Name:_____ Class number: _____
Section:_____Schedule:_____ Date: _____

Lesson Title: The LAN Security

Lesson Objectives:

At the end of this module, you should be able to:

1. Describe common LAN security attacks.
2. Explain how to use security best practices to mitigate LAN attacks

Materials:
SAS

References:
https://www.cisco.com/c/en/us/index.html
https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/98628-zone-design-guide.html

A. LESSON PREVIEW/REVIEW

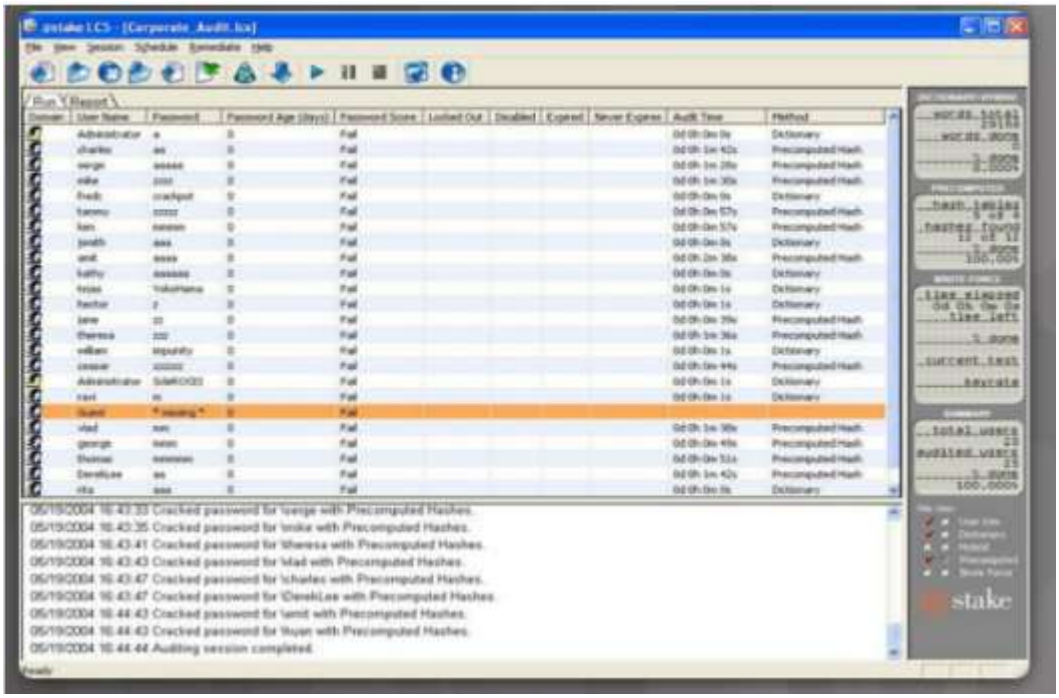
Introduction (2 mins)

Local network security is one of the primary concerns of systems administration and maintenance. Unfortunately, it is also one of the most overlooked. This module will elaborate some precautions in protecting your local network from threats and security issues.

B. MAIN LESSON

Content Notes (13 mins)

LAN Security Attacks: Telnet Attacks



There are two types of Telnet attacks:

