STANDARD OPEARTION PROCEDURE

Information Gathering

Web Search:

Input:
Target's Name.

Tools:
Search Engines (Google, Yahoo, MSN etc.).

Steps:
1. Enter target's name on the search bar and hit enter.
2. Browse through each and every possible information obtained by the target's home page and from third party sources.
3. Save all the relevant information obtained in the previous step.

Expected Output:
The possible information that could be obtained is target's location, contact details including email, mobile numbers and address etc.

Whois Lookup:

Input:
IP Address.

Tools:
Whois Command, Kali Terminal.

Steps:
1. Open kali Linux terminal.
2. Enter Whois commands with <IP address>.
3. Browse finding and save required information in the file.

Expected Output:
The information may include the name of the target's owner, organization, address, contact details including mobile, email etc., domain, server's name and admin's name.

Domain Name Lookup:

Input:
IP address.

Tools:
Dig Command, Kali Terminal.

Steps:
1. Open kali Linux Terminal.
2. Enter dig command along with an <IP address>.

3. Gather the information and save it in the file.

Expected Output:
The output will include DNS name servers information about its host addresses, name servers, mail exchanges, and related information.

Sub-Domain Lookup:

Input:
Web Address.

Tools:
www.netcraft.com

Steps:
1. Go to website i.e. www.netcraft.com
2. Under what's site running, type the target's web address.
3. Save the required findings in a file.

Expected Output:
Gather information regarding target's IP address, DNS Admin, OS, web server, domain etc.

Active OS Fingerprinting:

Input:
IP address.

Tools:
Xprobe2 command, Kali Terminal.

Steps:
1. Open kali Linux Terminal.
2. Enter command and <IP address>, hit enter.
3. Save the information regarding OS in a file.

Expected Output:
This command will provide the information regarding which OS is running on the target machine.

Scanning and Enumeration

In scanning we will find the information regarding open ports on the target machine and their states whether they are opened or not also to learn which services they are running. We will compile our results in a systemic order so that we can find the vulnerabilities of the target system.

Scanning:

Identifying Live Hosts and Services:

Input:
IP address.

Tools:
NMap command, kali Terminal.

Steps:
1. Open kali Linux Terminal.
2. Type nmap [parameter] [optional parameter] <IP address>.
3. Save the required information in a file.

Expected Output:
This command will provide us information regarding the open ports and services running by them, also it give the reasons for the state of the port, and it will also provide us with information of OS running on the target.

Banner Grabbing:

Input:
IP address, Port Number.

Tools:
TelNet command, kali Terminal.

Steps:
1. Open kali Linux Terminal.
2. Use Telnet command as telent <IP address> [port].
3. Type in HEAD HTTP and hit enter.
4. Save the useful information in a file.

Expected Output:
This command will provide us information related to server machine which that target machine is using and with the help of this information we can find the known vulnerabilities in that server.

Enumeration:

Collecting Information:

Input:

The data obtained from the information gathering and scanning phase.

Tools:
Excel spreadsheet or any other spreadsheet.
Steps:

1. Open spreadsheet.
2. Make columns and fill information related to servers found:
   - Open ports.
   - Services.
   - Server Domain names.
   - Server IP.
   - OS information.
3. Save the findings in the final results sheet.

Expected Output:
This procedure will aid the penetration tester to find the information regarding server and the relationship of the server machine with other network devices so that he/she could perform vulnerability scan to get the potential results for vulnerabilities.

Vulnerability Identification and Analysis

In this section-n we will find the vulnerabilities in our target's system, services and OS which can be exploited by identifying potential threats to each resource.

OpenVAS:

Input:
IP address.

Tools:
OpenVAS.

Steps:

1. Open the terminal to initialize OpenVAS.
2. Check the username and password.
3. If not redirected to the browser automatically then go to http://127.0.0.1:9392.
4. Log in to Greenbone Security Assistant.
5. Go to immediate scan and type the target's IP address.
6. The results will start to appear on the screen after sometime, click to explore the information.
7. Save all the results in form of a report under 'Report' section and save it in PDF and XML format.

