**Laboratory Weapons to Exploit Network Layer**

OBJECTIVES:

GENERAL:

* Understand how attacks work across the network layer.
* Understand the concepts related to a mina-in-the-middle-attack.

SPECIFIC:

* How to decode and interpret network packets in Wireshark.
* How to use scapy to sniff and modify network packets.
* How to use nfqueue and iptables to redirect and intercept network traffic.
* Lear about the ARP (Address Resolution Protocol) spoof attack.

**SECTION ONE**

**(CAPTURE NETWORK TRAFFIC WHIT SCAPY):**

**SNIFFING:**

Sniffing is a technique that involves capturing all the information that circulates through a network. This information is stored and interpreted to discover sensitive data such as passwords, bank information, etc. This attack is one of the main ones that are made when you try to steal information.

**SCAPY:**

Scapy is a powerful library written and supported in Python which allows the creation, manipulation and injection of packages from a network environment. It allows to perform different tasks such as Fingerprinting, Discovering, Enumeration, among others.

**EXPLAIN THE FOLLOWING TASKS SCAPY PERFORMS:**

|  |
| --- |
| **FINGERPRINTING:** |

|  |
| --- |
| **DISCOVERING:** |

|  |
| --- |
| **ENUMERATION:** |

**VERIFY YOURSELF AS A USER:**

1. **Open terminal.**
2. **Cd /etc.**
3. **Nano hostname.**
4. **Enter your last name.**
5. **Save and exit.**
6. **Reboot the machine.**

**CAPTURE NETWORK TRAFFIC WHIT SCAPY:**

1. **Open terminal.**
2. **Execute the command “scapy”.**

|  |
| --- |
| **<<< Enter your screenshot >>>** |

1. **Execute the command “sniff(count=20, prn=lambda x: x.summary())”.**

|  |
| --- |
| **<<< Enter your screenshot >>>** |

1. **Explain the parameters of the command used:**

|  |
| --- |
| **<<< Enter your answer >>>** |

1. **Explain that important packets were captured:**

|  |
| --- |
| **<<< Enter your answer >>>** |

1. **Execute the following commands:**
   1. **b=sniff(count=100).**
   2. **Ver=b [50].**
   3. **Ver.pdfdump().**

**Explain the information given by the pdf file.**

|  |
| --- |
| **<<< Enter your screenshot >>>** |

|  |
| --- |
| **<<< Enter you answer >>>** |

1. **Execute the following commands:**
   1. **a=sniff(count=300).**
   2. **a.plot(lambda x:len(x)).**

**Explain the information given by the graphic.**

|  |
| --- |
| **<<< Enter your screenshot >>>** |

|  |
| --- |
| **<<< Enter you answer >>>** |

**(CAPTURE NETWORK TRAFFIC WHIT WIRESHARK):**

**WIRESHARK:**

Multiplatform tool with graphical interface for network analysis. This allows you to see, even at a low and detailed level, everything that is happening on the network. It is open source and multiplatform. It is often used as a better option when auditing networks usually Ethernet networks and is compatible with some others.

**CAPTURE NETWORK TRAFFIC WHIT WIRESHARK:**

1. **Start the other machine.**
2. **Open terminal and start the services apache and mysql with the following commands:**
   1. **Service apache2 start.**
   2. **Service mysql start.**
3. **Execute the command “Wireshark” in the first machine.**

|  |
| --- |
| **<<< Enter your screenshot >>>** |

1. **Start traffic capture.**
2. **Open Firefox browser.**
3. **Enter to (second machine IP) / DVWA**

|  |
| --- |
| **<<< Enter your screenshot >>>** |

1. **Enter to DVWA.**
2. **Enter whit User= “1337” and password=” charley”.**

|  |
| --- |
| **<<< Enter your screenshot >>>** |

1. **Stop traffic capture.**
2. **Filter capture by http.**
3. **Discover the vulnerability and explain**

