

AI FOR CYBER SECURITY WITH IBM QRADAR

ASSIGNMENT-2

Name: Chikkam Venkat Satya Dhiraj

Date: 01/09/23

Explore the first 10 tools in Kali Linux

1. Information Gathering

For information gathering, a tool named dnsenum is used. It is a command-line tool used for DNS (Domain Name System) enumeration and information gathering. It is typically used by security professionals, network administrators, and ethical hackers to gather information about a target domain's DNS configuration.

For this, I have used www.wcofun.org website.



```
manasa13@kali:~$ dnsenum www.wcofun.org
dnsenum VERSION:1.2.6

Host's addresses:
www.wcofun.org.      248 IN A      104.26.3.85
www.wcofun.org.      248 IN A      104.26.2.85
www.wcofun.org.      248 IN A      172.67.71.160

Name Servers:
www.wcofun.org NS record query failed: NOERROR

manasa13@kali:~$ dnsenum -destserver 8.8.8.8 www.wcofun.org
dnsenum VERSION:1.2.6

Host's addresses:
www.wcofun.org.      300 IN A      172.67.71.160
www.wcofun.org.      300 IN A      104.26.3.85
www.wcofun.org.      300 IN A      104.26.2.85

Name Servers:
www.wcofun.org NS record query failed: NOERROR
```

2. Vulnerability Analysis

For vulnerability analysis, nmap tool is used. Nmap (Network Mapper) is a widely used open-source tool for network discovery and vulnerability analysis. It's primarily used for network scanning, mapping, and fingerprinting, but it can also assist in vulnerability assessment.



```
manasa13@kali:~$ nmap -v -sS 104.26.3.85
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-04 10:04 IST
Nmap scan report for wcofun.org (104.26.3.85)
Host is up (0.0000s latency).
Other addresses for wcofun.org (not scanned): 2006:4700:20::681a:355 2006:4700:20::681a:255 2006:4700:20::ac43:47a0 104.26.2.85 172.67.71.160
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
8080/tcp   open  http-proxy
8443/tcp   open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 4.87 seconds
```

