CYSE425

Mahish Mahendarkar

9/12/2021

Lab 1: Reconnaissance/Enumeration/Vulnerability Scan/Exploitation

Lab 1 purpose:

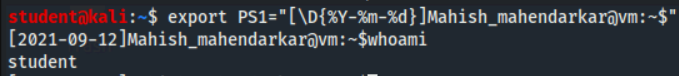
The purpose of this lab is to understand how to carry out a cyber attack with the intent of gaining root user privileges. There is a target system that is surveilled, attacks are drawn up, then the attack is run via a prefabricated framework.

**Reconnaissance**

The purpose of this reconnaissance is to find out

Pre-Lab configuration settings:

* A Virginia Cyber Range Virtual Machine is used for all Lab activities. This is logged into and hostname is changed as shown below.



Lab tasks:

1. Logon to Kali/Open Terminal/Run Route

This task dealt with the setting up of the terminal and the recon process.

**NETWORK ID: 10.1.128.0**

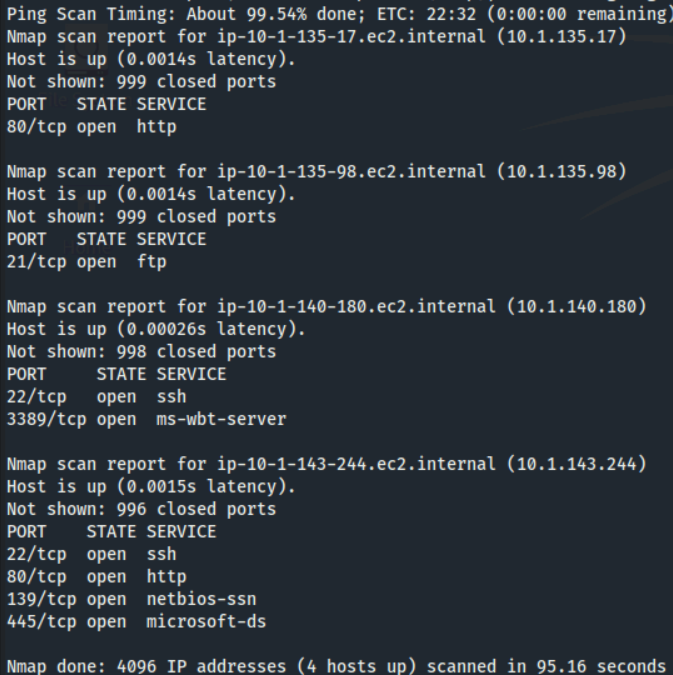
**Text

Description automatically generated**

Observations: This task had no issues or errors. Cyber range was joined and the cyber basics VM was turned on and used for this lab. The route command displayed output in an expected manner.

1. Run nmap

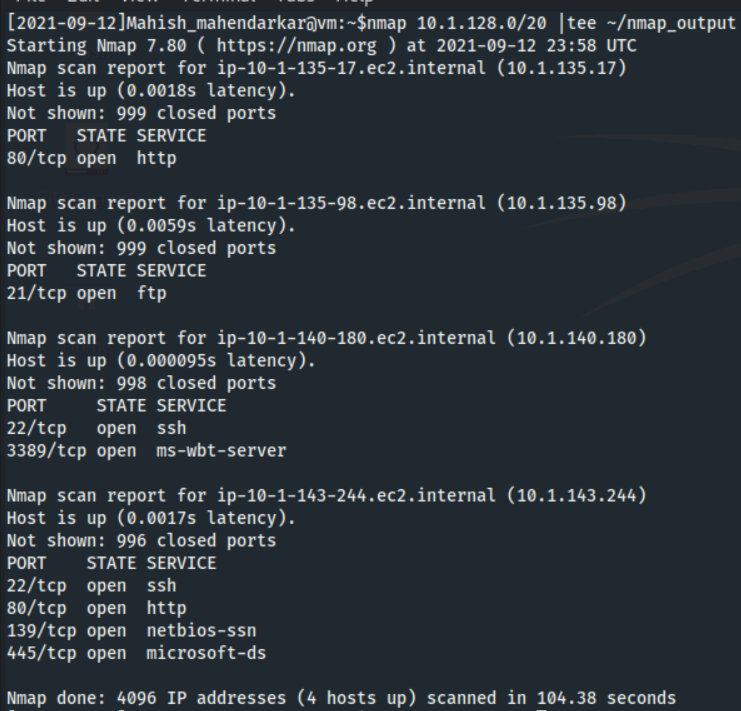
This task is focused on running a nmap scan on a specific target and successfully gaining new information.



