Assignment 2

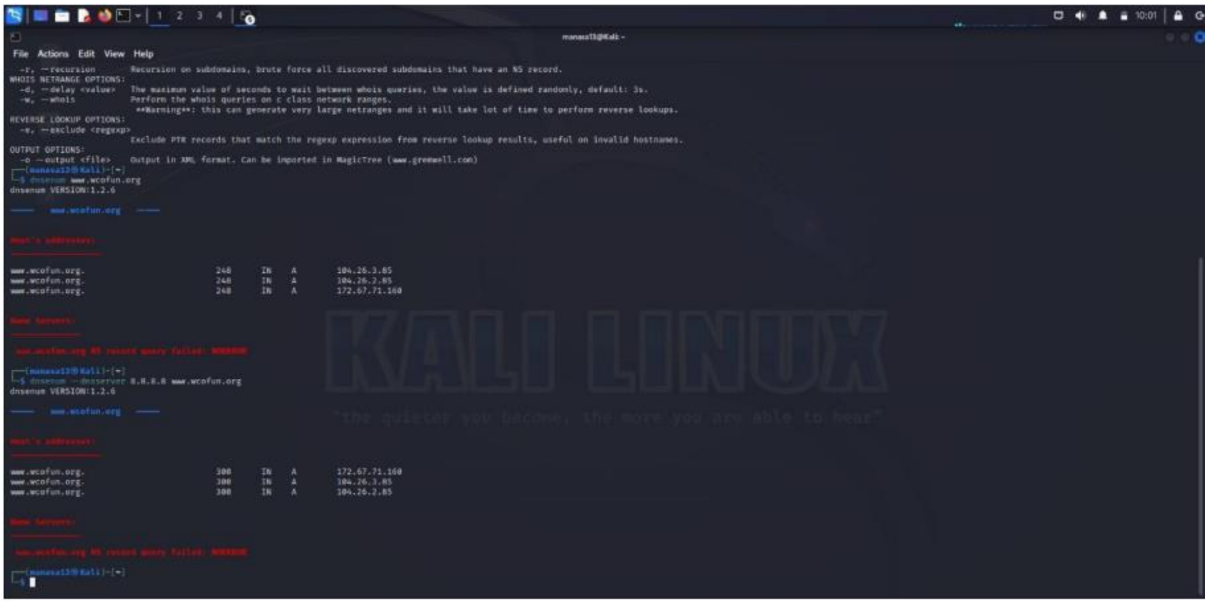
- **Hardik Kankane (21BCE10413)**

Overview:

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:

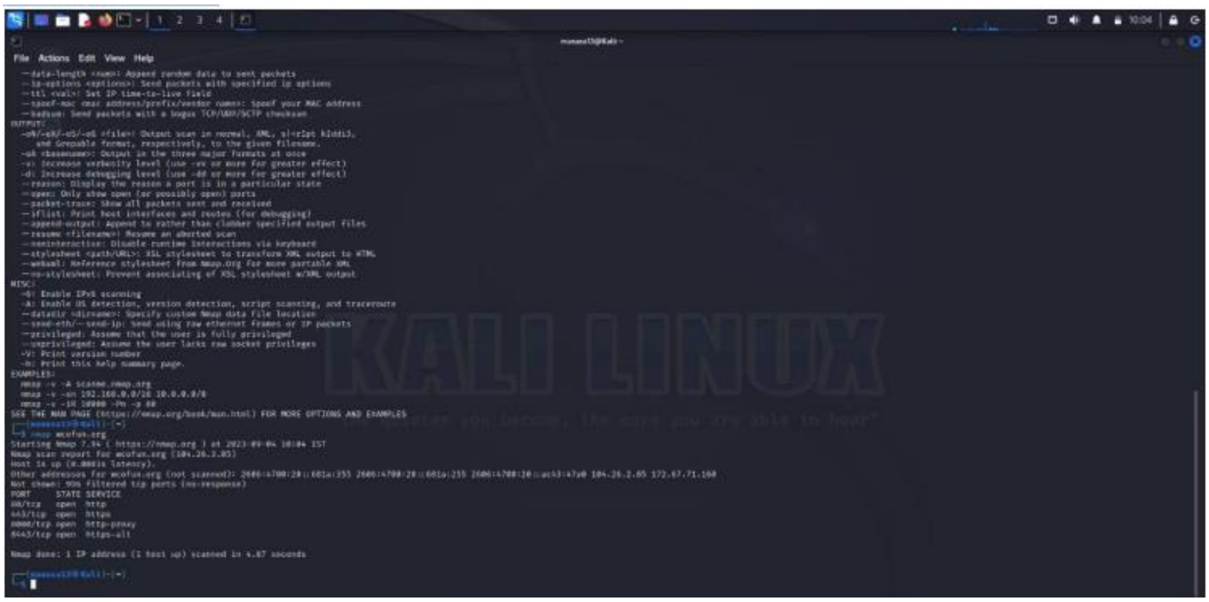
1. Information Gathering:
   Dnsenum is a command-line tool designed for DNS (Domain Name System) enumeration and information gathering. Security experts, network administrators, and ethical hackers rely on it to extract valuable insights about a target domain's DNS setup. By leveraging dnsenum, professionals can comprehensively assess the configuration and potential vulnerabilities of a given domain. In this instance, the tool was employed to scrutinize the DNS configuration of www.wcofun.org, enabling a detailed examination of its domain infrastructure. This process aids in identifying potential security gaps and ensuring robust safeguards for the website's digital assets and sensitive information.



```
  -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: NXDOMAIN

