## Part 1: Wireshark

1. Review your networking in Chapter 3, “The Fundamentals”, and Chapter 4, “Capturing Packets” of Wireshark for Security Professionals.
2. **Checkpoint 1: Do the following and show the answers in your report**

* Exercise 1 at the end of Chapter 3
* Exercises 1-6 at the end of Chapter 4
* Create some wireshark display filters to find the following:
  + DHCP traffic for a specific MAC address

ARP AND ETH0.ADDRESS= 00:00:5e:00:53:00

* + ARP traffic for a specific MAC address
  + Vmware\_f2:51:27 = ff:ff:ff:ff:ff:ff
  + DNS traffic for a specific domain name
  + Udp.port == 53, tcp,port == 53 and HTTP.host contains “Seneca.com” and “Mozilla.com”

THREE-WAY HANDSHAKE

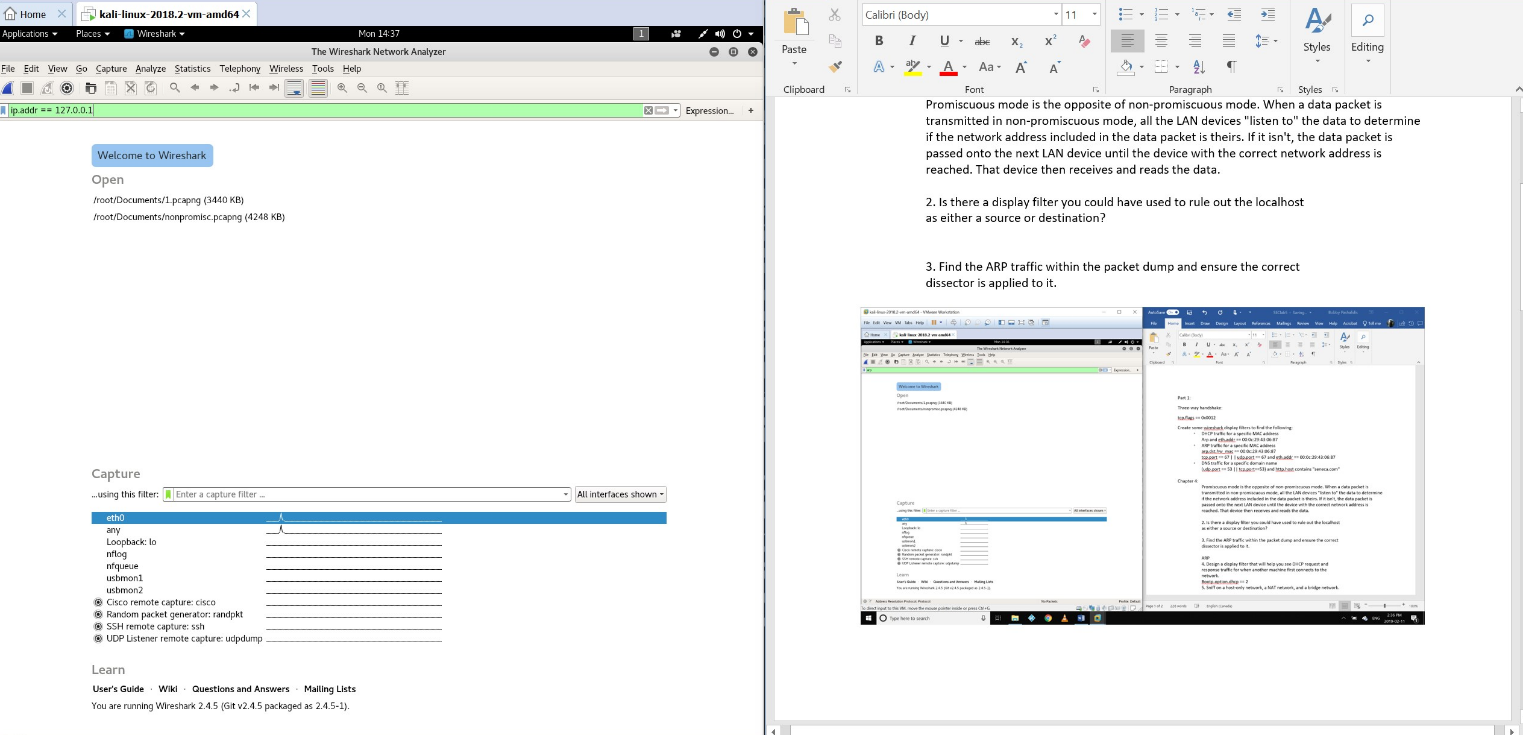
Chapter 3

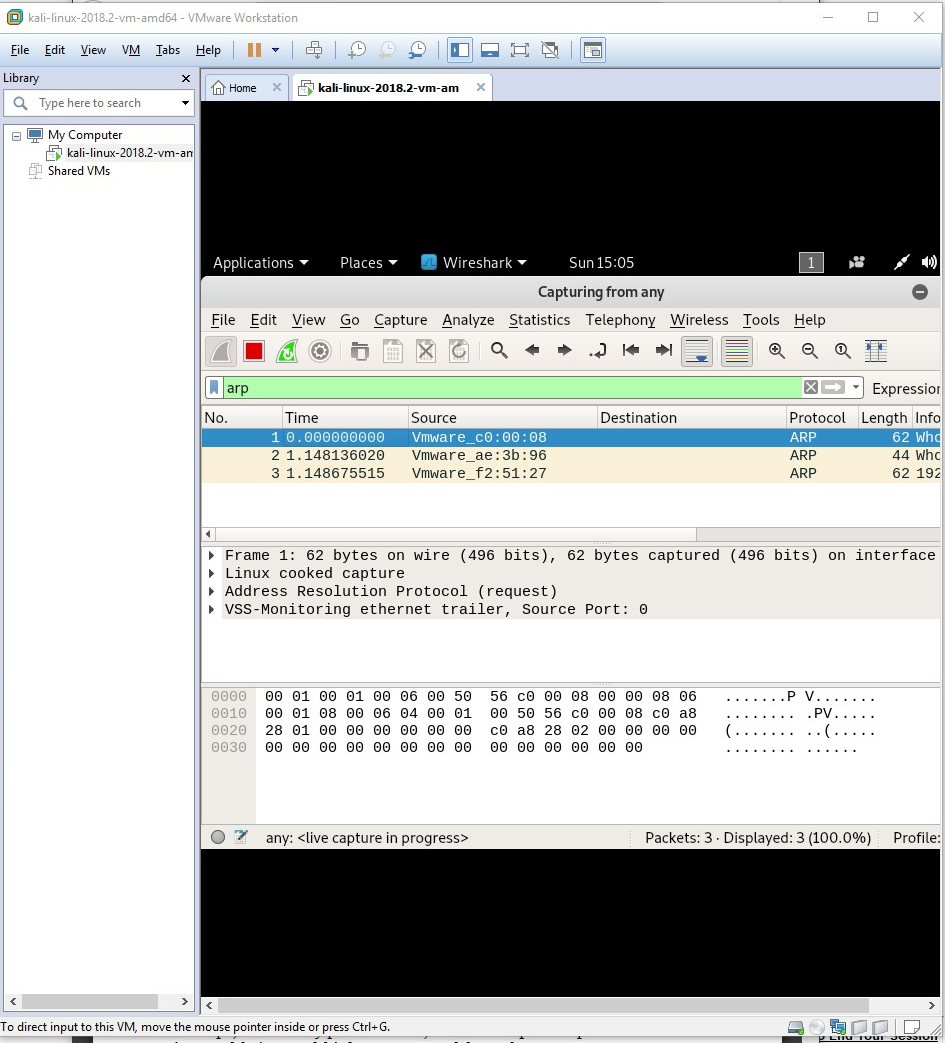
Eth.type = 0x0806

Tcp.flags = 0x0018

Chapter 4

1. In promiscuous moden the opposite of non-promiscuous mode, the lan devices that are listened too. Have data that is determined by transmitting a data packet to their devices. It can detail the network that is addressed from the packet onto the next LAN device, causing it to have the correct network to be reached no matter what, helping that device read its data



