Standard Operating Procedure

It is observed from the research that one of the main things that are required is a well-defined standard operating procedure which would be very helpful to show users a road map by which they could perform a penetration test. In the following section, a standard operating procedure was designed that help in performing a penetration test, comprised of the six steps and their description is also given. The list of six steps are given below:

- Information gathering
- Scanning
- Enumeration
- Vulnerability identification
- Exploitation
- Reporting

1. Information gathering

Information about the target will be provided in this section which will provide a standard road map to the penetration tester to perform test on the target. We will use this information in out next coming steps which will help in proceeding our attacks on the target and hence gathering of information in this step is very useful.

Table 1 Exploring Internet

Input	Name of the target.
Utilities	Searching on engines like Google, Yahoo, Bing, Duckduckgoo.
Actions	1 Type the name of the target in the search bar and get information about it. 2 Perform analysis of the target's site and try to gather as much information as could from it.
Outcome	The data or material of any type regarding the target on the internet including its location, email, phone numbers, fax also including information on its hardware or software the company is using.

Table 2 Whois

Input	IP of the target.
Utilities	1 Terminal 2 Whois (Whois, n.d.)
Actions	1 Run the terminal. 2 Enter command: "whois <target-ip>". 3 Save outcome in the file.
Outcome	The data including emails, phone numbers, fax, admin details, server details and any sort of administrative or technical details regarding target.

Table 3 Search for DNS

Input	IP of the target.
Utilities	1 Terminal 2 Dig (nixCraft, 2020)
Actions	1 Run the terminal. 2 Enter command: "dig <target-ip>". 3 Save outcome in the file.

Outcome	The details of the nameservers (DNS), hos address, mail exchange server or any useful information.

2.   Scanning

The services running on the target machine could be detected during the scanning process, also the port running them and if there is any port or ports which are open and not using any service, which could be exploited. Moreover, the version numbers of the services could be detected. Also, if possible, the server information and its version number could be founded. These results obtained are then documented and thus vulnerabilities that are found are exploited afterwards.

Table 4 Searching for live servers and services using Nmap

Input	IP of the target.
Utilities	1 Terminal 2 Nmap (Lyon, 1997).
Actions	1 Run the terminal. 2 Enter command on terminal: "nmap <parameter> <target-ip>". 3 Save outcome in the file.
Outcome	The details of the open ports, services running on them, state of the ports whether open or not also about the OS running.

Table 5 Searching for live servers and services using Nikto

Input	IP of the target.
Utilities	1 Terminal 2 Nikto (Sullo, 2014).
Actions	1 Run the terminal. 2 Enter the command: "Nikto -host <target-ip>". 3 Save outcome in the file.
Outcome	The details of the open ports, services running on them, state of the ports whether open or not also about the allowed HTTP methods.

Table 6 Banner grabbing

Input	IP and port number of the target.
Utilities	1 Terminal 2 Telnet (Digital Guide IONOS, 2019).
Actions	1 Run the terminal.

	2 Enter the command: "telnet <target>" or "telnet <ip-address> <port-number>" from step 1.
	3 Type the HEAD HTTP request.
	4 Save outcome in the file.
Outcome	The server's details including its version which is very useful in finding vulnerabilities in it which afterwards could be exploited.

3. Enumeration

Under this section, the gathered information is organized in a methodical manner, resulting in an organized structure that is easy to understand the working of the target system and knowing vulnerabilities which later are exploited.

Table 7 Data compilation

Input	The data which is obtained from the previous steps are used as an input.
Utilities	Microsoft Excel.
Actions	1 Run excel sheet.
	2 Insert a table with columns having details of all the servers found and then fill them with the following details:
	• Server's IP.
	• Name of the server's domain.
	• List of the open ports.
	• Ports running services on them.
	• Details about the OS of the server.
	3 Save outcome in the file.
Outcome	This information is very valuable in making the pen tester to plan the attacks and to find vulnerabilities on it with the above information.

4. Vulnerability analysis

Vulnerabilities are exploited using automated and manual vulnerability methods by initiating suitable attacks on the target.

Table 8 Searching know vulnerabilities.

Input	Keywords related to target.
Utilities	1 Web browser 2 Databases: • CVE Details. • CERT.
Actions	1 Enter https://www.cvedetails.com/ on the browser. 2 With help of keywords regarding target find information related to servers, services and OS used by them. 3 Save outcome in the file. 4 Search for www.kb.cert.org/vuls on the browser. 5 Enter keywords that relates to the target's services, server and OS. 6 Save outcome in the file.
Outcome	It is expected of getting server's information related to the target's version number. This information later is used to exploit known vulnerabilities.

Table 9 ZAP

Input	IP of the target/ URL.
Utilities	1 Zap (OpenVAS, 2005).
Actions	1 Run ZAP. 2 Enter IP/ URL in the provided section. 3 Select default spider. 4 Press AAttack
Outcome	The report on the vulnerabilities is generated but these results should be verified as automated results are not completely reliable, so the report need to be investigated to remove any false results.

10 Reviewing the vulnerabilities

Input	Report on the vulnerabilities detected.
Utilities	Excel sheet.

