

Lab 2

Secure LAN

ITSC 206: Advanced Networking for Offensive and Defensive Environments

Table of Contents

[Lab Outcomes 4](#_Toc503819985)

[Files/Download 4](#_Toc503819986)

[Introduction 4](#_Toc503819988)

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

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

[DHCP Starvation 7](#_Toc503819992)

[DHCP Server Spoofing 9](#_Toc503819993)

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)

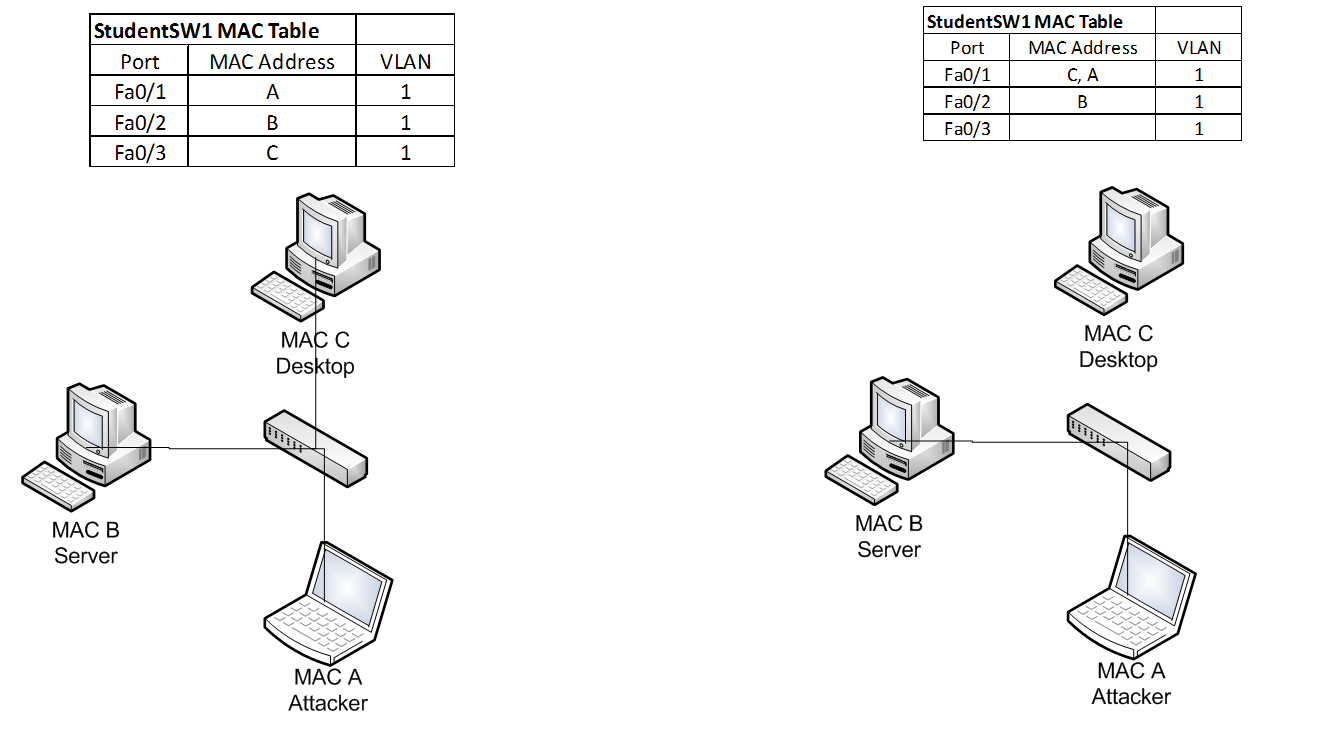
* Windows VM
  + TFTPD64 software
  + TMAC
* Kali Linux with Yersinia

Introduction

This lab gives you practice in basic network attack focused on OSI layer 2

MAC Address Spoofing - Demo

Within Linux (Kali) use macchanger.