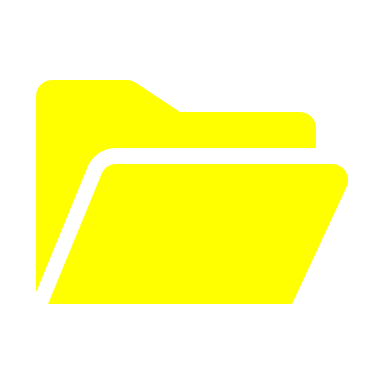
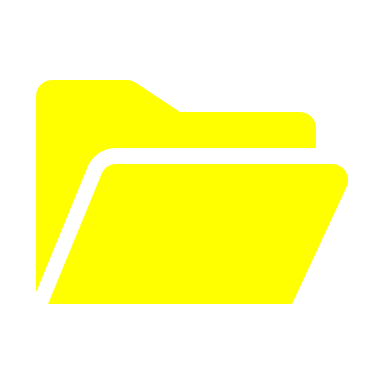
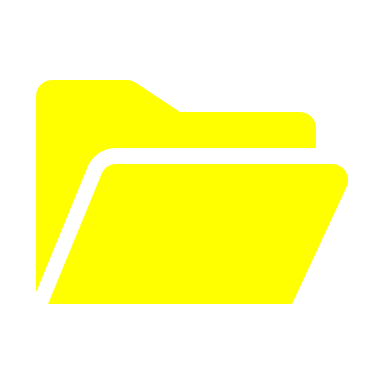
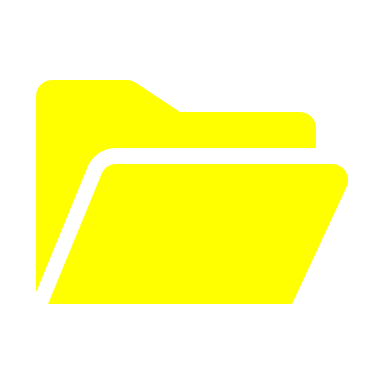
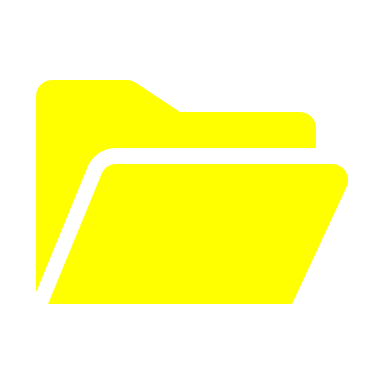
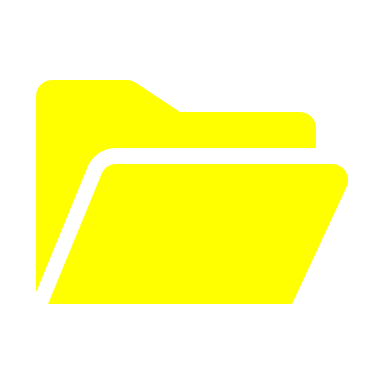
|  |
| --- |
| **<<< Enter your screenshot >>>** |

|  |
| --- |
| **<<< Enter your answer>>>** |

**SECTION TWO**

In section number two we are going to experience how to perform a man attack in the middle. For this we are going to need three machines, two of them sharing information and a third one that is going to be the spy or attacker, all within the same network.





Web Client

192.168.1.155

Internet Information Server

192.168.1.211

Man in the middle

192.168.1.204

When you have the machines running, check the IP's and MAC addresses, you would have to ping between all the machines.

|  |  |
| --- | --- |
| Web Client | **<<< Enter your answer>>>** |
| Internet Information Server | **<<< Enter your answer>>>** |
| Man in the middle | **<<< Enter your answer>>>** |
| MAC Web Client | **<<< Enter your answer>>>** |
| MAC Internet Information Server | **<<< Enter your answer>>>** |
| MAC Man in the middle | **<<< Enter your answer>>>** |

**Verification of the connection of all machines.**

|  |
| --- |
| **<<< Enter your screenshot >>>** |

|  |
| --- |
| **<<< Enter your screenshot >>>** |

|  |
| --- |
| **<<< Enter your screenshot >>>** |

Note that MAC addresses must be different:

1. **Run the following command "ifconfig eth0 down".**
2. **Run the following command "macchanger -A eth0" and explain what -A is for in the command.**

|  |
| --- |
| **<<< Enter your answer >>>** |

1. **Run the following command "ifconfig eth0 up".**

|  |
| --- |
| **<<< Enter your screenshot machine 1 >>>** |

|  |
| --- |
| **<<< Enter your screenshot machine 2>>>** |

1. **Verify with the command "ifconfig" that the MAC address was changed.**

|  |
| --- |
| **<<< Enter your screenshot machine 1>>>** |

|  |
| --- |
| **<<< Enter your screenshot machine 2>>>** |

1. **Finally, check the ARP tables of each machine with the command "arp" and "arp -a" in Windows.**

|  |
| --- |
| **<<< Enter your screenshot machine 1>>>** |

|  |
| --- |
| **<<< Enter your screenshot machine 2>>>** |

|  |
| --- |
| **<<< Enter your screenshot machine windows >>>** |

**SECTION THREE**

Config the internet information server with the following steps:

1. Go to control panel.
2. Go to programs and features.
3. Go to turn windows features on or off.
4. Search the item “Internet information services” and active.
5. Save the changes.
6. Change the folder “wwwroot” by the given. The folder is locater a C:/inetpub/wwwroot
7. Verified that the page http:IPWindows/Loggin.html works.

|  |
| --- |
| **<<< Enter your screenshot >>>** |

As we have the three machines connected in the same network, we will proceed to intercept packets with wireshark, for this you will have to execute the command "wireshark" in the spy machine, in addition you will have to disable the capture of packets in promiscuous mode.

|  |
| --- |
| **<<< Enter your screenshot >>>** |

To continue we must make sure that our ARP tables are spoofed clean, so we will remove their content on the server and client machines. Run the command "ip -s -s neigh flush all" for linux and “netsh interface ip delete arpcache” for windows.

|  |
| --- |
| **<<< Enter your screenshot >>>** |

|  |
| --- |
| **<<< Enter your screenshot >>>** |

Now open the browser from the client machine and go to the following address: http:IPWindows/Loggin.html

Stop capturing wireshark.

**Now display the server and client ARP tables:**

|  |
| --- |
| **<<< Enter your screenshot >>>** |

|  |
| --- |
| **<<< Enter your screenshot >>>** |

Did the spy machine see the connection? Why? explain with a diagram how the data traveled.

|  |
| --- |
| **<<< Enter your answer >>>** |

**SECTION FOUR**

Next, let's tell the client that the IP address of the server is in our MAC address, but before we do that, we should think about the consequences that this would bring. If from the spy machine we have a web server and we answer the requests, the client will realize it, so we will make the spy redirect the packets to the appropriate host so that it responds with the appropriate data. The spy will be in the middle of the connection and no one will notice.

Now our first step is to configure the machine that listens behind the scenes to redirect the packets to their legitimate final destination.

**How is this possible with the information the IP header is providing? Why is it crucial that the eavesdropper’s computer’s ARP tables are correct?**

|  |
| --- |
| **<<< Enter your answer >>>** |

Kali Linux provides a tool that among other uses allows to redirect IP packets to their legitimate destination: fragrouter.

**Execute the following command "fragrouter -i eth0 -B1" and explain what "fragrouter" works best and what "B1" is for.**

|  |
| --- |
| **<<< Enter your screenshot >>>** |

|  |
| --- |
| **<<< Enter your answer >>>** |

Now that the redirections are configured, we proceed to perform the ARP spoofing. So, run Wireshark and have it listened to on the network. Make sure you don't turn on promiscuous mode.

**Execute the command "man arpspoof" and explain what arpspoof is for and what is the difference between "target" and "host".**

|  |
| --- |
| **<<< Enter your screenshot >>>** |

|  |
| --- |
| **<<< Enter your answer >>>** |

**Run the command "arpspoof -i eth0 -t (IP WebClient) (IP Attacker) " set it to its IP addresses.**

|  |
| --- |
| **<<< Enter your screenshot >>>** |

Arpspoof is now running. Now run the client again. Before you stop Wireshark, check the ARP tables on both the client and server machines, then cancel (stop) arpspoof with Ctrl-C, and when it’s stopped, stop Wireshark’s sniffing.

**What happened this time? Can you now see both sides of the client-server conversation? Why?**

|  |
| --- |
| **<<< Enter your answer >>>** |

**why was it necessary to use the -t flag on arpspoof?**

|  |
| --- |
| **<<< Enter your answer >>>** |

**Draw a diagram that includes all three computers and illustrate how the connection was established and the data travelled.**

|  |
| --- |
| **<<< Enter your answer >>>** |

**ARP tables are cleared by the OS on a regular basis. To counter this, arpspoof sends lots of ARP replies. Do you think that this policy on the OS is a good or bad one? Please elaborate on your answer.**

|  |
| --- |
| **<<< Enter your answer >>>** |

**This attack allowed us to read information, but there are many small networks where this is possible by only sniffing the network on promiscuous mode. What application would need to change if we wanted to -change- packets as they travel? How? Why would someone want to do that?**

|  |
| --- |
| **<<< Enter your answer >>>** |

**How can a network administrator prevent this type of attacks on a network? How can they be logged? (The attacks, not the netadmin).**

|  |
| --- |
| **<<< Enter your answer >>>** |

**If a user’s computer is prone to this type of attacks, what can he/she do to avoid having his/her data read by a third part? What about being supplanted? How about being both read and written?**

|  |
| --- |
| **<<< Enter your answer >>>** |