Observations: This task was straightforward. The nmap command worked with the [/20] CIDR and the status of the attack was checked twice. The displayed results were as expected and the ports 22/80/139/445 were found to be open at the target.

1. Save nmap

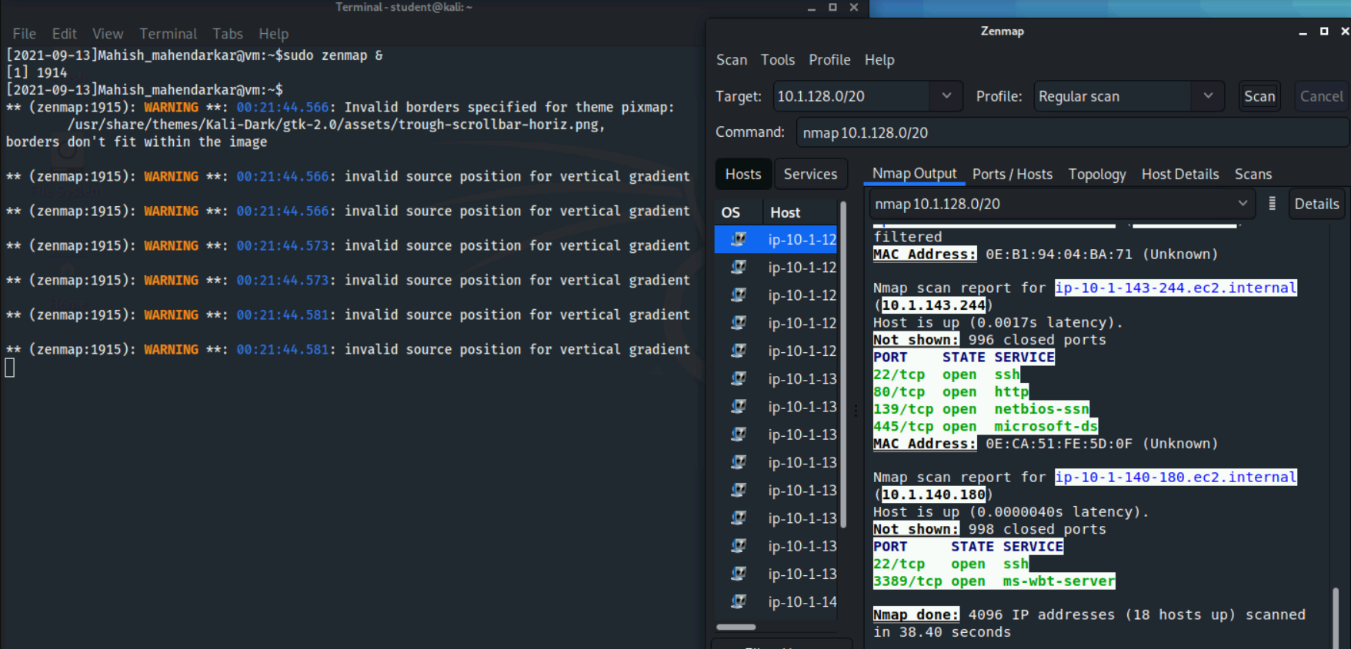
This task is focused on collecting the nmap data into a file format for future use.

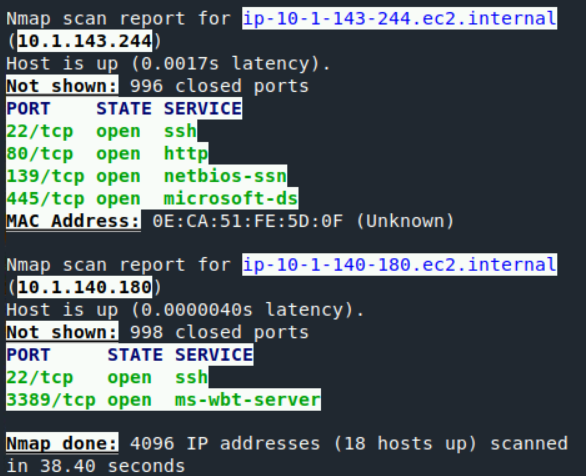




Observations: This task had no issues or errors. The commands ran successfully and a new file was created that had the same data as the nmap results.

