

# ASSIGNMENT 2

## Overview of Assignment

To explore 10 tools in Kali Linux, one from each different section of tools like information gathering, vulnerability analysis, wireless attacks etc. and write about them or show the action.

## KALI LINUX TOOLS

Kali Linux is a popular penetration testing and ethical hacking distribution that provides a wide range of tools across various categories. Let's explore one tool from each of the specified categories:

### 1. Information Gathering Tool - dnsenum:

**Purpose:** Dnsenum is a tool for gathering information about a target's DNS infrastructure. It can be used to discover subdomains, identify DNS misconfigurations, and gather data about the DNS zone.

**Action:** To use dnsenum, open a terminal in Kali Linux and run a command like ``dnsenum example.com`` to enumerate DNS information for the "example.com" domain.

```

root@kali:~# dnsenum zonetransfer.me
Smartmatch is experimental at /usr/bin/dnsenum line 698.
Smartmatch is experimental at /usr/bin/dnsenum line 698.
dnsenum VERSION:1.2.4

-----  zonetransfer.me  -----

Host's addresses:
-----
zonetransfer.me.                7199      IN      A       5.196.105.14

Name Servers:
-----
nsztml.digi.ninja.              10799     IN      A       81.4.108.41
nsztm2.digi.ninja.              10799     IN      A       34.225.33.2

Mail (MX) Servers:
-----
ASPMX.L.GOOGLE.COM.            292       IN      A       173.194.68.27
ALT1.ASPMX.L.GOOGLE.COM.        292       IN      A       172.217.192.27
ASPMX2.GOOGLEMAIL.COM.         292       IN      A       172.217.192.27
ALT2.ASPMX.L.GOOGLE.COM.        292       IN      A       209.85.202.27
ASPMX3.GOOGLEMAIL.COM.         292       IN      A       209.85.202.26
ASPMX4.GOOGLEMAIL.COM.         292       IN      A       173.194.76.26
ASPMX5.GOOGLEMAIL.COM.         292       IN      A       74.125.128.26

```

## 2. Vulnerability Analysis Tool - Nmap (Network Mapper):

**Purpose:** Nmap is a powerful open-source network scanning and vulnerability analysis tool. It's used to discover open ports, services, and vulnerabilities on target systems.

**Action:** To scan a target, use a command like `nmap -T4 -A -v target\_IP` to perform a thorough scan, including OS detection and service enumeration.

```

└─$ nmap -A -T4 scanme.nmap.org
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-10 01:29 IST
Warning: 45.33.32.156 giving up on port because retransmission cap hit (6).
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.070s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 976 closed tcp ports (reset)
PORT      STATE      SERVICE      VERSION
22/tcp    open      ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux;
protocol 2.0)
|_ ssh-hostkey:
|   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|   2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|   256  96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
|_  256  33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)
80/tcp    open      http         Apache httpd 2.4.7 ((Ubuntu))
|_ http-title: Go ahead and ScanMe!
|_ http-favicon: Nmap Project
|_ http-server-header: Apache/2.4.7 (Ubuntu)
100/tcp   filtered  newacct
139/tcp   filtered  netbios-ssn
366/tcp   filtered  odmr
445/tcp   filtered  microsoft-ds

```

### 3. Web Application Analysis Tool - WPScan:

Purpose: WPScan is a WordPress vulnerability scanner. It helps identify vulnerabilities, misconfigurations, and security issues in WordPress websites.

