

Lab 2

Secure LAN

ITSC 206: Advanced Networking for Offensive and Defensive Environments

Table of Contents

[Lab Outcomes 4](#_Toc503819985)

[Files/Download 4](#_Toc503819986)

[Reading 4](#_Toc503819987)

[Introduction 4](#_Toc503819988)

[MAC Address Spoofing - Demo 4](#_Toc503819989)

[ARP Address Spoofing (Poisoning) 5](#_Toc503819990)

[VLAN Hopping 6](#_Toc503819991)

[DHCP Starvation 7](#_Toc503819992)

[DHCP Server Spoofing 9](#_Toc503819993)

[STP Spoofing 10](#_Toc503819994)

Lab Outcomes

* Perform network setup and attack against network device.
* Learn how to use multiple tools to perform various network LAN attacks.

Lab Resources (Devices/OS/Files/Download)

* Windows 2012R2 VM – Either from instructor or locally on workstation
  + TFTPD64 software (rename from .txt to .exe) – D2L Student resources
  + TMAC – D2L Student resources
* Kali Linux with Yersinnia
* Cisco Switches (Cisco Catalyst 2960) within SAIT lab

Reading

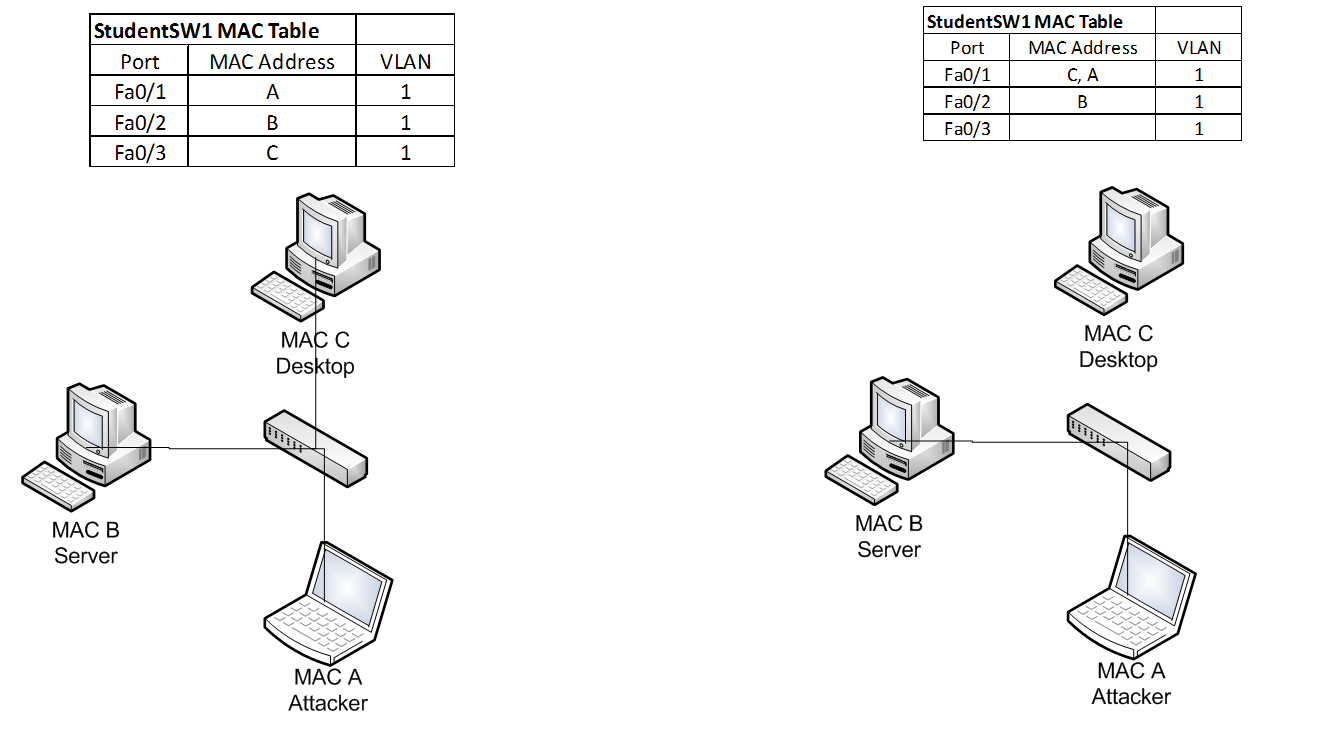
* None

Introduction

This lab gives you practice in basic network attack focused on OSI layer 2 (MAC).

MAC Address Spoofing - Demo

Within Linux (Kali) use macchanger.

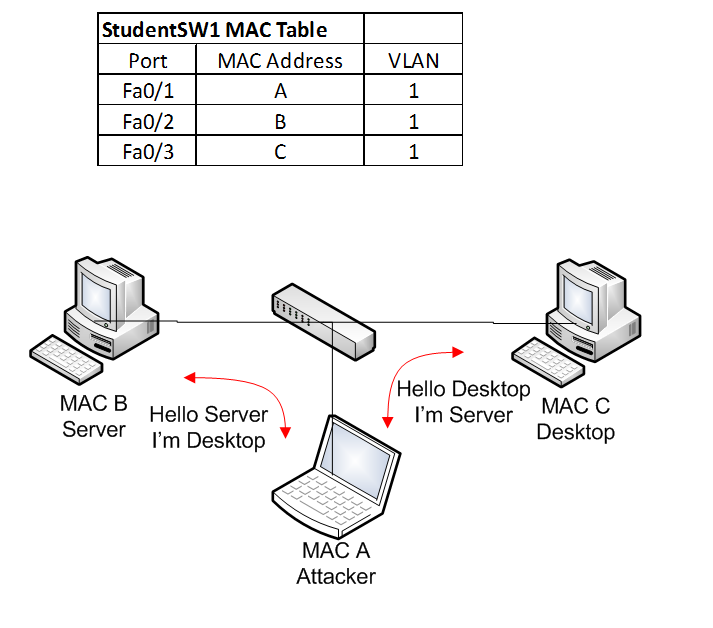


1. Write down initial MAC on the Attacker PC (Kali):\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
2. Execute command: macchanger -m 00:0c:29:1d:dc:58 eth0