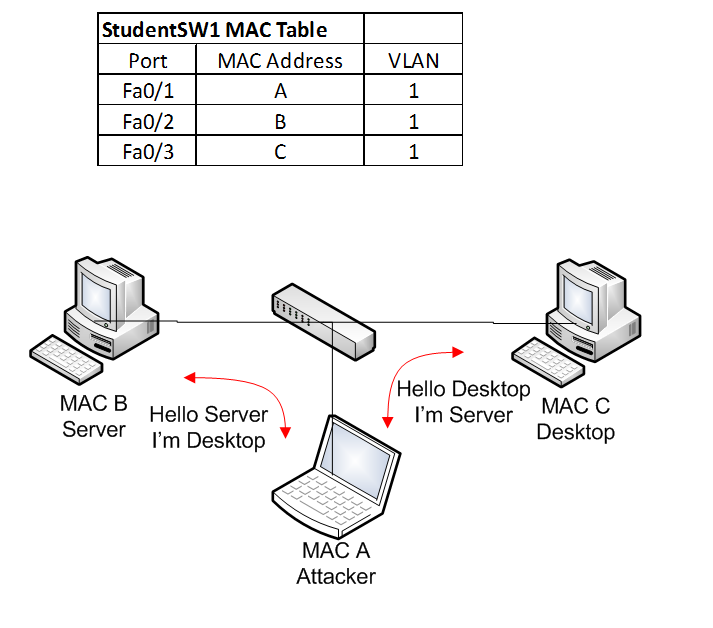
1. Write down initial MAC on the Attacker PC (Kali):\_\_\_08:00:27:35:60:db\_\_\_
2. Execute command: macchanger -m 00:0c:29:1d:dc:58 eth0

Within Windows 10 use TMAC

1. <https://technitium.com/tmac/> - Windows MAC Changer
2. Write down initial MAC on the Win10 PC (Test):\_\_\_08:00:27:33:c9:17\_\_
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?

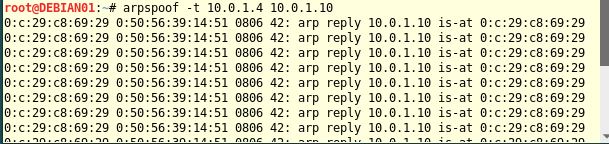
\_\_Because it stores hardware information, sometimes a DHCP server will assign you a new IP address because the MAC no longer matches the one on its records\_\_\_\_\_\_\_\_\_\_\_\_\_

ARP Address Spoofing (Poisoning)

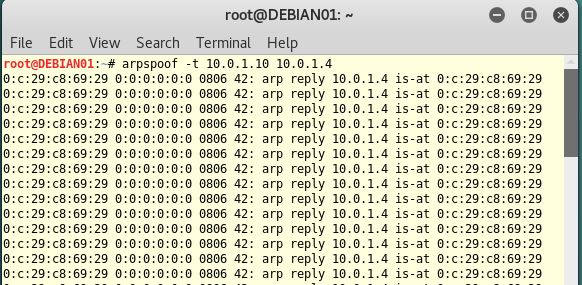


1. View initial ARP cache on the Victim PC
2. View initial ARP cache on the Attacker PC
3. Configure & start Wireshark to sniff on Attacker PC (Kali)
4. Start arpspoof attack application on the Attacker PC (Kali)

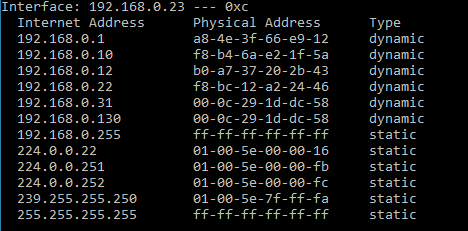
arpspoof -t desktopIP serverIP

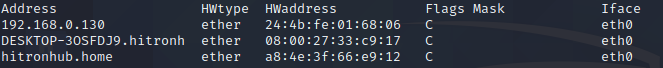


arpspoof -t serverIP desktopIP

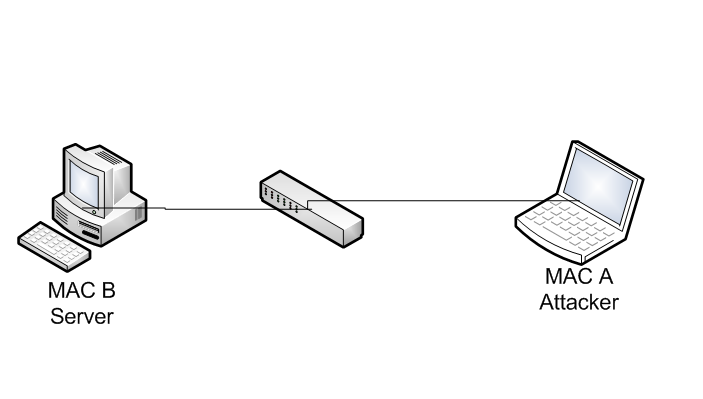


1. Start the MITM (ARP Poisoning) attack
2. View ARP cache on the Victim PC
3. View ARP cache on the Attacker PC (Kali)
4. Question: List the MAC addresses:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Victim: 

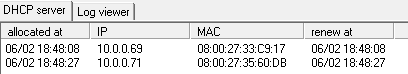
Attacker: 

