AI FOR CYBERSECURITY WITH IBM QRADAR

ASSIGNMENT – 2

NAME: ORRA RAGHAVENDRA REDDY

BRANCH: CSE – INFORMATIION SECURITY

COLLEGE: VIT – VELLORE

THERE ARE 13 SECTIONS WITH DIFFERENT TOOLS WITH RESPECTIVE USAGE.

1. Information Gathering
   These are all the tools available under this section

Nmap:

Nmap ("Network Mapper") is an open-source tool for network exploration and security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. While Nmap is commonly used for security audits, many systems and network administrators find it useful for routine tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

The output from Nmap is a list of scanned targets, with supplemental information on each depending on the options used. Key among that information is the "interesting ports table". That table lists the port number and protocol, service name, and state. The state is either open, filtered, closed, or unfiltered. Open means that an application on the target machine is listening for connections/packets on that port.

```
                              kali@kali: ~
File  Actions  Edit  View  Help
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-02 08:30 EDT
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.35 seconds

  ┌──(kali㉿kali)-[~]
  └─$ nmap -A 192.168.29.107
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-02 08:30 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try
-Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.24 seconds

  ┌──(kali㉿kali)-[~]
  └─$ nmap -Pn 192.168.29.107
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-02 08:30 EDT
Nmap scan report for 192.168.29.107
Host is up (0.0015s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
6646/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 5.26 seconds
```

2. Vulnerability analysis
   These are all the tools available under this section
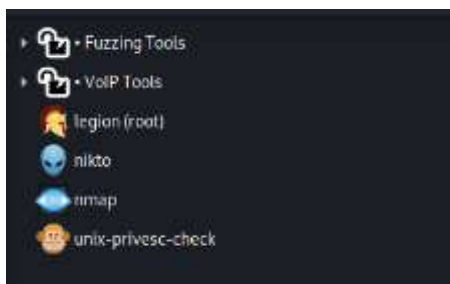
   Unix-privesc-check:

   It does a vulnerability analysis check on the system its running and gives a detailed information of the vulnerabilities that are found.

3. Web Application analysis

These are all the tools available under this section
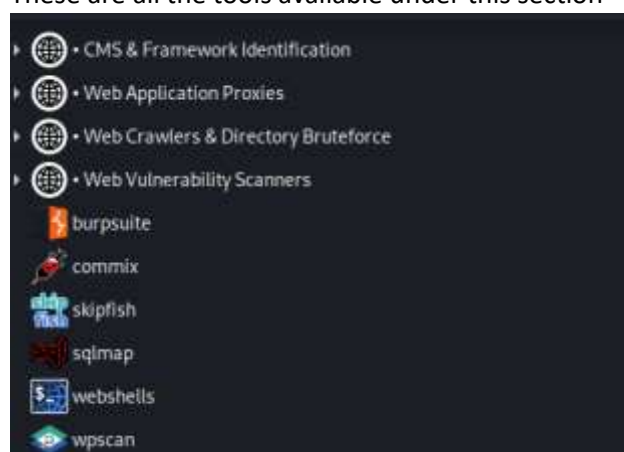
Skipfish:

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.

A new directory named google has been created. And the report that has been generated is stored in index.html file.

