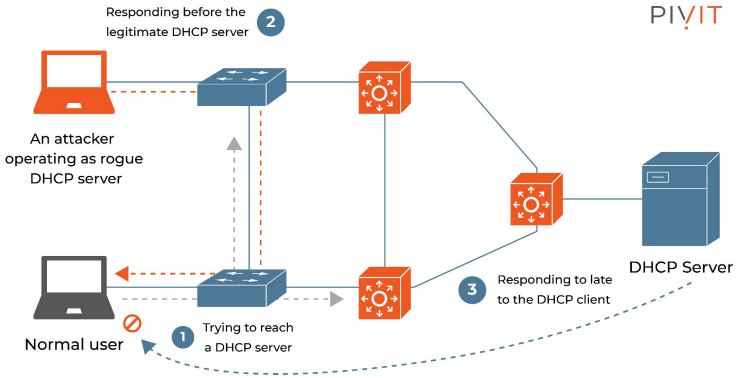




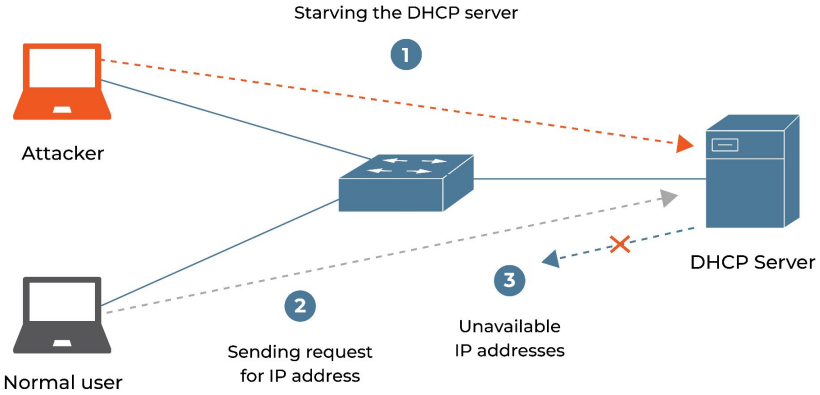
4. DHCP attacks

DHCP Spoofing attack

- Attacker sets up malicious server and responds to client requests with false configuration parameters.
- Attacker gains control over traffic, enabling eavesdropping, man-in-the-middle attacks, or traffic redirection.
- Attackers configure rogue DHCP servers to respond faster to avoid detection.
- Mitigation: Implement DHCP snooping to monitor and filter unauthorized server responses.



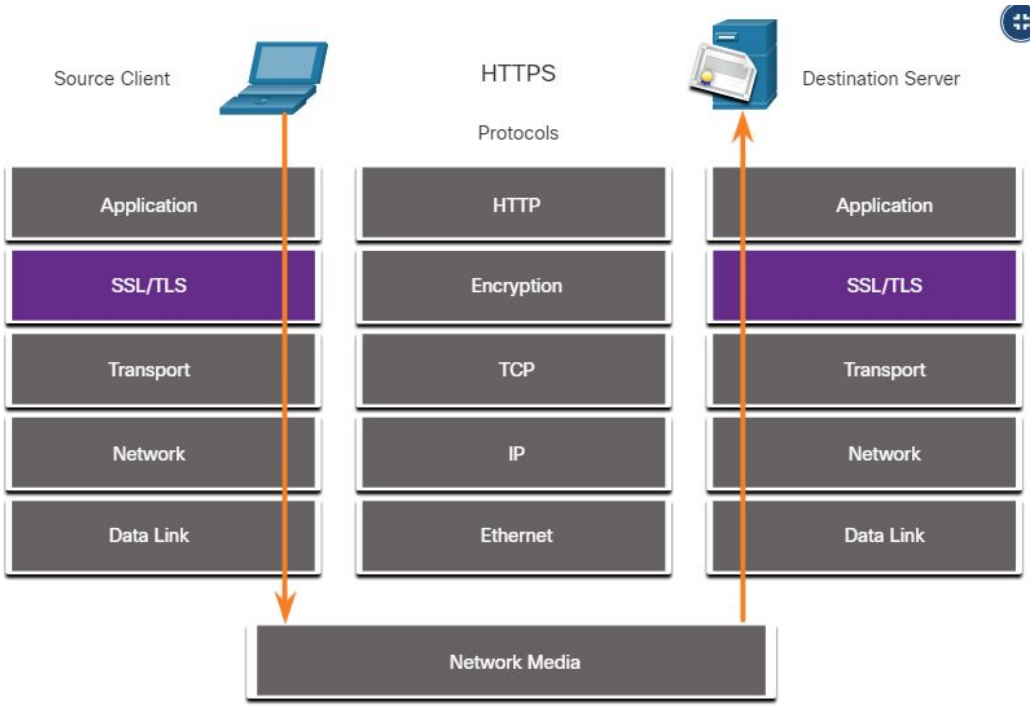
4. DHCP attacks

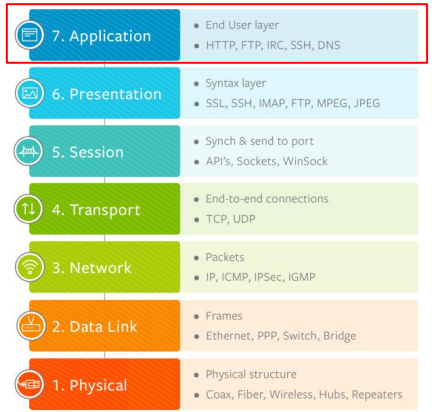


DHCP Starvation attack

- Attacker floods DHCP server with requests, depleting IP address pool and causing DoS.
- Attack facilitates DHCP spoofing by making rogue DHCP server more likely to respond.
- Mitigation: Implement security measures like rate limiting, DHCP snooping, and static IP addresses for critical devices.

