International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 12 Dec 2021, pp: 1287-1305 www.ijaem.net ISSN: 2395-5252

Learning of Penetration Testing Using Open Source Tools for Beginner

Kajal Kashyap, Arti Noor, Rekha Saraswat, V K Sharma
Centre for Development of Advanced Computing, Noida

Date of Submission: 10-12-2021 Revised: 20-12-2021 Date of Acceptance: 25-12-2021

ABSTRACT: In the digital world, everything is connected with the internet and information is at more risk than ever. Each new technical invention lead to new security threat that requires advanced solution. Further due to covid-19 issues, internet usage increases multifold as most of the activities are happening online whether work from home or online teaching & exam. According to recent news, in the year of 2020 there is 37% of rise in cyber-attacks in India. To counter the cyber-attacks, there is the need of awareness and preparedness at the very beginning level i.e. from students levels itself. Penetration testing is a method through which one can find vulnerabilities in systems & networks and take preventive measures to protect the systems, networks and web applications. Penetration testing should be conducted regularly to identify loop holes, risks in the system and maintain them to accomplish high security level. There are various methods to perform penetration testing. This paper gives an overview of different penetration open source tools available in Kali Linux. The step by step use of each penetration testing tools, tools analysis and comparison based on utility and portability are also discussed in the paper. The study is useful for learning the various tools available freely to secure systems and networks and web applications.

Keywords- Penetration Testing, Web Application Vulnerabilities, Network Vulnerabilities, Cyber Security, Kali Linux Tools, Pen testing

I. INTRODUCTION

Nowadays, Data and Information security is the first preference for IT organizations. Every organization needs to safeguard its information, assets to assure that they are following proper security standards.

Penetration testing is a process of measuring the security level of systems, networks, web applications and devices in an organization by finding and exploiting the vulnerabilities present in them. In this process entire organization is scrutinize and look for system configuration, software used, hardware used like firewalls, routers, switches, databases, antivirus, abnormal files and folders to identify loop holes and vulnerabilities.

There are various causes of vulnerabilities such as design and development errors, poor system configuration, human errors, insecure network, system complexity, use of week passwords etc. [1]

Penetration testing helps to assure the security level for an attacker if he tries to gain access into theinternal network. It defends the organization against any downfall by avoiding any financial loss. Nowadays penetration testing is the most important exercise to execute a simulated cyber attack to exploit vulnerabilities to test the security of any system. [4]

In IT Organization, there are various penetration testers to perform penetration testing and identify vulnerabilities before any attack happen. Penetration testing can be performed manually as well as with automated tools. [3]

Various factors have encouraged the authors to work on and write research papers in this particular domain. The Network and System Administration of the organization has lot of responsibilitiessuch as securing operating system, file sharing, directory services, software, hardware, backup process and most importantly to secure the network from outside attacks. Due to technology advancement, most of the Network and Security Administration may not always remain up-to-date and keep track of security threats. That is why penetration testing plays a vital role in Network and Administration domain in order to achieve high standards of security. [4]

II. LITERATURE SURVEY

In last few years, Penetration testing has become an important area in the field of Information Security. Several studies [1-4,13-15]have been developed and adapted to boost

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 12 Dec 2021, pp: 1287-1305 www.ijaem.net ISSN: 2395-5252

security standards. The researchers are always interested to conduct research on Identification of Vulnerabilities in the posture of an organization, its exploitation through Cyber Attacks and the Prevention Techniques.

Devanshu Bhatt [2] presents a survey about penetration testing on open source platform and compared various information gathering tools. The researcher explained the open source distributed has expanded Kali Linux platform to perform penetration testing with predefined applications and frameworks within it. In the research paper, he explained the steps to install,configure Virtual Environment and perform System Exploitation with Metasploit.

B. Surya Samantha, M.V.Phanindra [3] discussed the usage of various penetration tools in Kali Linux specially developed for Website hacking purposes. The researcher covered the Port Scanner named Zenmap, Vulnerability Scanner named Sparta, Web Application testing tool named BurpSuite, SQL Injection Attack tool named SQLMap, Watchword Guessing Instrument Crunch, Website Crawling Instrument Cewl, other tools like Nikto and HTTrack.

Suraj S. Mundalik [4] explained Kali Linux Open Source Tool, the successor of Backtrack Operating System, and Zero Entry Pen Testing Methodology. The researcher discussed four phases of Penetration Testing i.e. Information Gathering, Scanning, Exploitation and Post Exploitation & Maintaining Access. In the paper, the researcher also suggested various open source tools in Kali Linux to perform penetration testing to make web applications flaw free.

III. INTRODUCTION TO KALI LINUX

Kali Linux is freely available Linux distribution system based on Debian. It is specially designed for forensics analysis and penetration testing. It is present in different architectures x86, x86-64. One can use Kali Linux without installing it. one can set up Kali Linux by rebooting through DVD or virtual images that can be used in virtual environments like VMWare or Virtual Box. To installation of Kali Linux may be done using the links - **https://www.kali.org/downloads/**(Figure-1) and download "**Kali Linux 64-Bit (Live)**"(figure-2) from the website.

Figure 1: Kali Linux Website

Figure 2: Download Kali Linux

Once downloaded, **VMware Workstation** may be opened from the desktop. The penetration tester creates a new virtual machine by clicking on Custom (advanced)(figure-3).