3. Web Application Analysis

For Web Application Analysis, a tool named wpscan is used. WPScan is a popular open-source security scanner specifically designed for WordPress websites. It is used for identifying vulnerabilities, misconfigurations, and security issues in WordPress installations. It can be a valuable tool for security professionals, website administrators, and penetration testers to assess the security posture of WordPress sites.

```
manasa13@kali: ~
$ wpscan --url https://www.wcofun.org

WPScan
WordPress Security Scanner by the WPScan Team
Version 3.8.24
@_WPScan_, @ethicalhack3r, @erwan_lr, @Firefart

[+] Updating the Database ...
[+] Update completed.
[+] URL: https://www.wcofun.org/ [2606:4700:20::681a:355]
[+] Started: Mon Sep  4 17:09:18 2023

Interesting Finding(s):

[+] Headers
| Interesting Entries:
| - x-fastcgi-cache: HIT
| - cf-cache-status: DYNAMIC
| - report-to: [{"endpoints":[{"url":"https://a.nel.cloudflare.com/v/r/37s-6Y1alognvb5xmrWmPQs1bJXEUYcV4bh2NtZSmQXWC8chbYmXQaZbYnzDghDhVa725D1u8CnQ4ePxcwyNIQF3z62Bns11RU3z62IX75fGyX2BS2dFA"}], "group": "cf-nel", "max_age": 604800}]
| - nel: {"success_fraction": 0, "report_to": "cf-nel", "max_age": 604800}
| - servers: cloudflare
| - cf-ray: 8015f61be8673c07-BLR
| Found By: Headers (Passive Detection)
| Confidence: 100%

[+] robots.txt Found: https://www.wcofun.org/robots.txt
| Found By: Robots Txt (Aggressive Detection)
| Confidence: 100%

[+] XML-RPC seems to be enabled: https://www.wcofun.org/xmlrpc.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
| References:
| - http://codex.wordpress.org/XML-RPC_Pingback_API
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
| - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
```

```
manasa13@kali: ~
$ wpscan --url https://www.wcofun.org

[+] Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
| References:
| - http://codex.wordpress.org/XML-RPC_Pingback_API
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
| - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] The external WP-Cron seems to be enabled: https://www.wcofun.org/wp-cron.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 60%
| References:
| - https://www.iplocation.net/defend-wordpress-from-ddos
| - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 6.2.2 identified (Outdated, released on 2023-05-20).
| Found By: Rss Generator (Aggressive Detection)
| - https://www.wcofun.org/feed, <generator>https://wordpress.org/?v=6.2.2</generator>
| - https://www.wcofun.org/comments/feed, <generator>https://wordpress.org/?v=6.2.2</generator>

[+] The main theme could not be detected.

[+] Enumerating All Plugins (via Passive Methods)
[+] No plugins Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:00:11

[+] No Config Backups Found.

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

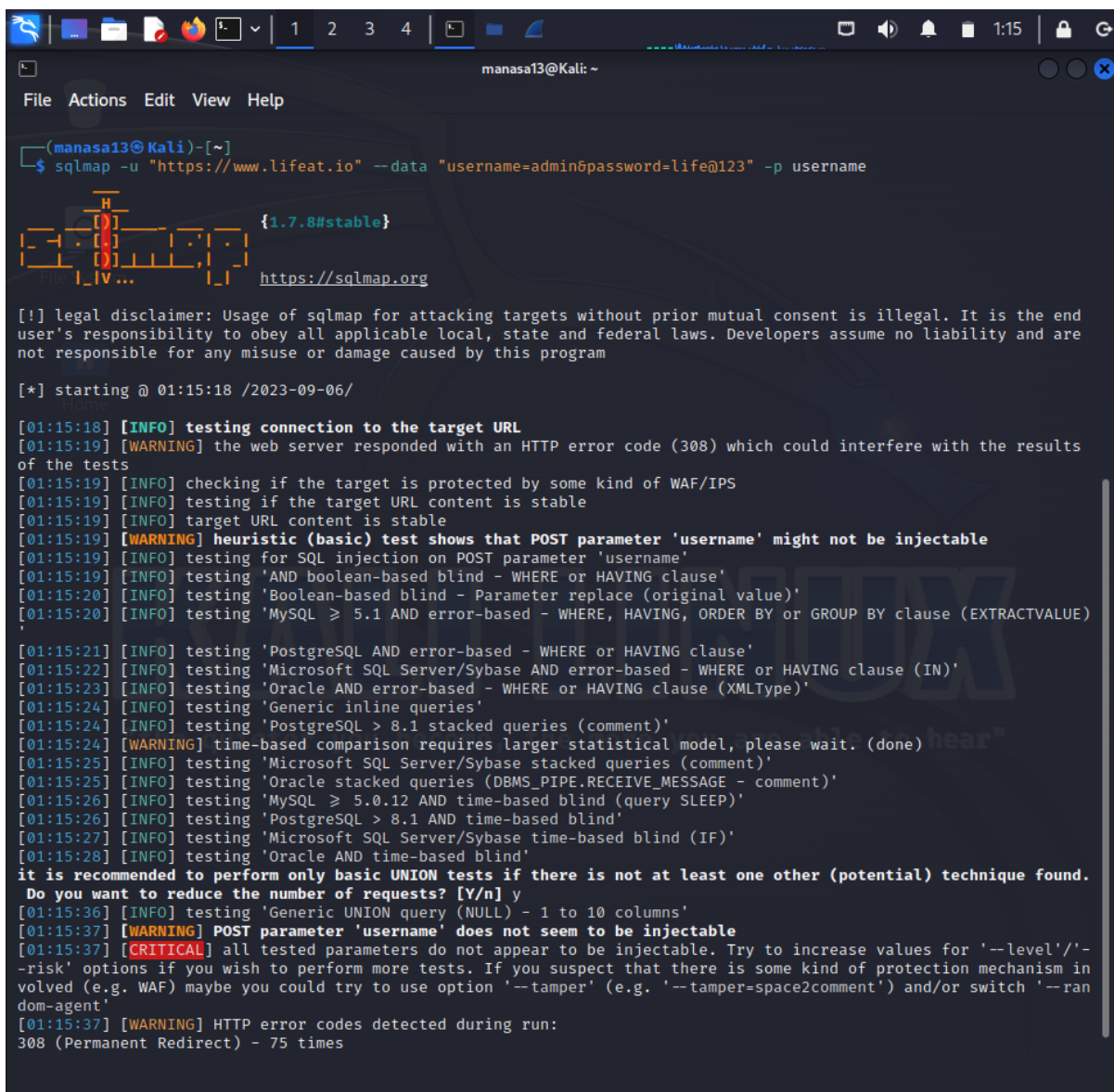
[+] Finished: Mon Sep  4 17:09:37 2023
[+] Requests Done: 188
[+] Cached Requests: 5
[+] Data Sent: 46.74 KB
[+] Data Received: 21.019 MB
[+] Memory used: 235.254 MB
[+] Elapsed time: 00:00:19

manasa13@kali: ~
```

