Cybersecurity

Assignment – 2

Name: Karthik G

Reg No: 21BEC0642

Kali Linux Tools

1.Nmap

Nmap is a network scanner. It is used to scan and discover hosts, ports, and services along with their versions over a network. Gordon Lyon created it to help map an entire network easily and find its open ports and services.

Features:

- Host discovery, which identifies hosts in any network.
- Port scanning lets you enumerate open ports on either a local or remote host.
- OS detection helps gather operating system and hardware info about any connected device.
- App version detection lets you determine the application name and version numbers.
- Scriptable interaction extends the Nmap default capabilities by using the Nmap Scripting Engine (or NSE).

2. Metasploit Framework

Metasploit Framework, or MSF for short, is a Ruby-based platform used by ethical hackers to develop, test, and execute exploits against remote hosts. Metasploit includes a

complete collection of security tools intended for penetration testing, plus a powerful terminal-based console known as msfconsole, which lets you find targets, exploit security flaws, launch scans, and collect all relevant available data. MSF is most likely one of the most potent security auditing Kali Linux tools freely available for cybersecurity professionals.

Metasploit Framework's features include:

- Network enumeration and discovery
- Evading detection on remote hosts
- Exploiting development and execution
- Scanning remote targets
- Exploiting vulnerabilities and collecting valuable data

3. Skipfish

Skipfish is a Kali Linux tool that scans many web applications. Skipfish acts as an effective auditing tool for crawling web-based data, giving pen testers a quick insight into how insecure any app is. Skipfish performs recursive crawl and dictionary-based tests over all URLs, using its recon capabilities. The crawl creates a digital map of security checks and their results.

Features:

- Automated learning capabilities.
- Differential security checks.
- Easy to use.
- A low false positive ratio.

- The ability to run high-speed security checks, with over 200 requests per second.

4. Nikto

Nikto enables ethical hackers and pen testers to conduct a complete web server scan to discover security vulnerabilities and related flaws. This scan collects results by detecting default file names, insecure file and app patterns, outdated server software, and server and software misconfigurations. In addition, it features support for host-based authentication, proxies, SSL encryption, and more.

Features:

- Scanning multiple ports on a server.
- Identifying installed software via headers, files, and favicons.
- Using custom configuration files.
-

5. Lynis

Lynis is most likely one of the most comprehensive tools available for cybersecurity compliance (e.g., PCI, HIPAA, SOx), system auditing, system hardening, and testing.Lynis also functions as an effective platform for vulnerability scanning and penetration testing.

Features:

- It runs on multiple platforms (macOS, Linux, BSD and more).
- It can run up to 300 security tests on the remote host.

6. John the Ripper

This hacker's resource is a multi-platform cryptography testing tool that works equally well on Linux, Windows, macOS, and Unix. It enables system administrators and security penetration testers to test the strength of any system password by launching brute force attacks. Additionally, John the Ripper can be used to test encryptions like DES, SHA-1, and many others. Its ability to change password decryption methods is set automatically and contingent on the detected algorithms.

Features:

- Brute force testing and dictionary attacks.
- Compatibility with most operating systems and CPU architectures.
- Allowing Pause and Resume options for any scan.
- It allows brute force customization rules.

7. 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. sqlmap comes pre-installed in Kali Linux.

8. Fluxion

Fluxion is a Wi-Fi analyzer specializing in MITM WPA attacks and lets you scan wireless networks. Pen testers use Fluxion to search for security flaws in corporate and personal networks. However, unlike similar Wi-Fi cracking tools, Fluxion does not launch time-consuming brute force cracking attempts. Instead, Fluxion creates an MDK3 process that forces all users on the targeted network to lose authentication or reauthenticate. Once this is accomplished, the user is prompted to connect to a false access point, requiring entering the Wi-Fi password. Then, the program reports the password to the pen tester to gain access.

9. Social Engineering Toolkit

The Social Engineering Toolkit, also known as SET, is an open-source Python-based penetration testing framework that is used to launch social-engineering attacks. It runs on Linux and Mac OS X.SET is an indispensable Kali Linux tool for hackers and pen testers interested in working with social engineering.

Attacks:

- Wi-Fi AP-based attacks, which redirect or intercept packets from Wi-Fi network users.
- SMS and email attacks, here, which attempt to trick and generate fake emails to harvest social credentials.
- Web-based attacks, which lets hackers clone a web page to drive real users by DNS spoofing and phishing attacks.

10. Autopsy

Autopsy is a digital forensics tool that is used to gather information from forensics. 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 recovery software to recover files from a memory card or a pen drive. Autopsy comes pre-installed in Kali Linux.

Thank You!