

ASSIGNMENT-2

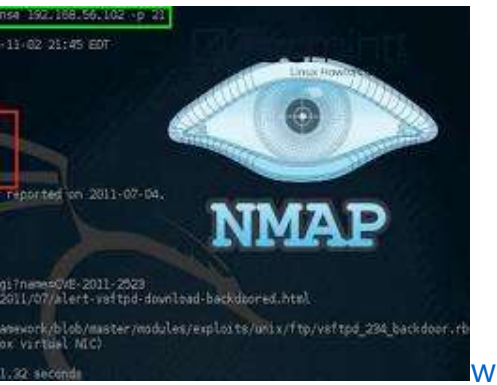
NAME: OMKAR SANJAY NARKAR

REG.NO.:21BCE8412

Kali Linux tools for information gathering, vulnerability analysis, and web application analysis:

Information Gathering Tools

- Nmap: A network scanner that can be used to discover hosts and services on a network. It can also be used to identify open ports and running services, which can be used as an initial step in penetration testing.



Nmap tool in Kali Linux

- TheHarvester: A tool that can be used to collect information about a target from public sources, such as social media, WHOIS records, and search engines.



TheHarvester tool in Kali Linux

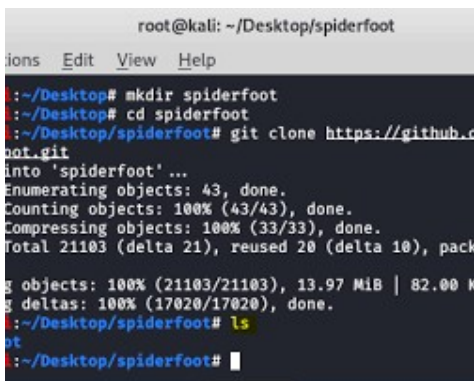
ASSIGNMENT-2

- Metagoofil: A tool that can be used to search for keywords in Google Drive, Dropbox, and other cloud storage services.



Metagoofil tool in Kali Linux

- Spiderfoot: A tool that can be used to collect information about a target from a variety of sources, including social media, the dark web, and public records.



Spiderfoot tool in Kali Linux

- Shodan: A search engine that can be used to find internet-connected devices, such as routers, cameras, and printers.

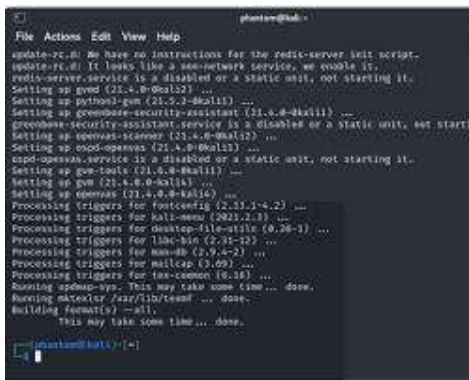
ASSIGNMENT-2



Shodan tool in Kali Linux

Vulnerability Analysis Tools

- OpenVAS: A vulnerability scanner that can be used to scan for vulnerabilities in hosts and networks.



OpenVAS tool in Kali Linux

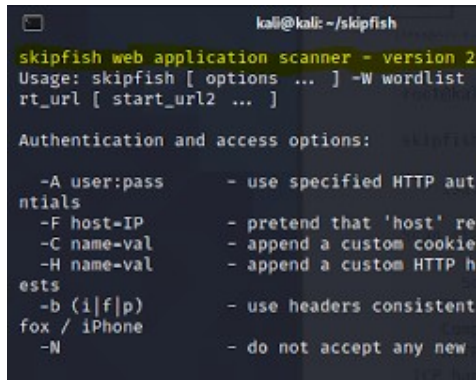
- Nikto: A web server scanner that can be used to identify security vulnerabilities in web applications.



ASSIGNMENT-2

Nikto tool in Kali Linux

- Skipfish: A web application scanner that can be used to identify hidden content and backdoors in web applications.

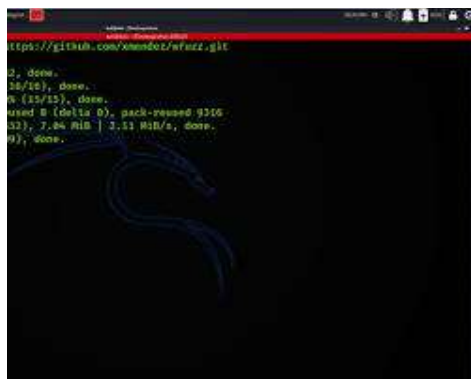
A terminal window with a black background and green text. The title bar shows 'kali@kali: ~/skipfish'. The text displays the Skipfish version (2), usage instructions, and a list of command-line options for authentication and access.

```
kali@kali: ~/skipfish
skipfish web application scanner - version 2
Usage: skipfish [ options ... ] -W wordlist
      rt_url [ start_url2 ... ]

Authentication and access options:
  -A user:pass      - use specified HTTP authentication
  -F host-IP        - pretend that 'host' request is from IP
  -C name=val       - append a custom cookie
  -H name=val       - append a custom HTTP header
  -b (i|f|p)       - use headers consistent with browser
  fox / iPhone
  -N                - do not accept any new connections
```

Skipfish tool in Kali Linux

- Wfuzz: A tool that can be used to fuzz web applications, which can help to identify security vulnerabilities.