4. Database Assessment

For Database Assessment, sqlmap tool is used. sqlmap is a popular open-source tool used for automated penetration testing and database assessment. Its primary purpose is to detect and exploit SQL injection vulnerabilities in web applications and their underlying

databases. SQL injection is a common attack vector where malicious SQL statements are inserted into input fields of a web application to manipulate the database or gain unauthorized access to sensitive data.



```
(manasa13@Kali)-[~]
$ sqlmap -u "https://www.lifeat.io" --data "username=admin&password=life@123" -p username

[!] 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 @ 01:15:18 /2023-09-06/

[01:15:18] [INFO] testing connection to the target URL
[01:15:19] [WARNING] the web server responded with an HTTP error code (308) which could interfere with the results
of the tests
[01:15:19] [INFO] checking if the target is protected by some kind of WAF/IPS
[01:15:19] [INFO] testing if the target URL content is stable
[01:15:19] [INFO] target URL content is stable
[01:15:19] [WARNING] heuristic (basic) test shows that POST parameter 'username' might not be injectable
[01:15:19] [INFO] testing for SQL injection on POST parameter 'username'
[01:15:19] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[01:15:20] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[01:15:20] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[01:15:21] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[01:15:22] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[01:15:23] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[01:15:24] [INFO] testing 'Generic inline queries'
[01:15:24] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[01:15:24] [WARNING] time-based comparison requires larger statistical model, please wait. (done)
[01:15:25] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[01:15:25] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[01:15:26] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[01:15:26] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[01:15:27] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[01:15:28] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found.
Do you want to reduce the number of requests? [Y/n] y
[01:15:36] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[01:15:37] [WARNING] POST parameter 'username' does not seem to be injectable
[01:15:37] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'-
risk' options if you wish to perform more tests. If you suspect that there is some kind of protection mechanism in
volved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/or switch '--ran
dom-agent'
[01:15:37] [WARNING] HTTP error codes detected during run:
308 (Permanent Redirect) - 75 times
```