DHCP Starvation

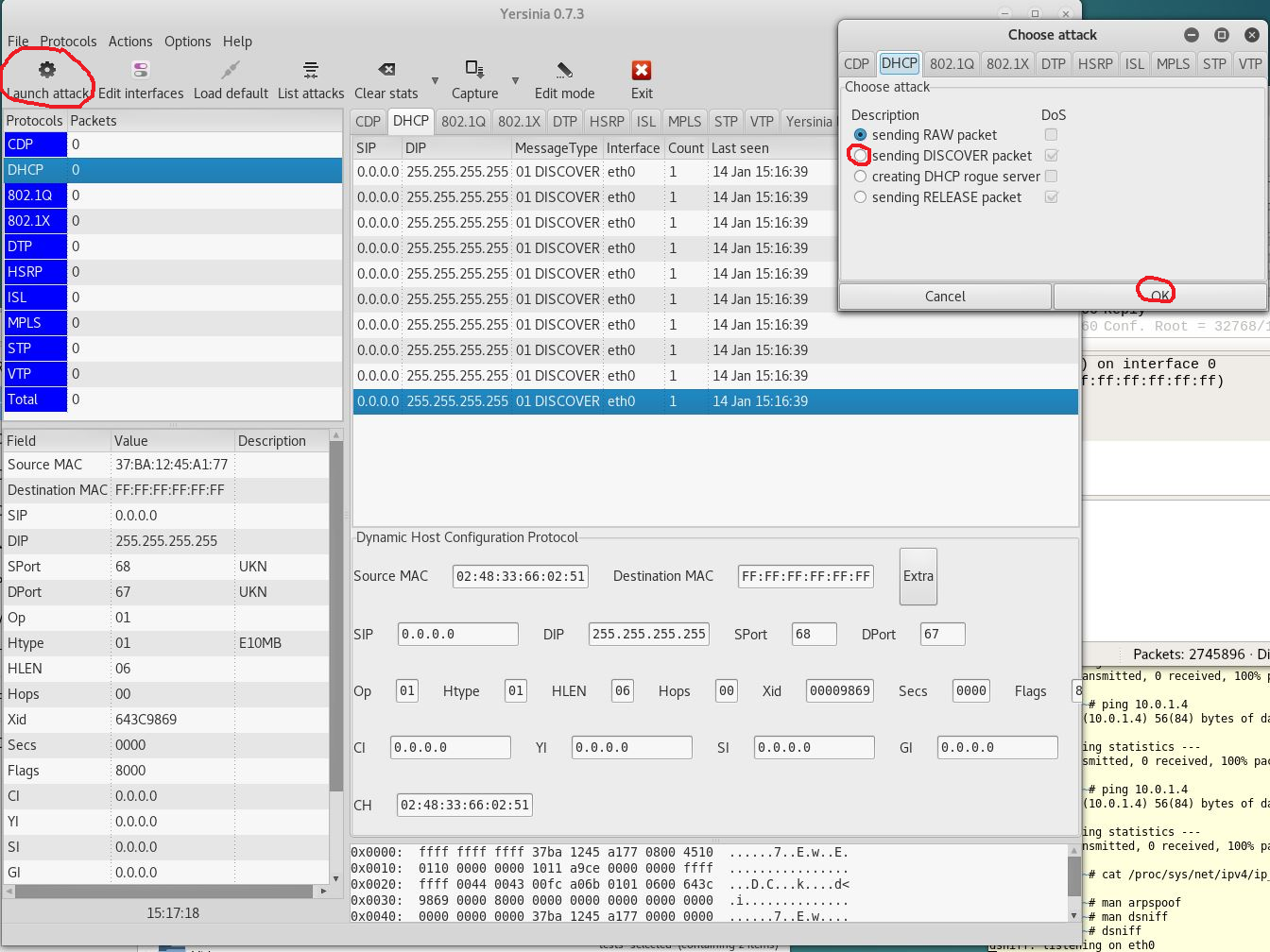


Yersinia DHCP tools (Discovery)

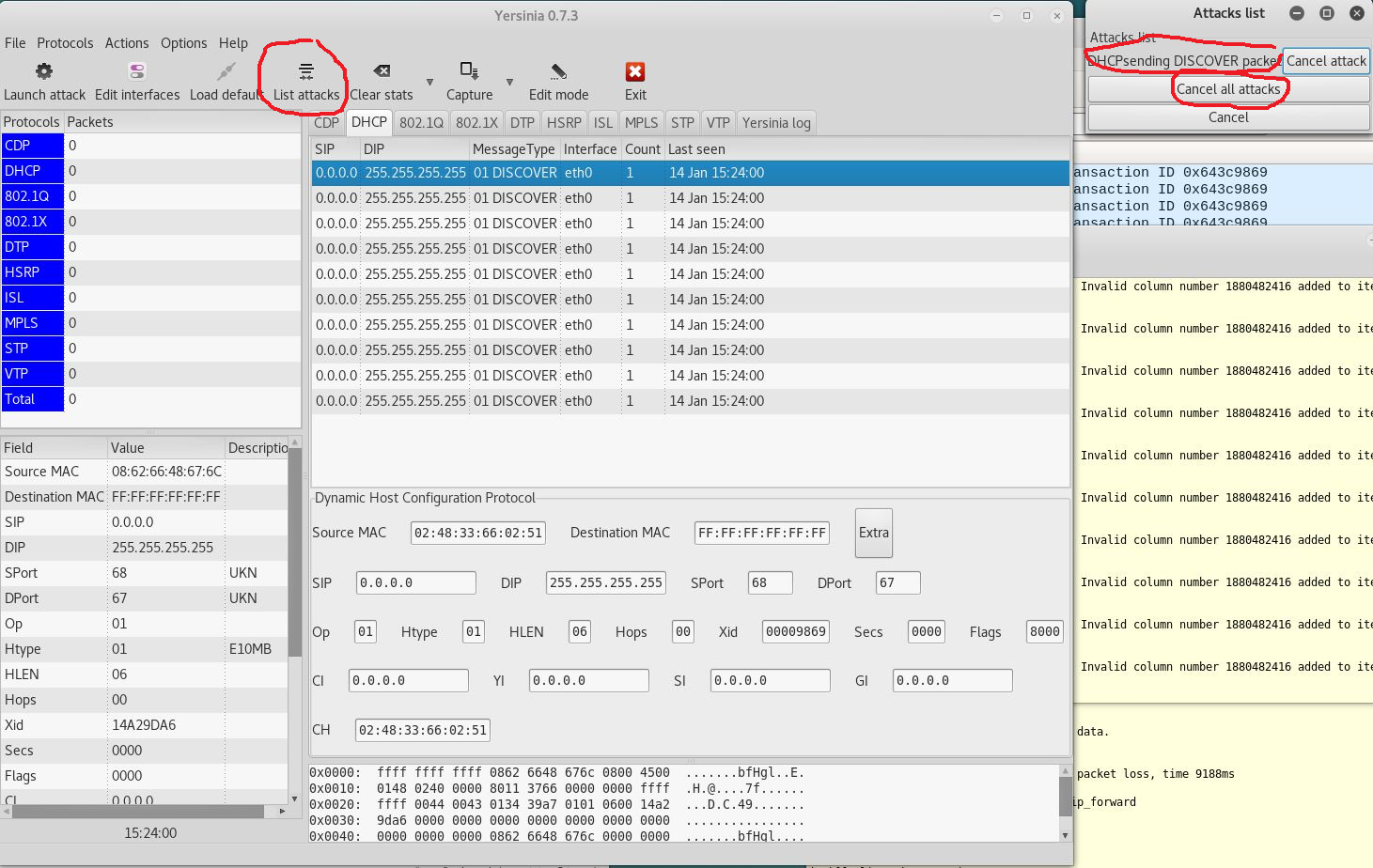
1. Install and configure DHCP server on Windows using tftpd
2. Question: How many and what are the MAC addresses shown on dhcp server?\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_



