

NAME: MUNGILI CHETAN SAI RAJU

ASSIGNMENT 2

KALI TOOLS

01- Information Gathering: theHarvester

- Tool: theHarvester
- Purpose: theHarvester is a command-line tool used for collecting email addresses, subdomains, virtual hosts, open ports, and employee names from various public sources. It's particularly useful during the information gathering phase to gather intelligence about a target.
- Usage Example:

Code:

```
theharvester -d example.com -l 500 -b all
```

```
root@kali:~# theHarvester -d kali.org -l 200 -b google
table results already exists

*****
*
* theHarvester
*
* theHarvester 3.1.0
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*
*****

[*] Target: kali.org
[*] Searching Google.
    Searching 0 results.
    Searching 100 results.
    Searching 200 results.

[*] No IPs found.
[*] Emails found: 2
-----
devel@kali.org
steev@kali.org

[*] Hosts found: 15
-----
archive-10.kali.org:167.114.101.149
bugs.kali.org:192.124.249.169
cdimage.kali.org:192.99.200.113
docs.kali.org:50.116.58.136
downloads.kali.org:149.56.27.8, 23.237.148.130, 199.189.86.7, 188.138.17.16, 192.99.63.209
forums.kali.org:192.124.249.12
http.kali.org:192.99.200.113
old.kali.org:54.39.49.227
pkg.kali.org:192.124.249.9
security.kali.org:192.99.200.113
status.kali.org:192.124.249.56
tools.kali.org:192.124.249.6
www.docs.kali.org:50.116.58.136
www.kali.org:192.124.249.10
x3www.kali.org:
root@kali:~#
```

This command instructs theHarvester to search for information related to the domain example.com, limit the number of results to 500, and use all available data sources.

02- Vulnerability Analysis: OpenVAS

- Tool: OpenVAS (Open Vulnerability Assessment System)
- Purpose: OpenVAS is a powerful vulnerability scanner that helps identify security vulnerabilities in target systems. It performs comprehensive

vulnerability assessments by scanning for known vulnerabilities and misconfigurations.

- Usage Example:
 - Install OpenVAS and set it up using the Kali Linux tools menu.
 - Access OpenVAS through a web interface and configure scan tasks.
 - Start vulnerability scans against target systems to identify potential security issues.

```
File Actions Edit View Help
(kali@kali)~[~/Downloads]
$ sudo apt-get install gvm*
[sudo] password for kali:
Reading package lists... Done
Building dependency tree
Reading state information... Done
Note, selecting 'gvm-tools' for glob 'gvm*'
Note, selecting 'gvmd-dbgSYM' for glob 'gvm*'
Note, selecting 'gvm' for glob 'gvm*'
Note, selecting 'gvmd-common' for glob 'gvm*'
Note, selecting 'gvmd' for glob 'gvm*'
gvm is already the newest version (20.8.0-0kali3).
gvm-tools is already the newest version (20.10.1-1).
gvm-tools set to manually installed.
gvmd is already the newest version (20.8.0+git20201111-0kali2).
gvmd-common is already the newest version (20.8.0+git20201111-0kali2).
gvmd-common set to manually installed.
The following package was automatically installed and is no longer required:
 liblvm10
Use 'sudo apt autoremove' to remove it.
The following NEW packages will be installed:
 gvmd-dbgSYM
0 upgraded, 1 newly installed, 0 to remove and 144 not upgraded.
Need to get 1,412 kB of archives.
After this operation, 1,565 kB of additional disk space will be used.
Do you want to continue? [Y/n]
```

03- Web Application Analysis: Burp Suite

- Tool: Burp Suite
- Purpose: Burp Suite is a widely used web application security testing tool. It helps penetration testers and security professionals assess the security of web applications by identifying vulnerabilities like SQL injection, cross-site scripting (XSS), and more.
- Usage Example:
 - Launch Burp Suite and configure your browser to proxy traffic through it.
 - Interact with the target web application to capture and analyze requests and responses.
 - Use built-in tools like the scanner to identify and report vulnerabilities.



