Yeswanth.S.P.V

Assessment-2

10 Kali Linux tools:

1. Nmap - Nmap is a network discovery and security auditing tool. It uses raw IP packets to probe networks for hosts, services, OS detection, and more. Nmap can do TCP/UDP port scans, version detection, OS fingerprinting, and scripts for advanced detection. It offers advanced techniques like TCP SYN/CONNECT scanning, TCP/IP fingerprinting, IP spoofing, fragmentation, manipulating packet contents, specifying custom packets, scripting engine (NSE scripts), and more. This network scanner allows you to scan networks and systems to determine what ports and services are open. It can be used for network mapping, service detection, and network audits. Nmap offers many advanced features like OS detection, version detection, scripting, and more. Nmap allows for advanced port scanning using TCP/IP packet crafting and other techniques. It can determine open ports, map networks, operating system detection, version detection, and more. Nmap offers options like SYN/CONNECT/ACK scans, IP spoofing, fragmentation, specifying custom packets, scripting engine, and more.

2. Wireshark - - Wireshark is a network protocol analyzer that captures network traffic and inspects it at a micro-level. It can analyze hundreds of protocols including TCP, UDP, ICMP, HTTP, DNS, SMB, VoIP protocols, and more. Useful features include deep inspection of packet contents, advanced TCP analysis and reassembly, real-time traffic capture, displaying hexadecimal dump, detailed statistics, GeoIP mapping, expert information, configurable coloring rules, export capabilities, and more. Used for network troubleshooting, analysis, debugging, security auditing, and more.Wireshark captures packets and allows you to inspect the data at a granular level. You can analyze hundreds of protocols including TCP, UDP, HTTP, DNS, and more. It allows filtering, coloring rules, detailed analysis, hexadecimal dump, exporting data, statistics, geoIP mapping, and more. Useful for network troubleshooting, analysis, and debugging.This network protocol analyzer allows you to capture network traffic and analyze it. You can inspect hundreds of protocols, see what data is being transmitted, and debug network issues. Wireshark is useful for network troubleshooting, analysis, software debugging, and more.

3. John the Ripper - John the Ripper is a highly customizable password cracking tool that supports various hashing algorithms like DES, MD5, NT, LM, bcrypt, etc. It can crack passwords using wordlists, rule-based mutilation, brute force, and masking attacks. Useful features include distributed network cracking, incremental cracking, external mode for integration with other tools, SIMD and CUDA acceleration, dictionary statistic analysis, guessing entropy, and more. Helpful for testing password strength and enforcing strong password policies. It can use wordlists, rules, brute force, and masking attacks. Useful features include distributed cracking, incremental cracking, external mode, and more. Helpful for testing password strength. This password cracker can be used to test password strength and break weak passwords. It supports many different hash types and can crack passwords by brute

force, dictionary attacks, and other more sophisticated methods. John the Ripper can be useful for pentesting and enforcing strong password policies.

4. Aircrack-ng - Aircrack-ng is a comprehensive suite of tools for auditing wireless networks. It can monitor 802.11 networks passively, capture WEP/WPA handshakes, replay attacks, packet injection, perform deauthentication attacks, fake authentication, and more. It cracks WEP and WPA PSK keys using brute force, dictionary attacks, PTW, and advanced techniques. Useful for wireless penetration testing, WiFi security assessments, and network auditing. Aircrack-ng is a 802.11 wireless auditor. It can monitor networks passively, capture WEP/WPA handshakes, replay attacks, packet injection, fake authentication, and more. It cracks WEP and WPA PSK keys using methods like brute force, dictionary, and PTW. Useful for wireless pentesting.This tool suite allows you to assess WiFi network security. It can capture wireless traffic, crack WEP and WPA encryption keys, perform replay attacks, and more. Aircrack-ng is useful for wireless pentesting and checking WiFi security.

5. Burp Suite - Burp Suite is a web application security testing tool that intercepts and manipulates traffic between browsers and web apps. It allows spiders sites, replays traffic, fuzzes parameters, performs active/passive scanning, and more. Scans for SQLi, XSS, XXE, SSRF, and other vulnerabilities are included. Useful features include content discovery, authentication testing, payload processing, data extraction, automation via extensions, and more. Helpful for web penetration testing and finding vulnerabilities in web apps. Burp Suite is a web app auditor that intercepts traffic, allowing manipulation and analysis. It spiders sites, replays requests, fuzzes parameters, and more. Scans like SQLi, XSS, XXE can be performed. Useful features include content discovery, auth testing, payload processing, and more. Helpful for web app security testing. This web application scanner performs vulnerability assessments of web apps. It can intercept traffic, fuzzle parameters, analyze responses, discover vulnerabilities like XSS and SQLi, and more. Burp is useful for web app audits during pentesting.