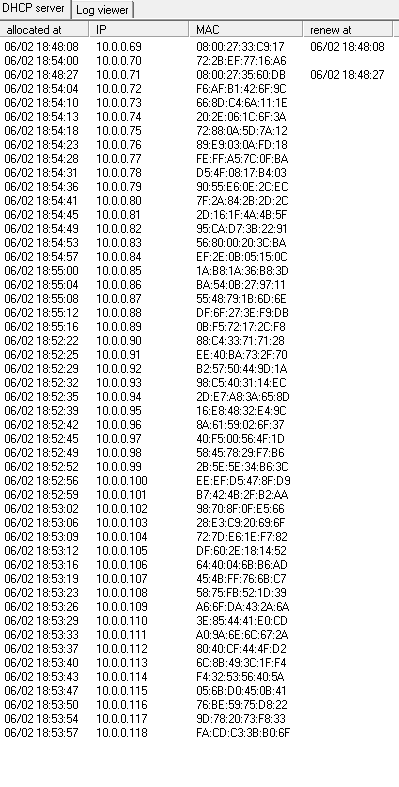
1. Configure Yersinia as pictured below by executing from Kali command shell: yersinia –G
2. Then click on the DHCP tab in the window, then the Launch Attack button, which brings up the pop up as seen below



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

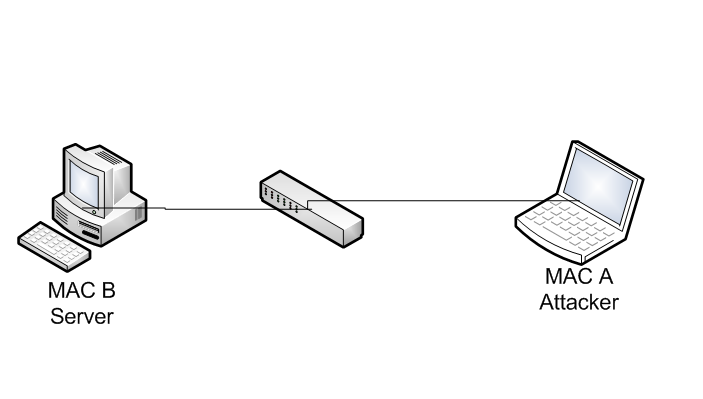


1. Question: How many MAC addresses were added to the table? \_A lot (48)\_\_\_ \_\_



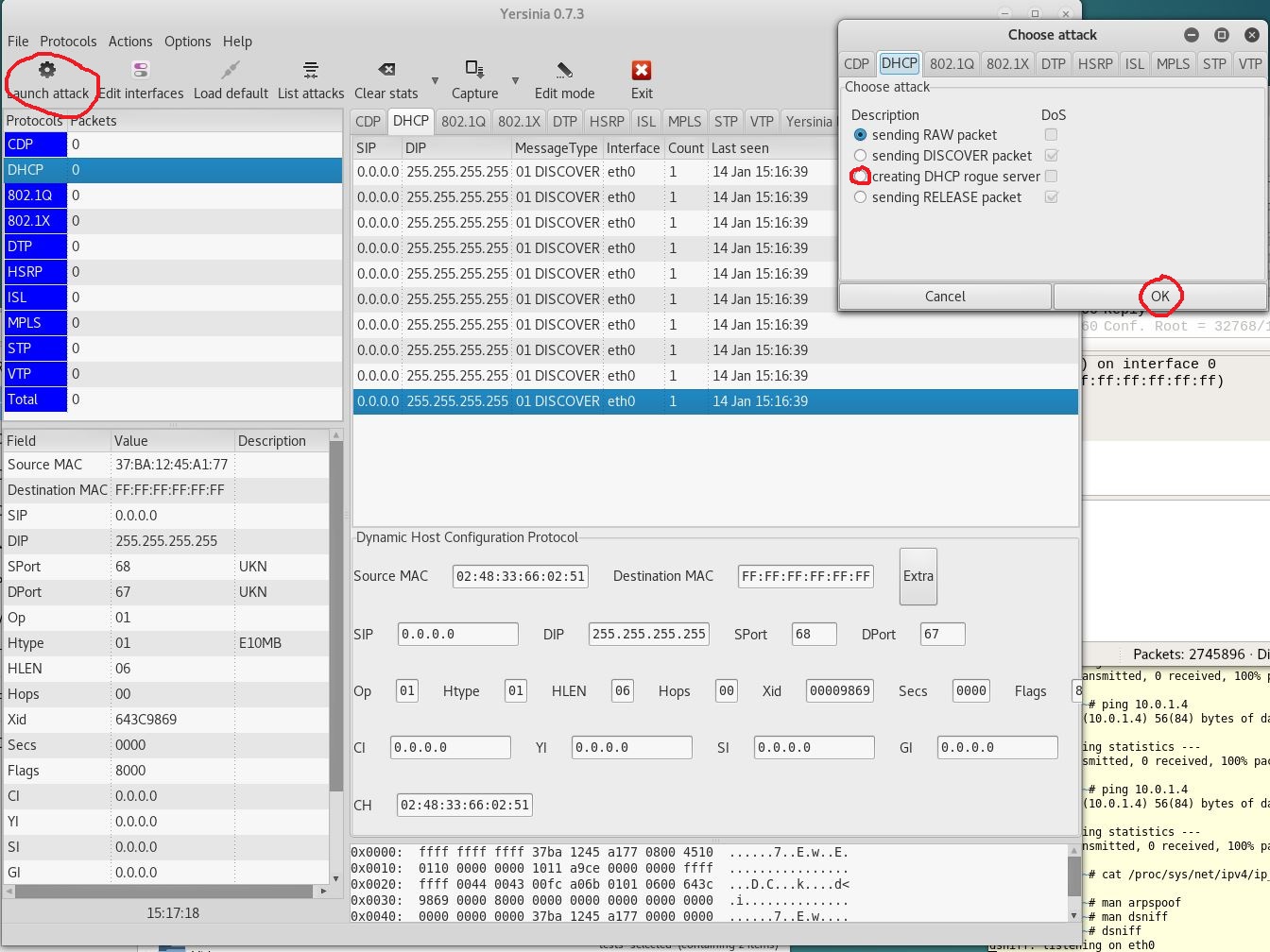
1. Question: Will this method fill up the CAM table? \_\_\_Yes\_\_\_\_\_\_\_