Within Windows 10 use TMAC

1. <https://technitium.com/tmac/> - Windows MAC Changer
2. Write down initial MAC on the Win10 PC (Test):\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
3. Install and open TMAC tool
4. Review http://blog.technitium.com/2011/05/tmac-issue-with-wireless-network.html
5. Question: Why is changing the MAC address not always a good idea? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ARP Address Spoofing (Poisoning)



Tools:

<http://www.macfro.com/ethical-hacking-sniffing-attack/> (Cain&Able) Windows10 - demo

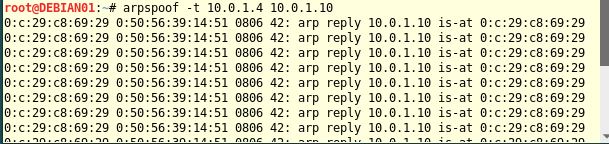
http://Cyberang3l.wikispaces.com/HOWTO+-+ARP+Poisoning+in+Linux (arpspoof & dsniff – Kali)

1. View initial ARP cache on the Victim PC (Windows 2k12Rs)
2. View initial ARP cache on the Attacker PC (Kali)
3. View initial MAC Address-Table on the Cisco Catalyst 2950/60

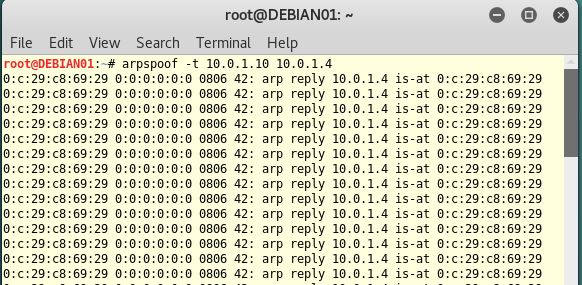
Student1Sw1#show mac address-table dynamic

1. Configure & start Wireshark to sniff on Attacker PC (Kali)
2. Start arpspoof attack application on the Attacker PC (Kali)

arpspoof -t desktopIP serverIP



arpspoof -t serverIP desktopIP

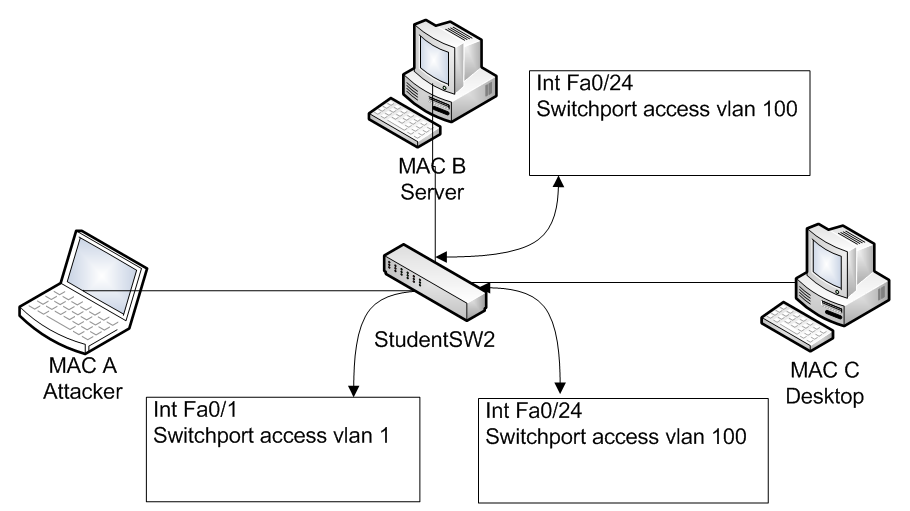


1. Start the MITM (ARP Poisoning) attack
2. View initial ARP cache on the Victim PC (Windows 2k12Rs)
3. View initial ARP cache on the Attacker PC (Kali)
4. View initial MAC Address-Table on the Cisco Catalyst 2950/60

Student1Sw1#show mac address-table dynamic

1. Question: List the MAC addresses:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

VLAN Hopping



Tools:

Yersinia - http://www.yersinia.net/index.net (Kali -DTP & DTP Trunk)

1. View initial Trunk Table on the Cisco Catalyst 2950/60

Student1Sw1#show interfaces trunk

\\SISLAPTOP14\Temp\SISLAPTOP10VMWrk\Henri\Projects\SISTek\Services\Projects\w_SAIT\ITSC206\labsupport\Lab2\SwTerminal-Initial.PNG