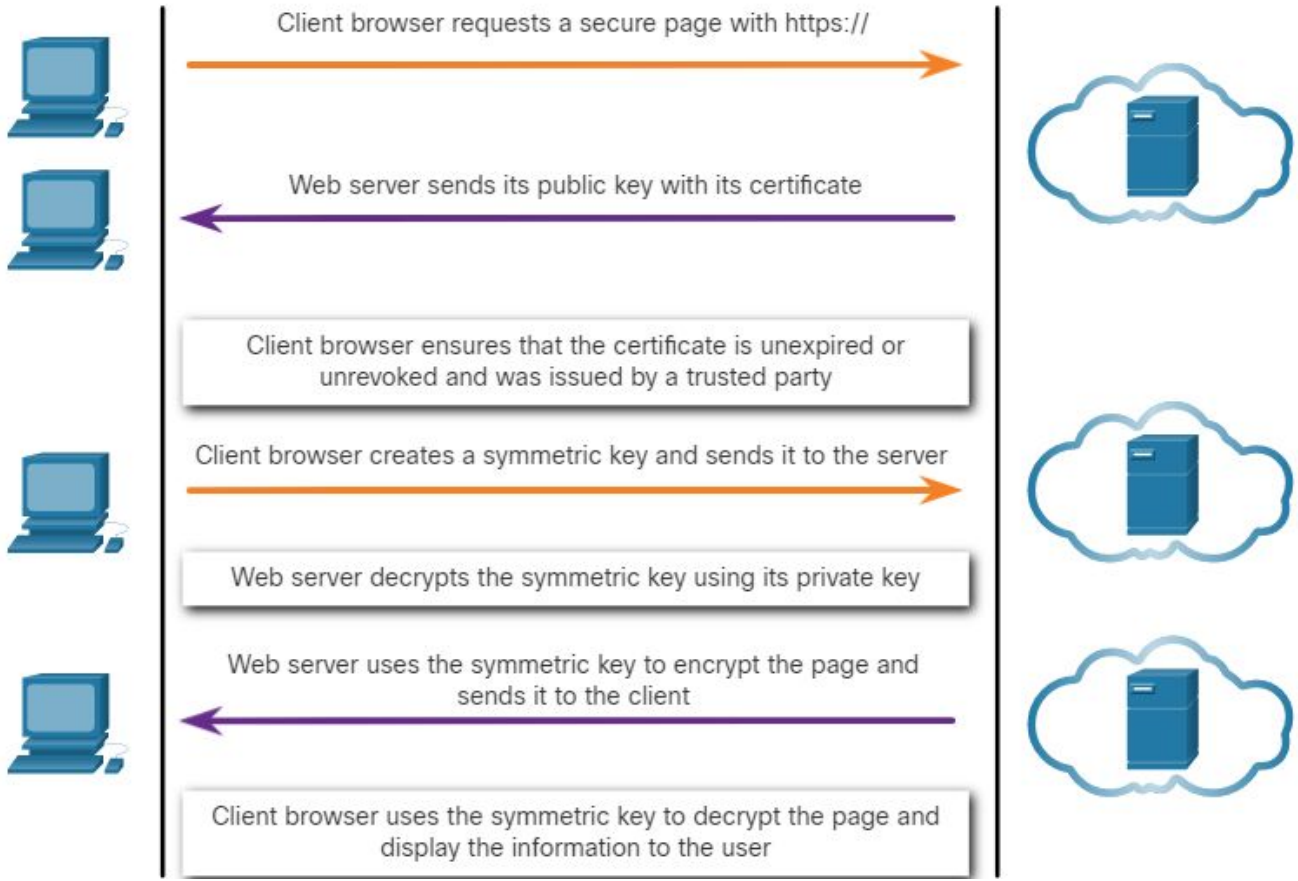
5. Hypertext Transfer Protocol Secure (HTTPS)





- Encryption: Uses TLS or SSL to encrypt data, ensuring confidentiality, integrity, and authenticity.
- Certificate Authorities (CAs): Trusted third parties that issue certificates to authenticate website identity and validate public encryption keys.

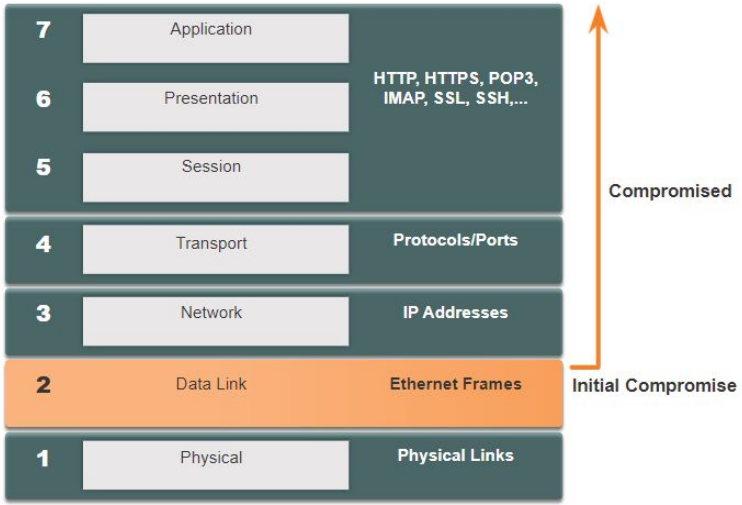
5. HTTP(s)