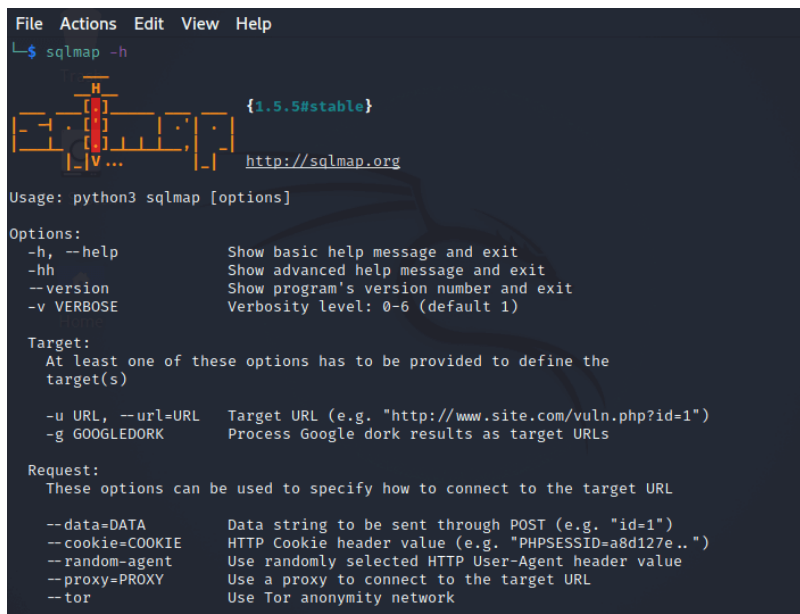
04- Database Assessment: SQLMap

- Tool: SQLMap
- Purpose: SQLMap is a popular command-line tool used for detecting and exploiting SQL injection vulnerabilities in web applications. It automates the process of identifying vulnerable parameters and extracting data from databases.
- Usage Example:

Code:

```
sqlmap -u "http://example.com/vulnerable_page.php?id=1" --dump
```

This command instructs SQLMap to test the given URL for SQL injection vulnerabilities and dump the database contents if successful.

A screenshot of a terminal window showing the help output for the SQLMap tool. The window has a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. The command prompt shows 'L-\$ sqlmap -h'. The output includes a logo, the version '{1.5.5#stable}', the website 'http://sqlmap.org', and a usage line 'Usage: python3 sqlmap [options]'. It then lists options: '-h, --help' (Show basic help message and exit), '-hh' (Show advanced help message and exit), '--version' (Show program's version number and exit), and '-v VERBOSE' (Verbosity level: 0-6 (default 1)). Under 'Target:', it says 'At least one of these options has to be provided to define the target(s)' and lists '-u URL, --url=URL' (Target URL (e.g. "http://www.site.com/vuln.php?id=1")) and '-g GOOGLEDORK' (Process Google dork results as target URLs). Under 'Request:', it says 'These options can be used to specify how to connect to the target URL' and lists '--data=DATA' (Data string to be sent through POST (e.g. "id=1")), '--cookie=COOKIE' (HTTP Cookie header value (e.g. "PHPSESSID=a8d127e..")), '--random-agent' (Use randomly selected HTTP User-Agent header value), '--proxy=PROXY' (Use a proxy to connect to the target URL), and '--tor' (Use Tor anonymity network).

05- Password Attacks: Hydra

- Tool: Hydra
- Purpose: Hydra is a versatile password-cracking tool that supports various protocols and services. It can perform brute-force attacks, dictionary attacks, and hybrid attacks to crack passwords for services like SSH, FTP, RDP, and more.
- Usage Example:

Code:

```
hydra -l username -P password_list.txt ssh://target_ip
```

This command tells Hydra to perform an SSH brute-force attack against the target IP address using a list of usernames and a password list.

```
File Actions Edit View Help
root@kali: ~
(root@kali)~# hydra -l testuser -P /usr/share/wordlists/rockyou.txt -f localhost ssh
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-09-27 16:40:36
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896 525 tries per task
[DATA] attacking ssh://localhost:22/
[STATUS] 161.00 tries/min, 161 tries in 00:01h, 14344238 to do in 1484:55h, 16 active
[22][ssh] host: localhost login: testuser password: peanut
[STATUS] attack finished for localhost (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-09-27 16:41:37

(root@kali)~#
```