┌──(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: NXDOMAIN

┌──(manasa13㉿Kali)-[~]
└─$ 
```

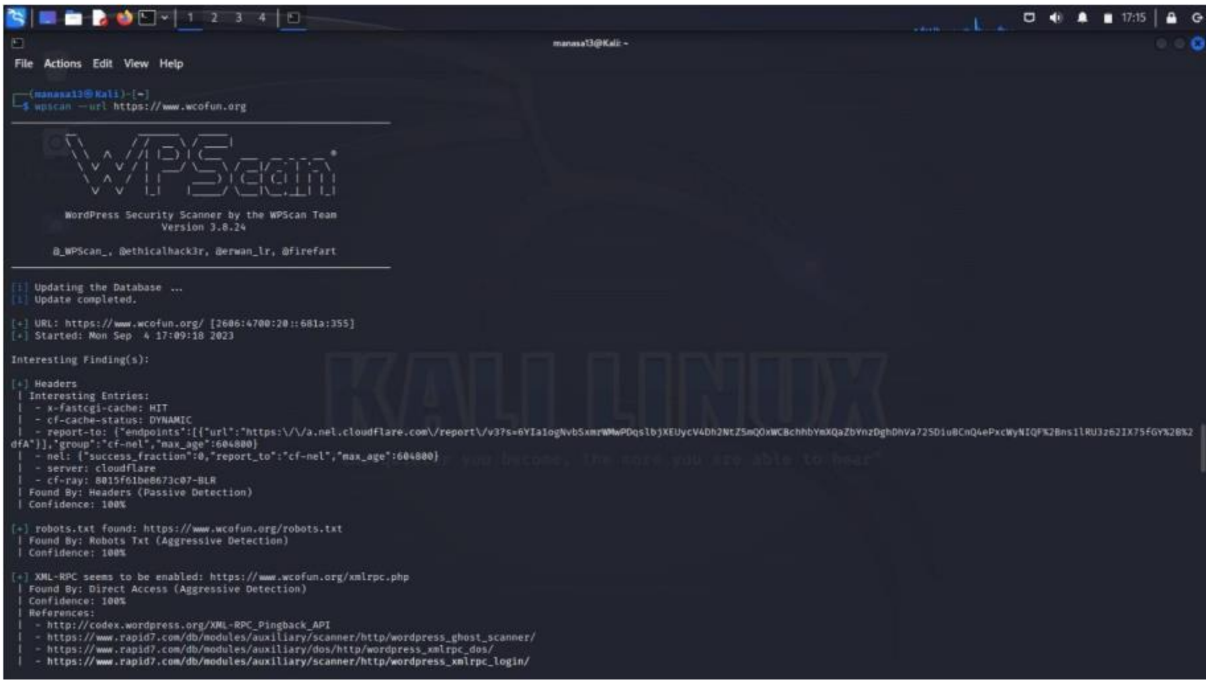
2. Vulnerability Analysis:
   Nmap, short for Network Mapper, is a prominent open-source tool employed for network exploration and vulnerability analysis. It excels in tasks such as network scanning, mapping, and fingerprinting, and also serves as a valuable resource for vulnerability assessment. Security professionals and network administrators widely rely on Nmap to identify and scrutinize potential weaknesses within a network's architecture. By leveraging its capabilities, users gain a comprehensive understanding of a network's configuration and potential vulnerabilities. This information is crucial

for fortifying defenses and ensuring the security of digital assets. In summary, Nmap plays a pivotal role in safeguarding networks and the sensitive data they contain.