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 12 Dec 2021, pp: 1287-1305 www.ijaem.net ISSN: 2395-5252

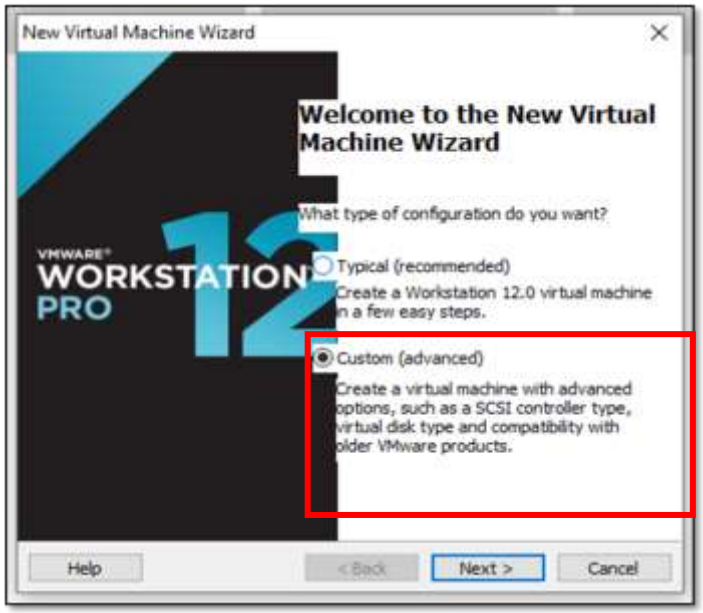


Figure 3: Virtual Machine Wizard

The tester then chooses the Virtual Machine Hardware Compatibility and select "**Installer Disc Image file (iso)**" (figure-4). Generally, VMware Workstation detects the Operating System automatically and initiates the Easy Install but this may not be the case with Kali Linux as warning with Yellow triangle may be seen in Figure 4. This can be ignored by the tester and may click on Next.

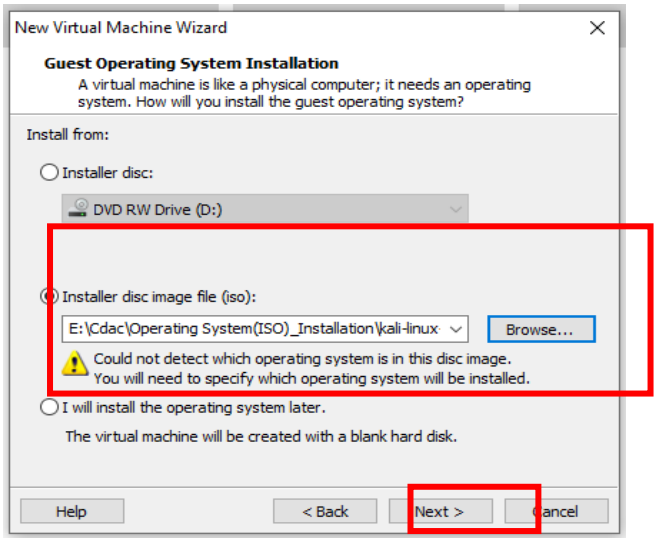


Figure 4: Installer Disk Image File (iso) Selection

The tester may click on "Linux" as Guest Operating System and select "Debian 8.x 64-bit" as its version. The name of the virtual machine may be provided as "Kali-2020" and the location may be selected. The penetration tester can even change the value of the processors and memory by using the dial as per the requirement. The network type may be selected as Network Address Translation (NAT) and I/O Controller type as LSI Logic (Fihure-5).

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 12 Dec 2021, pp: 1287-1305 www.ijaem.net ISSN: 2395-5252

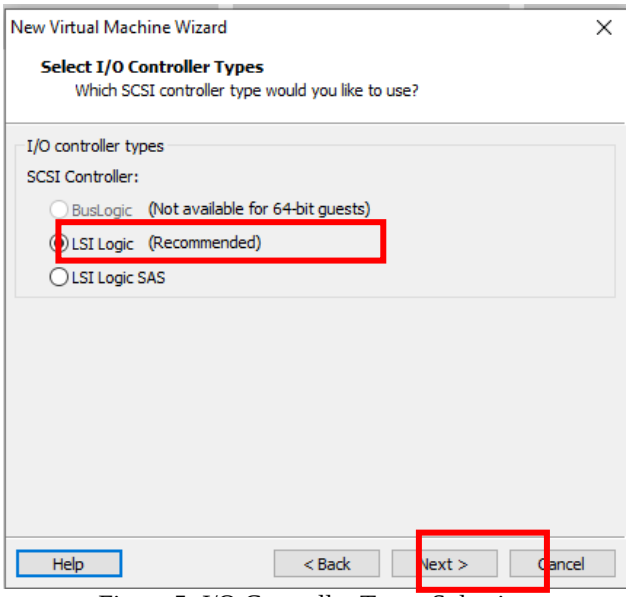


Figure 5: I/O Controller Types Selection

Next, the Disk type may be selected as SCSI for creating a new Virtual Disk. The disk capacity may be specified as 20 GB and"Split Virtual Disk into Multiple Files" may be chosen. The Disk file once selected, Virtual Machine Kali Linux is set to be created. After successful creation of the virtual machine, the installation process begins. The tester clicks on "Power on this virtual machine" and select Graphical Install(Figure-6).

Figure 6:Graphical Install Selection

The penetration tester may choose the language to be used for installation purpose, select the location, configure the Keyboard and configure the network. The tester may continue by providing user name and password(Figure-7).