06- Wireless Attacks: Aircrack-ng

- Tool: Aircrack-ng
- Purpose: Aircrack-ng is a suite of tools used for auditing wireless networks. It can crack WEP and WPA/WPA2 encryption keys, capture network traffic, and perform various wireless network-related tasks.
- Usage Example:
 - Use airmon-ng to put a wireless network interface into monitor mode.
 - Capture packets with airodump-ng.
 - Crack a WEP or WPA key using aircrack-ng.

```
kali@kali: ~
File Actions Edit View Help
root@kali:/home/kali# airmon-ng start wlan0 10

Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

  PID Name
  580 NetworkManager
  794 wpa_supplicant

PHY      Interface      Driver      Chipset
phy0     wlan0             iwlwifi     Intel Corporation Wireless-AC 9560 [Jefferson Peak] (rev 10)

(mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
(mac80211 station mode vif disabled for [phy0]wlan0)

root@kali:/home/kali#
```

07- Reverse Engineering: Ghidra

- Tool: Ghidra
- Purpose: Ghidra is an open-source software reverse engineering (SRE) framework developed by the National Security Agency (NSA). It helps analysts reverse engineer binary executables to understand their functionality and identify vulnerabilities.

- Usage Example:
 - Load a binary executable into Ghidra.
 - Analyze the disassembly code, debug the binary, and explore its functions and data structures.



08- Exploitation Tools: Metasploit Framework

- Tool: Metasploit Framework
- Purpose: Metasploit is a penetration testing framework that allows security professionals to develop, test, and execute exploit code against known vulnerabilities. It helps identify and validate vulnerabilities in target systems.
- Usage Example:
 - Search for exploits using msfconsole.
 - Configure and launch exploits against vulnerable targets.
 - Gain access to compromised systems for post-exploitation activities.

09- Sniffing & Spoofing: Wireshark

- Tool: Wireshark
- Purpose: Wireshark is a widely-used network protocol analyzer that allows users to capture and inspect network traffic in real-time. It is valuable for network troubleshooting, security analysis, and packet capture.
- Usage Example:
 - Start Wireshark and select the network interface to capture traffic.
 - Analyze captured packets to understand network behavior and identify potential security issues.

```

kali@kali: ~$ tshark -h
tshark (Wireshark) 3.2.1 (Git v3.2.1 packaged as 3.2.1-1)
Dump and analyze network traffic.
See https://www.wireshark.org for more information.

Usage: tshark [options] ...

Capture interface:
  -i <interface>, --interface <interface>      name or id of interface (def: first non-loopback)
  -f <capture filter>                          packet filter in libpcap filter syntax
  -s <snaplen>, --snapshot-length <snaplen>     packet snapshot length (def: appropriate maximum)
  -p, --no-promiscuous-mode                    don't capture in promiscuous mode
  -j, --monitor-mode                            Capture in monitor mode, if available
  -b <buffer size>, --buffer-size <buffer size>  size of kernel buffer (def: 2MB)
  -y <link type>, --linktype <link type>         link layer type (def: first appropriate)
  --time-stamp-type <types>                     timestamp method for interface
  -D, --list-interfaces                          print list of interfaces and exit
  -L, --list-data-link-types                     print list of link-layer types for iface and exit
  --list-time-stamp-types                       print list of timestamp types for iface and exit

Capture stop conditions:
  -c <packet count>                             stop after n packets (def: infinite)
  -a <autostop cond.> ...                        --autostop <autostop cond.> ...
  --duration:NUM                                stop after NUM seconds
  --filesize:NUM                                stop this file after NUM KB
  --files:NUM                                   stop after NUM files
  --packets:NUM                                 stop after NUM packets

Capture output:
  -b <ringbuffer opt.> ... --ring-buffer <ringbuffer opt.>

```

10- Post Exploitation: Meterpreter

- Tool: Meterpreter (part of the Metasploit Framework)
- Purpose: Meterpreter is a post-exploitation framework that provides an interactive shell on compromised systems. It allows attackers to maintain control over a compromised host, gather information, and perform various actions.
- Usage Example:
 - After successfully exploiting a target with Metasploit, a Meterpreter session can be opened to interact with the compromised system.
 - Commands within Meterpreter enable actions like file manipulation, privilege escalation, and further reconnaissance.