Sec+ 501 Get Certified Topic 3 - Networking

21 TCP	FTP	File Transfer Protocol is used to transfer files from host to host
22 TCP/UDP	SSH, SCP, SFTP	Secure Shell is used to remotely administer network devices and systems. SCP is used for secure copy and SFTP for secure FTP.
23 TCP/UDP	Telnet	Unencrypted method to remotely administer network devices (should not be used)
25 TCP	SMTP	Simple Mail Transfer Protocol is used to send email over the Internet
53 TCP/UDP	DNS	Domain Name Service is used to resolve hostnames to IPs and IPs to hostnames
69 UDP	TFTP	Trivial FTP is used as a simplified version of FTP to put a file on a remote host, or get a file from a remote host
80 TCP	HTTP	Hyper Text Transfer Protocol is used to transmit web page data to a client for unsecured web browsing
88 TCP/UDP	Kerberos	Used for network authentication using a system of tickets within a Windows domain
110 TCP	POP3	Post Office Protocol v3 is used to receive email from a mail server
119 TCP	NNTP	Network News Transfer Protocol is used to transport Usenet articles
135 TCP/UDP	RPC/DCOM-scm	Remote Procedure Call is used to located DCOM ports request a service from a program on another computer on the network
137-139 TCP/UDP	NetBIOS	NetBIOS is used to conduct name querying, sending of data, and other functions over a NetBIOS connection
143 TCP	IMAP	Internet Message Access Protocol is used to receive email from a mail server with more features than POP3
161 UDP	SNMP	Simple Network Management Protocol is used to remotely monitor network devices
162 TCP/UDP	SNMPTRAP	Used to send Trap and InformRequests to the SNMP Manager on a network
389 TCP/UDP	LDAP	Lightweight Directory Access Protocol is used to maintain directories of users and other objects
443 TCP	HTTPS	Hyper Text Transfer Protocol Secure is used to transmit web page data to a client over an SSL/TLS-encrypted connection
445 TCP	SMB	Server Message Block is used to provide shared access to files and other resources on a network
465/587 TCP	SMTP with SSL/TLS	Simple Mail Transfer Protocol used to send email over the Internet with an SSL and TLS secured connection
514 UDP	Syslog	Syslog is used to conduct computer message logging, especially for routers and firewall logs
636 TCP/UDP	LDAP SSL/TLS	LDAP is used to maintain directories of users and other objects over an encrypted SSL/TLS connection
860 TCP	iSCSI	iSCSI is used for linking data storage facilities over IP
989/990 TCP	FTPS	File Transfer Protocol Secure is used to transfer files from host to host over an encrypted connection
993 TCP	IMAP4 with SSL/TLS	Internet Message Access Protocol is used to receive email from a mail server over an SSL/TLS-encrypted connection
995 TCP	POP3 (SSL/TLS)	Post Office Protocol v3 is used to receive email from a mail server using an SSL/TLS-encrypted connection
1433 TCP	Ms-sql-s	Microsoft SQL server is used to receive SQL database queries from clients
1645/1646 UDP	RADIUS (alternative)	Remote Authentication Dial-In User Service is used for authentication and authorization (1645) and accounting (1646)
1701 UDP	L2TP	Layer 2 Tunnel Protocol is used as an underlying VPN protocol but has no inherent security
1723 TCP/UDP	PPTP	Point-to-Point Tunneling Protocol is an underlying VPN protocol with built-in security
1812/1813 UDP	RADIUS	Remote Authentication Dial-In User Service is used for authentication and authorization (1812) and accounting (1813)
3225 TCP/UDP	FCIP	Fibre Channel IP is used to encapsulate Fibre Channel frames within TCP/IP packets
3260 TCP	iSCSI Target	iSCSI Target is as the listening port for iSCSI-targeted devices when linking data storage facilities over IP
3389 TCP/UDP	RDP	Remote Desktop Protocol is used to remotely view and control other Windows systems via a Graphical User Interface
3868 TCP	Diameter	A more advanced AAA protocol that is a replacement for RADIUS
6514 TCP	Syslog over TLS	It is used to conduct computer message logging, especially for routers and firewall logs, over a TLS-encrypted connection