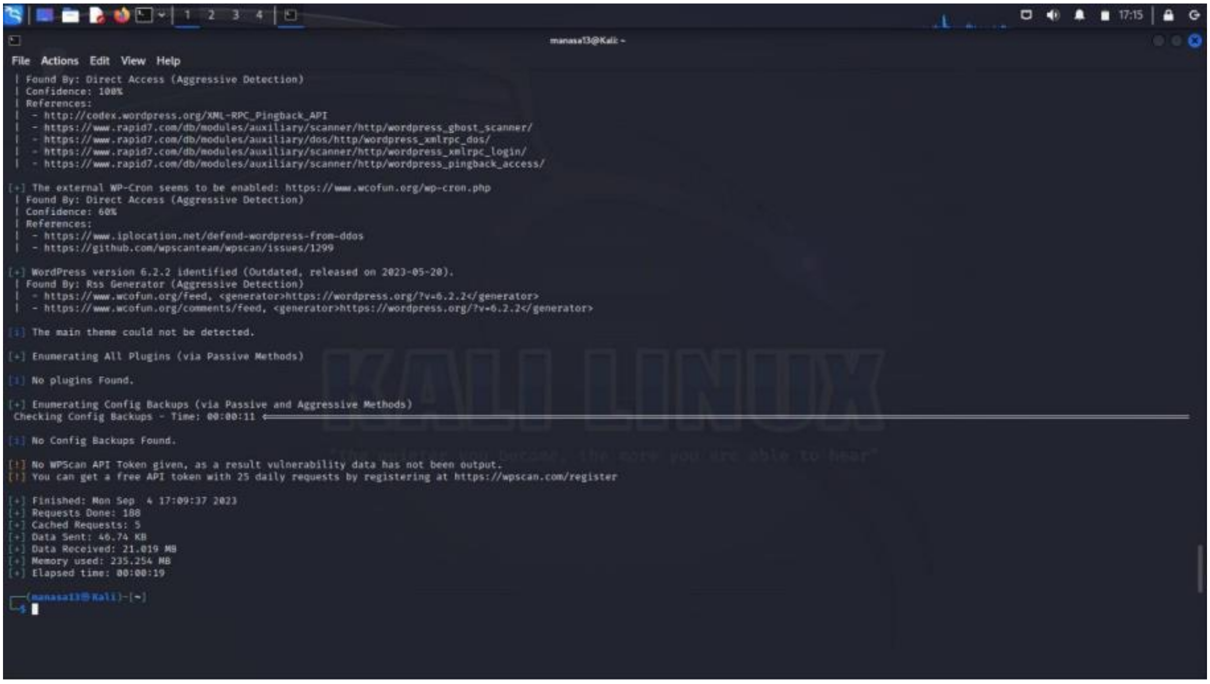


```
  --data-length <num>: Append random data to sent packets
  --ip-options <options>: Send packets with specified ip options
  --ttl <val>: Set IP time-to-live field
  --spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
  --badsum: Send packets with a bogus TCP/UDP/SCTP checksum
OUTPUT:
  -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:
   WPScan, a widely utilized open-source security scanner tailored for WordPress websites, is pivotal for web application analysis. It's designed to pinpoint vulnerabilities, misconfigurations, and security concerns within WordPress installations. This tool holds significant value for security experts, website administrators, and penetration testers, enabling them to comprehensively evaluate the security stance of WordPress sites. By leveraging WPScan's capabilities, professionals gain insights crucial for fortifying WordPress installations against potential threats. Its specialized focus on WordPress makes it an indispensable resource for ensuring the integrity and security of these widely used platforms. In essence, WPScan stands as an essential tool in the arsenal of those responsible for safeguarding WordPress websites and the data they manage.