5. Password Attacks

For exploring password attacks, ncrack tool is used. Ncrack is a powerful open-source network authentication cracking tool. It is primarily used for performing password attacks, including brute force attacks and dictionary attacks, against various network services and protocols. Ncrack is designed for legitimate security testing and auditing purposes to assess the strength of passwords used for authentication on network services.

```
manasa13@Kali: ~  
File Actions Edit View Help  
cr (connection retries): caps number of service connection attempts  
to (time-out): maximum cracking <time> for service, regardless of success so far  
-T<0-5>: Set timing template (higher is faster)  
--connection-limit <number>: threshold for total concurrent connections  
--stealthy-linear: try credentials using only one connection against each specified host  
until you hit the same host again. Overrides all other timing options.  
AUTHENTICATION:  
-U <filename>: username file  
-P <filename>: password file  
--user <username_list>: comma-separated username list  
--pass <password_list>: comma-separated password list  
--passwords-first: Iterate password list for each username. Default is opposite.  
--pairwise: Choose usernames and passwords in pairs.  
OUTPUT:  
-oN/-oX <file>: Output scan in normal and XML format, respectively, to the given filename.  
-oA <basename>: Output in the two major formats at once  
-v: Increase verbosity level (use twice or more for greater effect)  
-d[level]: Set or increase debugging level (Up to 10 is meaningful)  
--nsock-trace <level>: Set nsock trace level (Valid range: 0 - 10)  
--log-errors: Log errors/warnings to the normal-format output file  
--append-output: Append to rather than clobber specified output files  
MISC:  
--resume <file>: Continue previously saved session  
--save <file>: Save restoration file with specific filename  
-f: quit cracking service after one found credential  
-6: Enable IPv6 cracking  
-sL or --list: only list hosts and services  
--datadir <dirname>: Specify custom Ncrack data file location  
--proxy <type://proxy:port>: Make connections via socks4, 4a, http.  
-V: Print version number  
-h: Print this help summary page.  
MODULES:  
SSH, RDP, FTP, Telnet, HTTP(S), Wordpress, POP3(S), IMAP, CVS, SMB, VNC, SIP, Redis, PostgreSQL, MQTT, MySQL, MSS  
QL, MongoDB, Cassandra, WinRM, OWA, DICOM  
EXAMPLES:  
ncrack -v --user root localhost:22  
ncrack -v -T5 https://192.168.0.1  
ncrack -v -iX ~/nmap.xml -g CL=5,to=1h  
SEE THE MAN PAGE (http://nmap.org/ncrack/man.html) FOR MORE OPTIONS AND EXAMPLES  
(manasa13@Kali)-[~]  
$ ncrack -p ssh 127.0.0.1  
  
Starting Ncrack 0.7 ( http://ncrack.org ) at 2023-09-06 01:19 IST  
  
Ncrack done: 1 service scanned in 3.00 seconds.  
  
Ncrack finished.  
(manasa13@Kali)-[~]  
$
```

6. Wireless Attacks

For exploring wireless attacks, wifite tool is used. Wifite is a popular wireless auditing tool available in Kali Linux. It's designed to automate various wireless attacks, including WEP and WPA/WPA2-PSK cracking, using a combination of well-known attack methods.

```

File Actions Edit View Help
[ ] File "/usr/lib/python3/dist-packages/wifite/_main_.py", line 184, in entry_point
[ ] wifite.start()
[ ] File "/usr/lib/python3/dist-packages/wifite/_main_.py", line 57, in start
[ ] configuration.get_monitor_mode_interface()
[ ] File "/usr/lib/python3/dist-packages/wifite/config.py", line 229, in get_monitor_mode_interface
[ ] cls.interface = Airmon_ask()
[ ] File "/usr/lib/python3/dist-packages/wifite/tools/airmon.py", line 313, in ask
[ ] raise Exception('airmon-ng did not find any wireless interfaces')
[ ] Exception: airmon-ng did not find any wireless interfaces
[ ] Exiting

manass13@kali:~$ sudo wifite --wep
wifite2 3.7.8
a wireless auditor by derv02
maintained by kinocoder
https://github.com/kinocoder/wifite2

[ ] option: targeting WEP-encrypted networks
[ ] Conflicting processes: NetworkManager (PID 56)
[ ] If you have problems: kill -9 PID or re-run wifite with --kill

[ ] Checking airmon-ng...
[ ] airmon-ng did not find any wireless interfaces
[ ] Make sure your wireless device is connected
[ ] See https://www.aircrack-ng.org/doku.php?id=airmon-ng for more info

[ ] Error: airmon-ng did not find any wireless interfaces
[ ] Full stack trace below
[ ] Traceback (most recent call last):
[ ] File "/usr/lib/python3/dist-packages/wifite/_main_.py", line 184, in entry_point
[ ] wifite.start()
[ ] File "/usr/lib/python3/dist-packages/wifite/_main_.py", line 57, in start
[ ] configuration.get_monitor_mode_interface()
[ ] File "/usr/lib/python3/dist-packages/wifite/config.py", line 229, in get_monitor_mode_interface
[ ] cls.interface = Airmon_ask()
[ ] File "/usr/lib/python3/dist-packages/wifite/tools/airmon.py", line 313, in ask
[ ] raise Exception('airmon-ng did not find any wireless interfaces')
[ ] Exception: airmon-ng did not find any wireless interfaces
[ ] Exiting

manass13@kali:~$