DHCP Server Spoofing

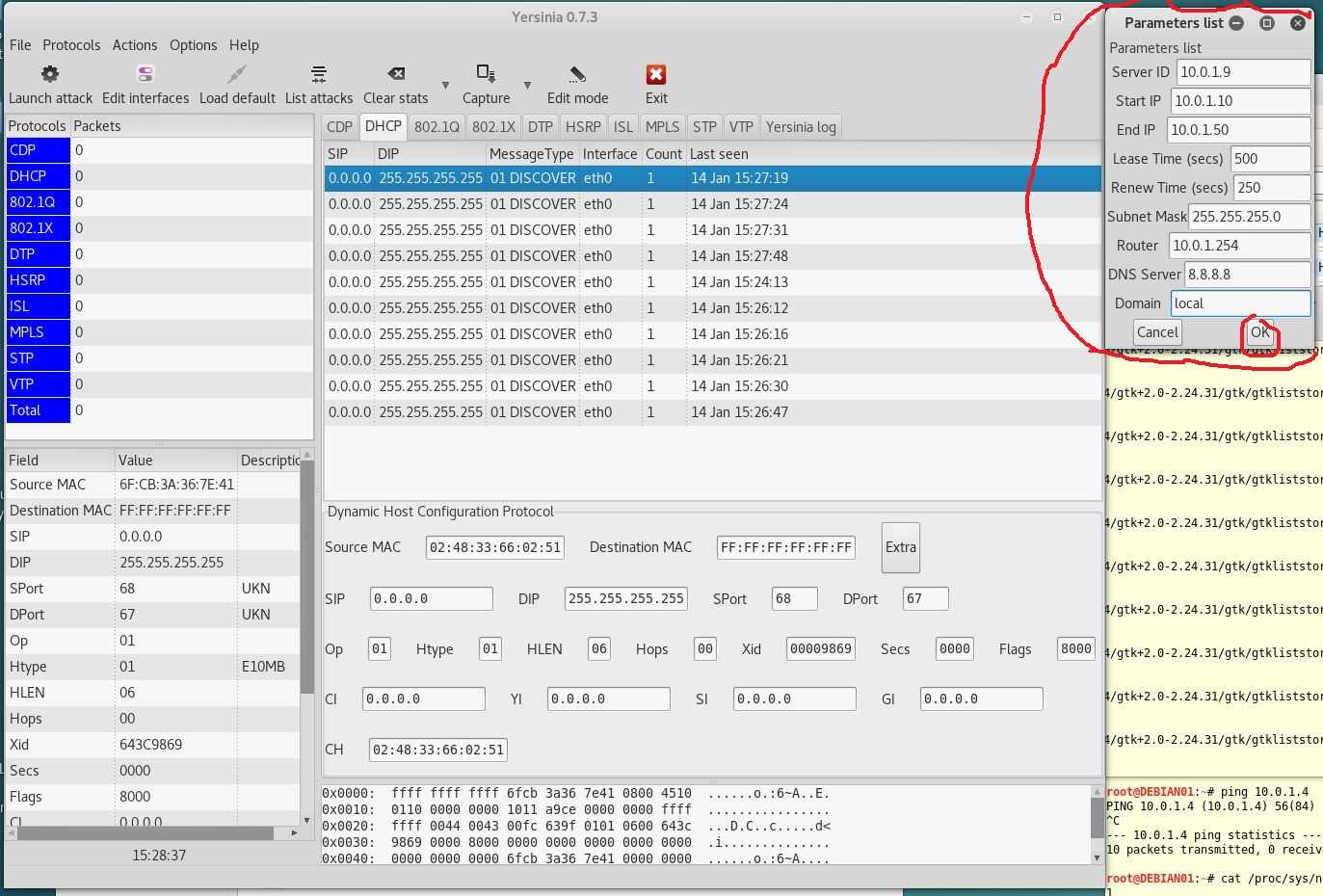


1. Question: How many and what are the MAC addresses shown on DHCP server?\_\_\_50 addresses (see earlier screenshot) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
2. Run yersinia –G in the terminal

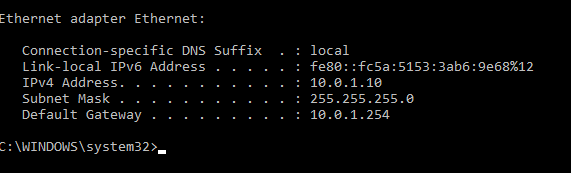
1. Then click on the DHCP tab in the window, then the Launch Attack button, which brings up the pop up as seen below



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



I used the same settings that you specified in yersinia, and the victim PC connected to the rouge DHCP server since the earlier attack used up all the available IP addresses

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.**