Client browser requests a secure page with https://
Web server sends its public key with its certificate
Client browser ensures that the certificate is unexpired or unrevoked and was issued by a trusted party
Client browser creates a symmetric key and sends it to the server
Web server decrypts the symmetric key using its private key
Web server uses the symmetric key to encrypt the page and sends it to the client
Client browser uses the symmetric key to decrypt the page and display the information to the user

6. OSI Layer 2 and security

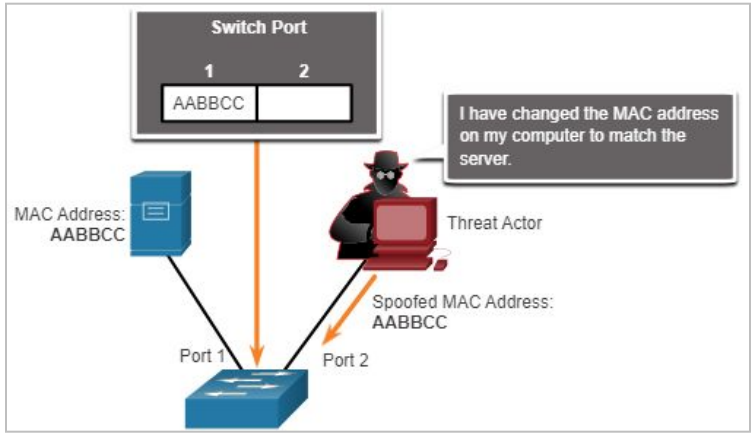
Layer 2

- Media Access control (MAC)
  - unique identifier for network devices used to locate and communicate with other devices on a network.
- Switch
  - connects devices on a LAN by forwarding data packets based on their MAC addresses
- Frame
  - unit of network data that includes a header and a payload with source and destination MAC addresses and control information used for data transfer
- Ethernet
- Address Resolution Protocol (ARP)
  - maps IP addresses to MAC addresses, enabling communication between devices on a local network



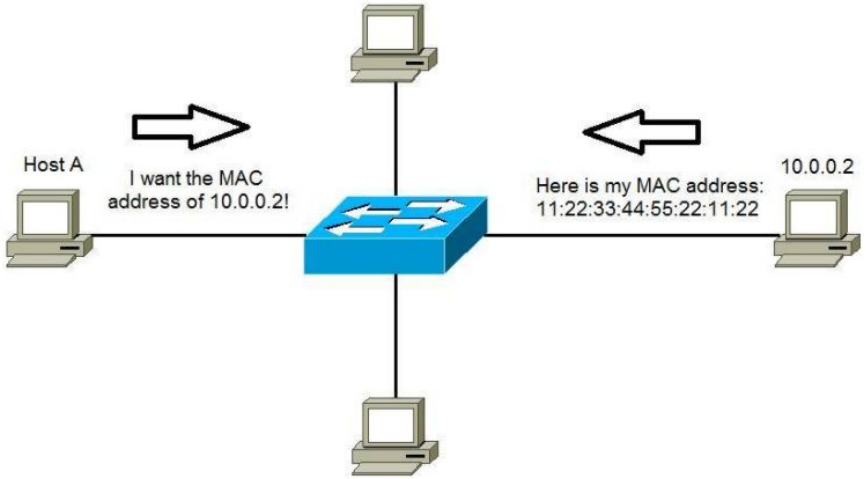
6. OSI Layer 2 and security - MAC address spoofing

- MAC address spoofing: Attackers impersonate targets on internal network by changing their MAC address.
- Attackers send frame with spoofed MAC address to network.
- Switch examines source MAC address, which lacks security mechanisms to verify source.
- L2 vulnerable to MAC address spoofing.



6. OSI Layer 2 and security - ARP

- ARP Request is used to discover MAC address of host with specific IP.
- Host with matching IP sends "gratuitous ARP Reply."
- Attacker poisons ARP cache of devices on local network.
- Attacker associates their MAC with default gateway IP in hosts' ARP caches on LAN segment.