A terminal window with a black background and green text. The title bar shows 'kali@kali: ~/wfuzz'. The text displays the output of a Wfuzz command, showing the URL being fuzzed and the results of the fuzzing process.

```
kali@kali: ~/wfuzz
https://github.com/xmendez/wfuzz.git
2, done.
38/10, done.
4 (10/10), done.
Used 5 (data 0), pack-reused 9306
32), 7.84 MiB | 3.11 MiB/s, done.
99), done.
```

Wfuzz tool in Kali Linux

- sqlmap: A tool that can be used to automate the process of manual SQL injection over a parameter on a website.

ASSIGNMENT-2



sqlmap tool in Kali Linux

Web Application Analysis Tools

- Burp Suite: A suite of tools that can be used to analyze web applications for security vulnerabilities.



Burp Suite tool in Kali Linux

- OWASP ZAP: A free and open-source web application security scanner.

ASSIGNMENT-2



OWASP ZAP tool in Kali Linux

- WebScarab: A web application security testing tool that can be used to intercept and analyze web traffic.



WebScarab tool in Kali Linux

- AWVS: A commercial web application vulnerability scanner.




AWVS tool in Kali Linux

- Netsparker: A commercial web application security scanner that can be used to scan for vulnerabilities and generate reports.

ASSIGNMENT-2

```

$ python sqlmap.py -u 'http://debiandev/sqlmap/mysql/get_int...'
 {1.0.5.63#dev}
http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets w...
is illegal. It is the end user's responsibility to obey all app...
licable laws. Developers assume no liability and are not responsi...
ble for any damages 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 param...
(possible DBMS: 'MySQL')

```

Netsparker tool in Kali Linux

Kali Linux tools for database assessment, password attacks, wireless attacks, reverse engineering, exploitation tools, sniffing and spoofing, post exploitation, forensics, and reporting:

Database Assessment Tools

- SQLmap: A tool that can be used to automate the process of manual SQL injection over a parameter on a website.

[illegible]

sqlmap tool in Kali Linux

- DBeaver: A tool that can be used to connect to and manage databases.

ASSIGNMENT-2



DBBeaver tool in Kali Linux

- Hydra: A tool that can be used to crack passwords for databases.

```
master@debian:~$ sudo apt-get install hydra-gtk
[sudo] password for master:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  firebird2.5-common firebird2.5-common-doc hydra libapr1 libap
  libfbclient2 libmysqlclient18 libpq5 libserf-1-1 libssh-4 lib
  mysql-common
The following NEW packages will be installed:
  firebird2.5-common firebird2.5-common-doc hydra hydra-gtk lib
  libaprutil1 libfbclient2 libmysqlclient18 libpq5 libserf-1-1
  libsvn1 mysql-common
0 upgraded, 13 newly installed, 0 to remove and 422 not upgraded
Need to get 3.83B of archives.
After this operation, 12.8 MB of additional disk space will be
Do you want to continue? [Y/n] y
WARNING: The following packages cannot be authenticated!
  libapr1 libaprutil1 libserf-1-1 hydra hydra-gtk
Install these packages without verification? [y/W] y
Get:1 http://ftp.istm.ac.in/debian/ jessie/main libapr1 amd64 1
Get:2 http://security.debian.org/ jessie/updates/main firebird2
  2.5.3.26778.dsc4-5+deb8u2 [654 kB]
Get:3 http://ftp.istm.ac.in/debian/ jessie/main libaprutil1 amd
  1.3.12-1 [108 kB]
```

Hydra tool in Kali Linux

- John the Ripper: A password cracking tool that can be used to crack passwords that are stored in a variety of formats.



