ICT2203/ICT2203X Network Security

2021-2022 Trimester 3

Laboratory 2:
Attacks and Defense of LAN with Switches Part 2

LEARNING OUTCOMES

Upon completion of this laboratory exercise, you should be able to:

- Conduct and defend against double tagging attack
- Conduct and defend against STP attack
- Capture and defend against CDP information leakage

REQUIRED HARDWARE

- 1 x Rack of Cisco network devices
- 1 x Box of Ethernet and console cables
- 3 x Laptops

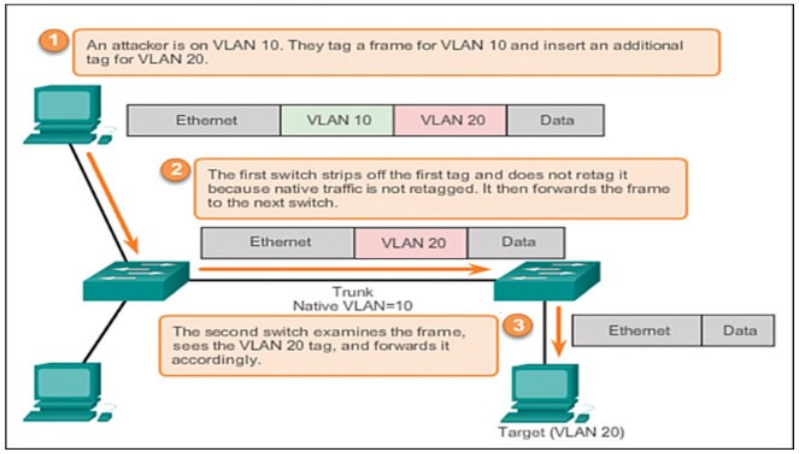
REQUIRED SOFTWARE

- Tera Term 4.106 http://ttssh2.osdn.jp/index.html.en
- Kali Linux Live Boot USB drive

EXERCISE 3: CONDUCT AND DEFEND AGAINST DOUBLE-TAGGING ATTACK

3.1: Conduct Double-Tagging Attack using Yersinia

3.1.1 Setup the network topology as shown:



3.1.2 Configure VLAN 10 for the interface connected to the attacker, and VLAN 20 for the interface connected to the target.

3.1.3 Configure VLAN 10 as the native VLAN for the trunk. An example of the command is shown in Lab 2 Notes pg 10.

3.1.4 Boot up attacker's host in Kali Linux and the others may be in Windows or Kali Linux.

3.1.5 Assign suitable IP addresses to the hosts manually.

3.1.6 Start Wireshark in Kali Linux at attacker's host to get ready to capture the double-tagging frame you are going to send out.

3.1.7 In addition, start Wireshark at target host to get ready to capture the double-tagging frame to be sent by attacker.

3.1.8 When ready, start Yersinia in interactive or graphical mode at the attacker's host.

3.1.9 Select 802.1Q, edit the necessary fields, especially the outer tag to 10 and inner tag to 20 of the double-tagging frame as shown in Lab 2 Notes pg 9, and launch the attack.

3.1.10 Stop the Wireshark at attacker's host. Can you see the double-tagging frame being sent out?

3.1.11 Stop the Wirehsark at the target host. Can you see the double-tagging frame sent by the attacker? Why or why not? Explain.

3.1.12 If you could not capture the double-tagging frame at the target host in 3.1.11, find out the problem and resolve it so that you are able to successfully capture it at the target host.

3.2: Defend against Double-Tagging Attack

3.2.1 Implement defense against double tagging attack as discussed in Lab 2 Notes pg 10.

3.2.2 Which VLAN do you expect the the double tagging frame will go to after your defense?

3.2.3 Modify your network setup in 3.1.1 if necessary to verify what you expect in 3.2.2.

3.2.4 Restart Wireshark in Kali Linux at attacker's host to get ready to capture the double-tagging frame you are going to send out.

3.2.5 Start Wireshark at the host of your modified network setup that you expect to receive the double-tagging frame sent by the attacker.