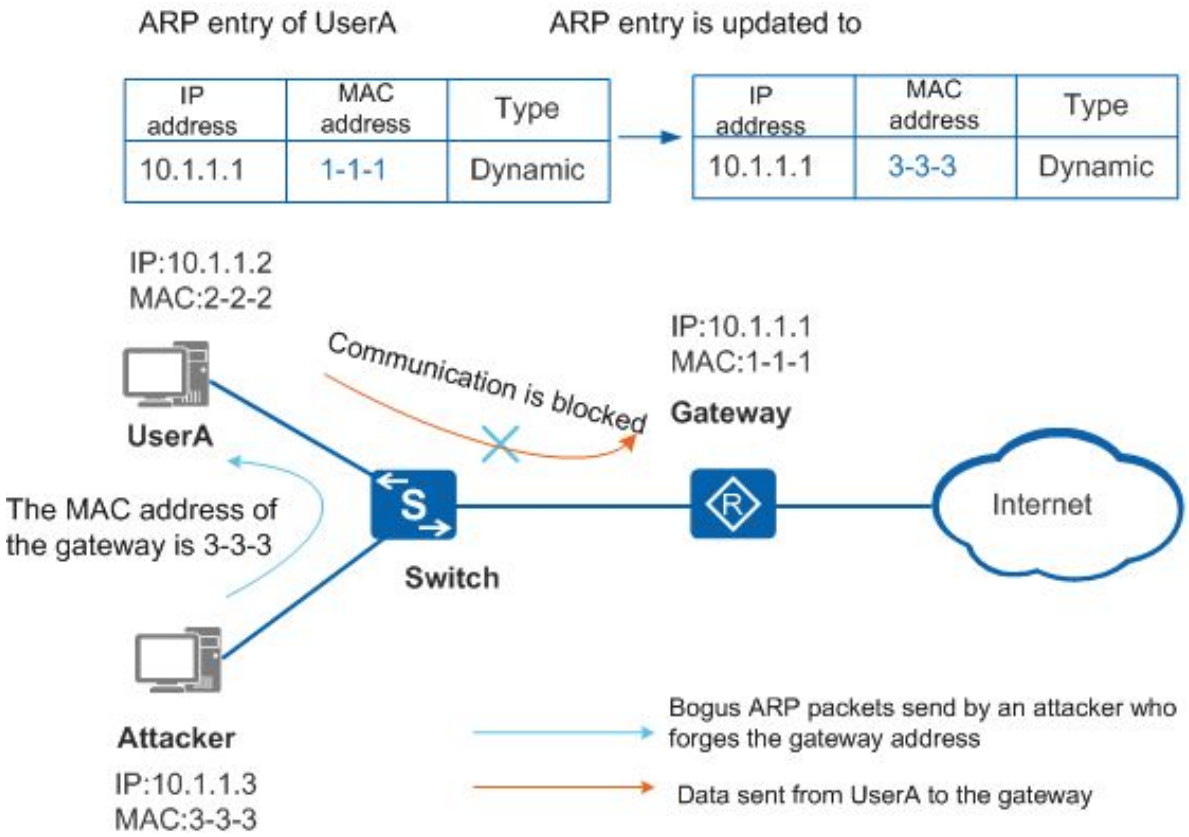


6. OSI Layer 2 and security - ARP

‘gratuitous ARP’

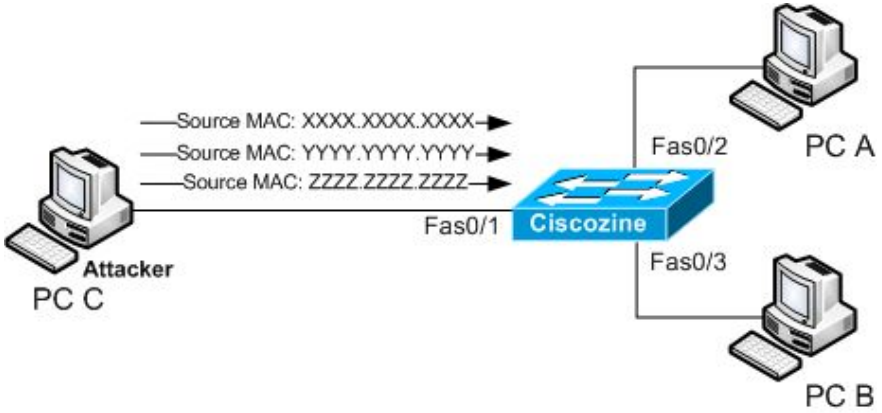
Cache Poisoning ⇒ poison the ARP cache of devices on the local network

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



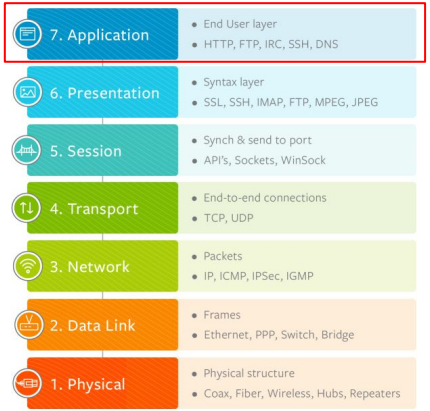
6. OSI Layer 2 and security - MAC Address Table Flooding

- Attackers flood switch with fake MAC addresses until table is full.
- Switches can run out of resources due to flooding attacks.
- Mitigation: Implement port security measures to prevent MAC address table overflow.



7. Other protocols and network security

- **Simple Network Management Protocol (SNMP)**
  - Application layer protocol for communication between managers and agents.
- **Network Time Protocol (NTP)**
  - Synchronizes clocks across Internet or local networks for accurate timekeeping.
- **Syslog**
  - Standardized protocol for collecting, transmitting, and storing log messages from network devices and systems for centralized monitoring and analysis.
  - Syslog servers may be a target due to their importance in security monitoring.