1. Configure student1sw1 to have vlan 100 on switch port 24

student1sw1#config t

student1sw1(config)# interface fa0/1

student1sw1(config-if)# vlan 1

student1sw1(config-if)#end

student1sw1#config t

student1sw1(config)# interface fa0/24

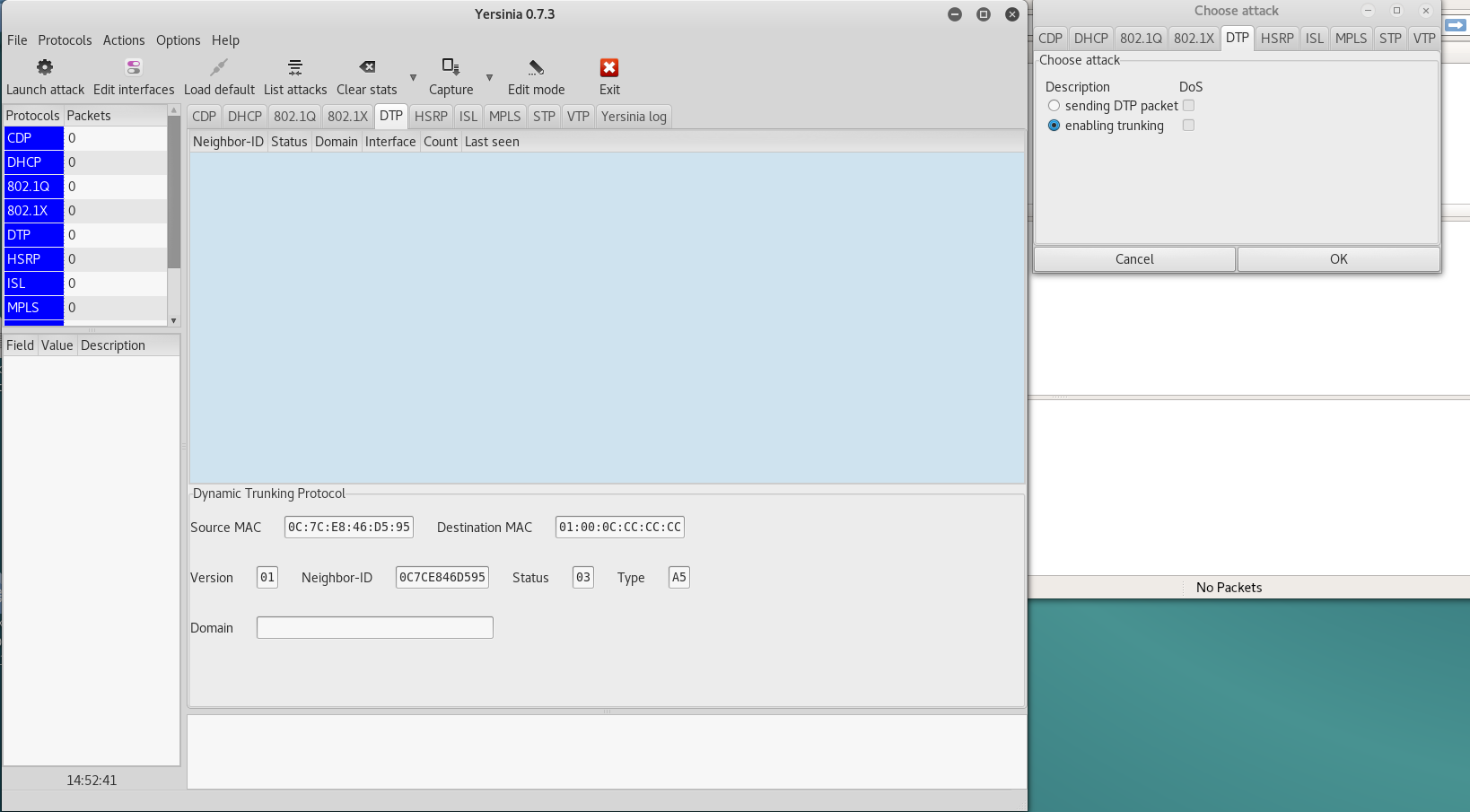
student1sw1(config-if)# vlan 100

student1sw1(config-if)#end

1. Use following command student1sw1# show interfaces trunk

Question: What is the displayed configuration? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

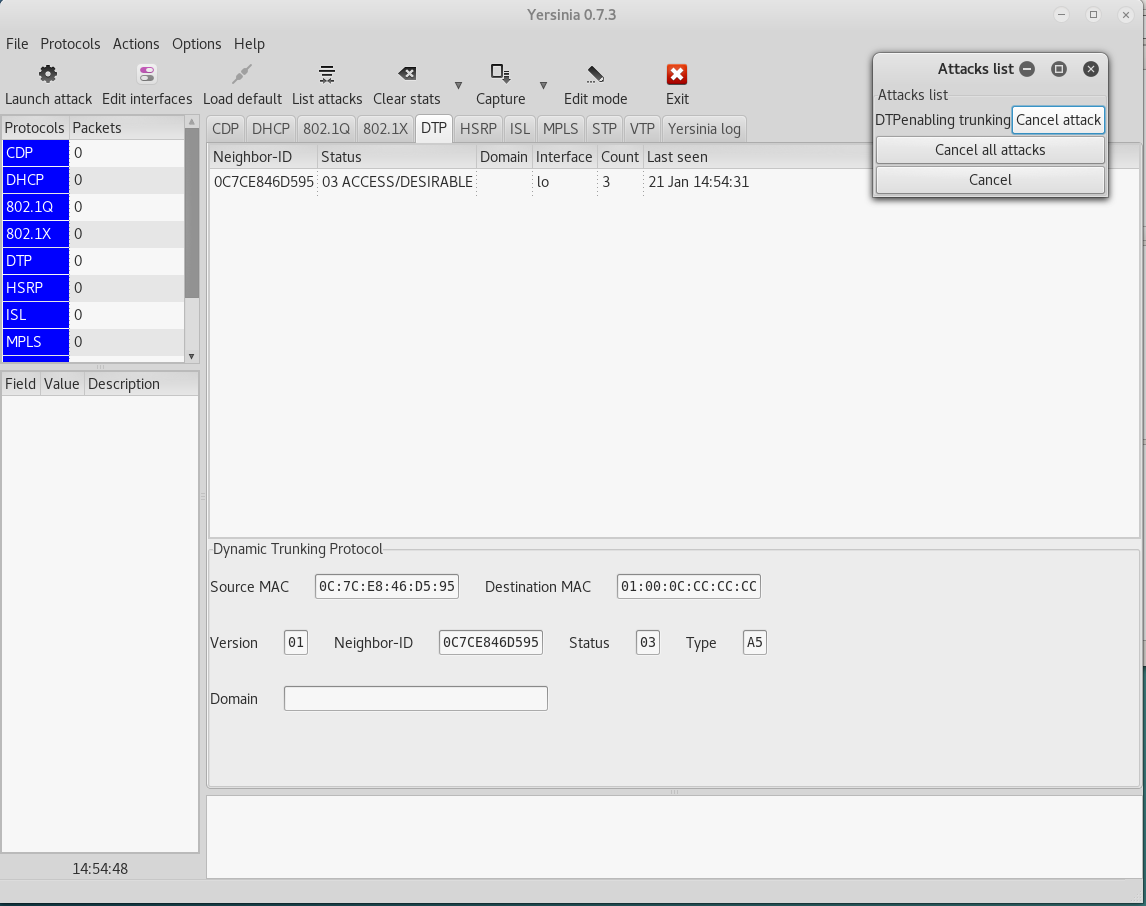
1. Kali, enter from terminal window ping the IP address of the desktop or server, Question: Are you successful? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
2. Kali, enter from terminal window, Yersinia –G, click on Launch attack button on left, the choose attack pop up window, select enabling trunking, click OK