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 12 Dec 2021, pp: 1287-1305 www.ijaem.net ISSN: 2395-5252

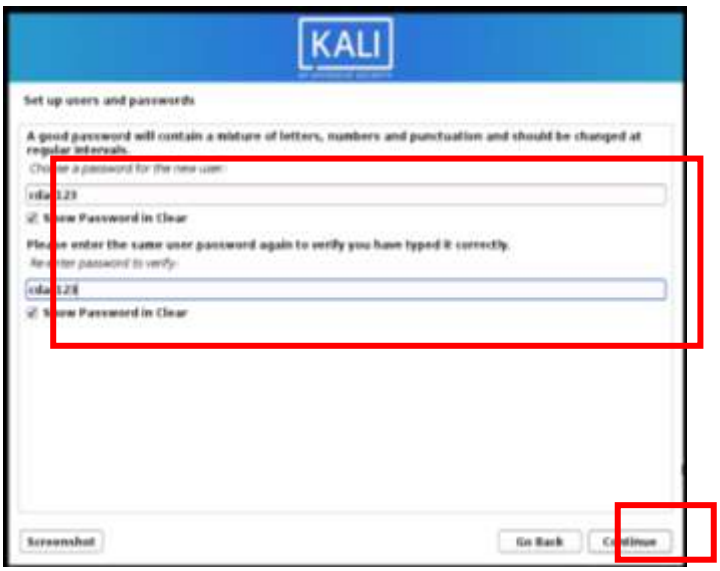


Figure 7: Set-up User and Password

Finally, the tester configures the clock and selects Partition Disk as Manual.The new partition may be created by providing the partition size, partition type as Primary, partition location as beginning and mentioning other partition settings. This will successfully installs Kali Linux Virtual Machine on the Virtualized Environment. The penetration tester may now be ready to perform penetration testing on the system, network and web applications.

IV. STEPS OF PENETRATION TESTING

The whole process of penetration testing is divided into multiple steps which together may provide the unique methodology. The major objective to use penetration testing methodology is to divide the complex process into simple, convenient and manageable tasks. There are many names given to the steps of Penetration testing by different researchers but the purpose of all is same. For example, some methodologies use the term "Information Gathering", whereas others use the term "Reconnaissance" or "Recon". There are mainly 7 steps performed in penetration testing. Figure-8 shows the steps which are explained below:

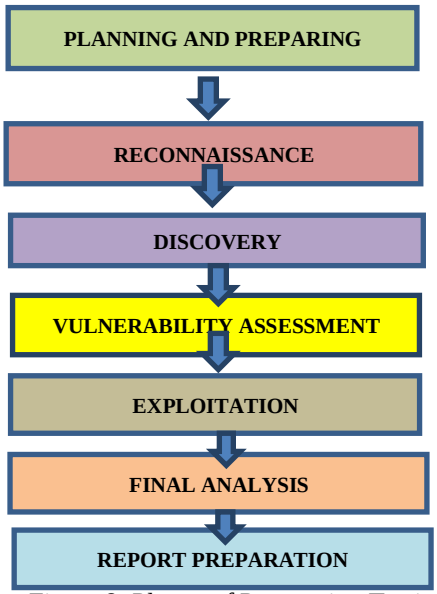


Figure 8: Phases of Penetration Testing

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 12 Dec 2021, pp: 1287-1305 www.ijaem.net ISSN: 2395-5252

STEP 1: PLANNING & PREPARING
This is the first step in penetration testing where goals, objectives and scope are defined in order to perform penetration testing. Documents and agreements are signed. The organization provides general information to penetration testing team.
STEP 2: RECONNAISSANCE
This is the phase where testing actually begins. Testers look for information that are hidden or not provided. This step is crucial as it helps the tester to gather complete information about organization.
There are two types of reconnaissance:

2.1 **Active Reconnaissance:** In this, pen-tester directly interacts with the targets with the help of resources and systems to gather information about vulnerabilities.
2.2 **PASSIVE RECONNAISSANCE:**In this type of Reconnaissance, pen-tester tries to gather information without engaging with resources and systems. The tester looks for information from the website of the organization.
STEP 3: DISCOVERY
Tester use various automated tools to scan the target to identify the risks & vulnerabilities.
STEP 4: VULNERABILITY ASSESSMENT
The tester gain basic knowledge of the system and identify vulnerabilities that could allow outsider to gain access to internal networks.

STEP 5: EXPLOITATION
Once the vulnerabilities are identified by the tester, then he tries to use various manual techniques or automated tools to exploit these vulnerabilities.
STEP 6: FINAL ANALYSIS
In this step Pen-testers ensures that every exploited system could be clear up and secure from outside threats.
STEP 7: REPORT PREPARATION
Testers prepare an in-depth report based on the previous steps and mention all the vulnerabilities and risks associated with the target. The vulnerabilities with high risk will be in high priority column list followed by lower risks in descending order.

V. PENETRATION TESTING TOOLS

There are multiple open source tools available for performing effective Penetration Testing on Systems, Networks and Web Applications in Kali Linux Virtual Machine. In this research paper, the following 10 penetration testing tools are discussed -

