Name: Sarath Rajan Senthilkumar Register No:21BCE5965

Assignment-2

Explore one tool for all Kali Linux tools (Explore any 10 tools)

1.Information gathering:

Spiderfoot:

This package contains an open source intelligence (OSINT) automation tool. Its goal is to automate the process of gathering intelligence about a given target, which may be an IP address, domain name, hostname, network subnet, ASN, e-mail address or person's name.

SpiderFoot can be used offensively, i.e. as part of a black-box penetration test to gather information about the target, or defensively to identify what information you or your organisation are freely providing for attackers to use against you.

2. Vulnerability Analysis:

NMAP:

Nmap is a utility for network exploration or security auditing. It supports ping scanning (determine which hosts are up), many port scanning techniques, version detection (determine service protocols and application versions listening behind ports), and TCP/IP fingerprinting (remote host OS or device identification). Nmap also offers flexible target and port specification, decoy/stealth scanning, sunRPC scanning, and more. Most Unix and Windows platforms are supported in both GUI and commandline modes. Several popular handheld devices are also supported, including the Sharp Zaurus and the iPAQ.

3.Web Application Analysis

Skipfish:

Skipfish is an active web application security reconnaissance tool. It prepares an interactive sitemap for the targeted site by carrying out a recursive crawl and dictionary-based probes. The resulting map is then annotated with the output from a number of active (but hopefully non-disruptive) security checks. The final report generated by the tool is meant to serve as a foundation for professional web application security assessments.

4.Database assessment:

Sqlmap:

sqlmap goal is to detect and take advantage of SQL injection vulnerabilities in web applications. Once it detects one or more SQL injections on the target host, the user can choose among a variety of options to perform an extensive back-end database management system fingerprint, retrieve DBMS session user and database, enumerate users, password hashes, privileges, databases, dump entire or user's specific DBMS tables/columns, run his own SQL statement, read specific files on the file system and more.

5.Password Attacks:

Hydra:

Hydra is a parallelized login cracker which supports numerous protocols to attack. It is very fast and flexible, and new modules are easy to add.

This tool makes it possible for researchers and security consultants to show how easy it would be to gain unauthorized access to a system remotely.

6.Wireless Attacks:

Wifite:

Hydra is a parallelized login cracker which supports numerous protocols to attack. It is very fast and flexible, and new modules are easy to add.

This tool makes it possible for researchers and security consultants to show how easy it would be to gain unauthorized access to a system remotely.

7.Reverse Engineering:

Radare2:

Radare2, or “r2,” is a powerful and versatile open-source reverse engineering toolkit. It can be used to analyze, disassemble, and debug a wide range of executable formats, including native applications, firmware, and even proprietary file formats.

8.Explotation tools:

Metasploit framework:

The Metasploit framework is a penetration testing tool for exploiting and validating vulnerabilities. It includes the fundamental architecture, particular content, and tools required for penetration testing and extensive security evaluation. It is a well-known exploitation framework that is routinely updated; new exploits are included as soon as they are announced. It includes a number of tools for constructing security workspaces for vulnerability and penetration testing systems.

9.Sniffing & spoofing:

Scapy:

Scapy is a powerful interactive packet manipulation tool, packet generator, network scanner, network discovery, packet sniffer, etc. It can for the moment replace hping, 85% of nmap, arpspoof, arp-sk, arping, tcpdump, tethereal, p0f.

In scapy you define a set of packets, then it sends them, receives answers, matches requests with answers and returns a list of packet couples (request, answer) and a list of unmatched packets. This has the big advantage over tools like nmap or hping that an answer is not reduced to (open/closed/filtered), but is the whole packet.

10.Post Exploitation:

Netcat:

A simple Unix utility which reads and writes data across network connections using TCP or UDP protocol. It is designed to be a reliable “back-end” tool that can be used directly or easily driven by other programs and scripts. At the same time it is a feature-rich network debugging and exploration tool, since it can create almost any kind of connection you would need and has several interesting built-in capabilities.