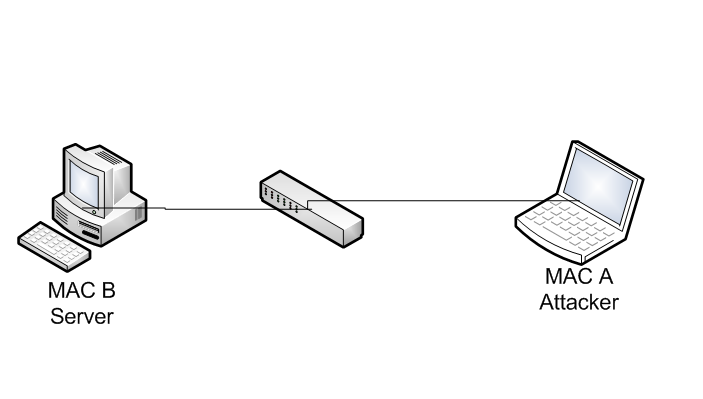
1. Waiting three minutes should be enough time to capture DTP traffic (left pane)
2. Kali, enter from terminal window, ping the IP address of the desktop or server, Question: Are you successful? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
3. Use following command student1sw1# show interfaces trunk

Question: What is the displayed configuration? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. In Kali, from the Yersinia window, click on List attacks button on center, in the choose cancel all attacks from the Attack list pop up window