1. NMAP
2. ZENMAP
3. NETCAT
4. UNICORNSCAN
5. OPENVAS
6. NIKTO
7. WPSCAN
8. CMSMAP
9. FLUXION
10. AIRCRACK-NG

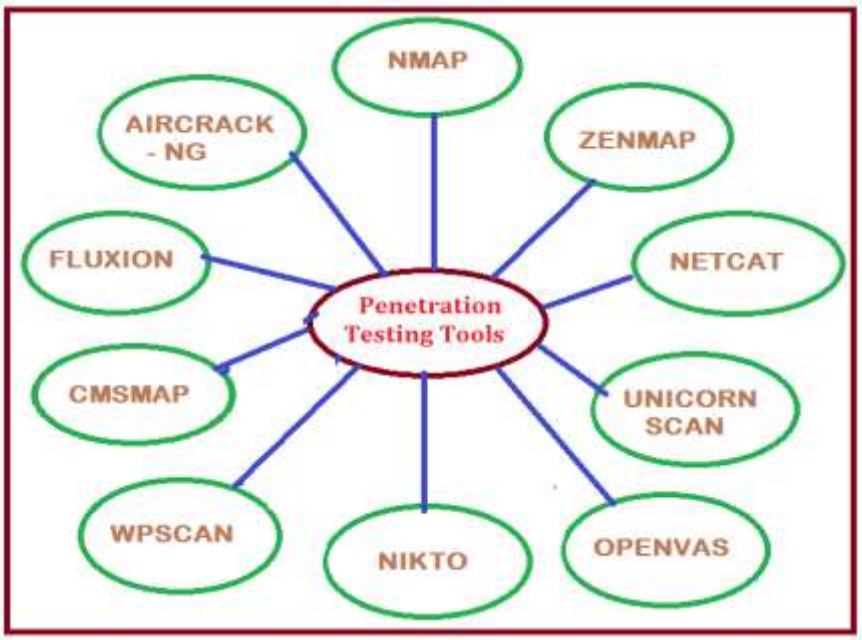


Figure 9: Penetration Testing Tools

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 12 Dec 2021, pp: 1287-1305 www.ijaem.net ISSN: 2395-5252

BRIEF OVERVIEW OF TOOLS

1. NMAP

It is also known as "Network Mapped" tool. NMAP is an open source and free tool used for the network discovery. This tool is very efficient and widely used by the security auditors. NMAP may be used for Host discovery, Scanning ports, Ports information, Service detection, Scanning scripts, OS detection and many other services.

Commands used in NMAP –

i) To scan any IP address

nmap<IP Address>

Example - nmap 192.168.45.130

Figure 10: NMAP Output Screen

ii)To scan specific ports or scan entire port ranges on a local orremoteserver –

nmap-p 1-65535 192.168.45.130

Figure 11: NMAP Entire Ports Scan Output

2. ZENMAP

ZENMAP is Graphical User Interface (GUI) tool for the NMAP security scanner. It is open source, multi-platform tool developed for easy usage as oppose to NMAPwhich is a bit typical tool to use.ZENMAP tool's main page looks like as shown in Figure 12 -

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 12 Dec 2021, pp: 1287-1305 www.ijaem.net ISSN: 2395-5252

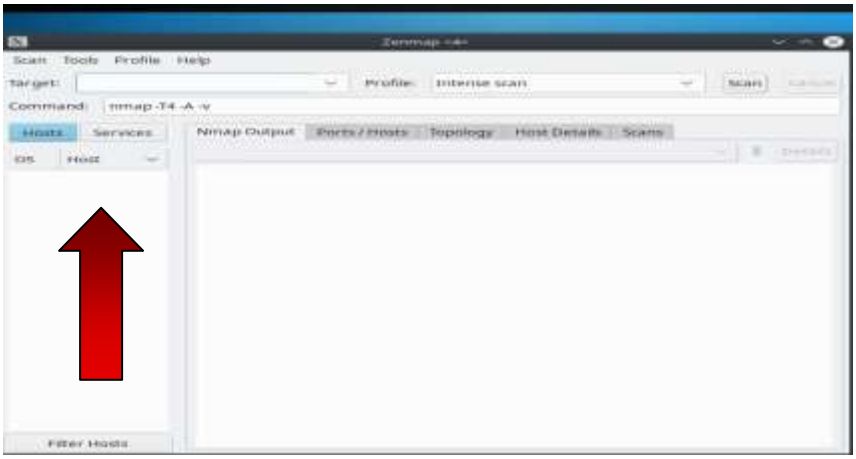


Figure 12: ZENMAP Interface

Zenmap supports various scan options :-

i. **Intense scan**
ii. **Intense scan plus UDP**
iii. **Intense scan, all TCP ports**
iv. **Intense scan, no ping**
v. **Ping scan**
vi. **Quick scan**
vii. **Quick scan plus**
viii. **Quick traceroute**
ix. **Regular scan**

i) INTENSE SCAN

The tester may provide IP Address of the target machine and select Intense Scan as Profile to gather information as mentioned in the Figure 13 –

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 12 Dec 2021, pp: 1287-1305 www.ijaem.net ISSN: 2395-5252

Figure 13: Intense Scan

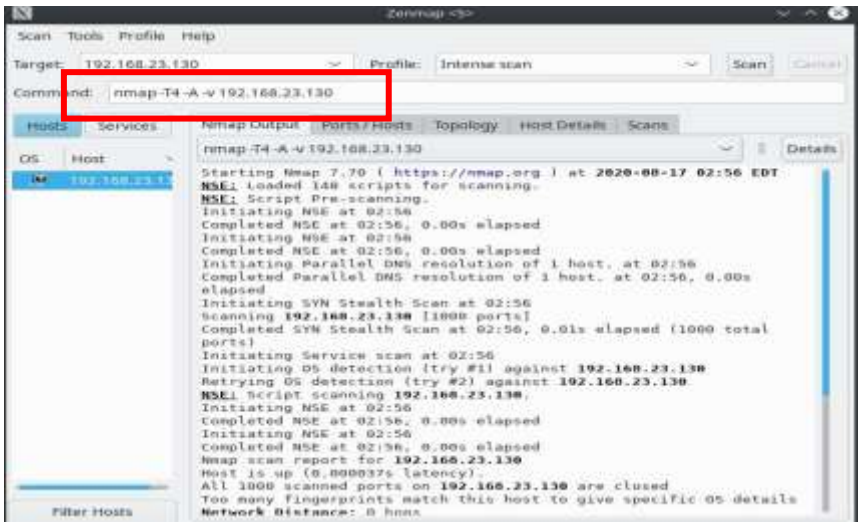


Figure 14: Intense Scan Output Screen

Intense scan is the most common profile selected inZENMAP(Figure-14). It quickly detects TCP ports and also determines the type of Operating System, their services and versions.