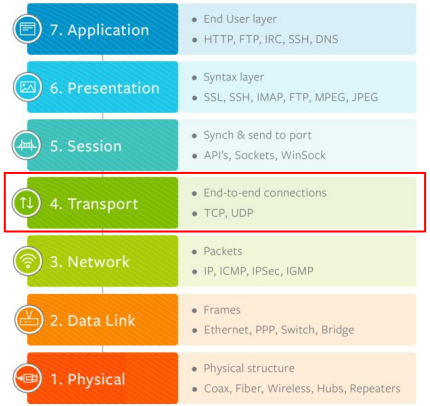


Networks & Security

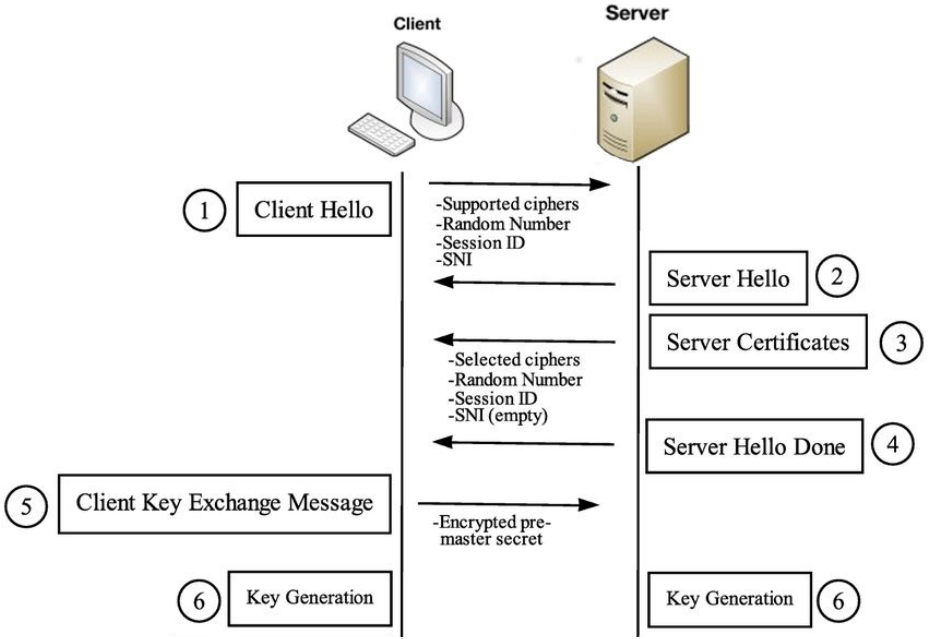
1. Introduction
2. Protocols and vulnerabilities & attacks
3. **Security technologies**
    1. **TLS**
    2. **IPsec**
    3. **SSH**
    4. **Secure configuration**
    5. **VLAN**
    6. **ACL**
    7. **Encryption**
    8. **VPN**
    9. **Firewalls**
    10. **SIEM**
    11. **Other network security technologies**

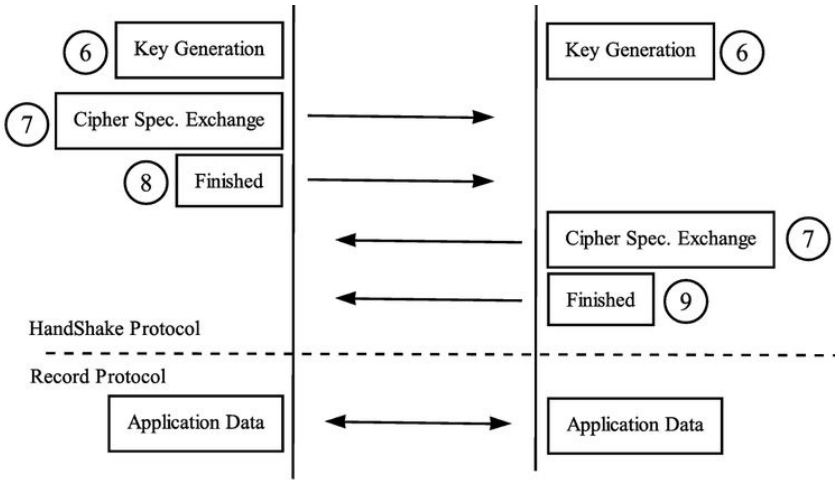
Transport Layer Security (TLS)

- Cryptographic protocol for secure communication over computer networks, commonly used for HTTPS.
- Successor to SSL, with improved security and performance.
- Operates at Layer 4, primarily securing TCP-based connections.
- Initiates secure connection through "handshake protocol" to negotiate algorithms, exchange keys, and establish shared secret for encryption.
- Widely used to secure web traffic, email, messaging, and other communication protocols for privacy and security.

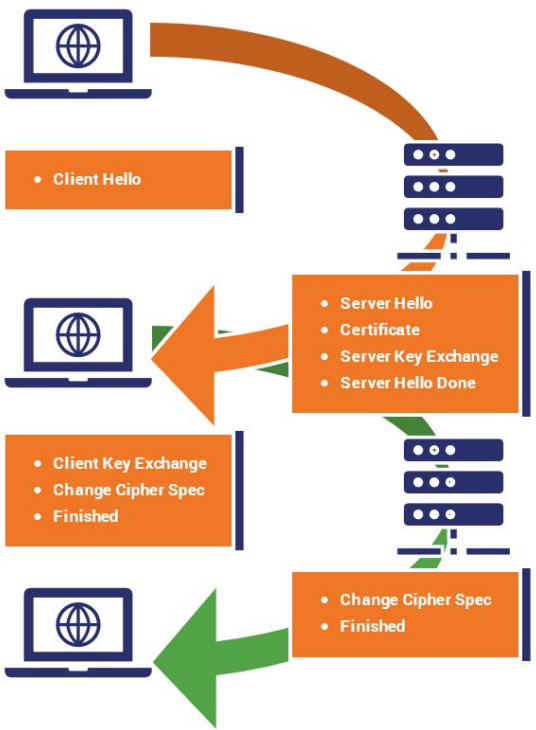


TLS handshake





TLS handshake



Process to establish secure communication between two devices.