1. Scan with zenmap





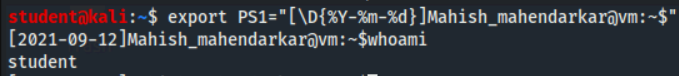
Observations: This task had no issues. The **zenmap results were more detailed (MAC addresses were shown).** The results were the same the zenmap provided more detail and latency statistics.

**Enumeration**

This lab will demonstrate the use of various Tools, Techniques, and Procedures for the enumeration of hosts discovered on a network. In network penetration testing, enumeration is the act of examining or observing a specific host or target to generate a list of services and ports for possible exploitation. A penetration tester will use enumeration to locate ports, services, and software versions for possible exploit during the penetration test.

Pre-Lab configuration settings:

* A Virginia Cyber Range Virtual Machine is used for all Lab activities. This is logged into and hostname is changed as shown below.



Lab tasks:

1. Examine the nmap results from the Reconnaissance task

The contents of the previous nmap scan file are opened and searched.

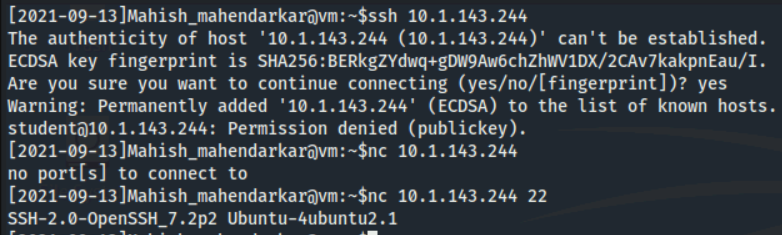
Text

Description automatically generated

Observations: This task worked as expected. The **specific host 10.1.143.244 had the ports 22/80/139/445 open.** This new target IP will be used in later steps. The open ports will probably be used to carry out the attack.

1. Enumerate port22 SSH

This task is focused on finding and ordering the useful information about port 22 that can be used to carry out an attack.