Command: nmap -T4 -A -v *<target>*

(-T4) is an option for timing which ranges from 0–5, where 0 is the slowest and 5 is the fastest.

(-A) is an option that determines the type of OS and it's versions. Along with the output.

(-v) is an option that gives feedback as Nmap makes progress in the scan.

ii) INTENSE SCAN PLUS UDP -

This profile option works as regular intense scan but also scans UDP Ports.

Command: nmap-sS-sU-T4-A-v<target>

-Ss tell nmap to scan TCP ports

-sU is an option that scans UDP ports as well

iii) INTENSE SCAN, ALL TCP PORTS –

NMAP usually scans top 1000 most common ports due to long time to scan all the ports. However, Intense Scan, all TCP Ports asks NMAP to scan all the ports from 1–65535(max)

Command: nmap-p 1-65535-T4-A-v<target>

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 12 Dec 2021, pp: 1287-1305 www.ijaem.net ISSN: 2395-5252

iv) INTENSE SCAN, NO PING -

This profile is exactly similar to other intense scan. However, this assumes that the host is up. This scan is helpful when the target is blocking ping request and it is known that the target is up.

Command: nmap-T4-A-v-Pn<target>

-Pn assumes that the host is up

v) PING SCAN –

This profile option only ping the target and does not scan the port(Figure-15).

Command: nmap-sn<target>

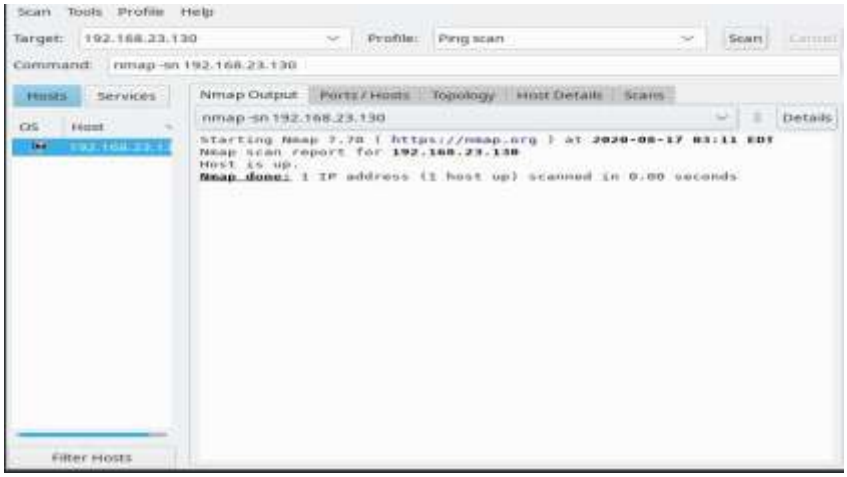


Figure 15: Ping Scan

vi) QUICK SCAN –

This command scans only limited number of TCP ports. i.e. Top 100 most common TCP ports.Instead of scanning all the ports, this profile option only scans few ports.

Command: nmap-T4-F<target>

-F is an option for fast scan

vii) QUICK SCAN PLUS–

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 12 Dec 2021, pp: 1287-1305 www.ijaem.net ISSN: 2395-5252

Command: nmap-Sv-t4-O-F--version-light<TARGET>

Here,-O is an option that detects the type of OS, then performs light scan

viii) QUICK TRACE ROUTE –

Traceroute is a program that records the route between the source computer and certain destination through Internet.

Command: nmap-sn—traceroute<target>

This command will traceroute and ping all the hosts defined in a target

ix) REGULAR SCAN –

This command issues a TCP SYN scan for the most common 1000 ports using ping request for host detection.

Command: nmap <target>

3. NETCAT

NETCAT is network analysis tool that is prominent among security industry, network and system administration domains.

NETCAT is a debugging tool which performs the following activities-

- Host discovery
- Scanning ports
- Operating System detection
- Detecting the version of application

The major features of NETCAT are-

- TCP and UDP port analysis
- Inbound and Outbound network connections
- Forward and Reverse DNS analysis
- Scanning of local and remote ports
- UDP and TCP tunneling mode feature

Google banner grabbing (Figure-16) may be possible using NETCAT by typing the following command in the terminal-

nc -v google.com 80

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 12 Dec 2021, pp: 1287-1305 www.ijaem.net ISSN: 2395-5252

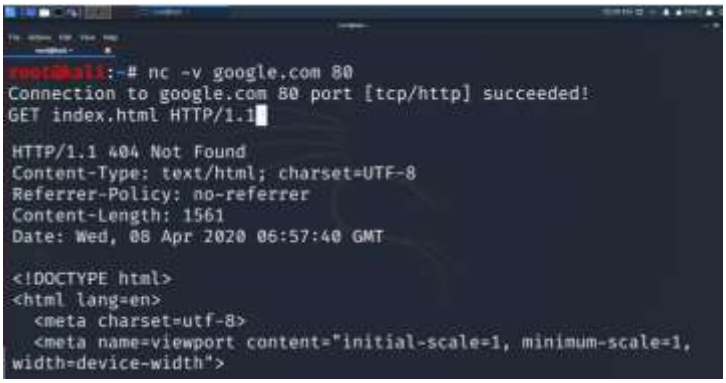
Figure 16: Google Banner Grabbing Command

Figure 17 shows that the connection to google.com is succeeded. NETCAT is connected to google.com on port 80 and its time to send some message.