- Client sends "Hello" message with TLS version and random number.
- Server responds with its own "Hello" message, version, random number, and SSL/TLS certificate.
- Client verifies certificate and sends "Finished" message with shared key encryption.
- Server sends its own "Finished" message with shared key encryption.
- Connection established and both can exchange encrypted data securely.

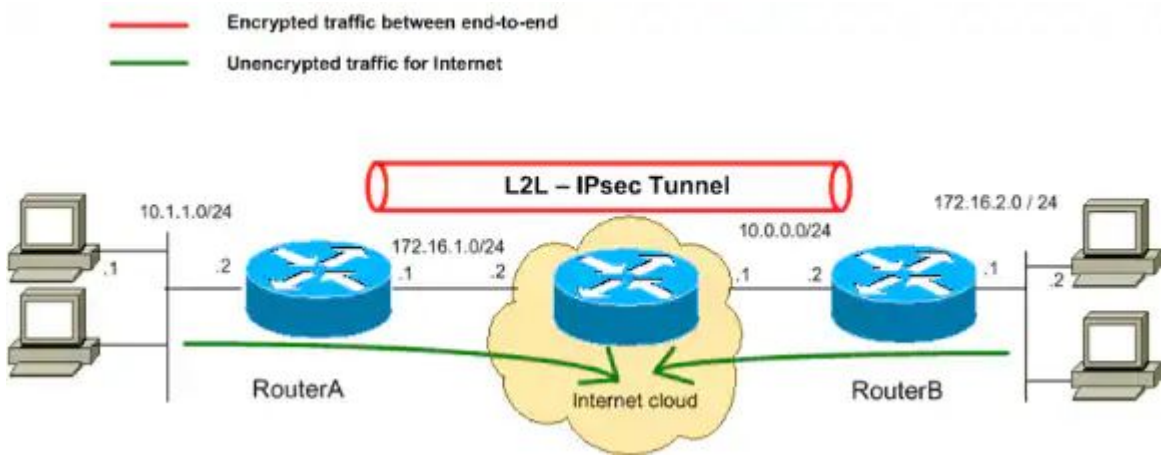
https://www.youtube.com/watch?v=86cQJ0MMses

TLS

- Confidentiality
  - TLS uses symmetric encryption to protect data and keep it confidential from eavesdroppers.
- Integrity
  - TLS employs cryptographic hash functions to create message authentication codes (MACs) that ensure data integrity and prevent tampering or corruption.
- Authentication
  - TLS uses asymmetric encryption and digital certificates to authenticate the server's identity, and optionally, the client's identity, to establish trust.
- PFS
  - TLS provides Perfect Forward Secrecy (PFS) using ephemeral key exchange algorithms like **Diffie-Hellman** or Elliptic Curve Diffie-Hellman to secure past session keys even if private keys are compromised.

Internet Protocol Security (IPsec)

Internet Protocol Security (IPsec) is a secure network protocol suite that authenticates and encrypts the packets of data to provide secure encrypted communication between two computers over an Internet Protocol network. It is used in Virtual Private Networks (VPNs).



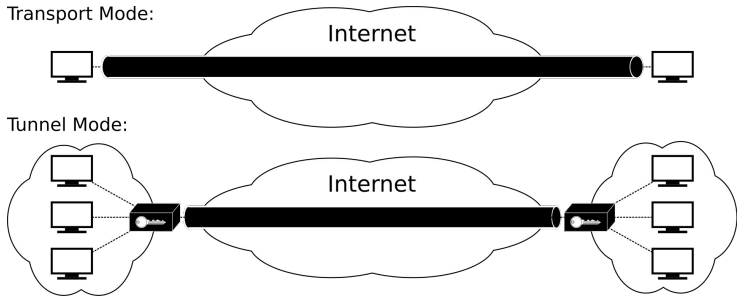
Internet Protocol Security (IPsec)

Transport mode

Only payload of IP packet is encrypted or authenticated, leaving IP header and routing intact.

Tunnel mode

Entire IP packet is encrypted and authenticated, and encapsulated into a new IP packet with a new header. Used for virtual private networks in various communication scenarios.

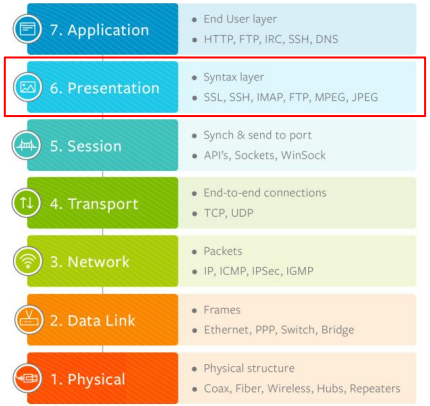


Internet Protocol Security (IPsec)

- Internet Key Exchange (IKE)
    - key management protocol for IPsec that negotiates and establishes Security Associations (SA) between communicating peers, allowing secure key exchange using Diffie-Hellman algorithm.
- Supports IPv4 and IPv6

Secure Shell (SSH)

- A cryptographic network protocol used for secure remote access, administration, and communication between devices over an unsecured network.
- Encrypted connection
- Authentication
    - SSH supports multiple authentication methods, including password-based, public key, and multi-factor authentication for enhanced security.
- Port 22 by default