John the Ripper tool in Kali Linux

ASSIGNMENT-2

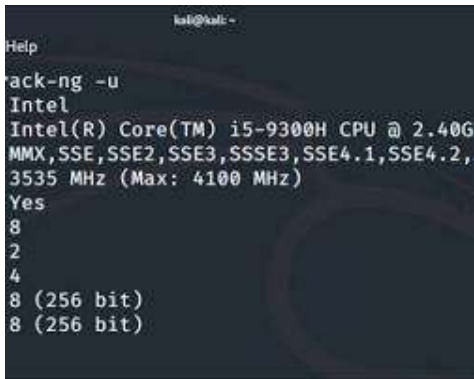
- Hashcat: A password cracking tool that can be used to crack passwords that are stored in a variety of formats, including hashes.



Hashcat tool in Kali Linux

Password Attacks Tools

- Aircrack-ng: A suite of tools for wireless network auditing and security testing. It can be used to crack WEP and WPA/WPA2 passwords, as well as to perform other attacks on wireless networks.



Aircrack-ng tool in Kali Linux

- John the Ripper: A password cracking tool that can be used to crack passwords that are stored in a variety of formats.

ASSIGNMENT-2

ASSIGNMENT-2

- RainbowCrack: A password cracking tool that uses a rainbow table to crack passwords.



RainbowCrack tool in Kali Linux

Wireless Attacks Tools

- Aircrack-ng: A suite of tools for wireless network auditing and security testing. It can be used to crack WEP and WPA/WPA2 passwords, as well as to perform other attacks on wireless networks.



Aircrack-ng tool in Kali Linux

- Kismet: A tool that can be used to detect and track wireless networks.

ASSIGNMENT-2



Kismet tool in Kali Linux

- NetStumbler: A tool that can be used to detect and track wireless networks.



NetStumbler tool in Kali Linux

- Wigle: A website that provides a database of wireless networks that have been scanned.



Wigle website

ASSIGNMENT-2

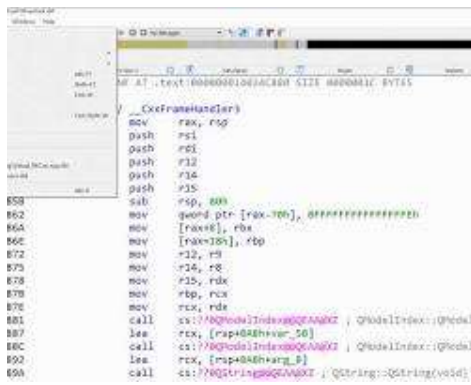
- Reaver: A tool that can be used to crack WPA/WPA2 passwords using a brute-force attack.



Reaver tool in Kali Linux

Reverse Engineering Tools

- IDA Pro: A disassembler and debugger that can be used to reverse engineer software.



IDA Pro tool in Kali Linux

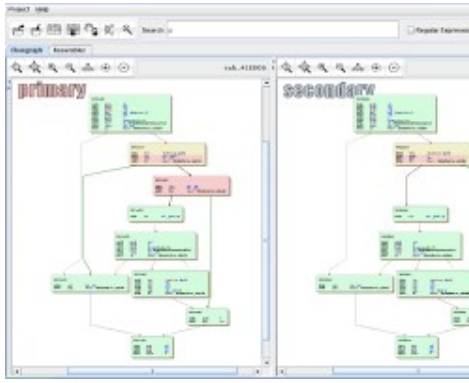
- Ghidra: A reverse engineering suite that can be used to decompile and analyze software.

ASSIGNMENT-2



Ghidra tool in Kali Linux

- BinDiff: A tool that can be used to compare two binary files and find the differences between them.



BinDiff tool in Kali Linux

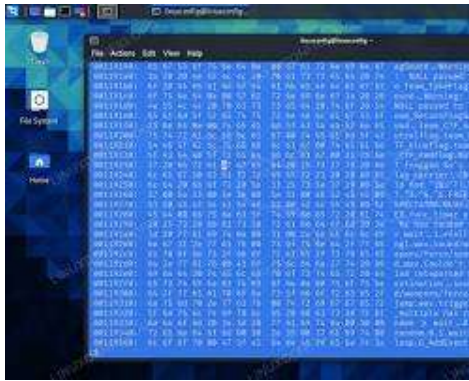
- Radare2: A reverse engineering framework that can be used to disassemble, decompile, and analyze software.

```
0x00000000 255 /usr/bin/r2l> pd $r0 sym.L94+4869 # 0
0x00000000 e970ef1fff jmp 0x100000000
0x00000001 8bba481000 mov edi, [ebx+8]
0x00000007 8b74247c mov esi, [esp+8]
0x0000000b 8b40094000 mov eax, [esp+8]
0x0000000c c742094000 mov dword [esp+8], eax
0x0000000d 890424 mov [esp], eax
0x0000000e e81e2ffff call 0x100000000
0x0000000f sym.imp.r_core_prompt()
0x00000010 85c0 test eax, eax
0x00000011 0f8e481000 jle 0x100000000
0x00000012 85f6 test esi, esi
0x00000013 7408 jz 0x100000000
0x00000014 893424 mov [esp], esi
0x00000015 e81e4ffff call 0x100000000
0x00000016 sym.imp.r_th_lock_enter()
0x00000017 8b40094000 mov edx, [esp+8]
0x00000018 891424 mov [esp], edx
0x00000019 e81e4ffff call 0x100000000
0x0000001a sym.imp.r_core_prompt_exec()
0x0000001b 8b40094000 mov [esp+8], eax
0x0000001c 83c0 add eax, 0
0x0000001d 0f42094000 jc 0x100000000
0x0000001e 85f6 test esi, esi
0x0000001f 7408 jz 0x100000000
```