Figure 17: CONNECTION TO GOOGLE.COM

Now, Let's try to fetch the index page (Figure-18 & 19) of google.com by writing the command as

Figure 18: Fetching Index Page of Google.com



4. UNICORNSCAN

UNICORNSCAN tool is used for gathering information. It has advanced asynchronous TCP and UDP scanning features that helps in port scanning, banner grabbing for applications, operating system detection and system service detection.

To scan open ports for a particulartarget, the IP

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 12 Dec 2021, pp: 1287-1305 www.ijaem.net ISSN: 2395-5252

Address of the target should be provided.

UNICORNSCAN target (IP address which you want to scan)

Example - Unicornscan10.226.37.66(Figure-20) and result is shown in Figure-21.

Figure 20: Unicornscan

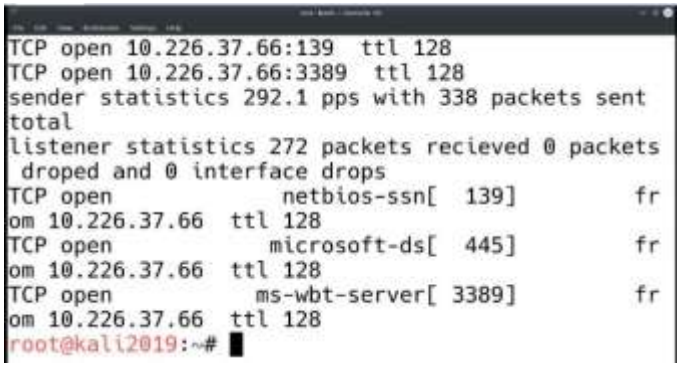


Figure21: UnicornscanResult

5. OPENVAS

OpenVas is Open Vulnerability Assessment System. It is developed by Nessus vulnerability scanner which can be freely used to discover vulnerabilities on local and remote systems.

Main features of OpenVas are as follows-

- Host discovery
- Develop your own security plugin
- Port scanner
- Schedule scans
- Converts results into XML, HTML formats
- Pause, stop and resume scans anytime
- Available for both windows and linux operating system

To use OpenVas, the testers may go to Applications folder in Kali Linux and look for OpenVas. Once OpenVas folder gets open, type https://localhost:9392 to open the web interface as shown below in Figure-22.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 12 Dec 2021, pp: 1287-1305 www.ijaem.net ISSN: 2395-5252

Figure 22: OpenVas Web Interface

The tester set- up the credentials username and password and set the target in OpenVas.

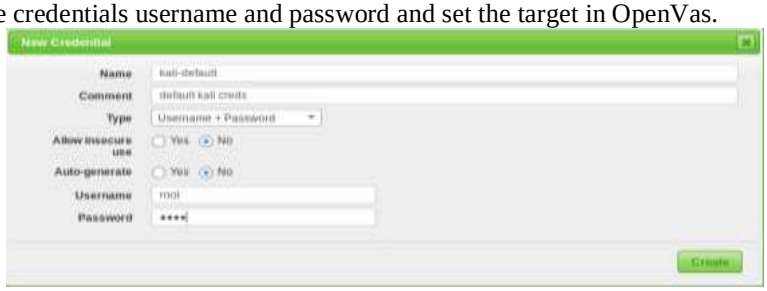


Figure 23: Setup Credentials

Set your target as shown in Figure-24

Figure 24: Setting the Targets

After running the tool, one can find the scanning result as output and same is shown below in Figure-25.

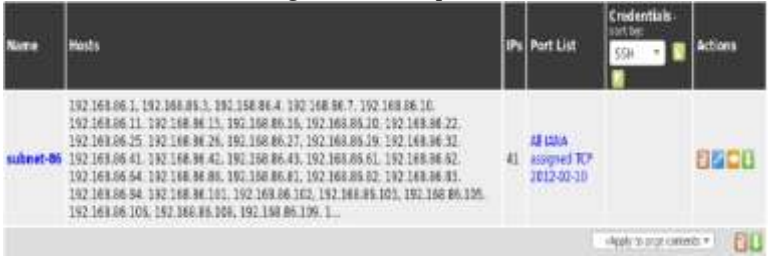


FIGURE 25: Scanning Result

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 12 Dec 2021, pp: 1287-1305 www.ijaem.net ISSN: 2395-5252

6. NIKTO

Nikto is an open source tool in Kali Linux that performs full scanning of web server and discover all the loop holes and vulnerabilities present in it.