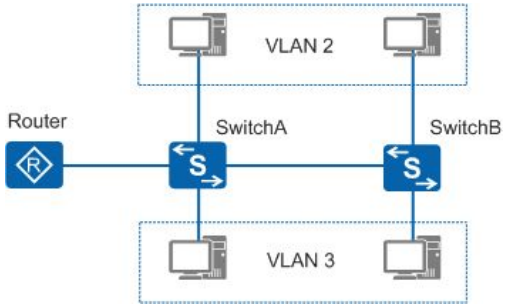


Secure Shell (SSH)

- CLI
  - SSH primarily allows users to access remote systems via a command-line interface, executing commands and managing files.
- Secure file transfer
  - SSH enables secure file transfer through protocols like SCP (Secure Copy Protocol) and SFTP (SSH File Transfer Protocol), providing encrypted alternatives to FTP.
- Tunneling
  - SSH can create encrypted tunnels for forwarding arbitrary network connections, enabling secure access to services or remote network resources.

Virtual Local Area Network (VLAN)

- A logical subdivision of a physical network, allowing devices to be grouped based on their function or department, rather than physical location.
- Layer 2 technology
  - VLAN operates at the data link layer (Layer 2) of the OSI model, using Ethernet switches to manage and segregate traffic.
- VLAN Tagging
  - VLAN membership is assigned by tagging Ethernet frames with a unique VLAN ID (802.1Q standard), enabling switches to identify and forward traffic to the correct VLAN.

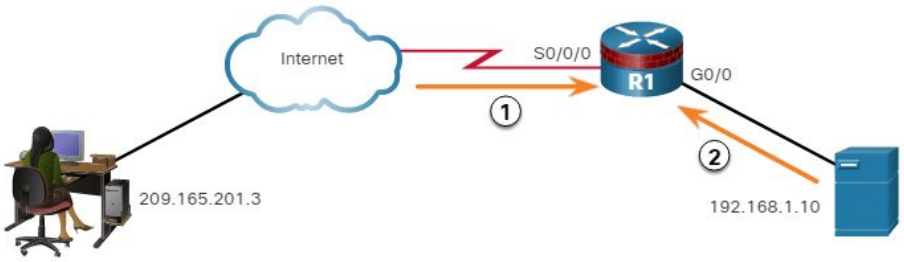


Virtual Local Area Network (VLAN)

- Improved security
  - VLANs separate network traffic, limiting broadcast domains, and reducing the risk of unauthorized access or eavesdropping.
- Simplified management
  - Network administrators can reconfigure VLAN membership remotely, without needing to physically move devices or cables.
- Enhanced performance
  - By segregating traffic, VLANs reduce network congestion, minimize broadcast traffic, and improve overall network performance.
- Scalability
  - VLANs enable easy expansion of network infrastructure and adaptability to changing organizational needs.

Access Control Lists (ACLs) & Firewalls

Access Control Lists (ACLs) and packet filtering are technologies that contribute to an evolving set of network security protections.



1. Rules on R1 for ICMP traffic from the Internet

```
access-list 112 permit icmp any any echo-reply
access-list 112 permit icmp any any source-quench
access-list 112 permit icmp any any unreachable
access-list 112 deny icmp any any
access-list 112 permit ip any any
```

2. Rules on R1 for ICMP traffic from inside the network

```
access-list 114 permit icmp 192.168.1.0 0.0.0.255 any echo
access-list 114 permit icmp 192.168.1.0 0.0.0.255 any parameter-problem
access-list 114 permit icmp 192.168.1.0 0.0.0.255 any packet-too-big
access-list 114 permit icmp 192.168.1.0 0.0.0.255 any source-quench
access-list 114 deny icmp any any
access-list 114 permit ip any any
```

Access Control Lists (ACLs)

ACLs specify permissions for accessing resources, devices, or services.

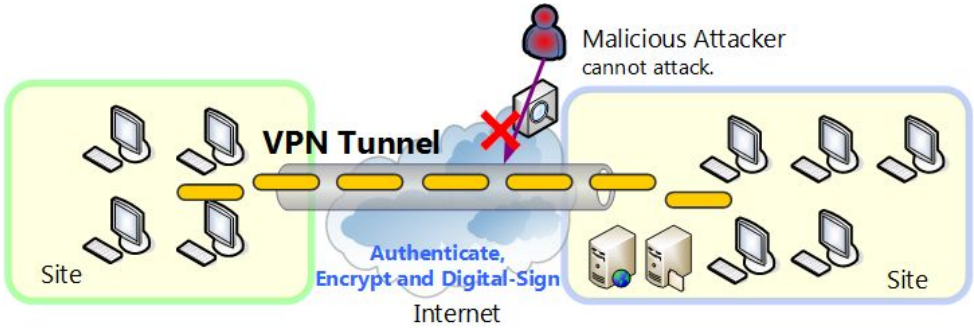
- Vulnerabilities
  - Attackers can discover allowed IP addresses, protocols, and ports through port scanning, penetration testing, or other reconnaissance methods.
  - Attackers can use spoofed source IP addresses in packets.
  - Applications can use arbitrary ports and manipulate protocol traffic, making rule-based security measures inadequate.
- Countermeasures
  - more advanced behavior and context-based security measures are required.
  - Next-Generation Firewalls, Advanced Malware Protection, and content appliances are designed to overcome the limitations of rule-based security measures.