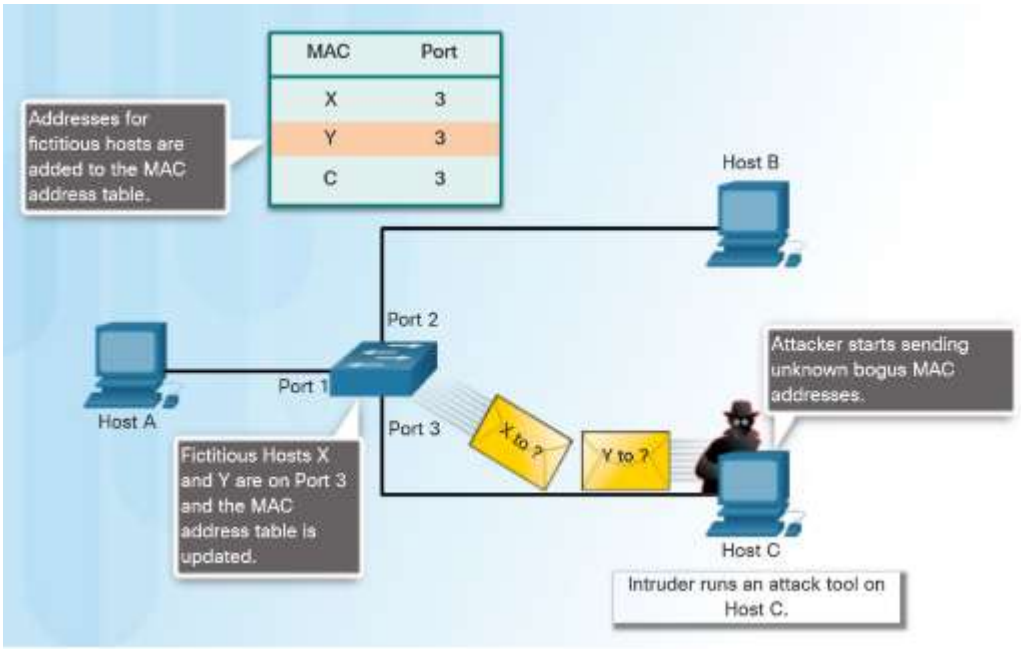
1. Brute Force Password Attack - trial-and-error method used to obtain the administrative password.
2. Telnet DoS Attack – Attacker continuously requests Telnet connections in an attempt to render the Telnet service unavailable.

Name:_____ Class number: _____
Section:_____Schedule:_____ Date: _____

To mitigate these attacks:

1. Use SSH
2. Use strong passwords that are changed frequently.
3. Limit access to the vty lines using an access control list (ACL)
4. Use AAA with either TACACS+ or RADIUS protocols.

LAN Security Attacks: MAC Address Table Flooding Attack



Common LAN switch attack is the MAC address table flooding attack.

1. An attacker sends fake source MAC addresses until the switch MAC address table is full and the switch is overwhelmed.
2. Switch is then in fail-open mode and broadcasts all frames, allowing the attacker to capture those frames.

Configure port security to mitigate these attacks.

LAN Security Attacks: DHCP Attacks

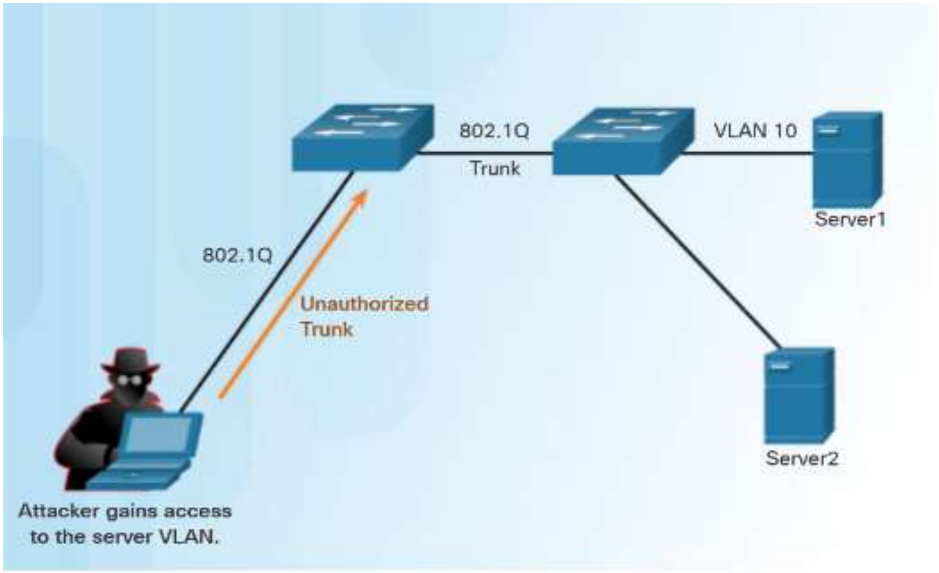
1. **DHCP spoofing attack** - An attacker configures a fake DHCP server on the network to issue IP addresses to clients.
2. **DHCP starvation attack** - An attacker floods the DHCP server with bogus DHCP requests and leases all of the available IP addresses. This results in a denial-of-service (DoS) attack as new clients cannot obtain an IP address.

