Sreya Gopakumar Nair
21BCI0214 - VIT Vellore
AI in Cyber Security with IBM Qrador
Assignment 2
Kali Linux Tools

1. Information Gathering

Nmap

Nmap (Network Mapper) is a network scanner created by Gordon Lyon. Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses.

Nmap provides a number of features for probing computer networks, including host discovery and service and operating system detection. These features are extensible by scripts that provide more advanced service detection,vulnerability detection,and other features. Nmap can adapt to network conditions including latency and congestion during a scan.

2. Vulnerability Analysis

Nikto

Nikto is a free software command-line vulnerability scanner that scans web servers for dangerous files/CGIs, outdated server software and other problems. It performs generic and server type specific checks. It also captures and prints any cookies received. The Nikto code itself is free software, but the data files it uses to drive the program are not.

Nikto can detect over 6700 potentially dangerous files/CGIs, checks for outdated versions of over 1250 servers, and version specific problems on over 270 servers. It also checks for server configuration items such as the presence of multiple index files and HTTP server options, and will attempt to identify installed web servers and software. Scan items and plugins are frequently updated and can be automatically updated.

3. Web Application Analysis

BurpSuite

Burp Suite is an integrated platform and graphical tool for performing security testing of web applications, it supports the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities. In addition to basic functionality, such as proxy server, scanner and intruder, the tool also contains more advanced options such as a spider, a repeater, a decoder, a comparer, an extender and a sequencer.

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

John the Ripper

John the Ripper is a free password cracking software tool. Originally developed for the Unix operating system, it can run on fifteen different platforms. It is among the most frequently used password testing and breaking programs as it combines a number of password crackers into one package, autodetects password hash types, and includes a customizable cracker. It can be run against various encrypted password formats including several crypt password hash types most commonly found on various Unix versions, Kerberos AFS, and Windows NT/2000/XP/2003 LM hash. Additional modules have extended its ability to include MD4-based password hashes and passwords stored in LDAP, MySQL, and others.

One of the modes John can use is the dictionary attack. It takes text string samples (usually from a file, called a wordlist, containing words found in a dictionary or real passwords cracked before), encrypting it in the same format as the password being examined (including both the encryption algorithm and key),

and comparing the output to the encrypted string. It can also perform a variety of alterations to the dictionary words and try these. Many of these alterations are also used in John's single attack mode, which modifies an associated plaintext (such as a username with an encrypted password) and checks the variations against the hashes.

John also offers a brute force mode. In this type of attack, the program goes through all the possible plaintexts, hashing each one and then comparing it to the input hash. John uses character frequency tables to try plaintexts containing more frequently used characters first. This method is useful for cracking passwords that do not appear in dictionary wordlists, but it takes a long time to run.

6. Wireless Attacks

Chirp

CHIRP is a free, open-source tool for programming your amateur radio. It supports a large number of manufacturers and models, as well as provides a way to interface with multiple data sources and formats.

7. Reverse Engineering

JAD

JAD is a Java Decompiler that's included with Kali Linux, and it seems like a useful tool for analyzing potentially dangerous Java applets that come from web pages. The biggest problem with it is that it has not had a maintainer since 2011, and so is difficult to find, except in the Kali repository and at Tomas Varaneckas's blog page, Jad Decompiler Download Mirror

8. Exploitation Tools

Metasploit Framework

The Metasploit Framework is an open source platform that supports vulnerability research, exploit development, and the creation of custom security tools. Metasploit is the world's leading open-source penetrating framework used by security engineers as a penetration testing system and a development platform that allows to create security tools and exploits. The framework makes hacking simple for both attackers and defenders.

9. Sniffing and Spoofing

Wireshark

Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Originally named Ethereal, the project was renamed Wireshark in May 2006 due to trademark issues.

Wireshark is cross-platform, using the Qt widget toolkit in current releases to implement its user interface, and using pcap to capture packets; it runs on Linux, macOS, BSD, Solaris, some other Unix-like operating systems, and Microsoft Windows. There is also a terminal-based (non-GUI) version called TShark. Wireshark, and the other programs distributed with it such as TShark, are free software, released under the terms of the GNU General Public License version 2 or any later version.

Wireshark lets the user put network interface controllers into promiscuous mode (if supported by the network interface controller), so they can see all the traffic visible on that interface including unicast traffic not sent to that network interface controller's MAC address. However, when capturing with a packet analyzer in promiscuous mode on a port on a network switch, not all traffic through the switch is necessarily sent to the port where the capture is done, so capturing in promiscuous mode is not necessarily sufficient to see all network traffic. Port mirroring or various network taps extend capture to any point on the network. Simple passive taps are extremely resistant to tampering
If a remote machine captures packets and sends the captured packets to a machine running Wireshark using the TZSP protocol or the protocol used by OmniPeek, Wireshark dissects those packets, so it can analyze packets captured on a remote machine at the time that they are captured.

10. Post Exploitation

Netcat

netcat (often abbreviated to nc) is a computer networking utility for reading from and writing to network connections using TCP or UDP. The command is designed to be a dependable back-end 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 investigation tool, since it can produce almost any kind of connection its user could need and has a number of built-in capabilities.

It is able to perform port scanning, file transferring and port listening.