Expected Output:
The report will include the list of vulnerabilities along with a specified port number. It will also tell the score of severity and its impact. Moreover the report will also explains the algorithms and will provide a feasible mitigation strategy. It is also expected that the results may contain false positive scenarios and penetration tester must look in to it and exclude the information.

Examine Vulnerabilities Exposed Online:

Input:
CVE Number and Keywords.

Tools:
CVE and CERT databases.

Steps:

1. Go to https://www.cvedetails.com/.
2. Enter CVE number obtained from the report or enter any keywords related to the target.
3. Save relevant information in the file.

Expected Output:
The expected output will give the evidence of the known vulnerabilities in the target's machine also if any exploit was done previously that would also be mentioned.

Manual Vulnerability Scanning:

Input:
Information acquired in enumeration phase.

Tools:
Excel spreadsheet or any other spreadsheet.

Steps:
1. Search for the vulnerabilities from data obtained through:
   - Open ports.
   - Services provided by them.
   - Operating system.
   - Banner grabbing.
2. Save the finding in a file.

Expected Output:
The expected output will be the list of the known vulnerabilities of the system.

Summarize Vulnerability Scan:

Input:
Information obtained by the automatic and manual vulnerability scan.

Tools:
Spreadsheet.

Steps:
1. Review all the vulnerabilities and rate them based on the severity level.
2. Sort them according to the level of their risk.

Expected Output:
This will be the final list of the known vulnerabilities.

Target Exploitation

In this section we will check all possible vulnerabilities we could exploit and try to find a break through to get access in or perform a sort of unauthorized action to the system.

Planning the Exploits:

Input:
Data obtained in the precious section.

Tools:
Spreadsheet.

Steps:
1. Identify vulnerabilities to exploit.
2. Try to exploit each and every possible vulnerability found.

Expected Output:
This will save a lot of time in the exploitation process

Metasploit:

Input:
XML file generated by OpenVAS.

Tools:
Metasploit.

Steps:
1. Open Metasploit.
2. Import the saved XML file in Metasploit.
3. Search for the exploitable vulnerabilities.
4. Load each exploit.
5. Set the parameters for every exploit accordingly.
6. Run the exploits.

Expected Output:
If exploits penetrates through then the test is successful and find the saving for post-exploitation phase.

DOS Attack:

Input:
<IP address>.

Tools:
Metasploit.

Steps:
1. Open Metasploit.
2. Search 'synflood'.

3. Use that auxiliary.
4. Set the parameters and run.
5. Now check the browser and again look for the target IP.

Expected Result:
The browser will give no respond and similarly by pinging there would be either severe loss in the data packets or no response from the target.

Brute Force Attack:

Input:
File with list of passwords, Username, <IP address>.

Tools:
Ncrack command, Kali Terminal.

Steps:
1. Find a list of passwords from the internet.
2. Open terminal.
3. Type command as ncrack- -user [username] –p [password list] <IP address>.

Expected Output:
If the exploit is successful we shall have the required password and we can easily gain access to the system.

Getting Directories:

Tools:
Dirbuster.

Steps:
1. Open Dirbuster.
2. Enter target URL i.e. http://<IP address>:port.
3. Select 'list based brute force'.
4. Browse and go to 'Dirbuster' directory and in 'wordlists' directory load the last file.
5. Start the execution and wait.
6. After getting the results go through the file system.

Expected Output:
The Dirbuster will reveal all the files from where we can easily find the confidential information.

SQL Injection:

Input:
URL, SQL Map commands.

Tools:
Kali Terminal.

Steps:
1. Open Kali Linux Terminal.

2. Type sqlmap -u [URL] --dbs, it will open the databases.
3. Type sqlmap -u [URL] -D [database name] --tables, it will show the list of tables.
4. Go through tables and get the required information.

Expected Output:

This procedure will give more confidential information and will allow access to open a particular target's website so one could easily change the settings and posts etc.

Post-Exploitation

The purpose of this phase is know how much is the machine being compromised and what necessary steps should be taken to maintain control of the machine for later use.

Exploitation Report:
This report contains all the possible exploits performed on the target also tells the mitigation strategies to that should be implemented to secure those vulnerabilities.

DNS Report:
The DNS report will give information regarding the DNS servers that have been compromised and has revealed the sensitive information.