Action: Run a command like `wpscan --url https://example.com` to scan a WordPress website for vulnerabilities.

```
msf5 > wmap_run -t
[*] Testing target:
[*]   Site: 192.168.198.130 (192.168.198.130)
[*]   Port: 80 SSL: false
=====
[*] Testing started. 2019-03-24 04:13:11 -0400
[*] Loading wmap modules...
[*] 39 wmap enabled modules loaded.
[*]
=[ SSL testing ]=
=====
[*] Target is not SSL. SSL modules disabled.
[*]
=[ Web Server testing ]=
=====
[*] Module auxiliary/scanner/http/http_version
[*] Module auxiliary/scanner/http/open_proxy
[*] Module auxiliary/admin/http/tomcat_administration
[*] Module auxiliary/admin/http/tomcat_utf8_traversal
[*] Module auxiliary/scanner/http/drupal_views_user_enum
[*] Module auxiliary/scanner/http/frontpage_login
[*] Module auxiliary/scanner/http/host_header_injection
[*] Module auxiliary/scanner/http/options
[*] Module auxiliary/scanner/http/robots_txt
[*] Module auxiliary/scanner/http/scraper
[*] Module auxiliary/scanner/http/svn_scanner
[*] Module auxiliary/scanner/http/trace
[*] Module auxiliary/scanner/http/vhost_scanner
[*] Module auxiliary/scanner/http/webdav_internal_ip
[*] Module auxiliary/scanner/http/webdav_scanner
[*] Module auxiliary/scanner/http/webdav_website_content
[*]
```

### 4. Database Assessment Tool - SQLmap:

Purpose: SQLmap is a tool for detecting and exploiting SQL injection vulnerabilities in web applications. It automates the process of identifying and exploiting these vulnerabilities.

Action: Use a command like `sqlmap -u "http://example.com/page?id=1"` to test a URL for SQL injection vulnerabilities.

```
$ python sqlmap.py -u "http://debiandev/sqlmap/mysql/get_int.php?id=1" --batch

{1.0.5.63#dev}

[!~] http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting at 17:43:06

[17:43:06] [INFO] testing connection to the target URL
[17:43:06] [INFO] heuristics detected web page charset 'ascii'
[17:43:06] [INFO] testing if the target URL is stable
[17:43:07] [INFO] target URL is stable
[17:43:07] [INFO] testing if GET parameter 'id' is dynamic
[17:43:07] [INFO] confirming that GET parameter 'id' is dynamic
[17:43:07] [INFO] GET parameter 'id' is dynamic
[17:43:07] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable (possible DBMS: 'MySQL')
```

## 5. Exploring Password Attacks Tool - Ncrack:

Purpose: Ncrack is a network authentication cracking tool. It can be used to perform brute-force attacks on various network protocols to crack passwords.

Action: Run a command like `ncrack -p 22 target\_IP` to attempt SSH password cracking on the specified IP.

```
root@kali:~# ncrack -U username.txt -P password.txt ftp://192.168.1.11 -oN res.txt

Starting Ncrack 0.7 ( http://ncrack.org ) at 2020-10-27 08:30 EDT

Discovered credentials for ftp on 192.168.1.11 21/tcp:
192.168.1.11 21/tcp ftp: 'msfadmin' 'msfadmin'
192.168.1.11 21/tcp ftp: 'shubham' 'neon'
192.168.1.11 21/tcp ftp: 'shubham' 'neon'
192.168.1.11 21/tcp ftp: 'shubham' 'neon'

Ncrack done: 1 service scanned in 18.00 seconds.

Ncrack finished.
root@kali:~# cat res.txt
# Ncrack 0.7 scan initiated Tue Oct 27 08:30:57 2020 as: ncrack -U username.txt -P password.txt -oN res.txt ftp://192.168.1.11
Discovered credentials for ftp on 192.168.1.11 21/tcp:
192.168.1.11 21/tcp ftp: 'msfadmin' 'msfadmin'
192.168.1.11 21/tcp ftp: 'shubham' 'neon'
192.168.1.11 21/tcp ftp: 'shubham' 'neon'
192.168.1.11 21/tcp ftp: 'shubham' 'neon'

# Ncrack done at Tue Oct 27 08:31:15 2020 -- 1 service scanned in 18.00 seconds.
root@kali:~#
```

## 6. Exploring Wireless Attacks Tool - Wifite:

Purpose: Wifite is a wireless penetration testing tool. It automates the process of auditing wireless networks, including WEP, WPA, and WPS attacks.