```

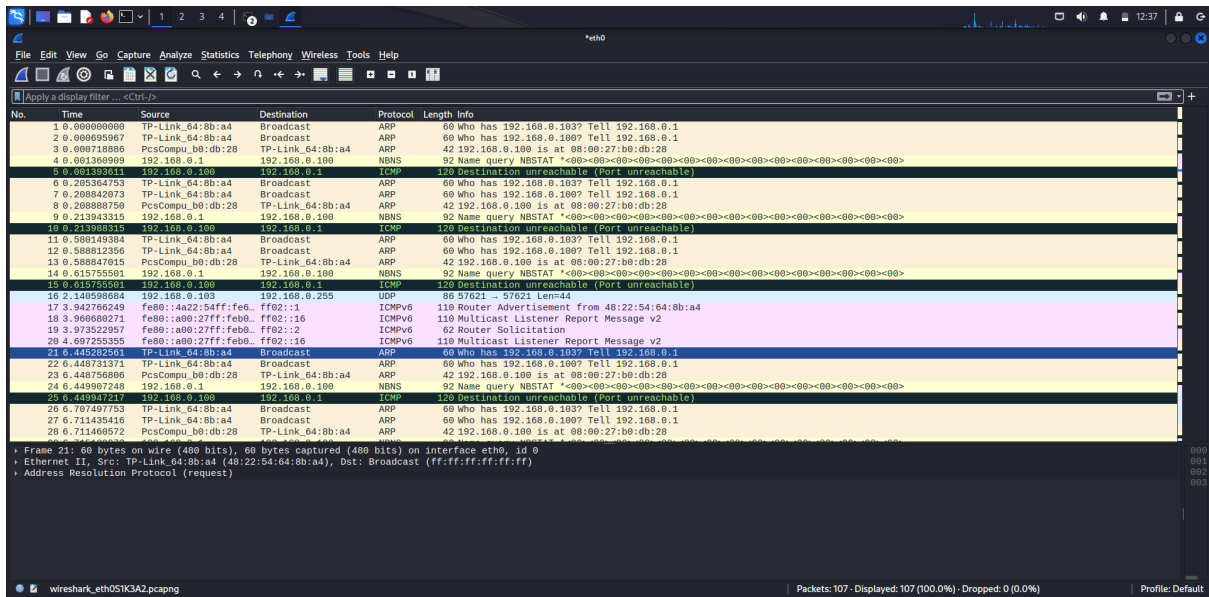
7. Reverse Engineering

For Reverse engineering, Clang and Ghidra are used. Clang is a popular open-source C and C++ compiler front end that is part of the LLVM project. Ghidra is a powerful open-source software reverse engineering framework developed by the National Security Agency (NSA).

The screenshot shows the CodeBrowser application interface. On the left, there's a sidebar with 'Program Trees', 'Symbol Tree', and 'Data Type Manager'. The main window is split into two panes. The left pane displays assembly code for 'myprogram.c' with addresses, hex values, and mnemonics. The right pane shows the decompiled C code for 'UndefinedFunction_0006'. The decompiled code includes a warning about control flow, a function signature 'void UndefinedFunction_0006(char param_1)', and several lines of C code involving memory operations and arithmetic. The bottom status bar shows the current address '0006' and instruction 'STZ 0x65'.

8. Exploitation Tools

For exploiting ip address, Metasploit Framework tool is used. The Metasploit Framework is a widely used open-source penetration testing and exploitation tool that provides a comprehensive set of tools for identifying vulnerabilities, creating and deploying exploits, and conducting security assessments. Metasploit is used by security professionals, penetration testers, and ethical hackers to test and assess the security of systems and applications.



10. Post Exploitation

For exploring Post exploitation, Mimikatz tool is used. Mimikatz is a powerful post-exploitation tool that is widely known for its capability to extract plaintext passwords, hashes, and other authentication credentials from memory, as well as performing other post-exploitation tasks on Windows systems. It is used by security professionals, penetration testers, and sometimes malicious actors for legitimate and malicious purposes.

