

Lab 2

CSCI6658-01 & Lab #2.1/2.2

Enumerating Hosts Using Wireshark, Windows, and Linux commands & Remote and Local Exploitation

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| TC-Github |  |  |  |  |

Table of Contents

1. [Executive Summary 2](#_Toc128249240)

[Lab 2.1](#_Toc128249241)

[LAB 2.2](#_Toc128249242)

[Objectives](#_Toc128249243)

1. [Lab Description Details 2](#_Toc128249244)

[LAB 2.1](#_Toc128249245)

[LAB 2.2](#_Toc128249246)

1. [Supporting Evidence 4](#_Toc128249247)

[LAB 2.1](#_Toc128249248)

[LAB 2.2](#_Toc128249249)

1. [Conclusion & Wrap-Up 13](#_Toc128249250)

[Summary with observations, Success & Failures, Challenges](#_Toc128249251)

# Executive Summary

## Lab 2.1

Within this lab the execution of certain Armitage commands which will provide an analysis and assessment of the system in question. Along with this there will be a section in with system commands will be used to list the resources being used on the target computer to detect where the vulnerability is.

## LAB 2.2

For this lab there will be the scanning of multiple hosts on a local area network configuration. This will be aided by Metasploit package and the Armitage package to exploit a machine with a multitude of different methods of attack.

## Objectives

Lab 2.1

* Use Armitage to scan a network.
* Commands such as ifconfig, nmap, postgressql will be used along with open-source distributions such as Kali Linux, Wireshark, and PostgreSQL
* Use the system commands to enumerate and list resources on a target system.

Lab 2.2

* Utilize nmap to do a ping scan on a network and a database scan as well.
* Use the tool Metasploit and Armitage to exploit multiple vulnerabilities within the system and its severs (breach the server)

# Lab Description Details

## Procedure

## LAB 2.1

* Log into Kali 2 Linux machine with 192.168.1.101 as its IP address
* Enter the user / pass = root / toor
* To check the ip address of the system type in the command ifconfig to list the ip address and its properties of the machine you are connected or remote hosting.
* To save an ipconfiguration to a file type the ifconfig > ip1.txt in order to save the information to be viewed with the cat ip1.txt command for fither research and in order to find the flag type in cat ip2.txt in order to retrieve flag 1
* Next step is to ensure that your system does not have an ip address by executing this command ifconfig eht0 0.0.0.0 up you can verify this has worked by typing ifconfig
* Proceed to Wireshark where you will capture traffic on the eth0 port ensure that the ip addresses 192.168.1.10, 192.168.1.20, 192.168.1.254 appear in the network traffic in order to continue with the procedure
* Return to the root kali2 command line and set up the network ip address and the network mask by using this command – ifconfig eth0 192.168.1.101 netmask 255.255.255.0 and add the default gateway by typing in route add default gw 192.168.1.254 then create a backup of the current reserve file with cp /etc/resolv.conf /etc/resolv.conf.backup1 and then utilize the car /etc/resolv.conf.bakcup command to view the resolve backup file use this same method (figure 2) to retrieve the challenge flag.
* Utilize echo nameserver 192.168.1.10 > /etc/resolv.conf command in order to set the DNS server you can utilize the command cat/etc/resolv.conf in order to view into the file associate and utilize this same method to secure the challenge flag (figure 4)
* Continuing onwards begin next step by loading into the windows 10 virtual machine sign out of the Microsoft account (ctrl + alt + delete bottom right corner sign out)
* Sign into the machine as a new user the user of administrator utilizing P@ssw0rd proceed to run the command prompt as administrator execute the following commands to enumerate all domains net view /domain.
* Net view /domain:campus to get more specific start entering other things located on a domain such as this command net view /domain:workgroup and then net view [\\server](file:///\\server) in order to enumerate through all the shares on the machine named server
* Utilize the command net view [\\metasploitable](file:///\\metasploitable) to enumerate through the shares on a machine named Metasploitable secure the flag by typing commands picture in figures 5 and 6 for the next two challenge flags
* To enumerate the IP and MAC address of the machine named server utilize the following command in order to run o nnormal server nbtstat -a server and then for the metasplotable machine nbtstat -a METASPLOITABLE (figure 7)
* Next navigate back to the kali 2 attack machine and begin by getting the postgresql service to start by executing the following command service postgresql start next navigating to the cd Armitage file directory and execute the msfconsole in order to load into the Metasploit package on kali linux
* Once inside of the msfconsole begin by executing db\_nmap -T4 -A -v 192.168.1.\* to scan the hosts (Figure 8)
* After hosts are verified and found launch into the armigtage app with the command msf>. /Armitage
* Following the launch begin by organizing the devices listed in a stack format then proceed to scan the printer icon or ip address 192.168.1.254 (Figure 9)

