Setup NAT Network

Click On Tools Menu Icon -> Select Network -> Go To NAT Network Tab -> Right Click On Empty Space And Click On Create -> Edit The Generated NAT Network -> Provide Name And Assign IP: 192.168.100.0/24 -> Check Enable DHCP Checkbox -> Click On Apply.

Assign NAT Networks To Machines

Right Click On Created Virtual Systems -> Select Settings -> Go To Network Section -> Select NAT Network In Attached To Dropdown -> Select Name Of Created NAT Network -> Select Promiscuous Mode To "Apply All" -> Click Ok.

Githublink: type "github syn flood ethical hacking" in google search and open first link.

A. Use the following tools to perform footprinting and reconnaissance.

i. Ping **ii. Tracert**

i. -> Ping

Step1: Open Windows Command(cmd) Line in Windows PC.

Stpe2: Enter The Command "Ping www.google.com" to ping.

Step3: Observe the following values: "www.google.com" is live, IP address of example.com, Round Trip Time, TTL value, Packet loss statistics.

ii. -> Tracert

Step1: Open Windows Command(cmd) Line in Windows PC.

Step2: Enter The Command "Tracert www.google.com" to ping.

Step3: From the output, you can get the information about hops between the source (your PC) and the destination (www.google.com), response times and other information.

Note: to perform Tracert using tools use any of the following tools: Path Analyzer Pro, Visual Route, Troute, 3D Traceroute.

B. Demonstrate the use of ADS Spy.

Step1: Open Windows Command(cmd) Line in Windows PC.

Step2: type the following command to create a file named file_1.txt. (echo "this is file no 1" > file_1.txt)

Step3: type the following command to write to the stream named secret.txt. (echo "this is a hidden file inside the file_1.txt" > file_1.txt:secret.txt)

Step4: The following command can be used to view or modify the stream hidden in file_1.txt (notepad file_1.txt:secret.txt)

Step5: Open the ADS spy tool.

Step6: As we store the file in the Document folder, Selecting Document folder to scan particular folder only.

Step7: Select an Option, if you want to scan for ADS, click "**Scan the system for ADS**"/ or click **removes** button to remove the file

Step8: Verify the created file will show as follows: ADS Spy has detected the **Testfile.txt:hidden.txt** file from the directory.

A. Demonstrate the use of Smart Whois to perform footprinting and reconnaissance.

Step1: Go to the URL **https://www.whois.com or https://whois.domaintools.com** A search of Target Domain.

Step2: You can download software "***SmartWhois***" from ***www.tamos.com*** for Whois lookup.

B. Demonstrate the use of Snow.

Step1: Create a text file with some data in the same directory where Snow Tool is installed.

Step2: Go to Command Prompt Change the directory to run Snow tool

Step3: Type the command

(Snow –C –m "text to be hide" –p "password" <Sourcefile> <Destinationfile>)

Step4: Go to the directory; you will see a new file **HelloWorld.txt**. Open the File, New File has the same text as an original file without any hidden information. This file can be sent to the target.

Step5: Recovering Hidden Information, On destination, Receiver can reveal information by using the command (Snow –C –p "password123" HelloWorld.txt)

B. Demonstrate the use of megaping.

Step1: Open the megaping application in your windows machine.

Step2: Go to "IP scanner" section and enter the IP range that you want to find.

Step3: Go to "port scanner" section and enter the target IP(listed in IP scanner step). And click on Start.

Step4: It will display all the open/ associated ports with the target.

A. Use wireshark and show password sniffing.

Step1: Open Kali Linux and launch the Wireshark Tool.

Step2: Open browser in Kali Linux and open following link http://testphp.vulnweb.com or type “vulnweb” on goolge.

Step3: Go to Wireshark -> Click on Capture button “capture Options” -> select all checkboxes and click on start.

Step4: Go to website -> sign up/login page -> enter any username and password. And click on sign up/login.

Step5: Go to wireshark and click on “stop capturing” button.

Step6: In Filters field enter following command “ http.request.method == "POST" “ or “ http.request.method == "GET"”.

Step7: Check the filtered results and check for login credentials.

B. Demonstrate Network scanning using any tool of your choice.

Use the following tools for network scanning:

i. Hping2 / Hping3
ii. Advanced IP Scanner
iii. Angry IP Scanner
iv. Masscan

A. Use Kali Linux and demonstrate the use of NMAP on Kali Linux.

For windows use the following tools: Zenmap, SuperScan, Hyena.

For Kali Linux:

1. nmap -sn <target ip address> sn: Just discover the live hosts without attempting to determine any specific ports that are open or any services(in-short scans host is up or down).
2. nmap -O <target ip address> O: Operating system detection.
3. nmap -A <target ip address> A:Aggressive what version running on the specific server.
4. nmap -f <target ip address> f:Sends fragmented packets to the target host aiming to bypass firewall rules or packet filtering, that might block a typical scan.

B. Demonstrate the use of Angry IP scanner and Advanced IP scanner

Step1: Download Angry IP scanner & Advanced IP scanner from there websites.
Step2: launch the S/W and enter the IP or IP range and click on Start.

A. Use Metasploit for Ddos attack.

Step1: select your target's IP address http://testphp.vulnweb.com
Step2: Get an IP address of the above URL, using Ping command i.e ping <URL>
Step3: Now run the console using superuser.
Step4: Launch the Metasploit console using "msfconsole" command.
Step5: Select the auxiliary using following command "use auxiliary/dos/tcp/synflood"
Step6: Now type "show options" command.
Step7: Now you can see you have all the available options that you can set, To set an option just you have to typeset and the option name and option.
Set two main options:

RHOST= target IP Address(e.g 192.168.0.2)
RPORT=target PORT Address(e.g 80) if RPORT is already 80 don't set it, just set RHOST.