6. Metasploit - Metasploit Framework is an advanced open source exploit development and attack orchestration tool. It has an extensive database of commercial, public, and community-contributed exploits targeting various operating systems, software, and devices. Allows you to search for applicable exploits, encode payloads, upgrade shells, pivot through networks, evade antivirus, and more. Useful for penetration testing and exploit research/development. Metasploit provides exploit development, payload handling, and attack automation. It has a database of commercial exploits and community contributions. You can search for exploits, use encodings to evade AV, upload shells, pivot through networks, and more. Helpful for pentesting and exploit research. This exploitation and payload framework allows you to search for, exploit, and create custom exploits for vulnerabilities. Metasploit can perform attacks, evade antivirus, upload shells, and more. It's useful for penetration testing and exploit development.

7. Maltego - Maltego is an open source intelligence and forensics tool that transforms and associates data points into relationship graphs/maps to visualize connections. It can take a single entity (name, IP address, domains, etc) and pivot through public and private data sources to map relationships. Useful for data mining, social engineering assessments, exploring attack infrastructure, threat

intelligence, investigations, and more. Maltego transforms and visualizes data relationships through link analysis and graphs. It can take an entity like a name, IP, domain, etc and map relationships by pivoting through public and private data sources. Useful for data mining, social engineering, threat intelligence and more. This forensic tool visually maps relationships between data points and entities. It transforms input into graphs to see connections. Maltego is useful for data mining, social engineering, and investigating threats.

8. OWASP ZAP - ZAP by OWASP is an open source web application security scanner designed for finding vulnerabilities in web apps and APIs. It can spider sites, perform passive and active scanning, fuzz parameters, and more. Configurable rules allow detection of SQLi, XSS, XXE, path traversal, and other vulnerabilities. Useful features include context-aware scanning, authentication testing, scripting console, plug-n-hack support, and more. Helpful for web app penetration tests. ZAP is a web app scanner that spiders sites, active/passive scans, fuzzes parameters, and more. It has configurable rules to detect SQLi, XSS, XXE, vulnerabilities. Useful features include context-aware scanning, authentication testing, script console, and more. Helpful for finding web app vulnerabilities. This web app scanner finds vulnerabilities like XSS, SQLi, XXE, and more. It can spider sites, active scan, fuzz parameters, and passive scan traffic. ZAP helps test web app security during pentesting.

9. sqlmap -- sqlmap is an open source SQL injection tool that detects and exploits SQL injection flaws in database-driven applications. It can automatically discover vulnerable parameters, extract contents of databases, read/write files to the server, execute commands on the OS, fingerprint the backend database, escalate privileges, and tamper with data. Useful for highlighting SQL injection issues and database takeovers. sqlmap detects and exploits SQL injection flaws in databases. It can determine vulnerable parameters, extract database contents, read/write files, execute commands, escalate privileges, and more. sqlmap can dump database data, perform OS takeovers, and modify data if SQLi is found. This tool automates SQL injection attacks and database takeovers. It can detect injection points, extract database contents, read files, execute commands, and more. sqlmap is useful for pentesting and highlighting SQLi vulnerabilities.

10. Nikto - Nikto scans web servers and web applications for vulnerabilities and misconfigurations. It checks for default/outdated files, programs, vulnerable software versions, and more. It uses a database of over 6500 potentially dangerous files/CGIs. Useful for hardening web servers and fixing vulnerabilities. Nikto is an open source web server and web application security scanner designed to find vulnerabilities and security misconfigurations. It uses a database of over 6500 potentially dangerous files and programs across various platforms and web servers like Apache, IIS, etc. Useful for hardening servers, fixing vulnerabilities and misconfigurations, and improving security posture.This scanner finds vulnerabilities and misconfigurations in web servers and web apps. It checks for outdated software versions, default files and configurations, and common vulnerabilities. Nikto is useful for web server audits and hardening.