Action: Run `wifite` from the command line to launch the tool, and follow the prompts to target and crack wireless networks.

```
root@kali:~# wifite

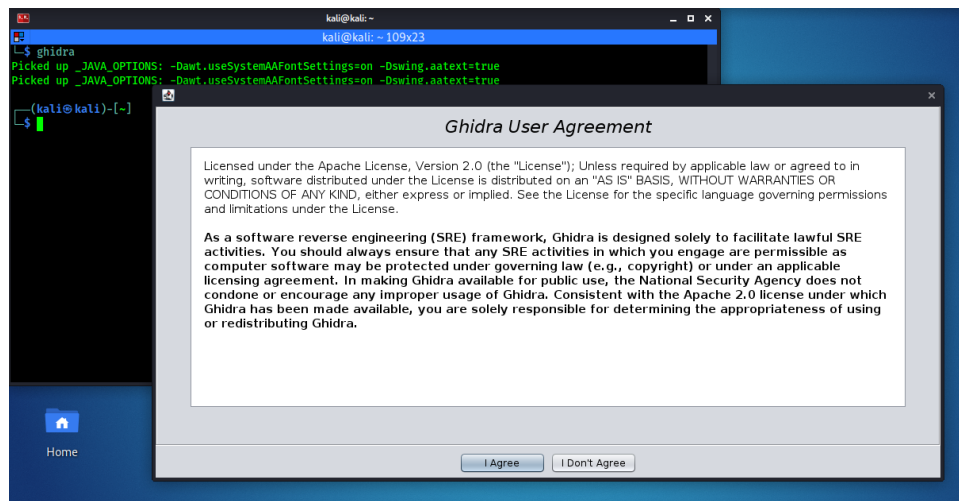
WiFiite v2 (r87)
automated wireless auditor
designed for Linux

[+] scanning for wireless devices...
[+] enabling monitor mode on wlan0... done
[+] initializing scan (wlan0mon), updates at 5 sec intervals, CTRL+C when ready.
[0:00:05] scanning wireless networks. 0 targets and 0 clients found
```

## 7. Reverse Engineering Tools - Clang and Ghidra:

Purpose: Clang is a compiler frontend for the C, C++, and Objective-C programming languages. Ghidra is a software reverse engineering framework. These tools are used to analyze and decompile software.

Action: Clang is used to compile and analyze code, while Ghidra is employed for decompilation and reverse engineering tasks.




## 8. Exploiting IP Address Tool - Metasploit Framework:

Purpose: The Metasploit Framework is a versatile tool for penetration testing and exploiting vulnerabilities. It provides a wide range of exploits and payloads.