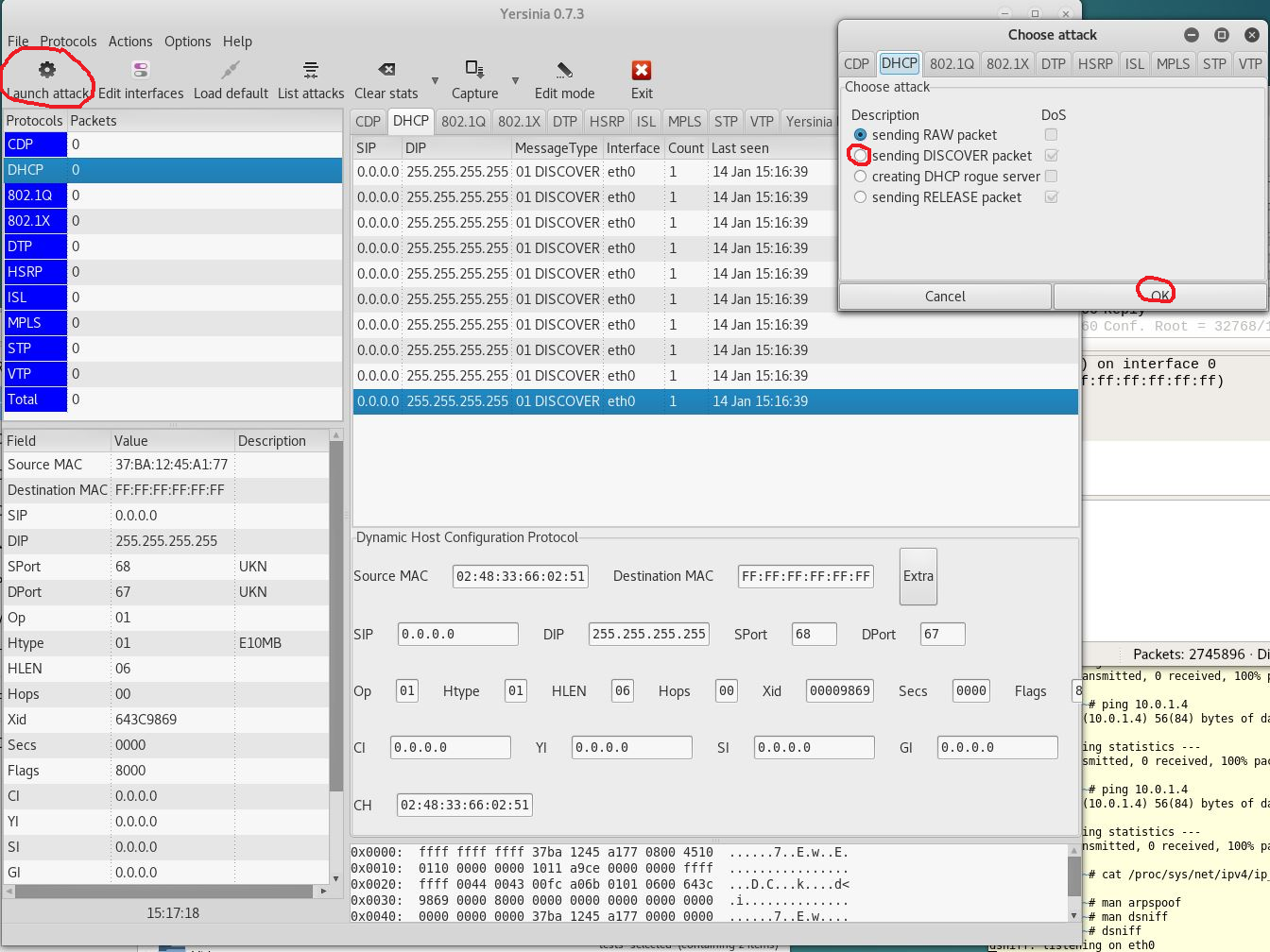
DHCP Starvation



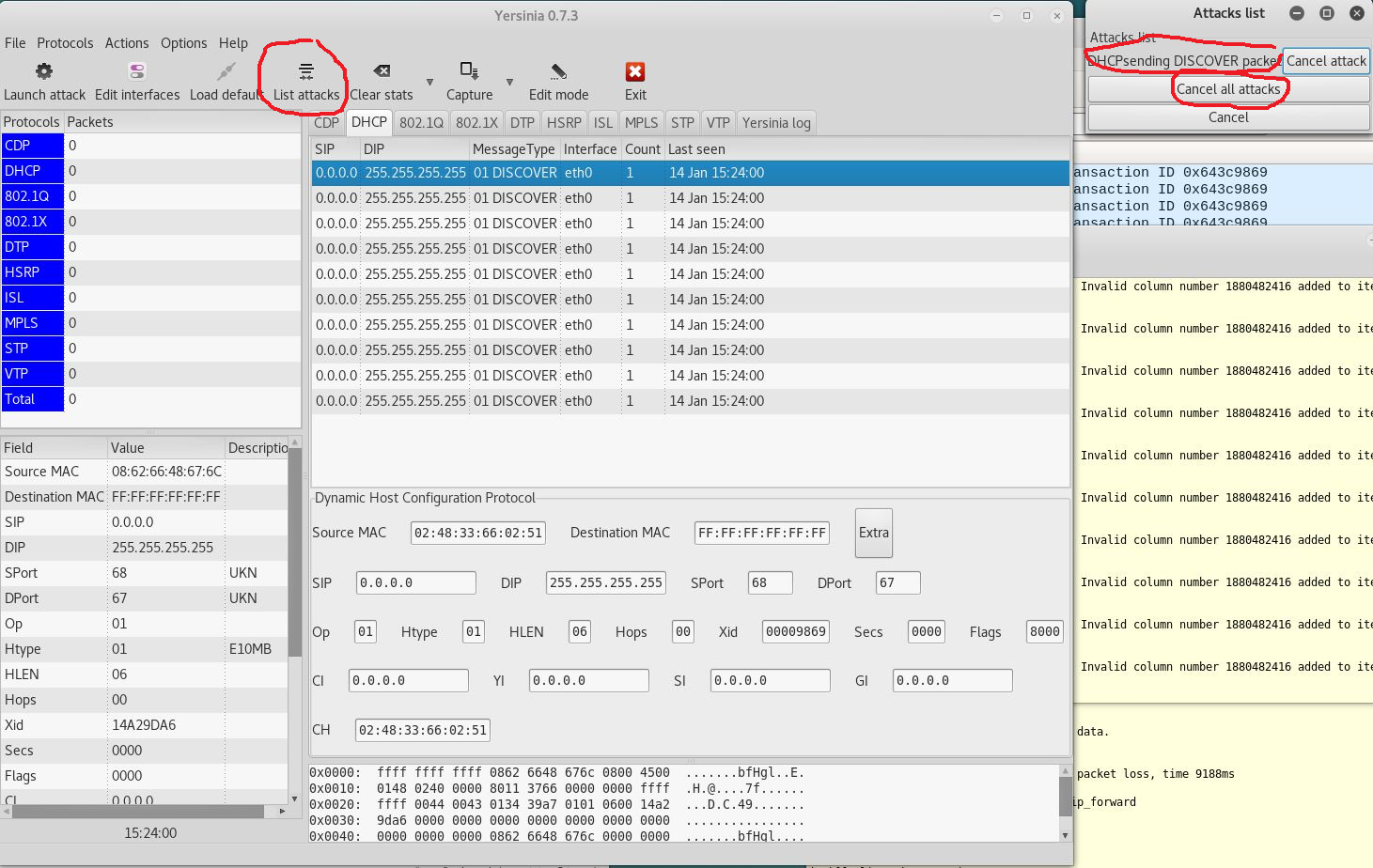
http://itsecurity.telelink.com/dhcp-attacks/

Yersinia DHCP tools (Discovery)

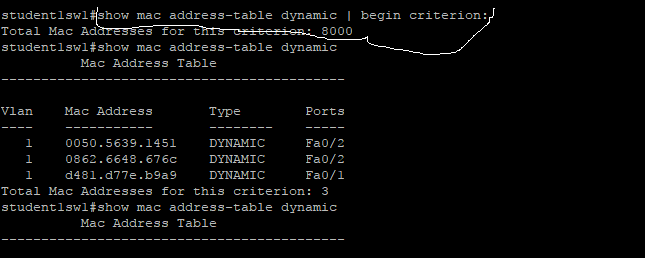
1. In the switch console window, run the following command: #show mac address-table dynamic
2. Question: How many and what are the MAC addresses shown?\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
3. Configure Yersinia as pictured below by executing from Kali command shell: yersinia –G
4. Then click on the DHCP tab in the window, then the Launch Attack button, which brings up the pop up as seen below