CH 3 – EXPLORING NETWORK TECHNOLOGIES AND TOOLS

- ICMP – Internet Control Message Protocol
  - Testing basic connectivity and includes tools such as ping, pathping and tracert.
  - Many DOS attacks use ICMP which is why we disable it usually in firewalls to disable ping responses.
- ARP – Address Resolution Protocol
  - IPv4 addresses to MACS. ARP poisoning falsifies ARP packets to give clients false hardware updates as well as to redirect and interrupt network traffic.
- RTP – Real Time Transport Protocol
  - Delivers audio and Video over IP Networks
- SRTP – Secure Real Time Transport Protocol
  - Provides encryption, message authentication and integrity for RTP.
  - Protects against Confidentiality of data and replay attacks
- VOIP – Voice over Internet Protocol
  - Communications, streaming media, video teleconferencing applications, push to talk features.
- FTP – File Transfer Protocol port 21. SFTP(Encrypted) Port 22
- TFTP – Trivial File Transfer Protocol uses UDP port 69. Transfer smaller amounts of data such as when communicating with network devices.
- FTPS (File Transfer Protocol Secure)– port 989/990
- IPSEC - A TCP/IP protocol that authenticates and encrypts IP packets and effectively securing communications between computers and devices
  - provides confidentiality (encryption), integrity (hashing), and authentication (key exchange)
- STARTTLS – Command to upgrade unencrypted connection to an encrypted connection on same port.
- TLS – Replacement for SSL
- SSL – Secure Socket Layer Protocol – secure HTTP traffic as HTTPS
  - Not secure and is not recommended for use as it has vulnerabilities. Use TLS instead.
- SSH – Port 22

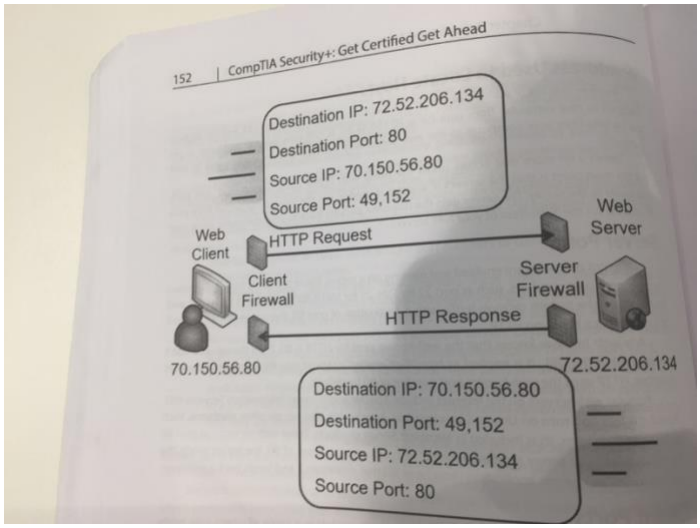
- **Remember: SSH encrypts over TCP port 22. TLS is a replacement for SSL and is used to encrypt many different protocols. SFTP uses SSH to encrypt traffic. FTPS uses TLS to encrypted traffic.**

EMAIL WEB USE CASES

- SMTP – Simple Mail Transfer Protocol
  - Port 25
  - Port 465 w/ SSL and port 587 with TLS.
  - Recommended to use 'STARTTLS' command to create a secure connection
- POP3/Secure POP – Post Office Protocol v3 (POP3) transfers emails from servers down to clients.
  - Uses TCP port 110 w/ STARTTLS
  - POP3 TLS/SSl or secure pop3 is used on port 995
- IMAP/ Secure IMAP
  - Used to store email on am email server and organise and manage email in folders on server.
  - Uses TCP port 143
  - Port 993 with SSL and TLS for encrypted w/ StartTLS
- HTTP – Hypertext Transfer protocol
  - Transmits web traffic on internet and intranets
  - Port 80 for HTTPS, 443 for HTTPS
- **Remember this:**
  - **SMTP sends email on TCP port 24, POP3 receives email on port 110, IMAP4 on storage of email on email server on port 143. STARTTLS allows an encrypted version of protocol to use same port of unencrypted version. HTTP/HTTPS are 80 and 443.**
- Kerberos port 88 UDP
- LDAP – Lightweight Directory Access Protocol
  - Communicates with directories
  - TCP port 389. For encrypted TLS use TCP port 636.
- RDP – Remote Desktop Protocol
  - Port 3389
- **Remember this:**