The index file is displayed in the browser

4. Database assessment
    These are all the tools available under this section
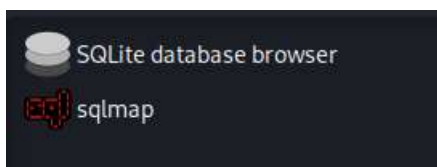
    SQlite database browser:
    SQLite Database Browser, also known as DB Browser for SQLite, is an open-source graphical user interface (GUI) tool for working with SQLite databases on Linux and other platforms. SQLite is a popular and lightweight relational database management system often used in embedded systems, mobile applications, and desktop software.
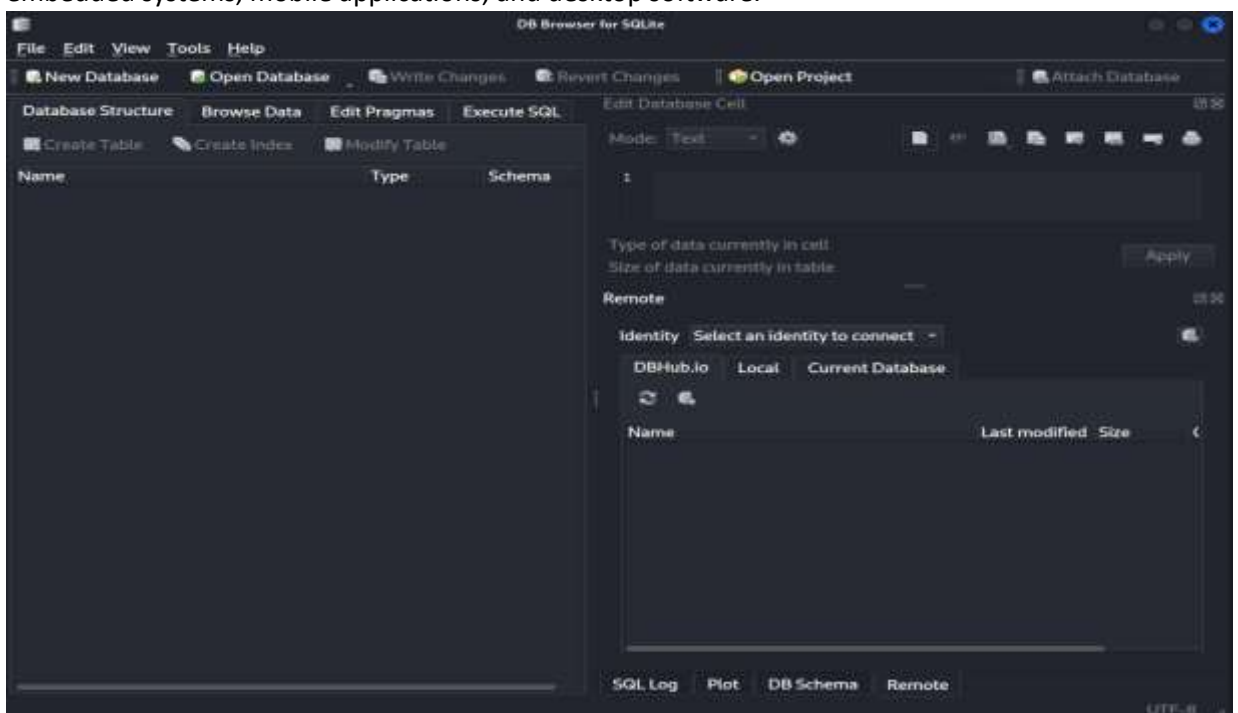
5. Password attacks

These are all the tools available under this section
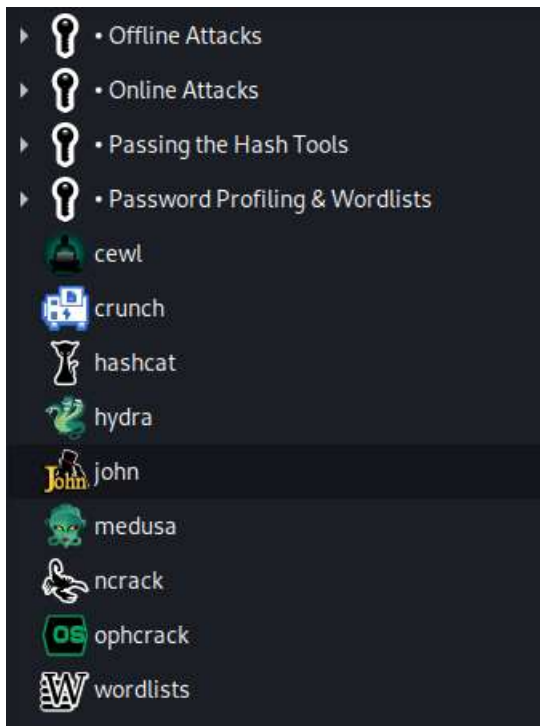
John the ripper:
This manual page documents briefly the john command. This manual page was written for the Debian GNU/Linux distribution because the original program does not have a manual page. john, better known as John the Ripper, is a tool to find weak passwords of users in a server. John can use a dictionary or some search pattern as well as a password file to check for passwords. John supports different cracking modes and understands many ciphertext formats, like several DES variants, MD5 and blowfish. It can also be used to extract AFS and Windows NT passwords.