1. Click on sending Discovery and then OK in the popup window,
2. Leave run for twenty to thirty seconds, click on List Attacks, and cancel the DHCP Discovery Attack

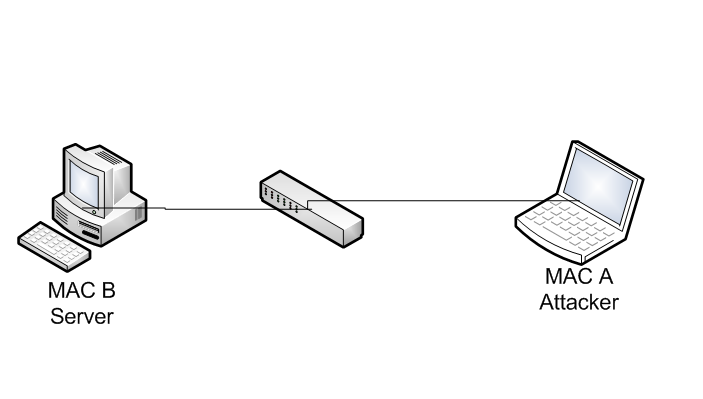


1. Within the switch console run: : #show mac address-table dynamic | begin criterion:



1. Question: How many MAC addresses were added to the table? \_\_\_\_\_\_\_\_\_\_\_\_\_\_
2. Question: Will this method fill up the CAM table? \_\_\_\_\_\_\_\_\_\_