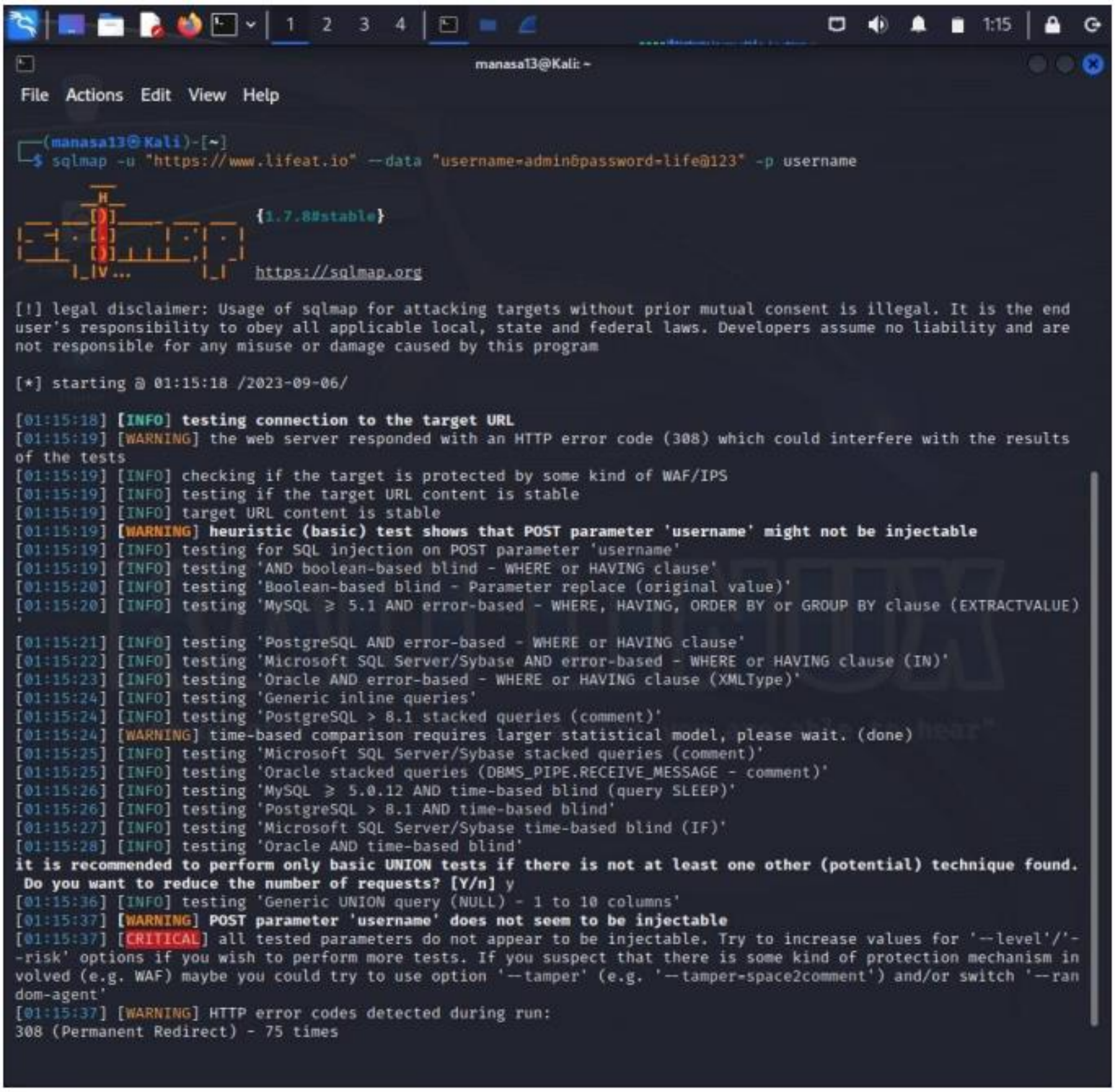
```
┌──(manasa13㉿Kali)-[~]
└─$ wpscan --url https://www.wcofun.org
_______________________________________________________________

         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::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\/report\/v3?s=6YIa1ogNvbSxmrWMwPDqslbjXEUycV4Dh2NtZ5mQOxWCBchhbYmXQaZbYnzDghDhVa725D1uBCnQ4ePxcWyNIQF%2Bns1lRU3z62IX75fGY%2B%2
dfA"}],"group":"cf-nel","max_age":604800}
 |  - nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
 |  - server: 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/
```



```
 | 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.

[!] 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)-[~]
└─$ 
```

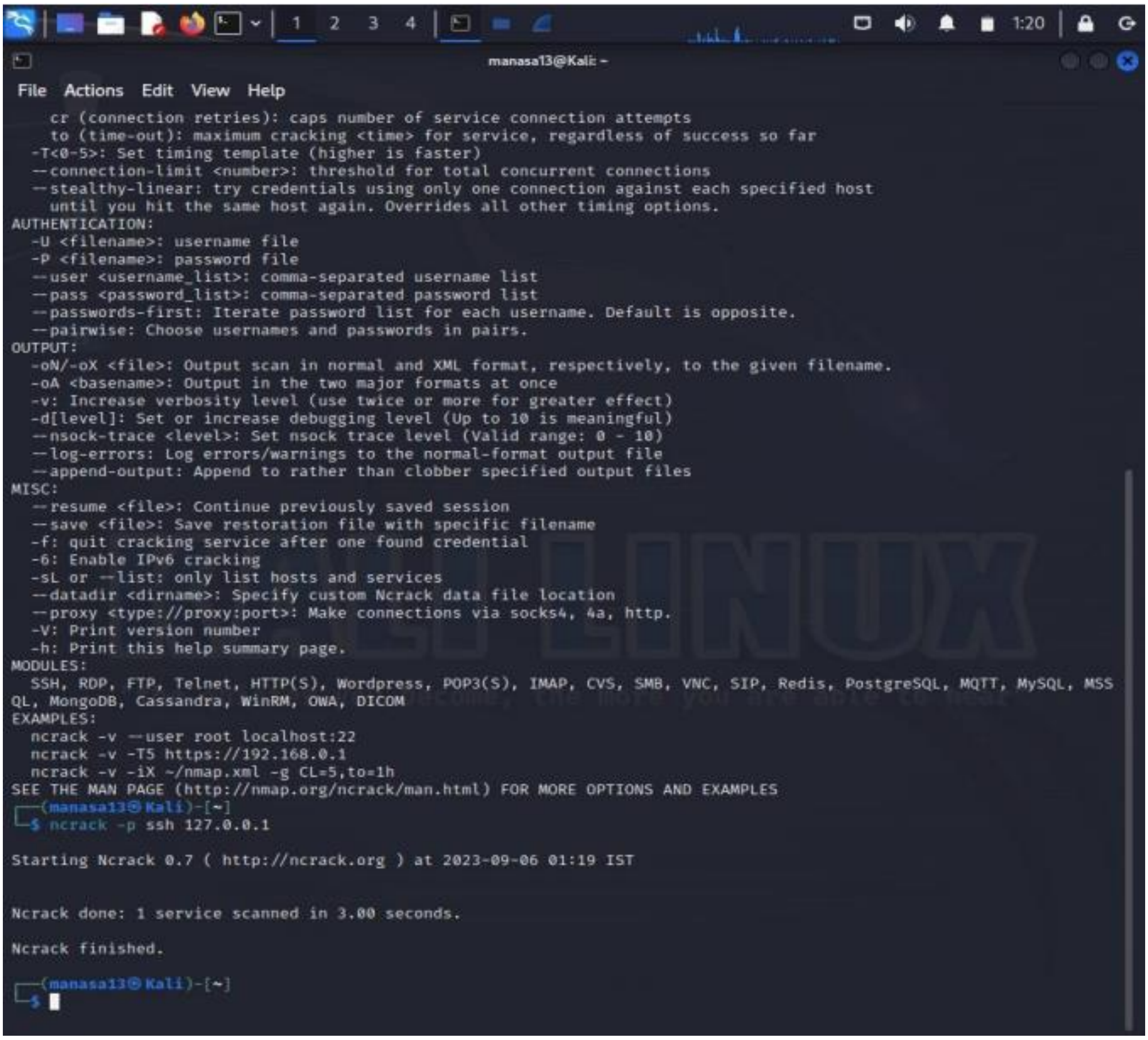
4. Database Management:
   Sqlmap, a widely adopted open-source tool, plays a pivotal role in database assessment. Specifically designed for automated penetration testing, it excels in evaluating database security. Sqlmap's primary objective is to identify and exploit SQL injection vulnerabilities within web applications and their associated databases. This form of attack involves injecting malicious SQL statements into input fields, potentially enabling unauthorized access to sensitive data or manipulation of the database. By utilizing sqlmap, security professionals and penetration testers can systematically scrutinize web applications for potential SQL injection vulnerabilities, ultimately fortifying defenses against this common and potentially devastating attack

vector. In essence, sqlmap stands as a critical tool in the arsenal of those responsible for safeguarding databases and the sensitive information they contain.



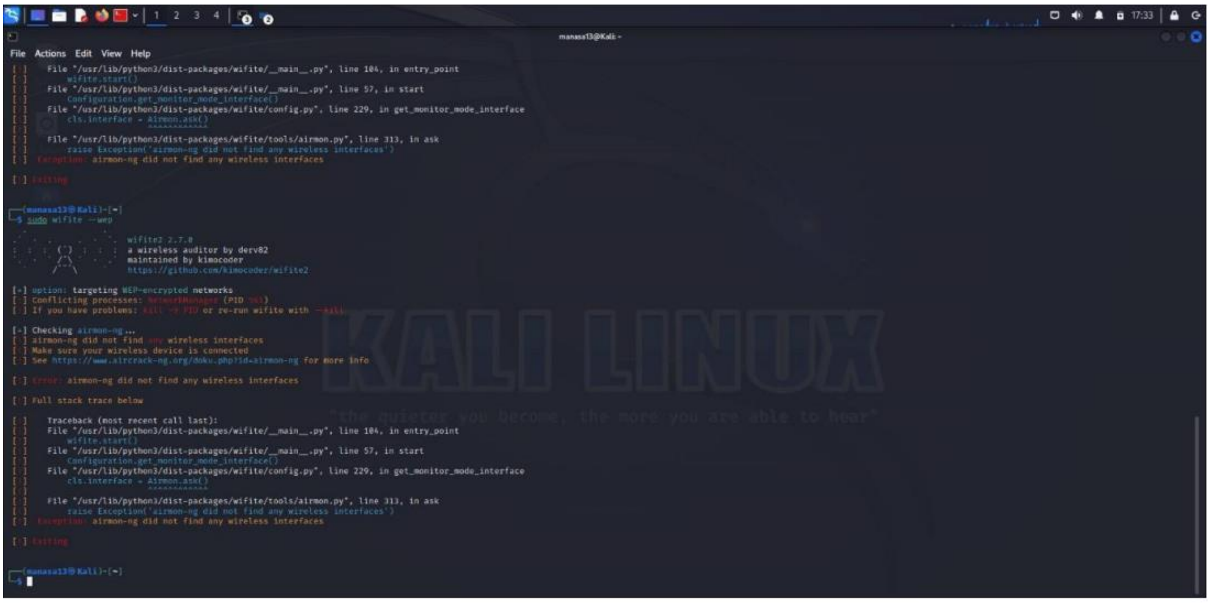
```
┌──(manasa13㉿Kali)-[~]
└─$ sqlmap -u "https://www.lifeat.io" --data "username=admin&password=life@123" -p username
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.7.8#stable}
|_ -| . [.]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] 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:
   Ncrack is a robust open-source network authentication cracking tool employed for password attack exploration. Its primary purpose is to conduct password attacks, encompassing both brute force and dictionary-based approaches, against a range of network services and protocols. Ncrack stands out for its capability to rigorously assess the strength of passwords used for authentication on various network services. It's specifically designed for legitimate security testing and auditing, providing security professionals with a controlled environment to evaluate password security and identify potential vulnerabilities. By utilizing Ncrack, analysts can proactively bolster authentication mechanisms, fortifying network services against unauthorized access and potential breaches. In summary, Ncrack is an essential tool for evaluating and enhancing the robustness of password security in network environments.