Commands as follows: "Set RHOST target ip" hit enter "Set RPORT port number".
Step8: To launch the attack type command "exploit".
Step9: To see the packets, open Wireshark and start capture.

A. Use Metasploit for information gathering and show any two possible outcomes.

<u>Prerequisites: Set up the NAT network.</u>

Step1: Run Kali Linux and open Metasploit tool.
Step2: enter "db_status" command.
Step3: enter command nmap -Pn -sS -A -oX Test <private ip range> e.g 10.10.0.0/24
Step4: enter command "db-import Test"
Step5: enter command "hosts".
Step6: enter command "db_nmap -sS -A <last largest ip>"
Step7: enter command "services".
Step8: enter command "use scanner/smb/smb_version".
Step9: enter command "show options".
Step10: enter command "set RHOSTS <start first ip - last ip>" e.g: 10.10.0.2-12
Step11: enter command "set THREADS 100/50"
Step12: enter command "show options"
Step13: enter command "run".
Stpe14: enter command "hosts".
Step15: check to columns for information. Observe the OS_Flavor field. SMB scanning scans for Operating System Flavor for the RHOST range configured.

B. Use Colasoft packet builder and create multiple data packets and send them to nearby IP

Step1: Download the software from www.colasoft.com
Step2: Open the application.
Step3: Add a new packet by clicking Add/button. Select the Packet type from the drop-down option. Available options are: - ARP Packet, IP Packet, TCP Packet, UDP Packet
Step4: After Selecting the Packet Type, now you can customize the packet, Select the Network Adapter and Send it towards the destination.

A. Scan the network in your lab and show the network layout. Use any tool of your choice. Make sure the tool used is apt for the demonstration.

Use the following tools to perform above operation:
Solar Wind Network Topology Mapper, OpManager, Network View, LANState Pro

B. Use emailtrackerpro and trace an email address.

Step1: Download emailtackerpro tool in windows.

Step2: launch the tool.

Step3: Click on Trace Headers/Trace email address and enter the Message Header and click Okay.

Step4: The Status of the Trace will be shown inside Trace Reports.

A. Demonstrate the use to HTTrack Website copier

Step1: Download and Install the WinHTTrack Website Copier Tool from the website **http://www.httrack.com.**

Step2: Install and launch the tool.

Step3: Enter the project name.

Step4: Add any website URL that you want to download.

Step5: click on set options button.

Step6: Click next and wait for process to finish.

Step7: Click Browse Mirrored Website.

B. Demonstrate enumeration using any two tools of your choice.

i. Use Zenmap tool in windows, enter following command “nmap -O <ip address>”

ii. NetBIOS Enumeration Tool in linux, enter following command “netstat -a>”

iii. SoftPerfect Network Scanner Tool and Hyena tool in windows, enter the ip range.

A. Explain steganography concept using any tool of your choice.

Step1: Open QuickStego application.

Step2: Upload an image and upload a text or enter text.

Step3: Click on hide text button.

Step4: save image

Step5: Recover the hidden text using QuickStego -> open saved image -> click on get text.

B. Demonstrate the use of Rainbowcrack using online tools.

Step1: Download tool Winrtgen rainbow tables generator in windows.

Step2: Open the tool and Click on "**Add Table**". After this, a new box will appear named "**Rainbow Table Properties**"

Step3: set Hash = lm, min length = 1, max length = 7, index = 0, chain length = 2400, chain count = 100000, no. of tables = 1, charset = all-space

Step4: click on benchmark then click on Ok. This will add the Rainbow Table to the queue in the main window of WinRTGen.

Step5: Select the Rainbow table that you want to process then click ok.

A. Demonstrate the use of Omnipeek network analyser.

Step1: download ominpeek network analyser tool in windows, And proceed further.

A. Use Hashcalc and show the file hash.

Step1: Download and open hashcalc tool in windows.

Step2: create new text file with some content in it.

Step3: select data format as file and upload file.

Step4: select hashing algorithms and click calculate.

Step5: now select the data format to text string and enter any string.

Step6: Select hashing algorithms and click calculate.

B. Demonstrate the concept of cryptography using any tool of your choice.

Step1: Download and install Advanced Encryption Package tool in windows.

Step2: Select the file you want to encrypt.

Step3: select password and Select algorithm and click encrypt.

Step4: Compare both files.

Step5: Load the encrypted file for decryption in Advanced Encryption Package tool, enter password and click ok.

A. Demonstrate web server attacks using Httprecon and IDserve

Step1: Open ID serve tool in windows enter the target URL or ip address click on query the server button.

Step2: Copy the displayed information and paste it in notepad.

Step1: Open httprecon tool in windows enter the target URL or ip address click on analyze.

Step2: Validate the displayed information.

A. Demonstrate the use of ProRat.

Step1: Download and install Prorat in windows if possible v1.9.

Step2: Click on create new server.

Step3: Add image file to bind with server.

Step4: Copy the created server in the target’s system and open that file.

Step5: Open Prorat in main system again and enter the target’s Ip address and click on connect, if connection is established then it will show connected.

Step6: Now you can check the target’s PC’s details and many more things.