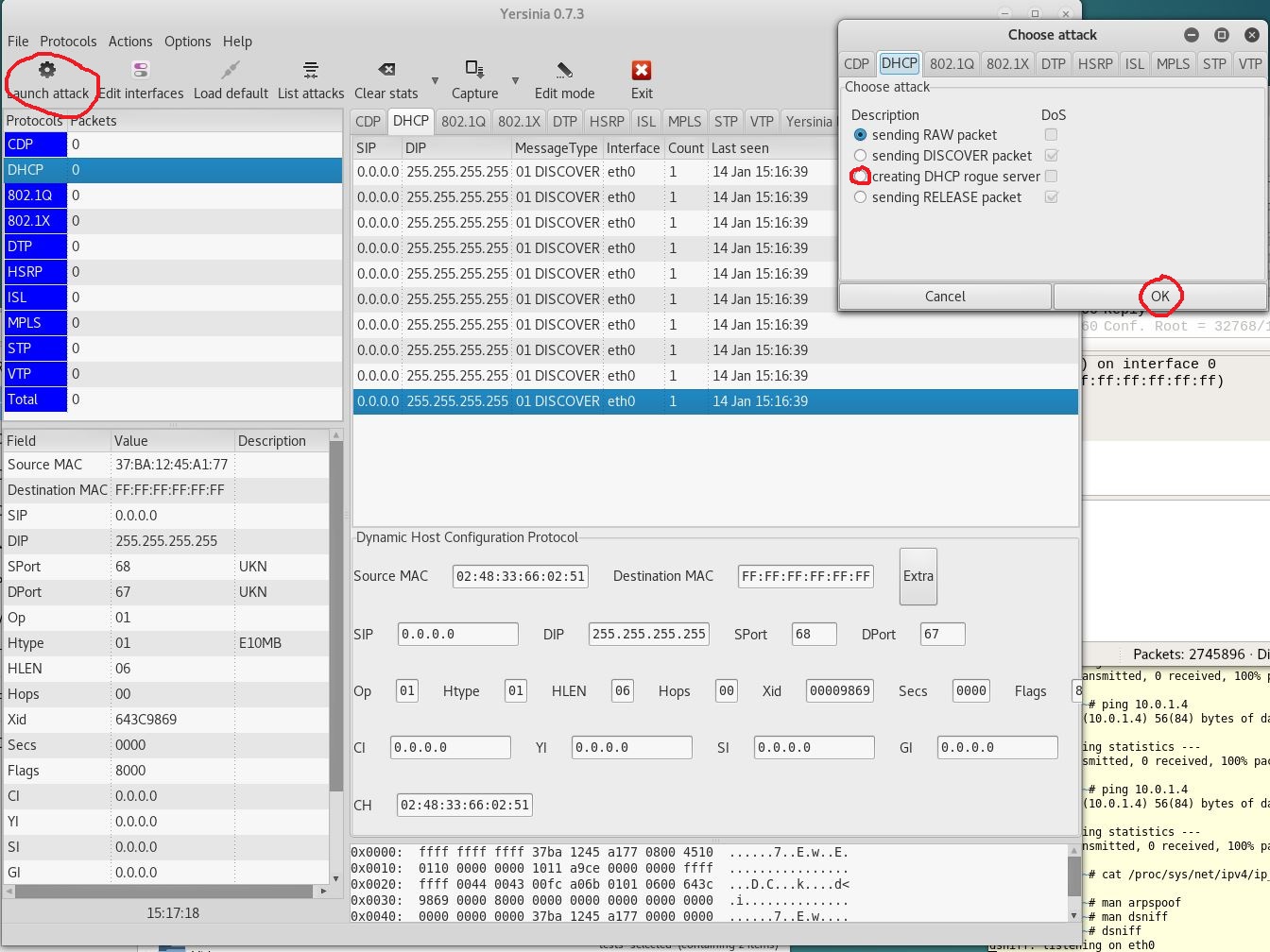
DHCP Server Spoofing



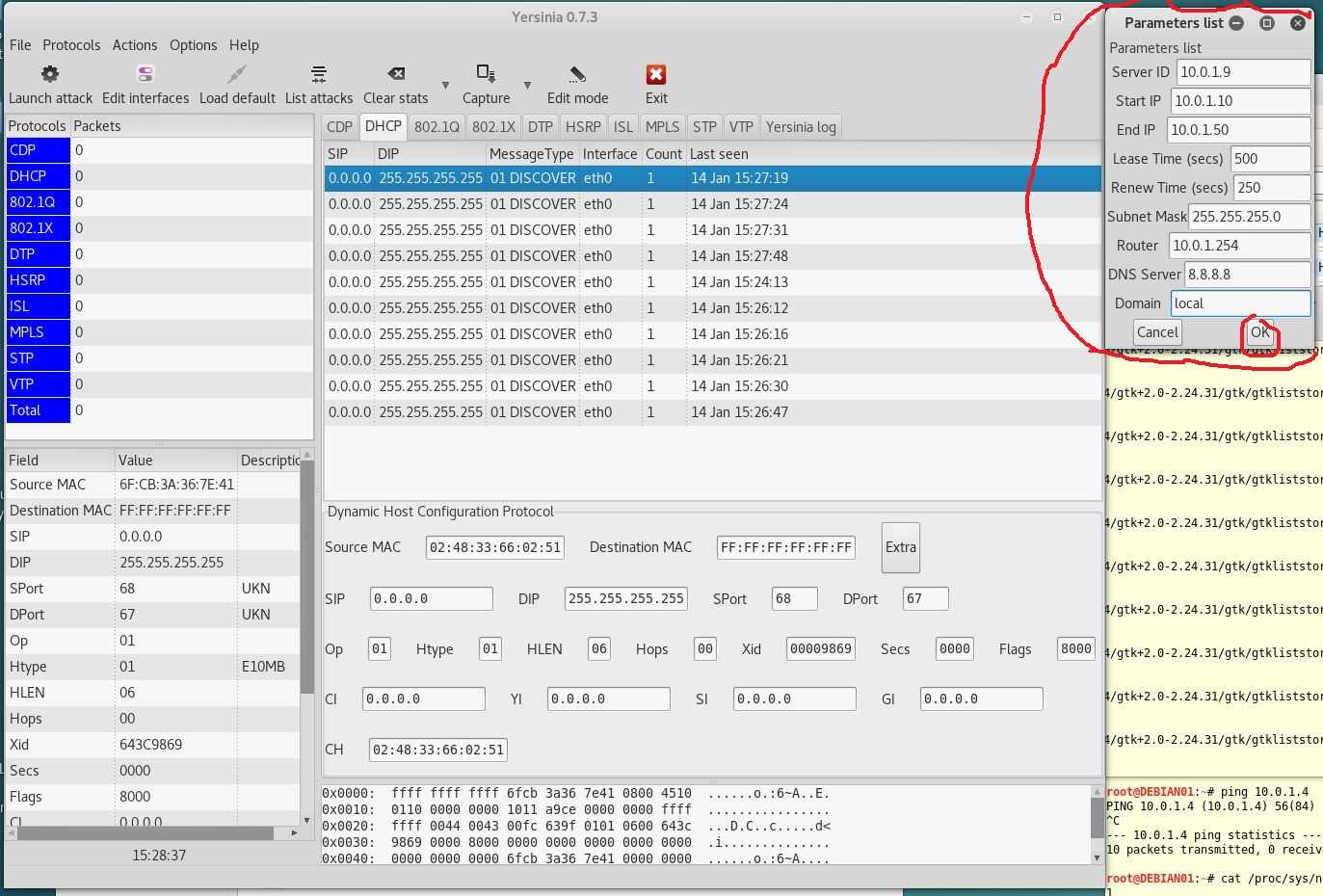
http://itsecurity.telelink.com/dhcp-attacks/

Yersinia DHCP tools (Discovery)

1. In the switch console window, run the following command: #show mac address-table dynamic
2. Question: How many and what are the MAC addresses shown?\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
3. It is expected that yersinia –G has run and the Yersinia tool is available
4. Then click on the DHCP tab in the window, then the Launch Attack button, which brings up the pop up as seen below



1. Click on sending DHCP rogue server and then OK in the popup window,
2. Another pop up window comes up with the DHCP details needed, click OK once