3.2.6 Launch Yersinia to conduct double tagging attack again.

3.2.7 Stop the Wireshark at attacker's host. Can you see the double-tagging frame being sent out?

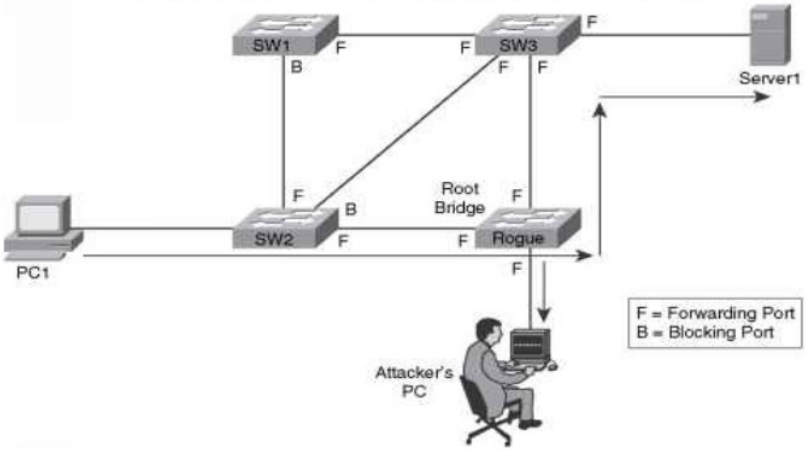
3.2.8 Stop the Wireshark at the host of your modified network. Can you see the double-tagging frame sent by the attacker?

3.2.9 Do you think the recommended defenses are effective against double-tagging attack? Briefly explain.

EXERCISE 4: CONDUCT AND DEFEND AGAINST STP ATTACK

4.1: Conduct STP Attack using Rogue Switch

4.1.1 Setup the network topology as shown, but without the rogue switch initially.



4.1.2 Assign suitable IP addresses to PC1 and Server manually.

4.1.3 Ping Server 1 from PC 1, and vice versa, to ensure your setup is working correctly.

4.1.4 Note the blocking ports of the switches and determine the path taken by the ping packets.

4.1.5 Now connect the rogue switch to the appropriate switches and configure it to take over as root switch.

Note: If you need help, refer to ICT1010 Lec on STP.

4.1.6 Note the changes to the blocking ports of the switches and deduce the new path that will be taken by frames between Server 1 and PC 1.

4.1.7 Connect the attacker's host to the rogue switch.

4.1.8 Configure SPAN (Switch Port Analyzer) on the rogue switch so that frames passing through it will be mirrored to the attacker's host as shown in Lab 2 Notes pg 16.

4.1.9 When done, start Wireshark at the attacker's host.

4.1.10 Ping Server 1 from PC 1 again.

4.1.11 Can the Wireshark at attacker's host capture the ping packets? Why or why not? Explain.

4.2: Defend against STP Attack

4.2.1 Reset the network to the initial setup in 4.1.1 without the rogue switch.

4.2.2 Implement appropriate defenses on the switches as discussed in Lab 2 Notes pg 18-20.

4.2.3 Again connect the rogue switch to the appropriate switches and configure it to take over as root switch.

4.2.4 Observe changes to the interfaces of the switches and briefly explain why.

4.2.5 Do you think the recommended defenses are effective against STP attack? Briefly explain.

EXERCISE 5: CAPTURE AND DEFEND AGAINST CDP INFORMATION LEAKAGE

5.1: Capture CDP Information

5.1.1 Reuse the network topology in 4.1.1.

5.1.2 Restart Wirkshark at attacker's host.

5.1.3 Can the Wireshark capture the CDP frames sent out by the switch similar as that shown in Lab 2 Notes pg 24?

5.1.4 Go through the details of the captured CDP frames to determine potential information useful for the attackers.

5.2: Defend against CDP Information Leakage

5.2.1 Implement defense against CDP information leakage as recommended in Lab 2 Notes pg 25.

5.2.2 When done, restart Wireshark at attacker's host.

5.2.3 Can the Wireshark capture any CDP frame now?

5.2.4 Do you think the recommended defense is effective against CDP information leakage? Briefly explain.