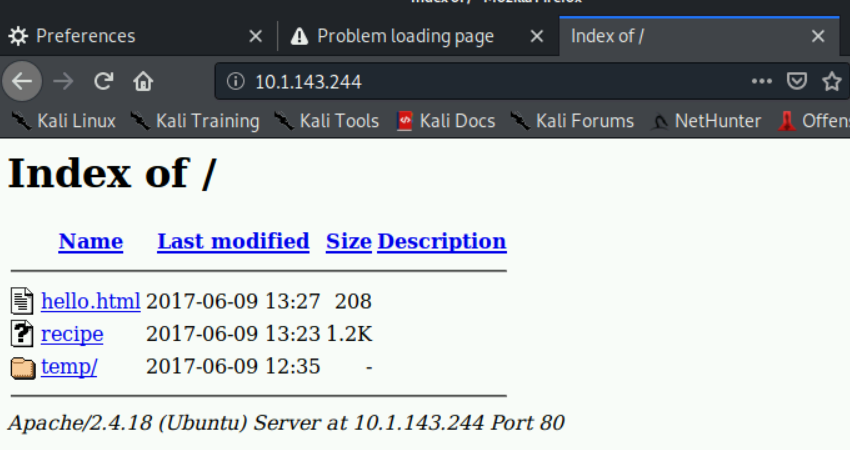
A screenshot of a computer

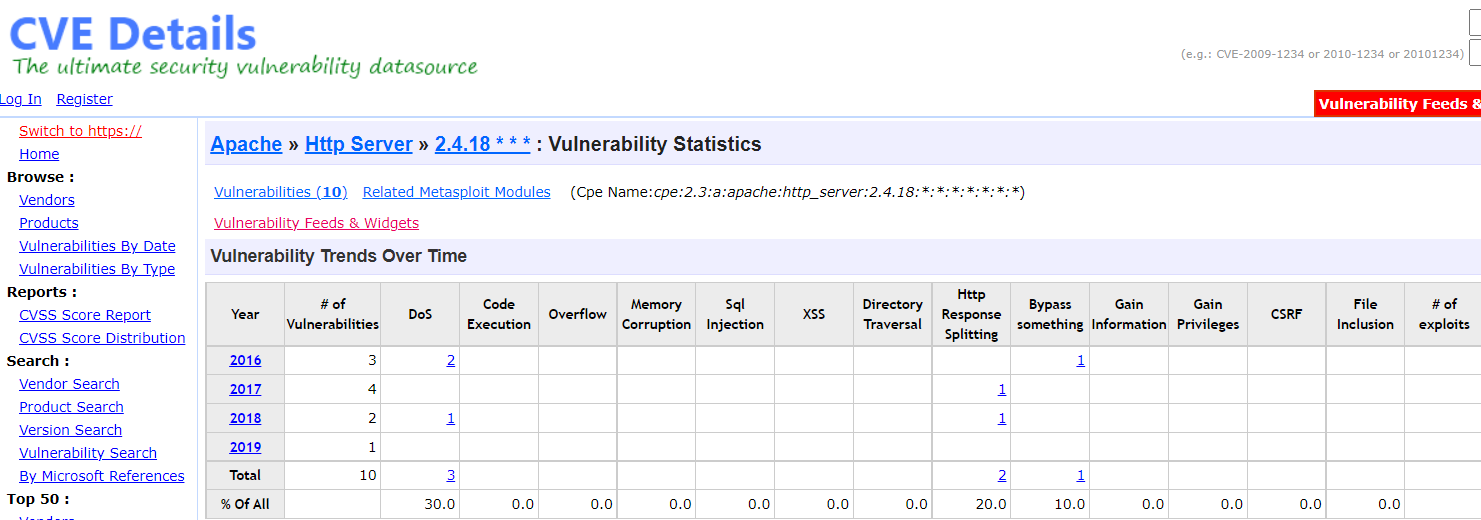
Description automatically generated

Observations: This task had no issues. The SSH server did not have any remote code execution vulnerabilities or any vulnerabilities currently active to use.

1. Enumerate port 80 HTTP

This task is focused on finding useful information about port 80 that can be used to carry out an attack.