The main features of Nikto are as follows -

- Scans multiple ports
- Works Intrusion Detection System
- Scan result can be converted into HTML, TXT XML, CSV format
- Scans directories
- Debug and verbose result
- Uses custom configuration files
- SSL support
- Report unusual headers
- Identifies Installed software

Command to scan the target in Nikto is as follows –

Nikto -h <IP address> -p 80

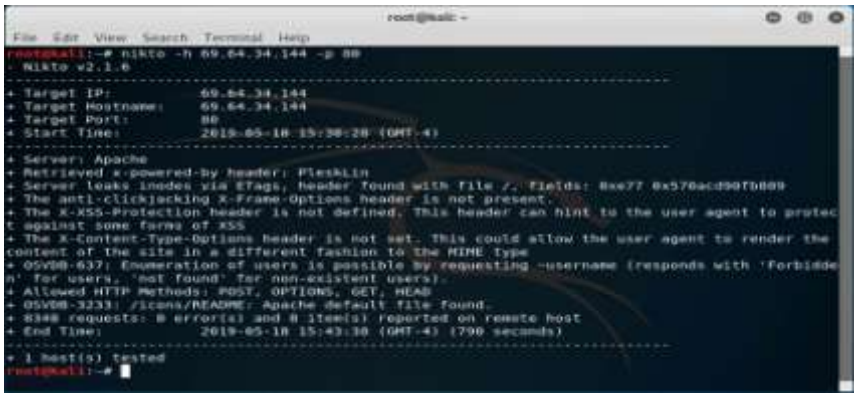


FIGURE 26: NIKTO SCAN RESULT

7. WPSCAN

WPScan is a tool used for scanning websites developed on WordPress platform. The testers use WPScan tool to check vulnerabilities in these websites. It scans the websites and finds all the vulnerabilities present in it.

Figure-27 shows the scanning using WPScan of a vulnerable website

Figure 27: Scanning WordPress Website

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 12 Dec 2021, pp: 1287-1305 www.ijaem.net ISSN: 2395-5252

The penetration tester uses WPSCAN to find the list of vulnerabilities present in the website(Figure-28).

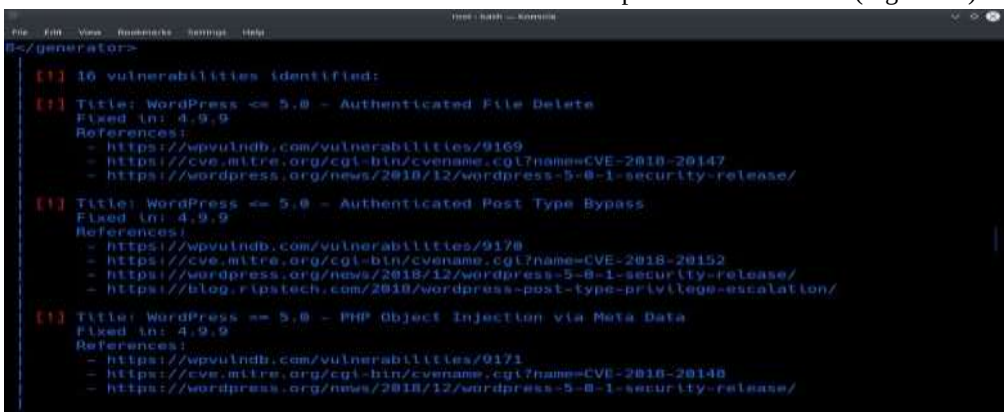


Figure 28: Vulnerabilities Identification

8. CMSMAP

It is an open source tool based on Python language that scans vulnerabilities in CMSs like Wordpress, Joomla, Drupal and Moodle. CMSMAP helps in automating the process of Vulnerability scanning and detecting majorly brute force attacks. The main features of CMSMAP are as follows -

- Performs multiple scans
- Ability to set header
- Support SSL encryption
- Verbose mode for debugging process
- Saves result in text file

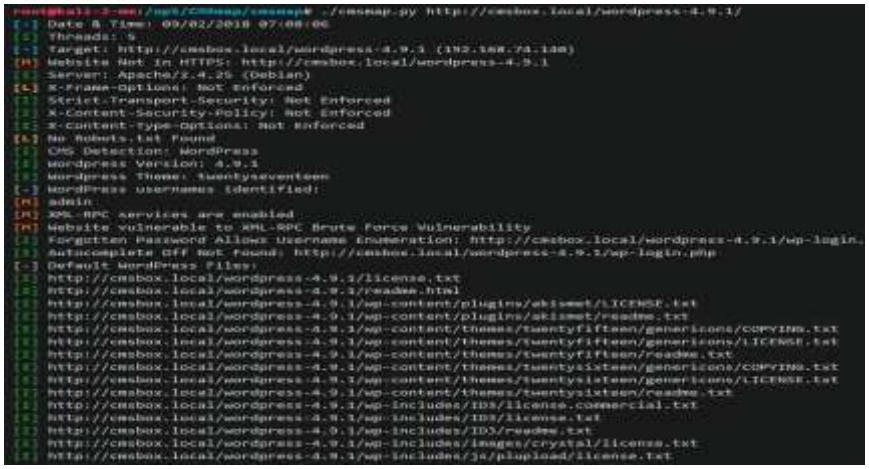


Figure 29: Website Scan Result

Figure shows the result obtained using CMSMAP scanning.

9. FLUXION

Fluxion is a Wi-FiAnalyzer that allows the pen tester to scan wireless networks and find vulnerabilities in personal or corporate networks. This tool is mostly used by security auditors.Figure-30 shows the Fluxion interface.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 12 Dec 2021, pp: 1287-1305 www.ijaem.net ISSN: 2395-5252

Figure 30: Fluxion Interface

10. AIRCRACK-NG

Aircrack-ng tool is wireless security software which has network packet analyzer, WEP network cracker and other auditing tools. Thistool is mainly used for password cracking. It focuses on different areas of Wi-Fi Security like Monitoring, Attacking, Testing and Cracking. The complete suite of tools are command line tools so allows heavy scripting(Figure-31).