Action: Launch Metasploit by running `msfconsole` in the terminal, and use it to select and launch exploits against target systems.

```
[root@kali:~# msfconsole]
[~] Failed to connect to the database: could not connect to server: Connection refused
Is the server running on host "localhost" (:::1) and accepting
TCP/IP connections on port 5432?
could not connect to server: Connection refused
Is the server running on host "localhost" (127.0.0.1) and accepting
TCP/IP connections on port 5432?
```



```
dBBBBbb dBBBp dBBBBBBp dBBBBbb
' dB' BBp
dB'dB'dB' dBBp dBp dB BB
dB'dB'dB' dBBp dBp dB BB
dB'dB'dB' dBBBBBp dBp dBBBBBBB

dBBBBBP dBBBBbb dBp dBBBBBp dBp dBBBBBBp
- - dB' dBp dB' .BP
| | dBp dBBBB' dBp dB'.BP dBp dBp
--o-- oBP dBp dBp dB'.BP dBp dBp
| dBBBBP dBp dBBBBBp dBBBBBp dBp dBp

To boldly go where no
shell has gone before

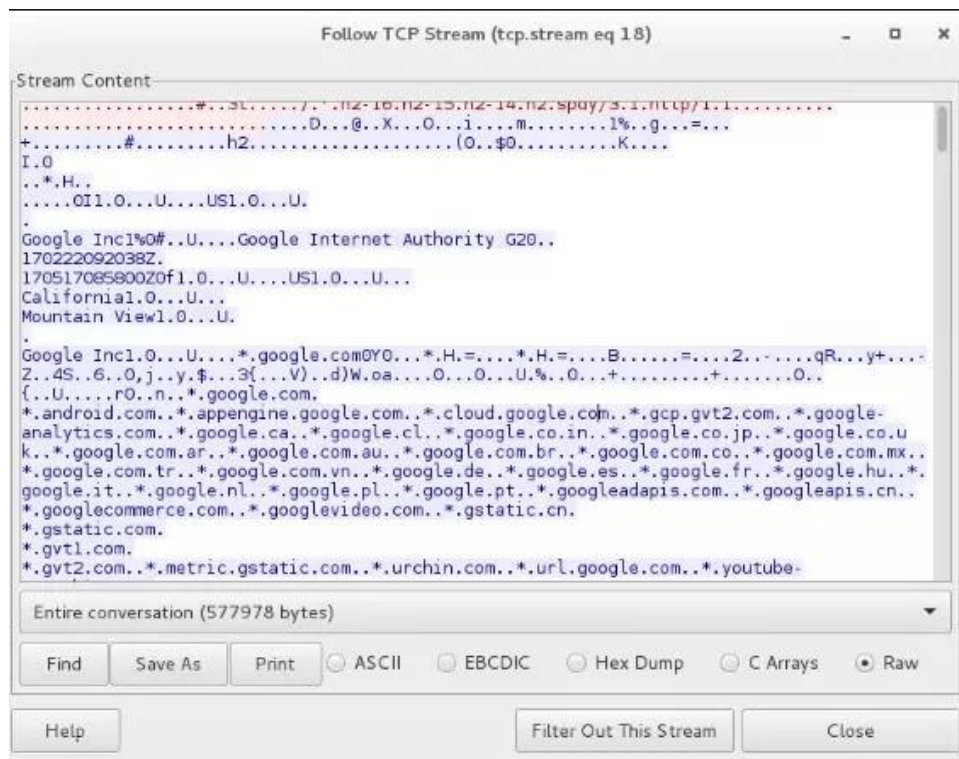
=[ metasploit v4.17.3-dev ]
+ -- ==[ 1795 exploits - 1019 auxiliary - 310 post ]
+ -- ==[ 538 payloads - 41 encoders - 10 nops ]
+ -- ==[ Free Metasploit Pro trial: http://r-7.co/trymsp ]
```

msf > |

## 9. Exploring Sniffing and Spoofing Tool - Wireshark:

Purpose: Wireshark is a popular network protocol analyzer used for network troubleshooting, analysis, and packet capturing. It can be used for network traffic analysis.

Action: Start Wireshark, select a network interface, and capture packets to analyze network traffic.



## 10. Exploring Post Exploitation Tool - Mimikatz:

**Purpose:** Mimikatz is a post-exploitation tool used for extracting passwords and other credentials from memory. It's often used after gaining unauthorized access to a system.

**Action:** Mimikatz is a powerful tool; its usage is extensive and can involve extracting credentials, keys, and tokens from compromised systems.

```
meterpreter > load mimikatz
Loading extension mimikatz...Success.
meterpreter > kerberos
[!] Not currently running as SYSTEM
[*] Attempting to getprivs
[+] Got SeDebugPrivilege
[*] Retrieving kerberos credentials
kerberos credentials
=====
```

AuthID	Package	Domain	User	Password
-----	-----	-----	----	-----
0;996	Negotiate	WORKGROUP	WIN-JWBPPZSXEfv\$	
0;67846	NTLM			
0;997	Negotiate	NT AUTHORITY	LOCAL SERVICE	
0;999	NTLM	WORKGROUP	WIN-JWBPPZSXEfv\$	
0;134956	NTLM	WIN-JWBPPZSXEfv	Administrator	P@ssw0rd

```
meterpreter > 
```