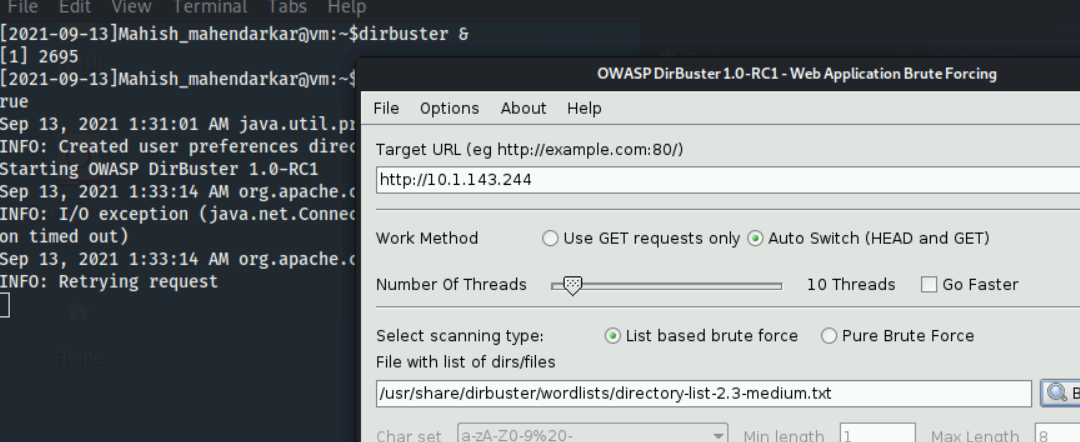


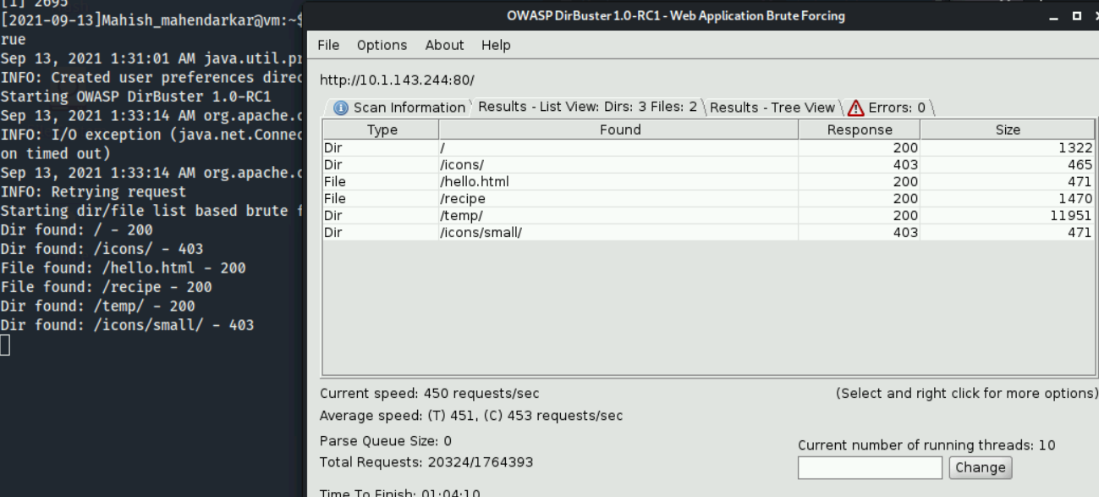


Observations: This task was straightforward. The previously found target address was accessed. There are no active exploits for this server.

1. Web Server directory enumeration using Dirbuster

This task uses dirbuster software to enumerate hidden files and directories.





Observations: This task used a powerful enumeration software and displayed all the information on the target. The files and directories did not contain any active exploits.

1. SMB port 445 enumeration using Nmap Scripting Engine

This task involves enumerating port 445 by using a prefabricated script designed to exploit the SMB protocol.

A screenshot of a computer

Description automatically generated with medium confidence

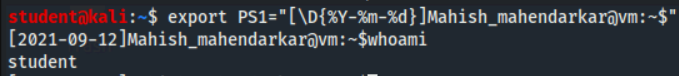
Observations: This task yielded interesting results. There was a vulnerability in Samba4.6.0 and this will be further exploited. The CVE was not found but the lab instructions detailed how to exploit the current systems in their current configuration. Metasploit software will be used to target the Samba 4.6.0 system via the SMB 445 protocol.

**Vulnerability Scanning**

The purpose of this reconnaissance

Pre-Lab configuration settings:

* A Virginia Cyber Range Virtual Machine is used for all Lab activities. This is logged into and hostname is changed as shown below.



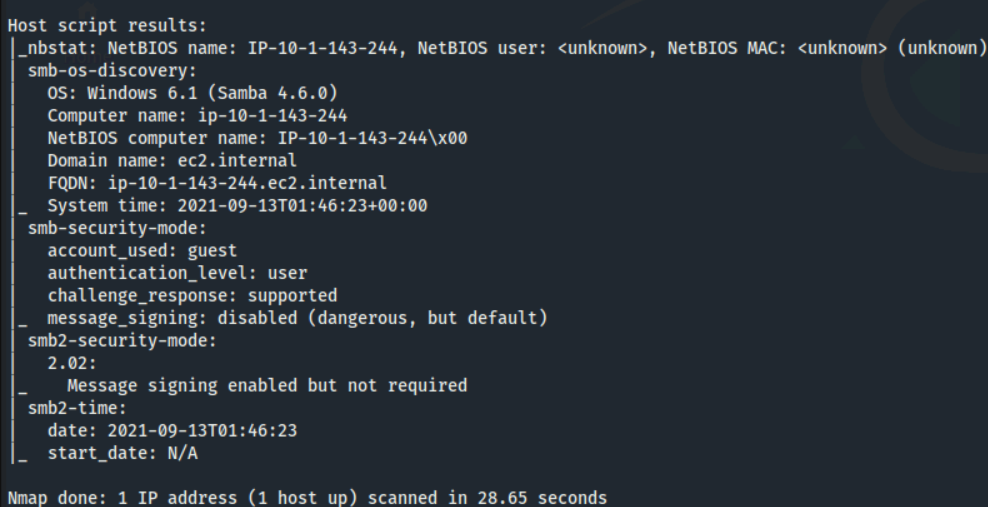
Lab tasks:

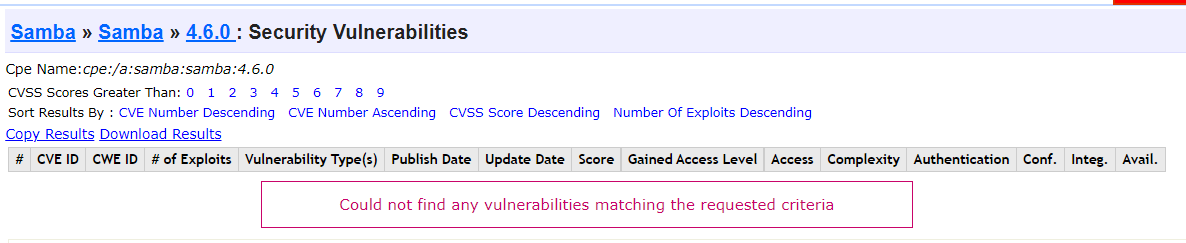
1. Use nmap scripts to scan for vulnerabilities

This task is focused on running a scripting program to find out more information about the target system.