Actions	1 Analyze the detected vulnerabilities list.
	2 Give them score on the basis of their severity and impact.
	3 Categorize according to the score.
Outcome	The final list is based on the basis of scores given to vulnerabilities.

5.   Exploitation

The vulnerabilities list obtained in the last section is very useful in executing several attacks on the targeted machine. These attacks could alter the services or to maneuver or attain unwarranted access to the data stored on targeted machine. The following tools are used to conduct the pen test and their procedure is written as follow:

Table 11 Metasploit

Input	Use the file generated by the automated software i.e. XML.
Utilities	Metasploit (Metasploit.com)
Actions	1 Run Metasploit. 2 The downloaded XML file is loaded/imported. 3 Initialize the parameters to set up exploits for the vulnerabilities found. 4 Run the exploits.
Outcome	If the exploits are implemented successfully, the penetration test is successful. Afterwards, write the mitigation report and give recommendations and if unsuccessful try the new exploit.

Table 12 Directory scan

Input	IP and port number of the target.
Utilities	Dirbuster (OWASP, n.d.).
Actions	1 Search Dirbuster and then run it. 2 In the target's URL filed, enter IP along with the port number of the target.. 3 Select the world list from usr/share/Dirbuster folder. 4 Set the number of threads. 5 Initiate the scan by clicking start. 6 Save outcome in the file.
Outcome	The results would be the list of directories that will help to discover further exploits on the targeted machine.

Table 13 SQLi attack

Input	URL of the target.
Utilities	Sqlmap (sqlmap, n.d.).
Actions	1 Run the terminal. 2 Run the Sqlmap on the system and if it is not installed than install by entering command: "https://github.com/sqlmapproject/sqlmap.git". 3 Run Sqlmap. 4 Enter command to get details regarding databases: "Sqlmap -u <target-url> --dbs". 5 Enter command for getting details of the tables: "Sqlmap -u <target-url> --tables".
Outcome	The successful exploit will reveal the confidential information from the database. Provide recommendations for its mitigation in the report otherwise run new exploits.

Table 14 Brute force attack

Input	IP of the target and passwords list.
Utilities	Medusa (Rubens, n.d.).
Actions	1 Run the terminal. 2 Search and download common list of used passwords from the web search. 3 Enter the command: "medusa -h <users-list OR target-ip> -u <user-name> -P <wordlist> -n <port-number>".
Outcome	The password is obtained for the user if the exploit is successful. Afterwards, it should be mentioned in the report with providing recommendations.

Table 15 Denial of service

Input	IP of the target.
Utilities	LOIC (Oliveira, 2019) or slowloris (Yaltirakli, 2020).
Actions	1 Download LOIC or slowloris form GitHub. 2 Run terminal in folder containing LOIC or slowloris.

	3	For running LOIC type and enter ./loic.sh and for slowloris type "./slowloris.py <target-ip>".
	4	The slowloris results will start coming and if using LOIC, enter the IP or the URL in the specified bar and then press the button named: "lock on".
	5	Press the button named: "IMMA CHARGIN MAH LAZER" to run the exploit.
Outcome	The flooding will likely be started and will flood the services if appropriate security measures are not taken. Mention in the report and provide recommendations and if unsuccessful try another exploit.	

Table 16 Man-in-the-middle

Input	IP of the target.	
Utilities	1	Arpspoof.
	2	Tcpdump (Hat), 2018).
Actions	1	Run the terminal.
	2	Install the arpspoof if not already installed by entering the command: "apt-get install dsniff".
	3	Execute "arpspoof [-I *interface*] [-t *target's ip*] host".
	4	Launch second terminal and execute "arpspoof [-I *interface*] [-t router's ip] host".
	5	Enter command "apt-get install tcpdump" to install tcpdump if not already installed.
	6	Make sure that the IP forwarding is not disabled, open third terminal, and execute: "echo 1 > /proc/sys/net/ipv4/ip_forward".
	7	Now execute: "tcpdump [-I *interface*] [-n *port*] [*target's* port] *and* host [target's ip].
	8	Capturing traffic will begin now.
Outcome	If the above-mentioned procedure is executed successfully then the flow of traffic from the target can be seen which means man-in-the-middle is successful. Afterwards mention it in the report and provide recommendations to mitigate it.	

Table 17 Fuzzing

Input	IP of the target.
Utilities	Sfuzz (Conole, n.d.).
Actions	1 Run the terminal. 2 If not installed, then type and enter: "sudo apt-get install sfuzz". 3 Go into the directory with the list of fuzzing scripts by entering "cd /usr/share/sfuzz-db". 4 To execute the script, type: "sfuzz -S [target's ip] [-p *port*] -T [-f *config-file*] [-L *output-file*] and press enter. 5 Analyze the results.
Outco me	To check for the memory leaks and any vulnerability that could be exploited, the target is tested by giving random scripts. If it is showing errors for such commands, it means the system is secure otherwise the founded vulnerability should be mentioned along with the mitigation strategy in the report.

6.   Post exploitation

The post exploitation is based on the report providing a detailed analysis of the penetration testing activities. It is explained that how the vulnerabilities are found and how they are exploited. The consequences of these vulnerabilities are also explained in the report. At the end, recommendations are provided for mitigating or removing the risk to make the system secure.