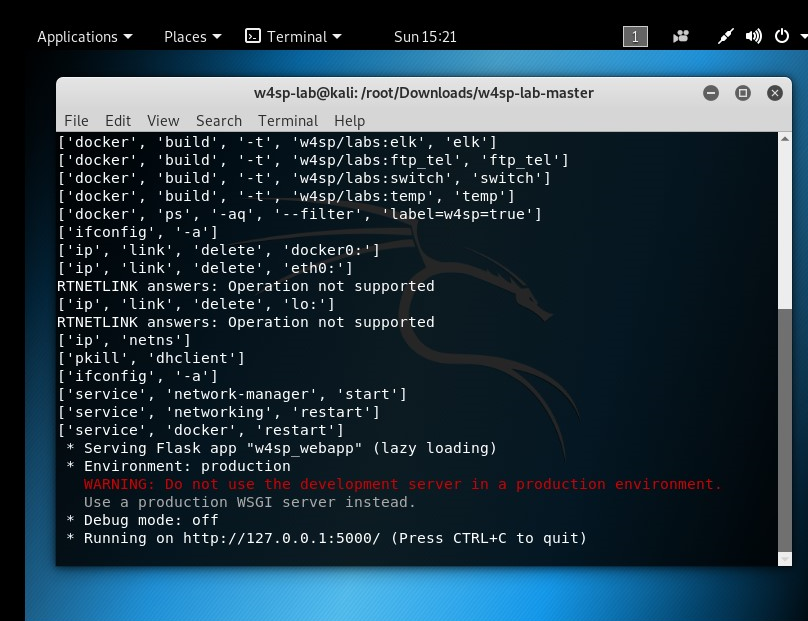


1. bootp.option.dhcp == 3 or bootp.dhcp.option == 2

## Part 2: Preparing the W4SP Lab

**Checkpoint 2: Gather evidence to show in your report that you have completed this step with a screenshot of the lab environment.**