To use John, you just need to supply it a password file and the desired options. If no mode is specified, john will try "single" first, then "wordlist" and finally "incremental".

    Once John finds a password, it will be printed to the terminal and saved into a file called ~/.john/john.pot. John will read this file when it restarts so it doesn't try to crack already done passwords.

First, create a text file with some md5 hash generated text in it.

Now we have to use John the ripper to decrypt the text

```
┌──(kali㊉kali)-[~/Desktop]
└─$ john password.txt --format=Raw-MD5
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8×3])
Warning: no OpenMP support for this hash type, consider --fork=4
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
password         (?)
1g 0:00:00:00 DONE 2/3 (2023-09-05 05:51) 20.00g/s 7680p/s 7680c/s 7680C/s 123456..larry
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

6. Wireless attacks

These are all the tools available under this section
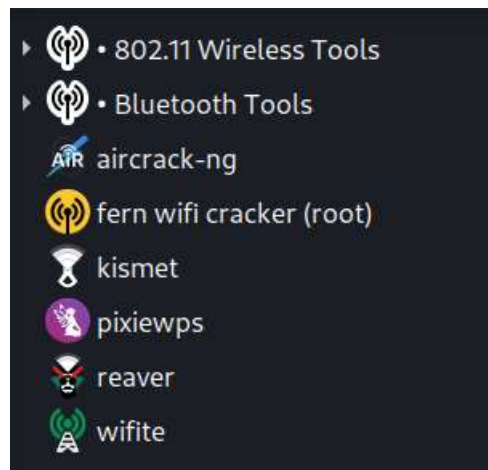
Kismet:

Nearly all of these options are run-time overrides for values in the kismet.conf configuration file. Permanent changes should be made to the configuration file.

It scans for the available wireless connection

```
┌──(kali⊛kali)-[~]
└─$ sudo kismet -c wlan0mon
[sudo] password for kali:
INFO: Including sub-config file: /etc/kismet/kismet_httpd.conf
INFO: Including sub-config file: /etc/kismet/kismet_memory.conf
INFO: Including sub-config file: /etc/kismet/kismet_alerts.conf
INFO: Including sub-config file: /etc/kismet/kismet_80211.conf
INFO: Including sub-config file: /etc/kismet/kismet_logging.conf
INFO: Including sub-config file: /etc/kismet/kismet_filter.conf
INFO: Including sub-config file: /etc/kismet/kismet_uav.conf
INFO: Loading config override file '/etc/kismet/kismet_package.conf'
INFO: Optional sub-config file not present: /etc/kismet/kismet_package.conf
INFO: Loading config override file '/etc/kismet/kismet_site.conf'
INFO: Optional sub-config file not present: /etc/kismet/kismet_site.conf
INFO: Local config and cache directory '/root/.kismet/' does not exist;
      creating it.