1. Leave run for two to three minutes, click on List Attacks, and cancel the DHCP rogue server Attack

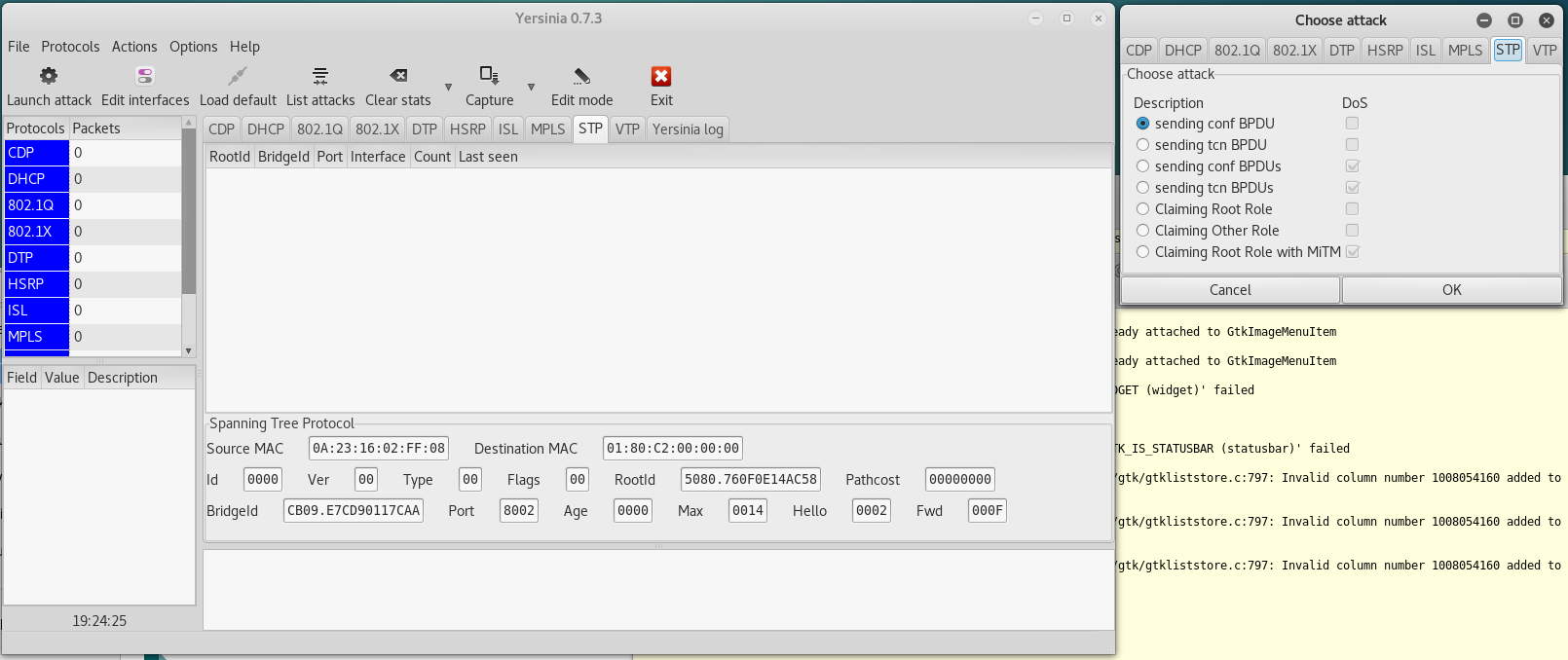
STP Spoofing

|  |
| --- |
| \\SISLAPTOP14\Temp\SISLAPTOP10VMWrk\Henri\Projects\SISTek\Services\Projects\w_SAIT\ITSC206\labsupport\Lab2\STPSpoofingDiagram.JPG  STP Network Diagram |

<http://www.ciscopress.com/articles/article.asp?p=1016582&seqNum=2>

Attack 1: Taking Over the Root Bridge

Taking over a root bridge is probably one of the most disruptive attacks. The default STP bridge priority is 32768. Once in root attack mode, Yersinia sends a BPDU every 2 sec with the same priority as the current root bridge, but with a slightly numerically lower MAC address, which ensures it a victory in the root-bridge election process. Below shows Yersinia's STP attack screen, followed by a show command capture on the LAN switch under attack.



1. Click on Claiming Root Role on Yersinia
2. Perform the following commands on the switch:

Student1SW1#show spanning-tree summary totals

Student1SW1#show spanning-tree vlan 100 interface fa0/24

Student1SW1#show spanning-tree vlan 100 root

1. Question: Does the RootId match the one on Yersinia: \_\_\_\_\_\_\_\_\_\_\_\_\_\_

Securing The LAN

1. On the switch enter the following commands:

Student1Sw1>enable

Student1Sw1# config terminal

Student1Sw1(config)# int range fa0/1-24

Student1Sw1(config -if-range)# switchport mode access

Student1Sw1(config -if-range)# switchport port-security maximum 3

Student1Sw1(config -if-range)# switchport port-security mac-address sticky

Student1Sw1(config -if-range)# switchport port-security violation restrict

Student1Sw1(config -if-range)#end

Student1Sw1#

1. Perform the same Yersinia testing as above and gather the same evidence as above:

ARP Address Spoofing (Poisoning)

Add the following commands to the switch:

Student1Sw1(config)# ip arp inspection validate

A

1. Question: List the MAC addresses:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

VLAN Hopping

On the switch enter the following commands:

Student1Sw1(config) )# int range fa0/1-24

Student1Sw1(config -if-range)#vlan 100

1. Use following command student1sw1# show interfaces trunk

Question: What is the displayed configuration? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Kali, enter from terminal window ping the IP address of the desktop or server, Question: Are you successful? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
2. Kali, enter from terminal window, ping the IP address of the desktop or server, Question: Are you successful? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
3. Use following command student1sw1# show interfaces trunk

Question: What is the displayed configuration? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

DHCP Starvation

Add the following commands to the switch:

Switch(config)# ip dhcp snooping

Switch(config)# ip dhcp snooping vlan 100

1. Question: How many and what are the MAC addresses shown?\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
2. Question: How many MAC addresses were added to the table? \_\_\_\_\_\_\_\_\_\_\_\_\_\_
3. Question: Will this method fill up the CAM table? \_\_\_\_\_\_\_\_\_\_

DHCP Server Spoofing

The extra protection should be implemented above

1. Question: How many and what are the MAC addresses shown?\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

STP Spoofing

On the switch enter the following commands:

Student1Sw1(config)# spanning-tree portfast bpduguard default

Student1Sw1(config-)#interface fa0/24

Student1Sw1(config-if)#spanning-tree portfast

Student1Sw1(config-if)#spanning-tree guard root

1. Question: Does the RootId match the one on Yersinia: \_\_\_\_\_\_\_\_\_\_\_\_\_\_

Blank page if necessary to make pages an even number

**DO NOT DELETE THE SECTION BREAK BELOW. DELETING IT MAY IMPACT THE FORMATTING IN THIS DOCUMENT.**