# **Week Four LAB: Sniffing Traffic (VCastle)**

In this lab assignment, you will perform the tasks you have been taught in the Guided Practices (iLabs content form EC-Council). You may review your prior labs to supplement your understanding of the material. This lab reinforces your learning and understanding and increases material retention through hands-on application.

# How does this practical lab apply in the real world?

Understanding how a spoofing attack impacts the overall security of the enterprise and the end-user is critical to global and individual security. A recent Internet Research project indicated approximately 30,0000 spoofing attacks per day (Dell, 2018). It is possible to spoof local traffic and major Internet connections, impacting the underlying fabric of the Internet on which society depends. We have seen examples of this with Russia and China, in which they have hacked the Border Gateway Protocol (BGP) and redirected critical communications from other nations through servers within their perspective countries, thus compromising security for individuals, governments, and corporations (Slate, 2018). To understand the importance of mitigating attacks of this nature, we must understand some of the tools used to compromise the security of ourselves and our families and the critical fabric of the Internet.

|  |
| --- |
| Special note: Please ensure you are using the Windows 10 Wireshark machine on the 172.31.X.X network. This means you will not be using the Windows 10 machine that is on the same subnet as the Android machine. Also you will need to close the CMD window that is currently running if is still active before proceeding further with the lab. |

# Resources Needed (PLEASE READ FIRST)

This lab assessment covers units three and four from your EC-Council lab content. Thus, all resources you need will be from your labs that you have completed in iLabs on Malware Threats and Sniffing.

* Windows 10

1. Wireshark
2. cmd

* Parrot OS

1. Wireshark
2. Macof
3. Arpspoof
4. terminal

# Level of Difficulty

Moderate

# Important

**Please note the following guidance**: This lab assignment should be performed in the VCASTLE Pod. Also, any screenshots here are for general reference and machines and IP address will vary to ensure they are meant only as a reference to encourage academic integrity.

## You are tasked with changing the mac address of the Windows 10 client using ParrotOS and macof as the tool. Basic assumptions are that you are able to use the tools listed and that you have completed the ilabs before starting the week 4 assessment.

# Instructions

# Malware Threats

***Steps***

1. Gain access to the system using a Trojan - use a software tool such as njRAT, ProRat, Theef RAT to build a Remote Access Trojan (RAT) server
2. (optional) Use an encryption tool such as SwayzCryptor to encrypt the RAT to make it more difficult for it to be detected by anti-virus utilities
3. Deliver the RAT to the target machine and execute it
4. From the attacker machine where you built the RAT, look at the existing connection to the target and explore your options of exploiting the target – document what you are doing to exploit the target (for example, using the keylogger, being able to control the mouse, webcam and microphone, being able to navigate the file system)

# Netlab arpspoof

***Steps***

1. Open Wireshark in Windows 10 as well as the command prompt.
2. While at the command prompt identify the Mac address and Ip address for the gateway device that the client is connected to.
3. Your screenshot will need to display that the mac address of the Windows 10 Machines gateway device as well as the IP address of the gateway machine and the local machine. This must be done from the command prompt only.
4. Your ParrotOS screenshot will show the actual arpspoof application running generating traffic as well as the command you used to start the process.
5. Your Wireshark on Windows 10 machine will now need to show the capture of the traffic from the ParrotOS machine. Now identify the the ip address of the source machine generating the traffic and what does it look like? Please provide a screenshot of the Wireshark output.
6. Leave Wireshark running for next lab

## Netlab macof

***Steps***

1. Restart Wireshark on both Windows 10 and ParrotOS
2. Now run the macof command using the correct switches and IP addresses to flood the Virtual switch. Provide a screenshot of the ParrotOS generating mac addresses flooding.
3. Please obtain a screenshot from each machine that is running Wireshark showing the duplicate packets.

***Step 3 (Arp spoof): Figure 1-A***

The critical aspect of this lab is the identification of an Arp attack please provide a screenshot verifying that you have successful attacked the Windows 10 machine thus a screenshot showing before and after the Arp attack.

A picture containing text, electronics, screenshot, software

Description automatically generated

***Step 4 (Arp spoof): Figure 1-B***

***A screenshot of a computer

Description automatically generated***

*\*\*Example Screenshot Only*

***Step 5 (Arp spoof) Figure 1-C***

***A screenshot of a computer

Description automatically generated***

***Step 2 (macof): Figure 2-A***

***A screenshot of a computer

Description automatically generated***

***Step 3 (macof): Figure 2-B***

***A screenshot of a computer

Description automatically generated with medium confidence***

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Deliverables Example for tasks one-X (EXAMPLE ONLY)**

* **Threat:** DNS Dumpster identified a Microsoft server using HTTP API/2.0 with an IP address of 121.171.142.220 in South Korea. The exploits available for this protocol include Banner Disclose vulnerable on WAP servers. (What Threat allowed this attack)
* **Mitigation** The Microsoft-HTTPAPI/2.0 vulnerability can be mitigated by disabling the server Header in the registry key via HKEY\_LOCAL\_MACHINE. (How would this be mitigated in a network?)
* **Summary:** This site has various potential vulnerabilities that must be remediated and verified. The use of DNS dumpster provided a DNS snapshot at a moment that indicated potential threats that the United Nations could face. Understanding each threat and making recommendations to prevent such threats is essential. There are more vulnerabilities within this organization that should be mitigated and then reverified as corrected. Please provide a summary of the lab as per the example above.

The following items should be addressed in the above content threat and mitigation.

* ArpSpoof
* Macof

## **Deliverables:** Complete this section, using the example above as a template for each answer. If there is more than one task, include as such. If there are less than 6 tasks, only include the tasks needed for the lab, as this is a template only.

Task 1:

Task 2:

Task 3:

Task 4:

Task 5:

Task 6: