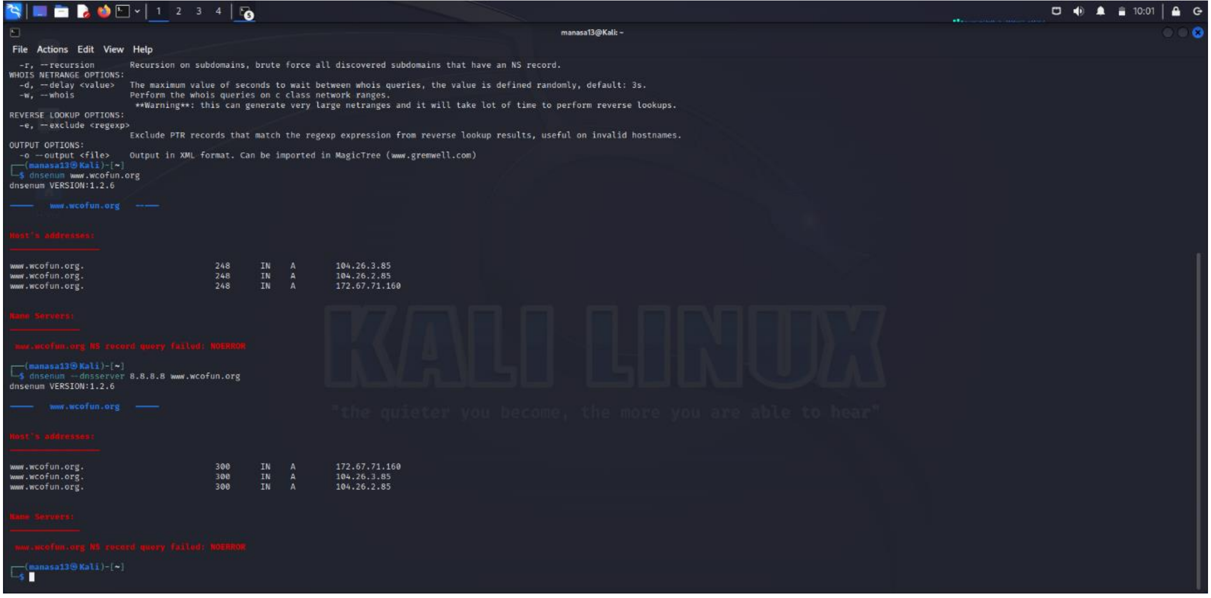
AI FOR CYBER SECURITY
ASSIGNMENT-2

Name: Vishnubhatla V L Sruta Keerthi
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.

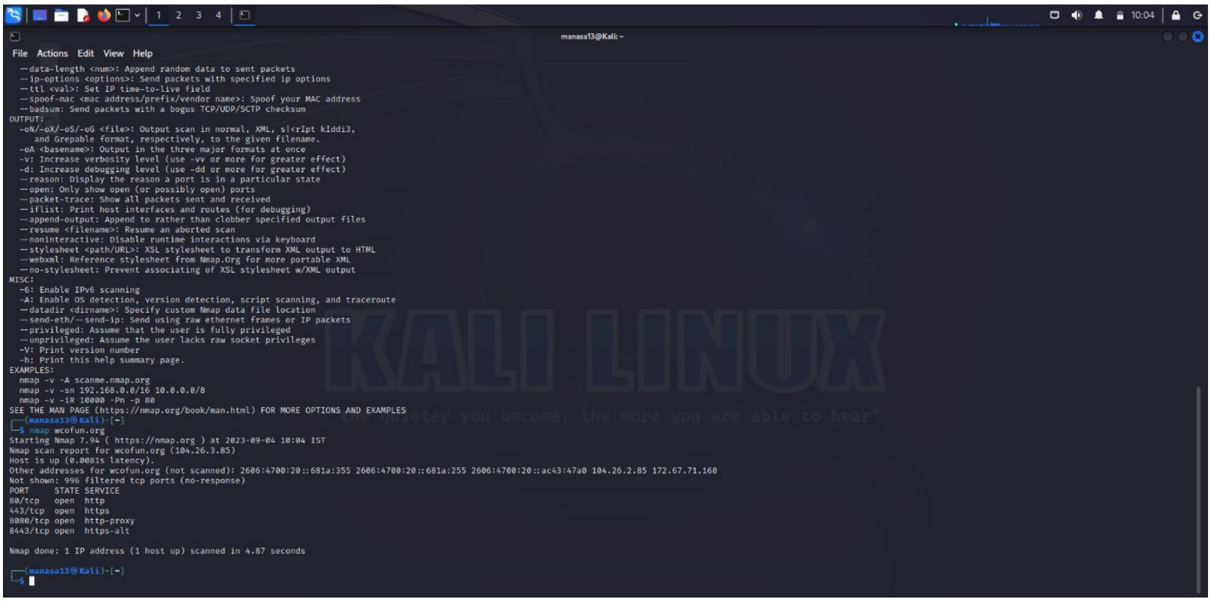


File Actions Edit View Help
manasa13@Kali: ~
KALI LINUX
"the quieter you become, the more you are able to hear"

```
  -r, --recursion       Recursion on subdomains, brute force all discovered subdomains that have an NS record.
WHOIS NETRANGE OPTIONS:
  -d, --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 <regexp>
                        Exclude PTR records that match the regexp expression from reverse lookup results, useful on invalid hostnames.
OUTPUT OPTIONS:
  -o --output <file>    Output in XML format. Can be imported in MagicTree (www.gremwell.com)
┌──(manasa13㉿Kali)-[~]
└─$ dnsenum www.wcofun.org
dnsenum VERSION:1.2.6

-----   www.wcofun.org   -----


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 --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        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: ~
File Actions Edit View Help
KALI LINUX
"the quieter you become, the more you are able to hear"

```
  --data-length <num>: Append random data to sent packets
  --ip-options <options>: Send packets with specified ip options
  --ttl <val>: Set IP time-to-live field
  --spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
  --badsum: Send packets with a bogus TCP/UDP/SCTP checksum
OUTPUT:
  -oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3,
     and Grepable format, respectively, to the given filename.
  -oA <basename>: 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)
  --reason: Display the reason a port is in a particular state
  --open: Only show open (or possibly open) ports
  --packet-trace: Show all packets sent and received
  --iflist: Print host interfaces and routes (for debugging)
  --append-output: Append to rather than clobber specified output files
  --resume <filename>: Resume an aborted scan
  --noninteractive: Disable runtime interactions via keyboard
  --stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
  --webxml: Reference stylesheet from Nmap.Org for more portable XML
  --no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
  -6: Enable IPv6 scanning
  -A: Enable OS detection, version detection, script scanning, and traceroute
  --datadir <dirname>: Specify custom Nmap data file location
  --send-eth/--send-ip: Send using raw ethernet frames or IP packets
  --privileged: Assume that the user is fully privileged
  --unprivileged: Assume the user lacks raw socket privileges
  -V: Print version number
  -h: Print this help summary page.
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
┌──(manasa13㉿Kali)-[~]
└─$ nmap wcofun.org
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 (0.0081s latency).
Other addresses for wcofun.org (not scanned): 2606:4700:20::681a:355 2606:4700:20::681a:255 2606:4700:20::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

┌──(manasa13㉿Kali)-[~]
└─$ 
```

3. Web Application Analysis

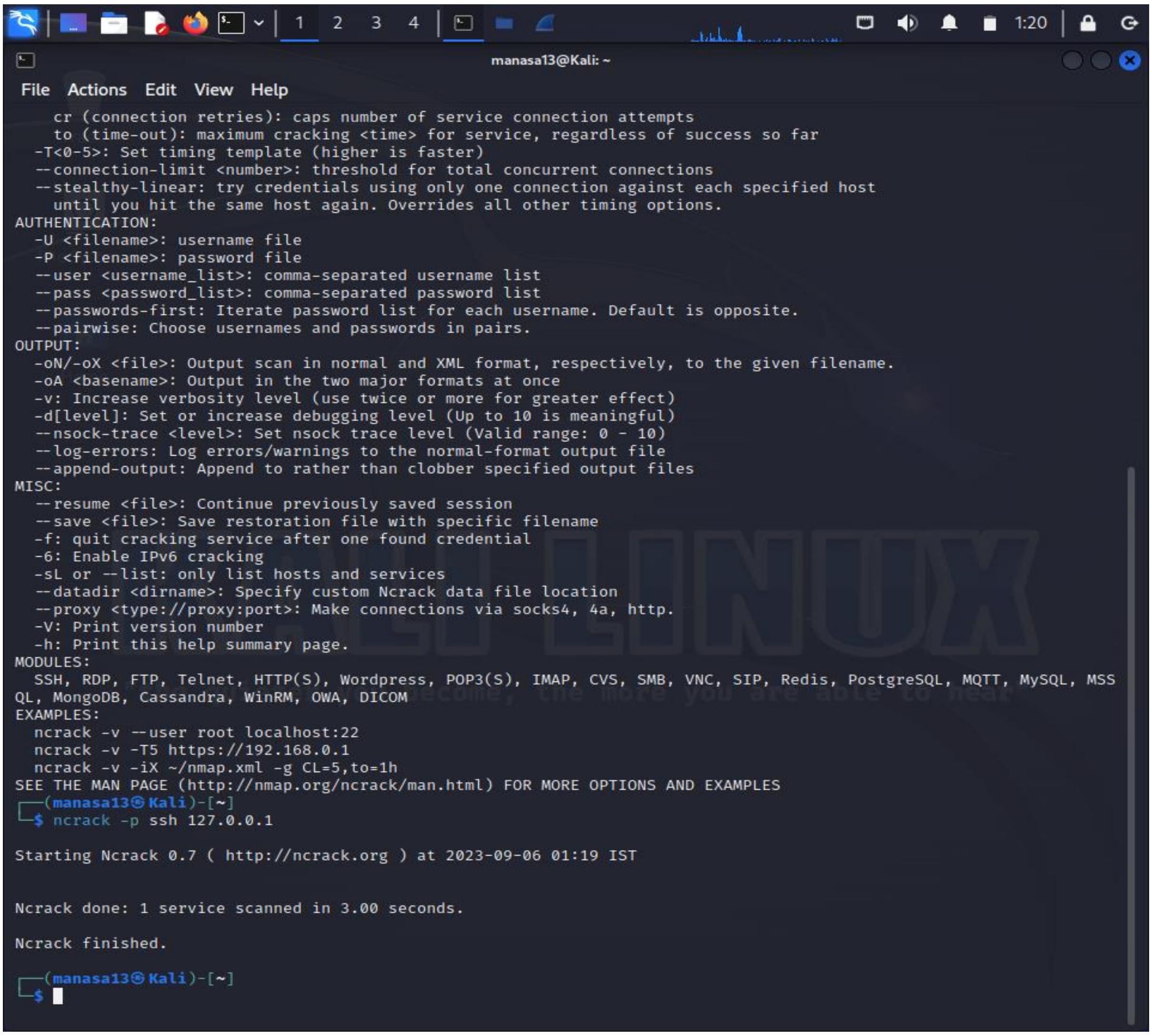
For Web Application Analysis, a tool named wpscan is used. WPScan is a popular open-source security scanner specifically designed for WordPress websites. It is used for identifying vulnerabilities, misconfigurations, and security issues in WordPress installations. It can be a valuable tool for security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

4. 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.

5. Password Attacks

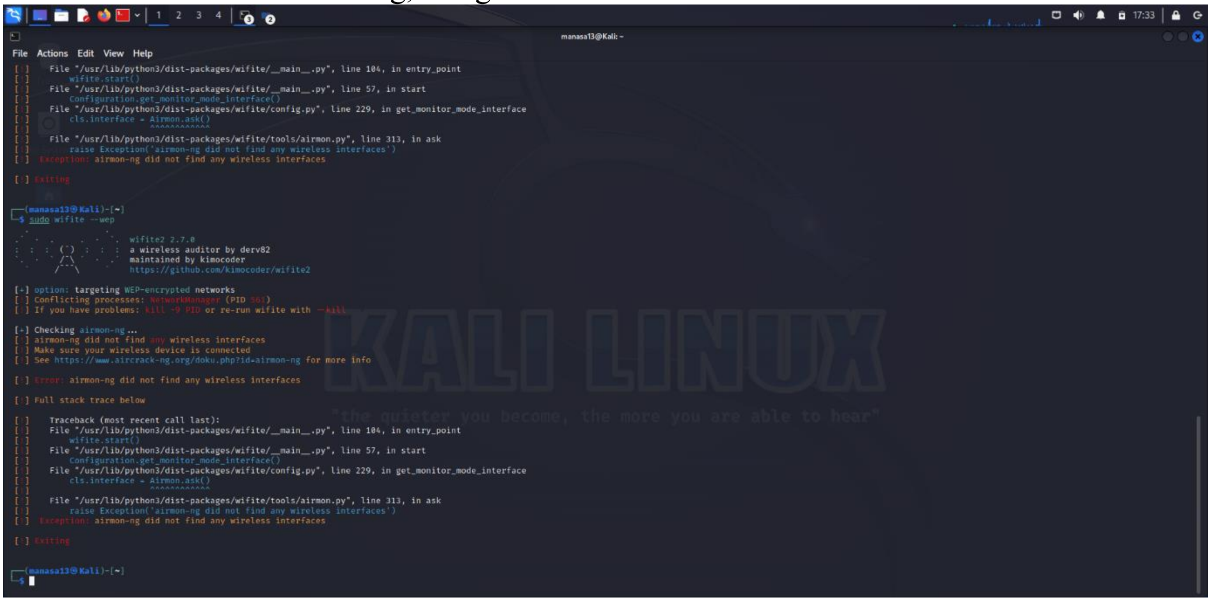
For exploring password attacks, ncrack tool is used. Ncrack is a powerful open-source network authentication cracking tool. It is primarily used for performing password attacks, including brute force attacks and dictionary attacks, against various network services and protocols. Ncrack is designed for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



```
    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

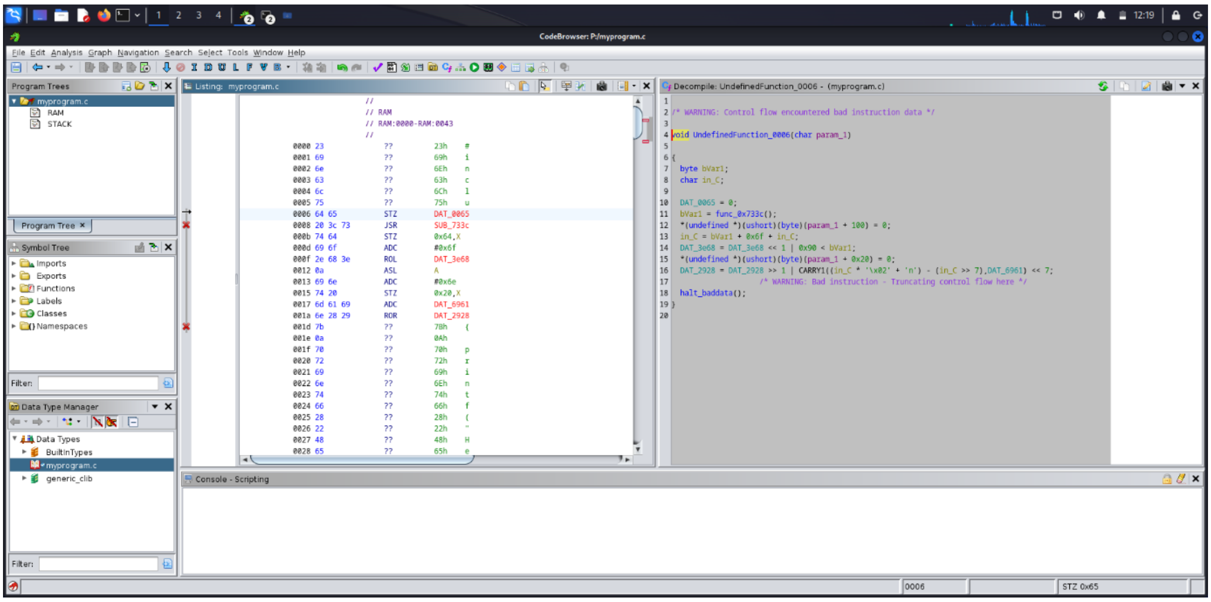
For exploring wireless attacks, wifite tool is used. Wifite is a popular wireless auditing tool available in Kali Linux. It's designed to automate various wireless attacks, including WEP and WPA/WPA2-PSK cracking, using a combination of well-known attack methods.



```
[!]    File "/usr/lib/python3/dist-packages/wifite/__main__.py", line 104, 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


┌──(manasa13㉿Kali)-[~]
└─$ sudo wifite --wep
   .               .
 .´  ·  .     .  ·  `.  wifite2 2.7.0
 :  :  :  (¯)  :  :  :  a wireless auditor by derv82
 `.  ·  ` /¯\ ´  ·  .´  maintained by kimocoder
   `     /¯¯¯\     ´    https://github.com/kimocoder/wifite2

[+] option: targeting WEP-encrypted networks
[!] Conflicting processes: NetworkManager (PID 561)
[!] 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 104, 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


┌──(manasa13㉿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).

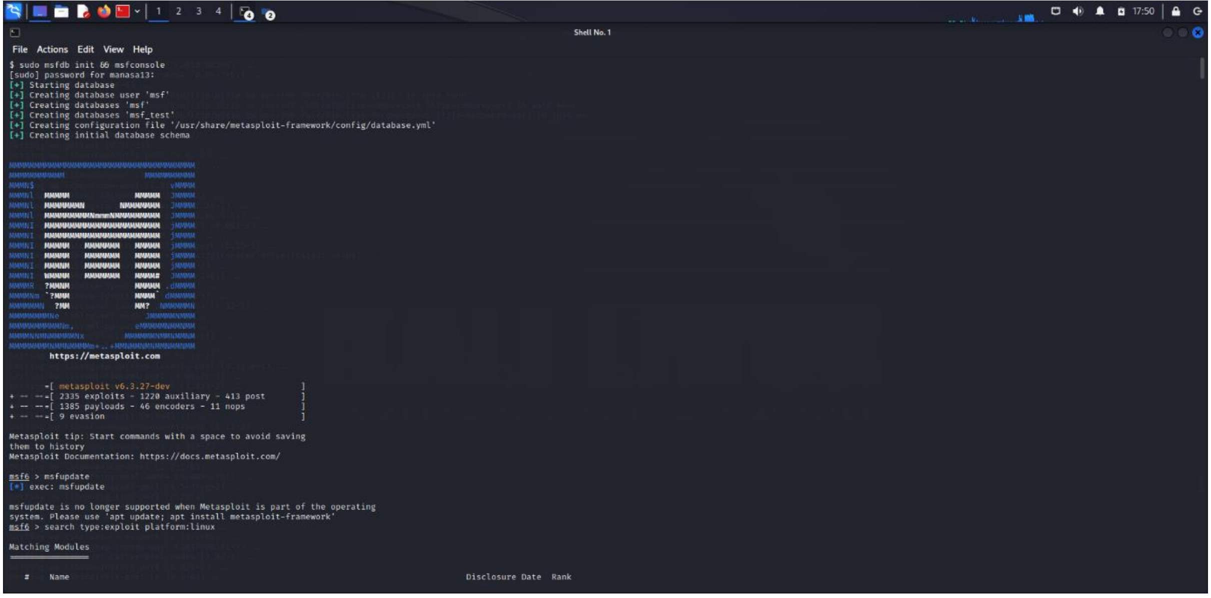


```
                    //
                    // RAM
                    // RAM:0000-RAM:0043
                    //
        0000 23          ??        23h    #
        0001 69          ??        69h    i
        0002 6e          ??        6Eh    n
        0003 63          ??        63h    c
        0004 6c          ??        6Ch    l
        0005 75          ??        75h    u
        0006 64 65       STZ       DAT_0065
        0008 20 3c 73    JSR       SUB_733c
        000b 74 64       STZ       0x64,X
        000d 69 6f       ADC       #0x6f
        000f 2e 68 3e    ROL       DAT_3e68
        0012 0a          ASL       A
        0013 69 6e       ADC       #0x6e
        0015 74 20       STZ       0x20,X
        0017 6d 61 69    ADC       DAT_6961
        001a 6e 28 29    ROR       DAT_2928
        001d 7b          ??        7Bh    {
        001e 0a          ??        0Ah
        001f 70          ??        70h    p
        0020 72          ??        72h    r
        0021 69          ??        69h    i
        0022 6e          ??        6Eh    n
        0023 74          ??        74h    t
        0024 66          ??        66h    f
        0025 28          ??        28h    (
        0026 22          ??        22h    "
        0027 48          ??        48h    H
        0028 65          ??        65h    e
```

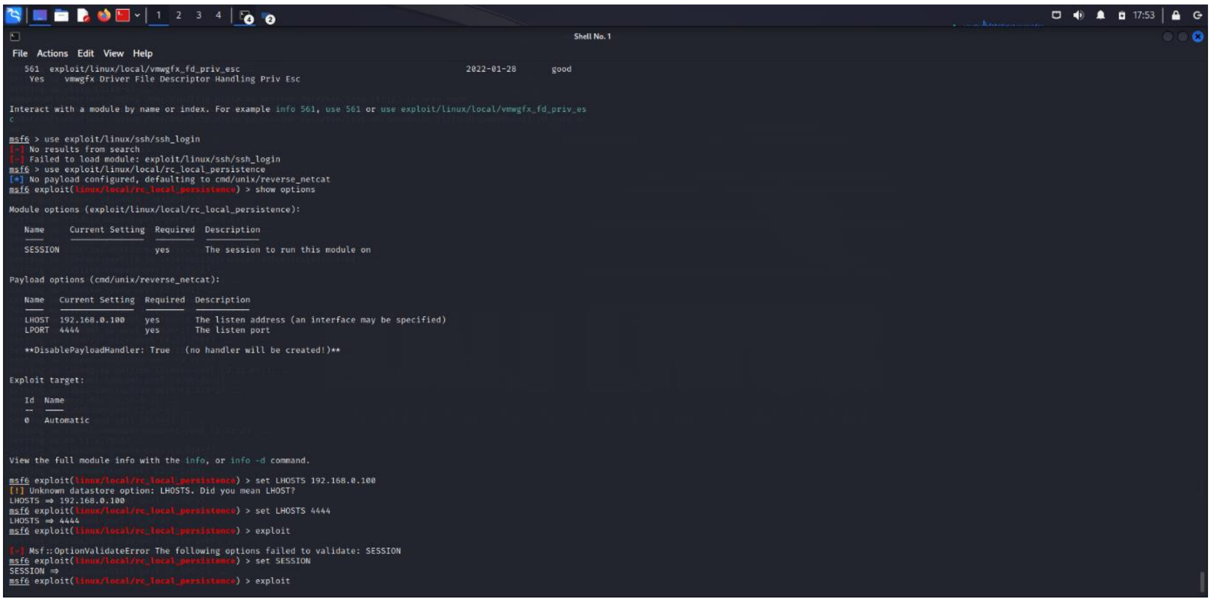
```

/* WARNING: Control flow encountered bad instruction data */

void UndefinedFunction_0006(char param_1)

{
  byte bVar1;
  char in_C;

  DAT_0065 = 0;
  bVar1 = func_0x733c();
  *(undefined *)(ushort)(byte)(param_1 + 100) = 0;
  in_C = bVar1 + 0x6f + in_C;
  DAT_3e68 = DAT_3e68 << 1 | 0x90 < bVar1;
  *(undefined *)(ushort)(byte)(param_1 + 0x20) = 0;
  DAT_2928 = DAT_2928 >> 1 | CARRY1((in_C * '\x02' + 'n') - (in_C >> 7),DAT_6961) << 7;
                    /* WARNING: Bad instruction - Truncating control flow here */
  halt_baddata();
}

```

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.



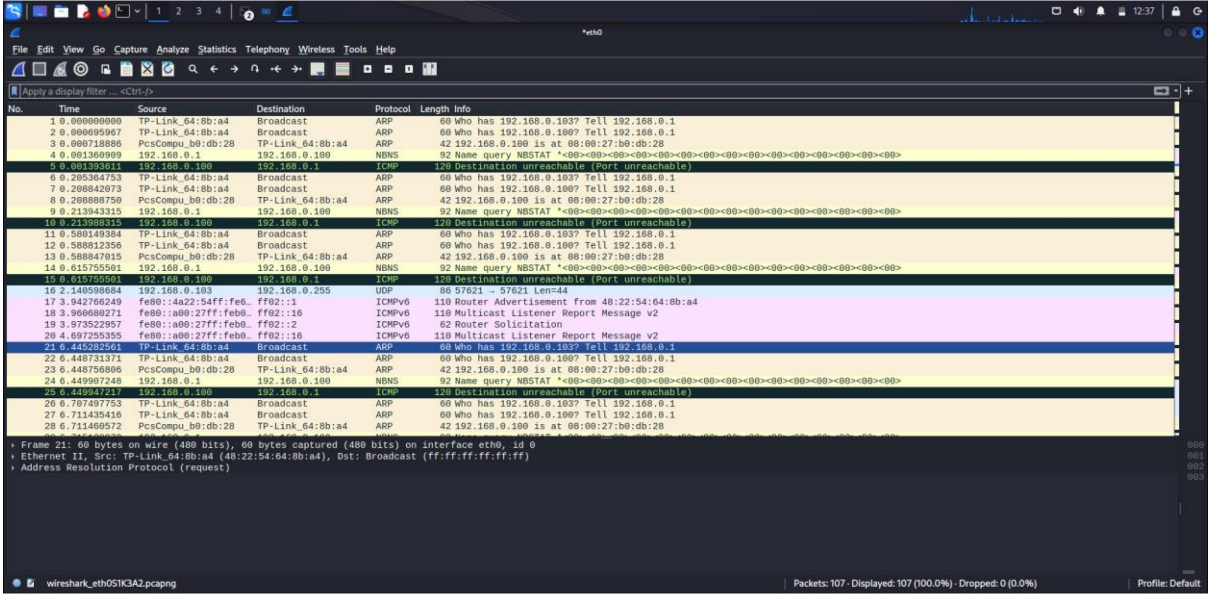
```
$ sudo msfdb init && msfconsole
[sudo] password for manasa13:
[+] Starting database
[+] Creating database user 'msf'
[+] Creating databases 'msf'
[+] Creating databases 'msf_test'
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'
[+] Creating initial database schema


MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMMMMMMMMM                MMMMMMMMMMMM
MMMN$                            vMMMM
MMMNl  MMMMM             MMMMM  JMMMM
MMMNl  MMMMMMMN       NMMMMMMM  JMMMM
MMMNl  MMMMMMMMMNmmmNMMMMMMMMM  JMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMNM   MMMMMMM   MMMMM  jMMMM
MMMNI  WMMMM   MMMMMMM   MMMM#  JMMMM
MMMMR  ?MMNM             MMMMM .dMMMM
MMMMNm `?MMM             MMMM` dMMMMM
MMMMMMN  ?MM             MM?  NMMMMMN
MMMMMMMMNe                 JMMMMMNMMM
MMMMMMMMMMNm,            eMMMMMNMMNMM
MMMMNNMNMMMMMNx        MMMMMMNMMNMMNM
MMMMMMMMNMMNMMMMm+..+MMNMMNMNMMNMMNMM
        https://metasploit.com


       =[ metasploit v6.3.27-dev                          ]
+ -- --=[ 2335 exploits - 1220 auxiliary - 413 post       ]
+ -- --=[ 1385 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Start commands with a space to avoid saving
them to history
Metasploit Documentation: https://docs.metasploit.com/

msf6 > msfupdate
[*] exec: msfupdate

msfupdate is no longer supported when Metasploit is part of the operating
system. Please use 'apt update; apt install metasploit-framework'
msf6 > search type:exploit platform:linux

Matching Modules
================

   #    Name                                                       Disclosure Date  Rank
```



```
   561  exploit/linux/local/vmwgfx_fd_priv_esc                    2022-01-28       good
    Yes    vmwgfx Driver File Descriptor Handling Priv Esc


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

msf6 > use exploit/linux/ssh/ssh_login
[-] No results from search
[-] Failed to load module: exploit/linux/ssh/ssh_login
msf6 > use exploit/linux/local/rc_local_persistence
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(linux/local/rc_local_persistence) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   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.

msf6 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
msf6 exploit(linux/local/rc_local_persistence) > set LHOSTS 4444
LHOSTS => 4444
msf6 exploit(linux/local/rc_local_persistence) > exploit

[-] Msf::OptionValidateError The following options failed to validate: SESSION
msf6 exploit(linux/local/rc_local_persistence) > set SESSION
SESSION =>
msf6 exploit(linux/local/rc_local_persistence) > exploit
```

9. Sniffing and Spoofing

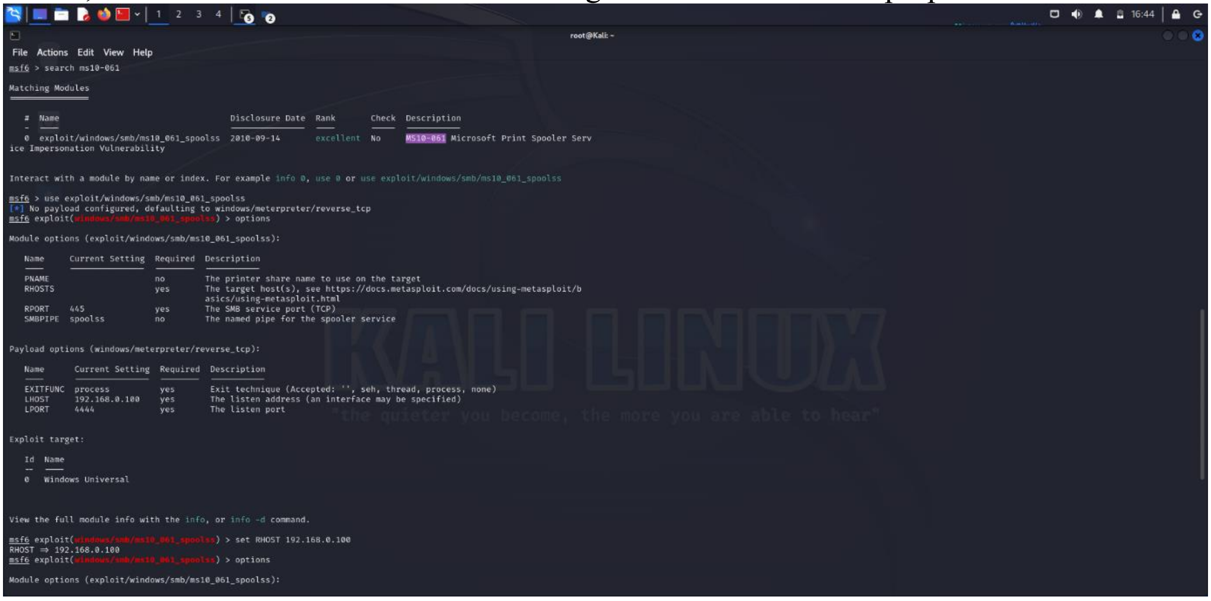
For exploring sniffing and spoofing, Wireshark tool is used. Wireshark is a widely used open-source network protocol analyzer. While it is primarily designed for network traffic analysis, it can be used for network sniffing. However, it's important to note that Wireshark is a legitimate tool for network 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.


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.   Time          Source               Destination         Protocol  Length Info
    1 0.000000000   TP-Link_64:8b:a4     Broadcast           ARP        60 Who has 192.168.0.103? Tell 192.168.0.1
    2 0.000695967   TP-Link_64:8b:a4     Broadcast           ARP        60 Who has 192.168.0.100? Tell 192.168.0.1
    3 0.000718886   PcsCompu_b0:db:28    TP-Link_64:8b:a4    ARP        42 192.168.0.100 is at 08:00:27:b0:db:28
    4 0.001360909   192.168.0.1          192.168.0.100       NBNS       92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>
    5 0.001393611   192.168.0.100        192.168.0.1         ICMP      120 Destination unreachable (Port unreachable)
    6 0.205364753   TP-Link_64:8b:a4     Broadcast           ARP        60 Who has 192.168.0.103? Tell 192.168.0.1
    7 0.208842073   TP-Link_64:8b:a4     Broadcast           ARP        60 Who has 192.168.0.100? Tell 192.168.0.1
    8 0.208888750   PcsCompu_b0:db:28    TP-Link_64:8b:a4    ARP        42 192.168.0.100 is at 08:00:27:b0:db:28
    9 0.213943315   192.168.0.1          192.168.0.100       NBNS       92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>
   10 0.213988315   192.168.0.100        192.168.0.1         ICMP      120 Destination unreachable (Port unreachable)
   11 0.580149384   TP-Link_64:8b:a4     Broadcast           ARP        60 Who has 192.168.0.103? Tell 192.168.0.1
   12 0.588812356   TP-Link_64:8b:a4     Broadcast           ARP        60 Who has 192.168.0.100? Tell 192.168.0.1
   13 0.588847015   PcsCompu_b0:db:28    TP-Link_64:8b:a4    ARP        42 192.168.0.100 is at 08:00:27:b0:db:28
   14 0.615755501   192.168.0.1          192.168.0.100       NBNS       92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>
   15 0.615755501   192.168.0.100        192.168.0.1         ICMP      120 Destination unreachable (Port unreachable)
   16 2.140598684   192.168.0.103        192.168.0.255       UDP        86 57621 → 57621 Len=44
   17 3.942766249   fe80::4a22:54ff:fe6… ff02::1             ICMPv6    110 Router Advertisement from 48:22:54:64:8b:a4
   18 3.960680271   fe80::a00:27ff:feb0… ff02::16            ICMPv6    110 Multicast Listener Report Message v2
   19 3.973522957   fe80::a00:27ff:feb0… ff02::2             ICMPv6     62 Router Solicitation
   20 4.697255355   fe80::a00:27ff:feb0… ff02::16            ICMPv6    110 Multicast Listener Report Message v2
   21 6.445282561   TP-Link_64:8b:a4     Broadcast           ARP        60 Who has 192.168.0.103? Tell 192.168.0.1
   22 6.448731371   TP-Link_64:8b:a4     Broadcast           ARP        60 Who has 192.168.0.100? Tell 192.168.0.1
   23 6.448756806   PcsCompu_b0:db:28    TP-Link_64:8b:a4    ARP        42 192.168.0.100 is at 08:00:27:b0:db:28
   24 6.449907248   192.168.0.1          192.168.0.100       NBNS       92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>
   25 6.449947217   192.168.0.100        192.168.0.1         ICMP      120 Destination unreachable (Port unreachable)
   26 6.707497753   TP-Link_64:8b:a4     Broadcast           ARP        60 Who has 192.168.0.103? Tell 192.168.0.1
   27 6.711435416   TP-Link_64:8b:a4     Broadcast           ARP        60 Who has 192.168.0.100? Tell 192.168.0.1
   28 6.711460572   PcsCompu_b0:db:28    TP-Link_64:8b:a4    ARP        42 192.168.0.100 is at 08:00:27:b0:db:28

› Frame 21: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0
› Ethernet II, Src: TP-Link_64:8b:a4 (48:22:54:64:8b:a4), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
› Address Resolution Protocol (request)

wireshark_eth0S1K3A2.pcapng          Packets: 107 · Displayed: 107 (100.0%) · Dropped: 0 (0.0%)          Profile: Default
```

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.


root@Kali: ~
File Actions Edit View Help
KALI LINUX
"the quieter you become, the more you are able to hear"

```
msf6 > search ms10-061

Matching Modules
================

   #  Name                                   Disclosure Date  Rank       Check  Description
   -  ----                                   ---------------  ----       -----  -----------
   0  exploit/windows/smb/ms10_061_spoolss  2010-09-14       excellent  No     MS10-061 Microsoft Print Spooler Serv
ice Impersonation Vulnerability


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

msf6 > use exploit/windows/smb/ms10_061_spoolss
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms10_061_spoolss) > options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   PNAME                     no        The printer share name to use on the target
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/b
                                       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.

msf6 exploit(windows/smb/ms10_061_spoolss) > set RHOST 192.168.0.100
RHOST => 192.168.0.100
msf6 exploit(windows/smb/ms10_061_spoolss) > options

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