## LAB 2.2

* Begin by loading into Kali 2 OpenVas virtual machine in order to begin the nmap procedure once prompted with the login select other and type root for the username and toor for the password and then proceed to click the terminal icon for linux
* Once within the terminal execute the command nmap 203.0.113.100 –system-dns this will scan the firewall for open ports to exploit (Figure 10)
* Follow this by loading into the zenmap program and put the target ip address as 203.0.113.100 and then select scan once the nmap is done click the Prots/Hosts tab to view the open ports and corresponding banner messages that are displayed and take note of the postgresql port and host that is open close out of zenmap
* Go back to the terminal and execute the command /home/scripts/openvas\_start in order to initialize the OpenVAS scanner once the user prompt is received open the iceweasel browser type in the following into the search bar <https://127.0.0.1:9392> continue by allowing the connection to go through by clicking I understand the risks and then add exception
* When prompted to accept the security exception click confirm security exception you will then be promoted with a log in type in admin, admin for the username and password.
* Once logged in proceed to enter the IP address 203.0.113.100 to be scanned the following screen will appear click on the percentage complete to ensure that the scan is fully completed (figure 11)
* Click on the date in order to see all the scans done and click on the one that is postgresql weak password and then read into the vulnerability result and see that you can login to the user postgres with the password postgres
* After ensuring you can attack on that port with this new knowledge proceed to the kali 2 Metasploit external address virtual machine and enter root/toor as user/pass
* Go into the terminal and typ e in service postgresql start to start that service and after entering the command masfconsole and then banner this will then display how many exploits are available (figure 12)
* Following detecting the exploits available search for the known one with the command search postgres\_login
* After utilize the command to use the PostgreSQL login aux model and the command is use auxiliary/scanner/postgres/postgres\_login once in use the command info in order to see more then notice the USERNAME postgres on this machine we have all we need now we know that this does exist
* Now being a remote host in to the target IP address with the following command set RHOSTS 203.0.113.100, then use the set USER\_AS\_PASS true and enable stop on success with set STOP\_ON\_SUCCESS true (figure 14)
* After exploiting the system utilize the command execute -f /bin/bash -i, then navigate to /var/lib/postgresql/8.3/main$ whoami then type in cat /etc/shadow select y to terminate the channel then type background (Figures 15 – 16)
* After begin to execute commands to search udev\_netlink and the use exploit/linux/local/udev\_netlink then use this to execute the payload on the computer after set SESSION 1 command is entered select exploit enter the commands execute -f /bin/bash -i then whoami then tail/etc/shadow then tail/etc/passwd (figures 15 -16) (These commands were the same used in the above step as well this was replicating in order to retrieve the flags associated with these specific commands)

# Supporting Evidence

## LAB 2.1

Text

Description automatically generated

Figure 1

Text

Description automatically generated

Figure 2

Text

Description automatically generated

Figure 3

Graphical user interface, application

Description automatically generated

Figure 4

Text

Description automatically generated

Figure 5

Text

Description automatically generated

Figure 6

Text

Description automatically generated

Figure 7

Graphical user interface, text

Description automatically generated

Figure 8

Graphical user interface

Description automatically generated

Figure 9

## LAB 2.2

Text

Description automatically generated

Figure 10

Graphical user interface, email, website

Description automatically generated

Figure 11

Text

Description automatically generated

Figure 12

Text

Description automatically generated

Figure 13

Text

Description automatically generated

Figure 14

Text

Description automatically generated

Figure 15

Text

Description automatically generated

Figure 16

# Conclusion & Wrap-Up

## Summary with observations, Success & Failures, Challenges

To conclude for all labs since this was done in a controlled environment and every flag for each section of the lab was found with minimal to no error these labs included enumerating Host Using Wireshark, windows, and linux commands and remote and local exploitation. Each task that was listed within the objectives for each of the labs was successfully completed, refer to supporting evidence section and notes within the procedure to find specific evidence of all flags found within the labs) The main draw back of this lab was waiting for the proper network traffic to appear when in the enumerating a host with Wireshark, in this it was needed that three IP addresses would appear and it took about an extra two minutes more than the 5 listed. Other than that there were no errors within the lab and it was executing to the specifications of the guided lab environment with the premade attack and victim machines. In turn it was a success in scanning through a network in order to retrieve certain information by scanning network files and documents containing flags, along with this in the remote and local exploitation the machine was able to be logged into through the use of exploitations through Metasploit and using vulnerability detecting server iceweasel to find the port for postgresql had the username and password set as postgre and postgre. Then led to the exploitation on this machine. In general each of the proposed goals for each of the labs were met and successfully executed.