Text

Description automatically generated





Observations: This task was successfully completed. Finding active exploits was hard because this vulnerability has clearly been patched but some research on SMB vulnerabilities was conducted.

1. Use Nikto to scan for vulnerabilities

This task uses Nikto software to scan the target for vulnerabilities.

Text

Description automatically generated

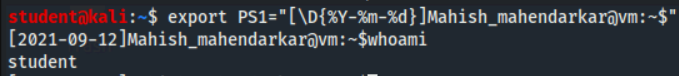
Observations: This task was completed successfully and the lab instructions explain what the final Lab objective will be. An important thing to note are the OSVDB numbers. This will be useful for future recon and vulnerability assessments.

**Exploitation**

The purpose of this reconnaissance

Pre-Lab configuration settings:

* A Virginia Cyber Range Virtual Machine is used for all Lab activities. This is logged into and hostname is changed as shown below.



Lab tasks:

1. Examine the details of the vulnerability

This task involved reading the CVE being used to carry out the exploit.

Graphical user interface, text, application, email

Description automatically generated

Observations: This task was informative and was up to date information on all aspects of the CVE.

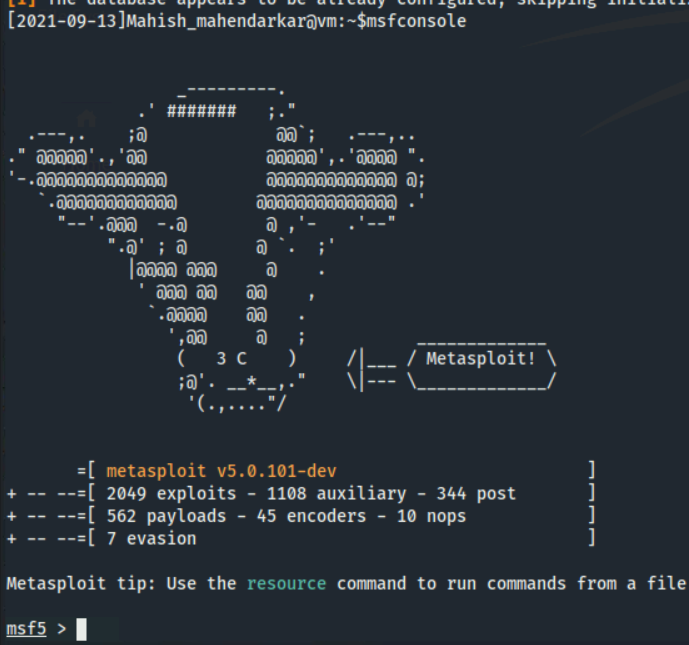
1. Start Metasploit

This task involves setting up the correct parameters to be able to run the

Metasploit software.

Text

Description automatically generated



Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Observations: This task was successful. The commands were displayed and the metasploit software booted up without any issue and the CLI prompt became a >. Root user access was gained and a bash shell was obtained as well.

Lab notes: TCP ports 22/80/139/445

Nmap(need target IP/CIDR) – zenmap (GUI version)=== need IP/CIDR – nmap networkID/CIDR

Route (command for finding network ID)

Nmap netowrkID/CIDR > output\_file (no display)

Nmap netowrkID/CIDR | tee output\_file(display)

nmap -sC target\_ip (safe to run scripts – no breaking of target system)

nikto -host target\_ip (scanner – common vuln – shows vuln and OSVDB number)

nc target\_ip 22 (connect to any port given IP)

change browser proxy settings before enumeration of port80(HTTP) - TCP Port 80 is the port of a web server

dirbuster target IP needed

SMB port445 – scripting engine -- nmap --script smb-os-discovery.nse target\_ip

Msfconsole interact with Metasploit framework of scripts (service postgresql start - sudo msfdb init – msfconsole == msf prompt on CLI)

python -c ‘import pty; pty.spawn(“/bin/bash”)’ == python shell bash in targeted system

---------------------------------------------------------------------------------------------------------------------