    - **Administrators connect to servers remotely using protocols such as SSH and RDP. In some cases, administrators use VPN's to connect to remote systems**
- NTP – Network Time protocol
    - Commonly used protocol for time synchronization
- DHCP – Dynamic Host Configuration Protocol
    - Dynamically assigns IP addresses to hosts and other TCP/IP information such as subnet masks, default gateways etc.
- IPv4 – 32 bit IP addresses in dot format w/ four decimals. (192.168.1.5)
- IPv6: 128-bit IP addresses in hexadecimal format. Are unique local addresses
    - FE80:0000:0000:0000:02d4:3ff7:003f:de62
- Class A
    - 10.0.0.0 to 10.255.255.255
- Class B
    - 172.16.0.0 to 172.31.0.0
- Class C
    - 192.168.0.0 to 192.168.255.25
- Remember this: Private networks should only have private IP addresses.
- DNS: Domain Name System for Domain Name resolution
    - DNS Client → (Can you give me IP address of google.com?) → DNS Server
    - DNS Server→ (IP 72.45.301.22) → Back to DNS Client
- DNS Cache Poisoning/ DNS Poisoning: Attacker modifies DNS cache with bogus IP address to redirect you from the website you want to go to to a malicious website.
    - To counter use DNSSEC- DNSSecure which provides validation for DNS responses by adding digital signature to each record that provides data integrity.
- DNS host data in zones. Zones include multiple records:
    - A – host record. Holds host name and IPv4 address and is commonly used record in DNS server.
    - AAAAA – host record for IPv6
    - PTR- Pointer Record

        - Opposite of A record. DNS client queries DNS with IP address instead of DNS client querying DNS with name.
    - MX – Mail Exchange
        - Identifies mail server used for email
    - CNAME – Canonical Name/ Alias
        - Allows single system to have multiple IP's
    - SOA – Start of Authority
        - SOA record includes info about DNS zones and settings include TTL (Time to Live). TTL is used to determine how long to cache results and is usually in seconds.
    - Most DNS servers run BIND (Berkeley Internet Name Domain) Software on Unix/Linux Servers.
- **Remember this:**
    - **DNS zones include records such as A records for IPv4 addresses and AAAA records for IPv6 addresses. DNS uses TCP port 53 for zones transfers and UDP port 53 for DNS client queries. Most Internet-based DNS servers run BIND software on Unix or Linux servers, and its common to configure DNS servers to only use secure zone transfers. DNSSEC helps prevents DNS poisoning attacks. NSlookup and dig are two cmd tools used to test DNS.**
- Ports – Logical numbers used by TCP/IP to identify what service or application should handle data received by system.
- Ports can be any number between 0 and 65,535
- Well-Known Ports
    - Ports 0 to 1023 are considered well-known and are assigned by the Internet Assigned Numbers Authority (IANA)
- Registered Ports
    - Ports 1024 to 49,151 are considered registered and are usually assigned to proprietary protocols
- Dynamic &Private Ports
    - Ports 49,152 to 65,535 can be used by any application without being registered with IANA



- Ports and protocols are not the same thing. Protocol analysers capture and examine IP headers to determine protocol number and port as well as read unencrypted data.

UNDERSTANDING BASIC NETWORK DEVICES

- Unicast: One to one Traffic.
  - One host sends traffic to another host, using a destination IP address.
- Broadcast: One to all Traffic.
  - One hosts sends traffic to all other hosts on the subnet using a broad address such as 255.255.255.255.
- Switch: Can learn which computers are attached to each of its physical ports. Then creates internal switched connections when two computers communicate with each other.
  - Reduces risk of an attacker capturing data with a protocol analyser. Switches also increase the efficiency of a network.
- **Remember this:**
  - **Port security: Includes disabling unused ports and limiting the number of MAC addresses per port. A more advanced implementation is to restrict each physical port to only a single specific MAC address. Switch remembers the first one/two MAC addresses that connect to a port. It then blocks access to systems using any other MAC addresses. Can also configure each port to accept traffic only from a specific MAC address.**

