AI for Cyber Security with IBM Qradar

Assignment-2

Name: MAYANDI VARUN

Kali Linux is a Debian-derived Linux distribution that is maintained by Offensive Security. Kali Linux is a specially designed OS for network analysts, Penetration testers and for cybersecurity and analysis. Sometimes we have to automate our tasks while performing penetration testing or hacking as there could be thousands of conditions and payloads to test and testing them manually is a difficult task, So to increase the time efficiency we use tools that come pre-packed with Kali Linux. These tools not only saves our time but also captures the accurate data and output the specific result. Kali Linux comes packed with more than 350 tools which could be useful for hacking or penetration testing. Here we have the list of important Kali Linux tools.

1. Nmap

Nmap is an open-source network scanner that is used to recon/scan networks. It is used to discover hosts, ports, and services along with their versions over a network. It sends packets to the host and then analyzes the responses in order to produce the desired results. It could even be used for host discovery, operating system detection, or scanning for open ports. It is one of the most popular reconnaissance tools. To use nmap:

Ping the host with ping command to get the IP address

- ping hostname

Open the terminal and enter the following command there:

- nmap -sV ipaddress

Replace the IP address with the IP address of the host you want to scan.

It will display all the captured details of the host.

2. Burp Suite

Burp Suite is one of the most popular web application security testing software. It is used as a proxy, so all the requests from the browser with the proxy pass through it. And as the request passes through the burp suite, it allows us to make changes to those requests as per our need which is good for testing vulnerabilities like XSS or SQLi or even any vulnerability related to the web. Kali Linux comes with burp suite community edition which is free but there is a paid edition of this tool known as burp suite professional which has a lot many functions as compared to burp suite community edition.

3. Wireshark

Wireshark is a network security tool used to analyze or work with data sent over a network. It is used to analyze the packets transmitted over a network. These packets may have information like the source IP and the destination IP, the protocol used, the data, and some headers. The packets generally have an extension of ".pcap" which could be read using the Wireshark tool.

4. Metasploit Framework

Metasploit is an open-source tool that was designed by Rapid7 technologies. It is one of the world's most used penetration testing frameworks. It comes packed with a lot of exploits to exploit the vulnerabilities over a network or operating systems. Metasploit generally works over a local network but we can use Metasploit for hosts over the internet using "port forwarding". Basically Metasploit is a CLI based tool but it even has a GUI package called "armitage" which makes the use of Metasploit more convenient and feasible.

5. Aircrack-ng

Aircrack is an all in one packet sniffer, WEP and WPA/WPA2 cracker, analyzing tool and a hash capturing tool. It is a tool used for wifi hacking. It helps in capturing the package and reading the hashes out of them and even cracking

those hashes by various attacks like dictionary attacks. It supports almost all the latest wireless interfaces. To use aircrack-ng:

aircrack-ng comes pre-compiled with Kali Linux.

Simply type aircrack-ng in the terminal to use it.

6. Netcat

Netcat is a networking tool used to work with ports and performing actions like port scanning, port listening, or port redirection. This command is even used for Network Debugging or even network daemon testing. This tool is considered as the Swiss army knife of networking tools. It could even be used to do the operating related to TCP, UDP, or UNIX-domain sockets or to open remote connections and much more. To use netcat:

Netcat comes pre-installed with Kali Linux.

Just type “nc” or “netcat” in the terminal to use the tool.

7. John the Ripper

John the Ripper is a great tool for cracking passwords using some famous brute force attacks like dictionary attack or custom wordlist attack etc. It is even used to crack the hashes or passwords for the zipped or compressed files and even locked files as well. It has many available options to crack hashes or passwords. To use John the Ripper:

John the ripper comes pre-installed in Kali Linux.

Just type “john” in the terminal to use the tool.

8. sqlmap

sqlmap is one of the best tools to perform SQL injection attacks. It just automates the process of testing a parameter for SQL injection and even automates the process of exploitation of the vulnerable parameter. It is a great tool as it detects the database on its own so we just have to provide a URL to check whether the

parameter in the URL is vulnerable or not, we could even use the requested file to check for POST parameters. To use sqlmap tool:

sqlmap comes pre-installed in Kali Linux

Just type sqlmap in the terminal to use the tool.

9. Autopsy

Autopsy is a digital forensics tool that is used to gather information from forensics. Or in other words, this tool is used to investigate files or logs to learn about what exactly was done with the system. It could even be used as a recovery software to recover files from a memory card or a pen drive. To use autopsy tool:

Autopsy comes pre-installed in Kali Linux

Just type “autopsy” in the terminal.

10. Social Engineering Toolkit

Social Engineering Toolkit is a collection of tools that could be used to perform social engineering attacks. These tools use and manipulate human behavior for information gathering. it is a great tool to phish the websites even. To use Social Engineering Toolkit

Social Engineering Toolkit comes pre-installed with Kali Linux

Just type “setoolkit” in the terminal.

Agree to the terms and conditions to start using the social engineering toolkit.