TACACS+ used for authentication

Fire extinguisher

pre-action → system minimizes the risk of accidental release from a wet pipe system. With pre-action system, both a detector actuation like a smoke detector and sprinkler must be tripped prior to water being released.

wet pipe → most basic type of fire supression system, and is involved using sprinkler system and pipe that always contain water.

clean Agent system → use halocarbon agent or inert gas.

HVAC → Heating ventilation Air conditioning

802.11g - 5GHz
802.11g - 2.4 GHz

- { time domain reflectors } used to determine the characteristics of electrical lines by observing reflected waveforms to characterize and locate fault in copper cables

Attack

- { Ransomeware } is a type of malware from cryptovirology that threatens to publish the victims personal data or block access to it unless a ransom is paid

- { malware } is any software intentionally designed to cause damage to computers, servers, client, or computer network.
malware includes worms, viruses logic bombs and many other malicious types of code.

- { phishing } is a types of social engineering where an attacker sends a fraudulent email designed to trick a human victim into revealing sensitive data

- { Brute-force attack } consists of an attacker submitting many passwords or passphrases with hope of eventually guessing correctly

baseline - A
of regular
network

baseline → A process for studying the network at regular intervals to ensure that the network is working as desired.

historical data

IEEE

IEEE - 802.1X - Network authentication protocol used to authenticate user to use network which is verified by RADIUS server.

LACP → IEEE 802.3ad
PoE → 802.3af

→ spectrum analyzer → measure ~~Input of~~ magnitude of input signal's frequency
→ wifi analyzer → used to gather information about available wireless networks, troubleshoot networking issue
→ tone generator → used with tone probe to accurately identify the location of cable pair or conductor within wiring bundle cross connection point, or at the remote end.

* ARP ~~spoofing~~ → Address Resolution protocol connects IP address to mac address

* ARP spoofing → malicious actor falsified ARP over LAN. This results in the linking of an attackers MAC address with IP address of legitimate computer servers

* Evil Twin → rouge wireless access point that masquerades as a legitimate wifi access point.

* patch → is designed to fix known vulnerability.

* severity level (0 - 7)

0 - most severe (system unusable)
1 - Alert condition (Alert most Address)
2 - critical condition (cause immediate action)
3 - Error condition (not proper functioning)
4 - warning condition (an error will occur)
5 - Notice condition
6 - Information condition
7 - debugging condition

SDN Layers

Application layer -) focus on communicating resource requests or information about the network

control layer -) uses information from the application to decide how to route data ~~traffic~~ (packet on network and decide about how traffic should prioritized, secure, where to forward.

Infrastructure -) contains the physical networking devices that receive information from the control layer where to move the data then perform those movements

management plane -) used to monitor traffic condition, the status of the network.

Network troubleshoot methodology for

1. Determine the cause by testing or theory
2. Identify the problem
3. establish theory of probable cause
4. Test theory to determine the cause
5. establish a plan of action to resolve the problem and identify potential effects
6. Implement the solution or escalate as necessary
7. Verify full system functionality and if applicable prevent measure
8. Document finding, action, outcomes and lesson learned