- Physical security of a switch such as keeping it in a secure area ensures attackers don't have physical access to switch or other network devices.
- In some situations, a network can develop a switching loop or bridge loop problem. Switch continuously sends and resends unicast transmissions through the switch. STP and RSTP is necessary to protect against switching loop problems such as those caused when 2 ports of a switch are connected together.
    - For loop prevention use:
        - STP -Spanning Tree Protocol
        - RSTP – Rapid Spanning Tree protocol
- MAC Flood Attack – attempts to overload switch with different MAC addresses associated with each physical port.
    - Attacker sends large amount of traffic with spoofed MAC addresses to the same port.
    - Switches can fail-open when flooded and begin to act like a hub where traffic is sent to any port of the switch and attacker can connect to a protocol analyser to any port and collect all traffic sent through switch.
- Flood Guard – Protects against MAC flood attacks.
    - When used, switch will limit amount of memory used to store MAC addresses for each port.
    - Sends a SNMP (Simple Network Management Protocol) trap or error message in response to alert. Can also disable port.
- Physical Port – Plug in
- Logical Port – Number embedded in a packet and identifies services and protocols
- Router – connects multiple network segments together in to a single network and routes traffic between segment. Routes traffic from segment to segment.
    - Works at Layer 3 OSI Model (Network)
- ACL – Access Control List.
    - Rules implemented on a router and firewall to identify what traffic is allowed and denied.
    - Provide basic packet filtering on:
        - IP Addresses and networks

        - Ports
        - Protocol Numbers
            - E.G: ICMP, PPTP, IpSEC etc.
- Implicit Deny – All traffic that isn't explicitly allowed is implicitly denied. Last rule of ACL.
    - E.G: Deny TCP any any port any, DENY ANY ANY, DENY ALL ALL
- Explicit Allow
    - Traffic is allowed to enter or leave the network because there is an ACL rule that specifically allows it
    - Example: allow TCP 10.0.0.2 any port 80
- Explicit Deny
    - Traffic is denied the ability to enter or leave the network because there is an ACL rule that specifically denies it
    - Example: deny TCP any any port 23
- Spoofing – Impersonating to be something/someone else
- Antispoofing- Can implement antispoofing on router by modifying access list to block private IP addresses
    - Deny ip 10.0.0.0.0.255.255.255 any
    - Deny ip 172.16.0.0.0.15.255.255 any
- **Remember this:**
    - **Routers and stateless firewalls (packet filtering firewalls) perform basic filtering with an ACL. ACL identify what traffic is allowed and what traffic is blocked. An ACL can control traffic based on networks, subnets, IP addresses, ports, and some protocols. Implicit deny blocks all access that has not been explicitly granted. Routers and firewalls use implicit deny as last rule in ACL. Antispoofing methods block traffic using ACL rules.**
- Bridge – Network bridge connects multiple networks together and can be used as a router in some situations.
    - Directs Traffic based on destination MAC.
- Aggregation Switch – Connects multiple switches together in an network.
- **Remember this:**

    - **Host-based firewalls provide protection for individual hosts, such as servers and workstations. A host based firewall provides intrusion protection for the host. Linux systems support xtables for firewall capabilities. Network based firewalls are often dedicated servers or appliances and provide protection for network.**
- Application Firewall – Software running on system.
- Network based firewall – Dedicated system with additional software installed to monitor, filter and log traffic through NICS (Network Interface Cards). All traffic goes through firewall.
- Stateless firewall rules – Rules implemented as ACLs to identify allowed and blocked traffic.
    - Permission – PERMIT/ ALLOW, DENY
    - Protocol – UDP, TCP
    - Source – Source IP address
    - Destination – Destination IP address
    - Port or protocols
- Remember this: Firewalls use a deny any any, deny any, or drop all statement at end of ACL to enforce an implicit deny strategy. Statement forces firewall to block any traffic that wasn't previously allowed in the ACL.
- Stateful Firewall – Inspects traffic and makes decision based on context/state of traffic
    - Problem with stateful firewall: Misconfigured ACLs
- WAF – Web application firewall
    - Designed to protect web application usually on a web server. Provides additional layer of protection for web application
- **Remember this:**
    - **A stateless firewall blocks traffic using an ACL. A stateful firewall blocks traffic based on the state of the packet within a session. Web application firewalls provide strong protection for web servers. Protect against several different types of attacks, with a focus on web application attacks and can include load balancing features**
- Intranet – Internal network
    - Used to communicate and share content with each other