Encryption

- part of VPN technologies. In VPNs, IP is used to carry encrypted traffic.
- The encrypted traffic essentially establishes a virtual point-to-point connection between networks over public facilities.
- makes the traffic unreadable to any other devices but the VPN endpoints.
- Malware can establish an encrypted tunnel that rides on a common and trusted protocol, and use it to exfiltrate data from the network.
- can present challenges to security monitoring by making packet details unreadable.

Virtual Private Network (VPN) and Tunneling

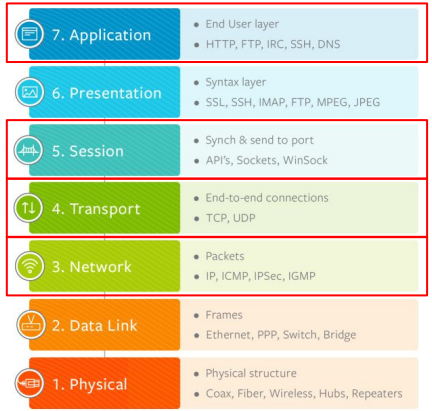
- VPNs create a secure, encrypted connection between a user and a private network over the internet.
- VPNs use tunneling protocols to encapsulate and encrypt data packets as they traverse the internet, protecting them from interception and manipulation.



- Tunneling involves the encapsulation of one network protocol within another to create a secure virtual connection between two endpoints.

Firewalls

- Packet filtering stateless
- Stateful firewalls
- Application gateway firewall (proxy firewall)
- Next Generation Firewall (NGFW)



Firewalls

Packet filtering stateless

- Packet Filtering firewalls are part of a router firewall, which permits or denies traffic based on Layer 3 and Layer 4 information.
- They are stateless firewalls that use a simple policy table look-up that filters traffic based on specific criteria.

Stateful firewall

- Stateful firewalls are the most versatile and the most common firewall technologies in use.
- These firewalls provide stateful packet filtering by using connection information maintained in a state table

Firewalls

Application gateway firewall (aka. application-level gateway (ALG) or proxy firewall)

- Application gateway firewall filters information at Layers 3, 4, 5, and 7 of the OSI reference model. Most of the firewall control and filtering is done in the software.

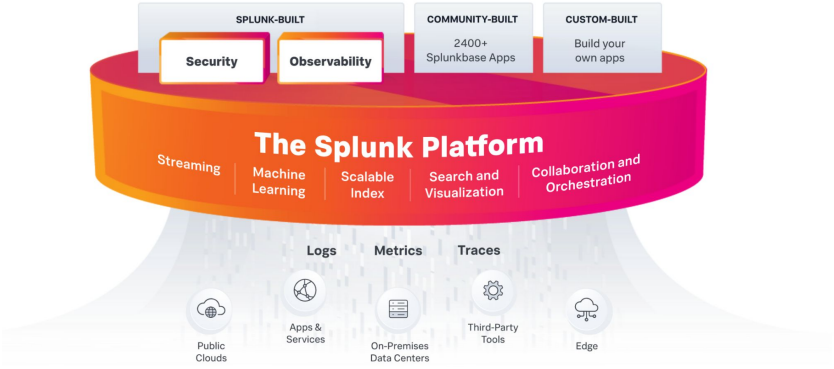
Next Generation Firewall (NGFW)

- NGFW go beyond stateful firewalls by providing:
  - intrusion prevention
  - deep packet inspection
  - application-awareness
  - threat intelligence
- enhanced visibility, control, and protection against sophisticated and evolving cyber threats.

Security Information and Event Management (SIEM)

SIEM is a cybersecurity solution that aggregates, correlates, and analyzes security events and data from **multiple sources** to identify and respond to potential security threats **in real-time**.

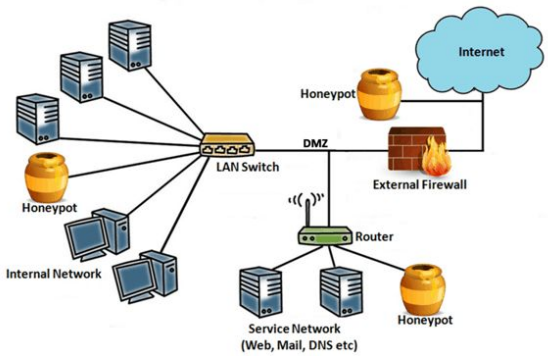
Figure: Splunk Enterprise Security, Threat Hunting dashboard



- Splunk is the leading vendor in the SIEM market, with a significant market share and a large user base worldwide.
- data analytics and visualization tool used for searching, monitoring, and analyzing machine-generated data.
- collects and indexes data from various sources, such as logs, sensors, and events, **in real-time**.
- offers advanced analytics capabilities, such as **machine learning** and **predictive analytics**, to help organizations gain insights and make informed decisions.
- Overview of Splunk Enterprise Security

Other network based security technologies

- Network based malware protection
  - Network-based malware prevention devices are capable of sharing information among themselves to make better informed decisions.
- IDS/IPS
  - IDS: Intrusion Detection System ➔ IDS detects and reports
  - IPS: Intrusion Prevention System ➔ IPS detects and reacts
- Honeypot
  - "Setting a trap for hackers"
  - Hacker wastes time on useless device
  - If properly configured with fake information ➔ confusion
  - Discover the methodology of the hacker
  - Also used to detect spam



end