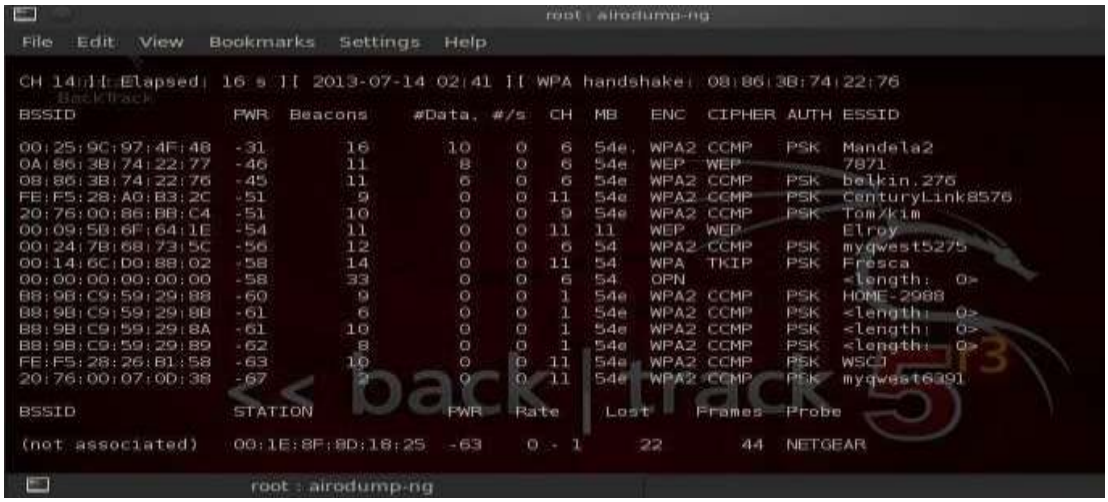


Figure 31: Aircrack-ng Scan Result

VI. 6. COMPARISION AND EVALUATION OF TOOLS

Table 1: Comparison of tools

NAME	SPECIFIC PURPOSE	PORTABILITY	LICENCE
NMAP	● Network Scanning ● Port Scanning ● OS Detection	Linux, Windows, MAC	Free
ZENMAP (GUI for NAMP)	● Network Scanning ● Port Scanning ● OS Detection	Linux, Windows, MAC	Free
NETCAT	● Port Scanning ● Banner Grabbing	Linux, Windows	Free

	● Provide Chat Interface ● File Transfer ● Create Backdoor		
UNICORNSCAN	● Port Scanning ● OS Detection ● File Logging & Filtering	Linux, Windows	Free
OPENVAS	● Vulnerability Scanning	Linux, Windows	Free
NIKTO	● Scan Multiple Ports ● HTTP Proxy Support	Linux, Windows	Free
WPSCAN	● Scans only WordPress Website for Vulnerabilities	Linux	Free
CMSMAP	● Scans Vulnerabilities for WordPress, Joomla or Drupal Sites	Linux	Free
FLUXION	● Captures WPA Psswords	Linux	Free
AIRCRACK-NG	● Analyze Week Wifi Networks	Linux	Free

VII. CONCLUSION

The penetration testing is the very important process to focus on any system, network or web application / standalone machine. Penetration testing allows the developer to verify and define the system related security issues. There are many open source tools which may be used to identify the security posture of an organization by providing the list of vulnerabilities present in the system. There are few tools which also provide the possible solutions to remove the vulnerabilities. The penetration tester should have an in-depth knowledge and understanding of these tools. Testing time and scope should also be increased in order to acquire more accurate information and more loop holes/ vulnerabilities can be identified. After performing penetration testing on the system, network and web application, steps must be taken to protect the system. The tools are very useful for learning and hands-on purpose.

VIII. ACKNOWLEDGEMENT

Authors are thankful to late Dr Neha Bajpai to give the idea for writing the research paper on penetration testing as part of project.

REFERENCES

[1]. V. S. KUMAR, "Ethical Hacking and PenetrationTesting Strategies," International Journal ofEmerging Technology in Computer Science &Electronics (IJETCSE), vol. 11, no. 2, pp. ISSN0976-1353, 2014.

[2]. Devanshu Bhatt, "Modern Day Penetration Testing Distribution Open Source Platform - Kali Linux - Study Paper", International Journal of Scientific & Technology Research, Volume 7, Issue 4, April 2018, ISSN 2277 - 8616

[3]. B. Surya Samantha, M.V. Phanindra, "An Overview on the Utilization of Kali Linux Tools", - International Journal of Research and Analytical Reviews, Volume 5, Issue 2, April – June 2018, ISSN 2349 - 5138

[4]. Suraj S. Mundalik, "Penetration Testing: An Art of Securing the System (Using Kali

Linux)", Volume 5, Issue 10, October-2015 ISSN: 2277 128X
[5]. https://tools.kali.org/
[6]. https://www.cisco.com/c/en_in/products/security/common-cyberattacks.html
[7] https://securitytrails.com/blog/kali-linux-penetration-testing-tools
[8]. https://itsfoss.com/best-kali-linux-tools/
[9]. https://thehackernews.com/
[10]. https://www.tutorialspoint.com/kali_linux/index.htm
[11]. http://indexof.es/Varios2/Hacking%20with%20Kali%20Practical%20Penetration%20Testing%20Techniques.pdf
[12]. https://www.exploit-db.com/papers
[13]. Kevin M. Henry (2012). Penetration Testing: Protecting Networks and Systems. IT Governance Ltd. ISBN 978-1-849-28371-7.
[14]. https://www.ncsc.gov.uk/guidance/penetration-testing;
[15]. Patrick Engebretson, The basics of hacking and penetration testing Archived 2017-01-04 at the Wayback Machine, Elsevier, 2013