    - Only used with one company involved.
- Extranet – Part of network that can be accessed by authorized entities from outside network.
    - Specialized type of DMZ that is created for your partner organizations to access over a wide area network
    - E.G: Authorized business partners/ vendors
- **Remember this: DMZ – Demilitarized Zone**
    - **Buffered zone between private network and internet. Allows access to services while segmenting access to internal network. Internet clients can access services hosted on services in DMZ, but DMZ provides layer of protection for intranet (internal network)**
- Network Address Translation(NAT) – Not compatible with IPSec
    - Process of changing an IP address while it transits across a router
    - Using NAT can help us hide our network IPs from internet
    - Static Nat – uses single public IP address in one-to-one mapping. Maps private IP address with a single public IP address.
    - Dynamic NAT – Uses multiple public IP addresses in a one-to-many mapping. Decides which public IP address to use based on load.
- Port Address Translation(PAT)
    - Router keeps track of requests from internal hosts by assigning them random high number ports for each request
- **Remember this:**
    - **NAT translates public IP addresses to private IP addresses, and private IP addresses back to public. A common form of NAT is Port Address Translation. Dynamic NAT uses multiple public IP addresses while static NAT uses a single public IP Address.**
- Airgap – Metaphor for physical isolation. Ensures network isn't connected to any other network.
    - E.G: SCADA Systems in powerplants are separated from internet and networks so attackers can't access internal computers.

- Remember this:
    - VLANS (Virtual Local Area Networks) separate or segment traffic on physical networks and can create multiple VLANs with a single Layer 3 switch. A VLAN can logically group several different computers together, or logically separate computers, without regard to their physical location. VLANs are also used to separate traffic types, such as voice traffic on VLAN and data traffic on a separate VLAN.
- Media Gateway – Device that converts data from format used on one network to format used on another network.
    - E.G: VOIP gateway converts telephony traffic between traditional phone lines and an IP based network.
- **Remember this:**
    - **A proxy server forwards requests for services from a client. It provides caching to improve performance and reduce Internet bandwidth usage. Transparent proxy servers use URL filters to restrict access to certain sites, and can log user activity. Proxy servers can also include logs that record each site visited by users.**
- Transparent proxy – Accept and forward requests without modifying them.
- Non-Transparent Proxy – Can modify and filter requests.
    - Used to restrict what users can access with URL filters such as gambling, social sites.
- Reverse proxy – Accepts requests from internet, typically for a single web server.
- Application proxy – proxy for specific applications.
- **Remember this:**
    - **UTM – Unified threat Management**
        - **UTM combines multiple security controls into a single appliance. Can inspect data streams and often include URL filtering, malware inspection, content inspection. Most UTM's include DDOS mitigators.**
- Mail Gateway – Server that examines all incoming and outgoing emails and attempts to reduce risks associated with email. Often includes DLP and supports encryption.

SUMMARIZING ROUTING AND SWITCHING USE CASES

- Prevent Switching Loops – Implement STP or RTP on switches
- Block flood attacks – Use Floor Guards
- Prevent unauthorized users from connecting to unused ports
- Provide increased segmentation of user computers – VLANS
- Prevent IP address spoofing – Antispoofing through implementation of rules of ACLs
- Provide secure management of routers – SNMPv3 is used to securely manage network devices such as routers.
- SNMPV3 uses UDP port 161. V3 more secure than V1/2. Simple Network Management Protocol monitors and manages network devices such as routers or switches.
- Remember this:
    - Admins use SNMPv3 to manage and monitor network devices and SNMP uses UDP ports 161 and 162. It includes strong authentication mechanisms and is more secure than earlier versions.