INFO: Enabling channel hopping by default on sources which support channel
      control.
INFO: Setting default channel hop rate to 5/sec
INFO: Enabling channel list splitting on sources which share the same list
      of channels
INFO: Enabling channel list shuffling to optimize overlaps
INFO: Sources will be re-opened if they encounter an error
INFO: Saving datasources to the Kismet database log evert 30 seconds
INFO: Launching remote capture server on 127.0.0.1 3501
INFO: Data sources passed on the command line (via -c source), ignoring
      source= definitions in the Kismet config file.
INFO: Probing interface 'wlan0mon' to find datasource type
INFO: Opened kismetdb log file './/Kismet-20230905-10-11-20-1.kismet'
INFO: Saving packets to the Kismet database log.
INFO: GPS track will be logged to the Kismet logfile
ALERT: ROOTUSER Kismet is running as root; this is less secure.  If you
       are running Kismet at boot via systemd, make sure to use `systemctl
       edit kismet.service` to change the user.  For more information, see
       the Kismet README for setting up Kismet with minimal privileges.
INFO: Starting Kismet web server ...
INFO: HTTP server listening on 0.0.0.0:2501
INFO: Could not open system plugin directory (/usr/lib/x86_64-linux-gnu/kis
      met/), skipping: No such file or directory
INFO: Did not find a user plugin directory (/root/.kismet//plugins/),
      skipping: No such file or directory
ERROR: Unable to find driver for 'wlan0mon'.  Make sure that any required
       plugins are loaded, the interface is available, and any required
       Kismet helper packages are installed.
ERROR: Data source 'wlan0mon' failed to launch: Unable to find driver for
       'wlan0mon'.  Make sure that any required plugins are loaded, the
       interface is available, and any required Kismet helper packages are
       installed.
```

7. Reverse engineering
   These are all the available tools under this section

8. Exploitation tools

These are all the available tools under this section
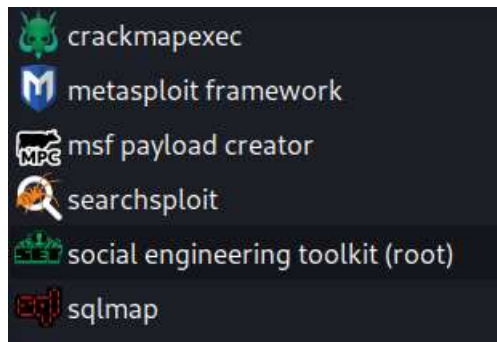
9. Sniffing and Spoofing
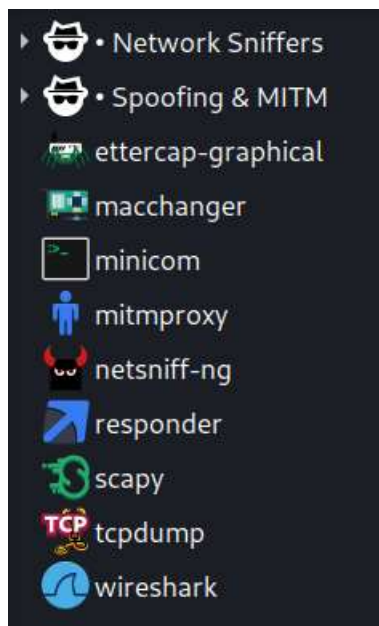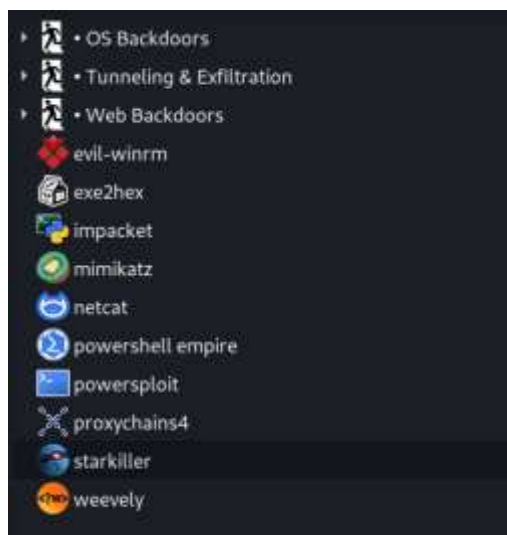
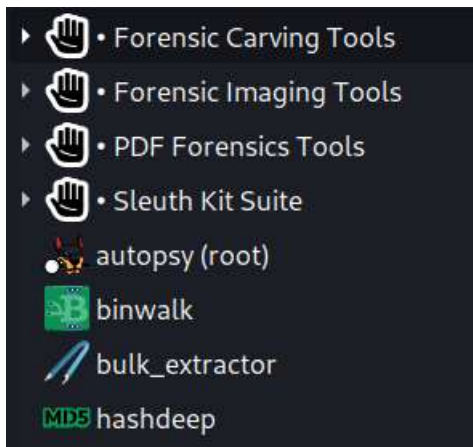These are all the available tools under this section

10. Post Exploitation:

These are all the available tools under this section

11. Forensics

These are all the available tools under this section

▸ 🖐 • Forensic Carving Tools
▸ 🖐 • Forensic Imaging Tools
▸ 🖐 • PDF Forensics Tools
▸ 🖐 • Sleuth Kit Suite
   autopsy (root)
   binwalk
   bulk_extractor
   hashdeep

12. Reporting tools

These are all the available tools under this section

   CherryTree
   cutycapt
   faraday start
   maltego (installer)
   pipal
   recordmydesktop

13. Social Engineering tools

These are all the available tools under this section

   maltego (installer)
   msf payload creator
   social engineering toolkit (root)