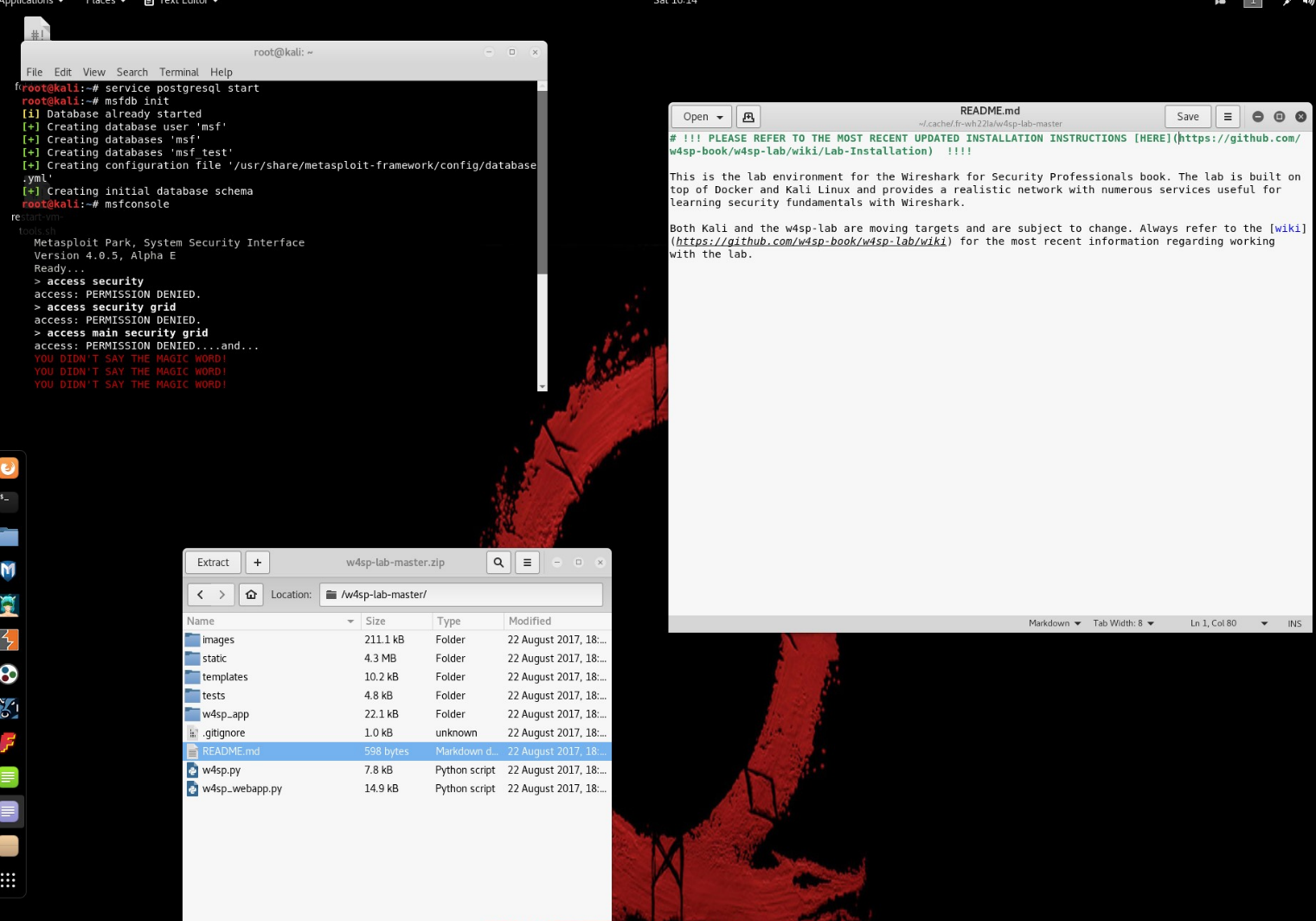
### 



### The Metasploit Framework

**Checkpoint 3: Gather evidence to show in your report that you have updated Metasploit.**

UPDATING METASPLOITE

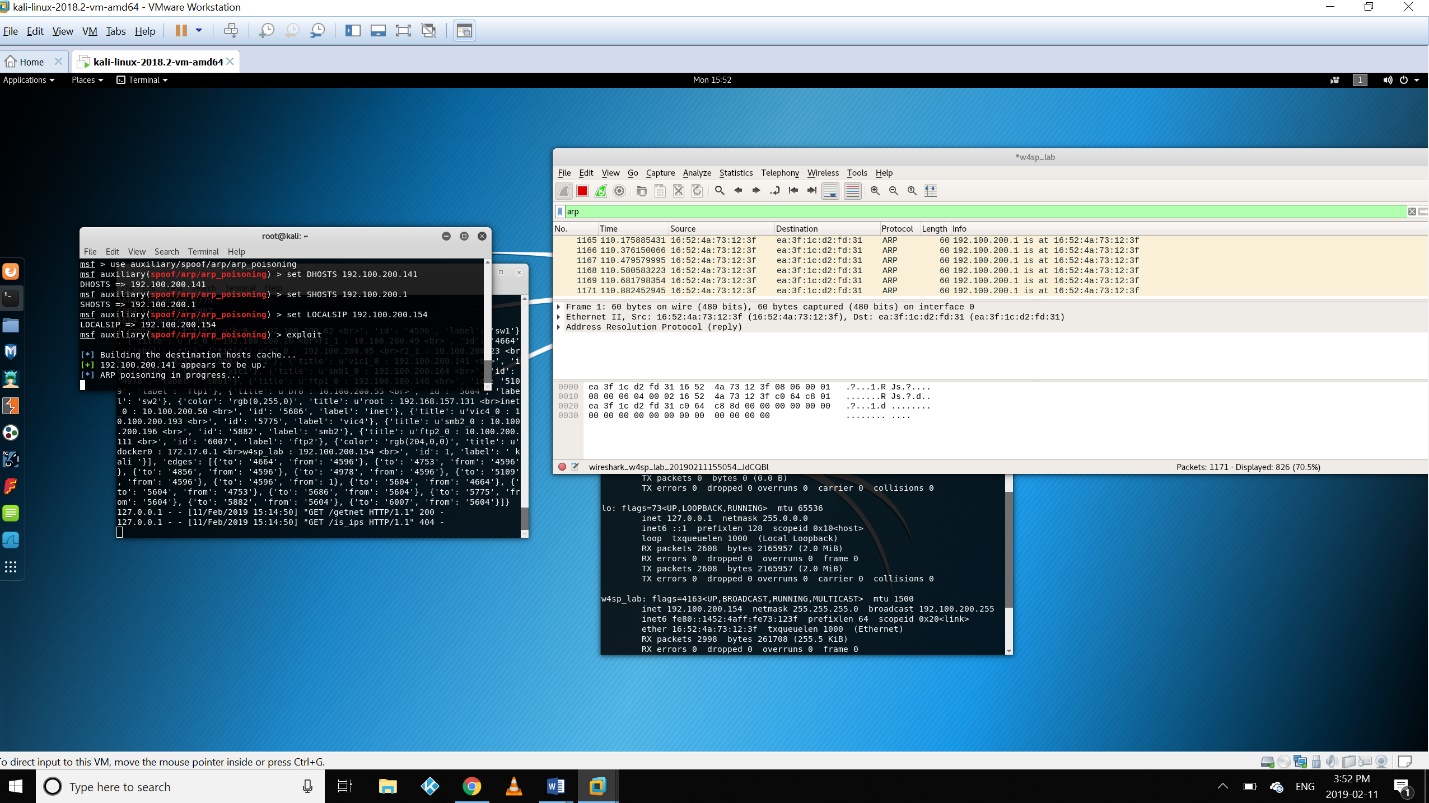


Once your environment is ready, we will experiment with some Man-in-the-Middle (MitM) attacks.

The book associated with the lab explans how we can do this.

**Checkpoint 4: Gather the following evidence to show in your report that your ARP MitM attack was successful:**

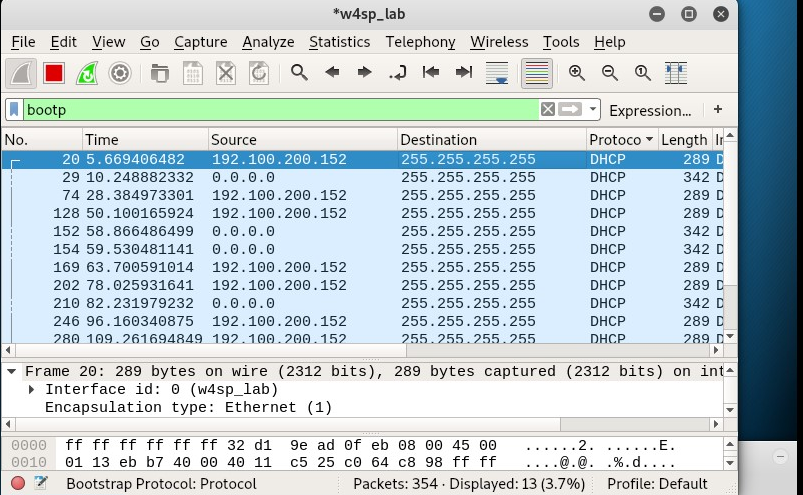
|  |  |  |  |
| --- | --- | --- | --- |
| Setting | Description | IP | System |
| DHOSTS | Target | 192.100.200.149 | Vic1 |
| SHOSTS | Spoofed IP | 192.100.200.1 | Gateway |
| LOCALSIP | Local IP | 192.100.200.152 | Kali/Metasploit |



* spoofed arp
* captured FTP credentials from vic1

**Checkpoint 5: As you perform your DNS MitM attack, gather the following evidence to show in your report that it was successful.**

* fake DHCP transaction



* fake DNS transaction
* captured FTP credentials from fake FTP server

**Checkpoint 6: Do the following and show the answers in your report**

* Exercises 2 and 4 at the end of Chapter 5

To prevent a Mitm Attack

* We have to check the ARP table to check the Mac address of the router in the network and make sure that the information we are going to send is going through the correct router, not other device. Hacker can fake the MAC address of the router and make victim think that they still send information through the correct gateway. Another attack could be DNS spoofing and what user can secure the network from being attacked by hacker using DNS spoofing is that they have to carefully check the DNS and hosts record on the machine to check if it points to any potential faked URL. Whenever user go to the Internet, carefully check the URL of the website.

### Report

### Use screenshots, accompanied by explanations, to show that you completed the work above.

In your own words, describe, in technical detail, how the attacks we have studied work. Make sure to describe the protocols involved, how those protocols work, and how were exploited.

Describe how we can mitigate each of these attacks.