Methods to mitigate DHCP attacks:

1. Configure DHCP snooping
2. Configure port security

Name:_____ Class number: _____
Section:_____Schedule:_____ Date: _____

LAN Security Attacks: VLAN Attacks



Switch spoofing attack - an example of a VLAN attack. Attacker can gain VLAN access by configuring a host to spoof a switch and use the 802.1Q trunking protocol and DTP to trunk with the connecting switch.

Methods to mitigate VLAN attacks:

1. Explicitly configure access links.
2. Disable auto trunking.
3. Manually enable trunk links.
4. Disable unused ports, make them access ports, and assign to a black hole VLAN.
5. Change the default native VLAN.
6. Implement port security.

LAN Security Best Practices

1. **Secure the LAN**
   a. Always use secure variants of protocols such as SSH, SCP, and SSL.
   b. Use strong passwords and change often.
   c. Enable CDP on select ports only.
   d. Secure Telnet access.
   e. Use a dedicated management VLAN
   f. Use ACLs to filter unwanted access.
2. **Mitigate MAC Address Flooding Table Attacks**
   a. Enable port security to prevent MAC table flooding attacks.
   b. Port security allows an administrator to do the following:
      - statically specify MAC addresses for a port.
      - permit the switch to dynamically learn a limited number of MAC addresses.
      - when the maximum number of MAC addresses is reached, any additional attempts to connect by unknown MAC addresses will generate a security violation.

Name:_____ Class number: _____
Section:_____Schedule:_____ Date: _____

3. **Mitigate VLAN Attacks**
   a. Disable DTP (auto trunking) negotiations on non-trunk ports and use switchport mode access.
   b. Manually enable trunk links using switchport mode trunk.
   c. Disable DTP (auto trunking) negotiations on trunking and non- trunking ports using switchport nonegotiate.
   d. Change the native VLAN from VLAN 1.
   e. Disable unused ports and assign them to an unused VLAN.
4. **Mitigate DHCP Attacks**
   a. With DHCP snooping enabled on an interface, the switch will deny packets containing:
      - Unauthorized DHCP server messages coming from an untrusted port.
      - Unauthorized DHCP client messages not adhering to the DHCP Snooping Binding Database or rate limits.
   b. DHCP snooping recognizes two types of ports:
      - Trusted DHCP ports - Only ports connecting to upstream DHCP servers should be trusted.
      - Untrusted ports - These ports connect to hosts that should not be providing DHCP server messages.
5. **Secure Administrative Access using AAA**
   a. Local AAA Authentication
      - Client establishes a connection with the router.
      - AAA router prompts the user for username and password.
      - Router authenticates the username and password using the local database, and allows user access.
   b. Server-Based AAA Authentication
      - Client establishes a connection with the router.
      - AAA router prompts the user for a username and password.
      - The router authenticates the username and password using a remote AAA server.

   The AAA router uses Terminal Access Controller Access Control System (TACACS+) or Remote Authentication Dial-In User Service (RADIUS) protocol to communicate with the AAA server

Name:_____ Class number: _____
Section:_____Schedule:_____ Date: _____

Skill-building Activities (18 mins + 2 mins checking)

Identify the following acronyms:

1. DDoS
2. ACL
3. DHCP
4. VLAN
5. MAC

Check for Understanding (3 mins)

Which of the following are practices in securing your local network? Write **Y** for Yes, and **N** for No.

_____ 1. Using strong and regularly changing passwords
_____ 2. Disabling port security for faster access
_____ 3. Enabling all ports
_____ 4. Using SSH and SSL
_____ 5. Manually enabling trunk lists

C. LESSON WRAP-UP

THINKING ABOUT LEARNING (7 mins)

Tell students to shade the number of the module that they have finished.

You are done with the session! Let's track your progress.

Period 1											Period 2										Period 3									
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

Rate the session for today by encircling the emoji that best captures your experience:

In Love Excited Happy Confused Sad Need Help Frustrated

Reason:

_____
_____
_____

Name:_____ Class number: _____
Section:_____Schedule:_____ Date: _____

KEY TO CORRECTIONS

Answers in Skill Building Activity

1. Distributed Denial of Service
2. Access Control List
3. Dynamic Host Configuration Protocol
4. Virtual Local Area Network
5. Media Access Control