Radare2 tool in Kali Linux

ASSIGNMENT-2

- FLOSS Hex Editor: A hex editor that can be used to view and edit the contents of binary files.



FLOSS Hex Editor tool in Kali Linux

Exploitation Tools

- Metasploit Framework: A penetration testing framework that includes a variety of tools for attacking computer systems.



Metasploit Framework tool in Kali Linux

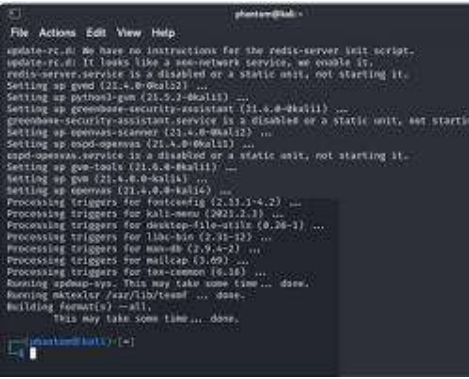
- Nessus: A vulnerability scanner that can be used to scan for vulnerabilities in hosts and networks.

ASSIGNMENT-2



Nessus tool in Kali Linux

- OpenVAS: A vulnerability scanner that can be used to scan for vulnerabilities in hosts and networks.



OpenVAS tool in Kali Linux

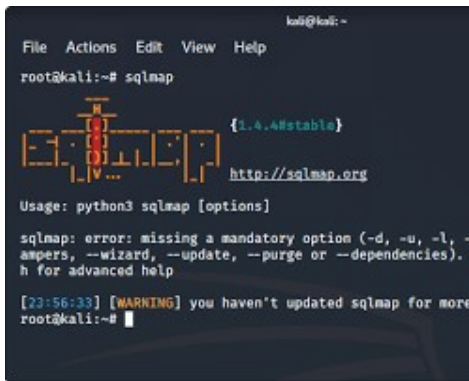
- Wfuzz: A tool that can be used to fuzz web applications, which can help to identify security vulnerabilities.



Wfuzz tool in Kali Linux

ASSIGNMENT-2

- sqlmap: A tool that can be used to automate the process of manual SQL injection over a parameter on a website.



```
root@kali:~# sqlmap
{1.4.4#stable}
http://sqlmap.org
Usage: python3 sqlmap [options]
sqlmap: error: missing a mandatory option (-d, -u, -l, --ampers, --wizard, --update, --purge or --dependencies). Run -h for advanced help
[23:56:33] [WARNING] you haven't updated sqlmap for more than 30 days
root@kali:~#
```

sqlmap tool in Kali Linux

- **Sniffing and spoofing tools** are used to capture and manipulate network traffic. Some of the most popular sniffing and spoofing tools include:
 - Wireshark is a packet analyzer that can be used to capture and analyze network traffic.
 - tcpdump is a command-line packet analyzer.
 - ettercap is a tool for sniffing and spoofing network traffic.
- **Post exploitation tools** are used to gain control of a compromised system. Some of the most popular post exploitation tools include:
 - Metasploit is a penetration testing framework that includes modules for post exploitation tasks, such as maintaining access to a compromised system and gathering information.
 - Nessus is a vulnerability scanner that can be used to identify vulnerabilities in a compromised system.
 - OpenVAS is a free and open-source vulnerability scanner.

ASSIGNMENT-2

- **Forensics tools** are used to collect and analyze evidence from a computer system. Some of the most popular forensics tools include:
 - Autopsy is a free and open-source digital forensics platform.
 - EnCase is a commercial digital forensics tool.
 - FTK Imager is a free and open-source tool for creating forensic images of hard drives.
- **Reporting tools** are used to create reports of security assessments or incidents. Some of the most popular reporting tools include:
 - Serpico is a free and open-source reporting tool for security assessments.
 - Nessus can also be used to generate reports of vulnerability scans.
 - OpenVAS can also be used to generate reports of vulnerability scans.