```
    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)-[~]
└─$ █
```

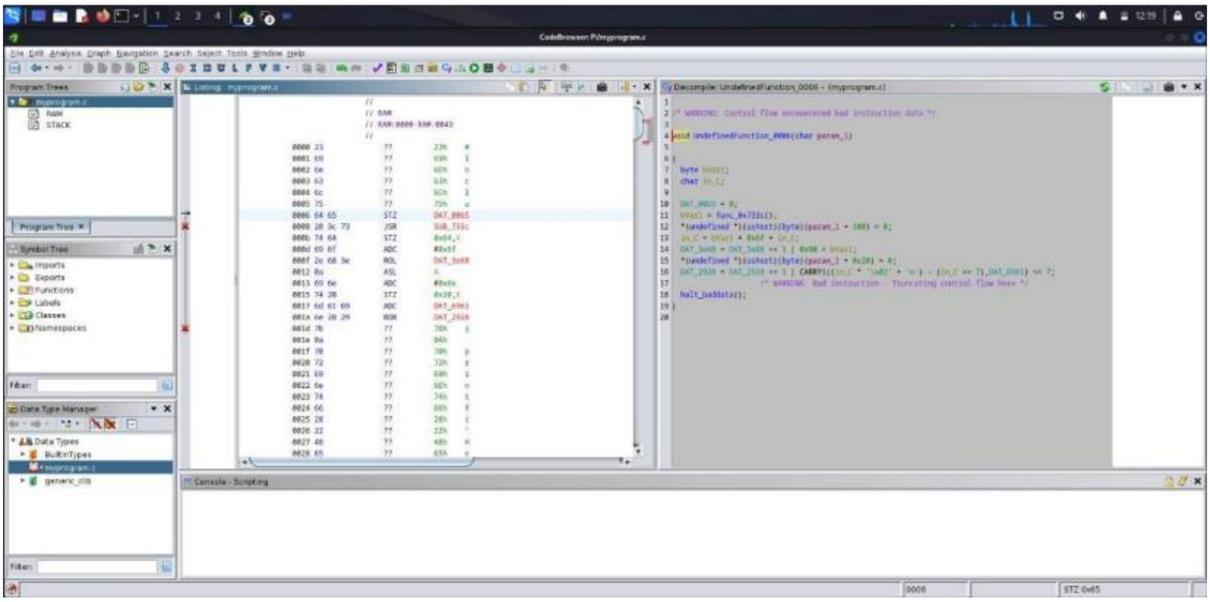
6. Wireless Attacks:
   Wifite is a widely recognized wireless auditing tool, integrated into Kali Linux. It's tailored for automating a range of wireless attacks, with a specific focus on WEP and WPA/WPA2-PSK cracking. By employing established attack methodologies, Wifite streamlines the process of probing and exploiting vulnerabilities in wireless networks. This tool is invaluable for security professionals and ethical hackers seeking to evaluate the resilience of wireless security measures. Its automation capabilities enhance efficiency in identifying potential weaknesses, empowering users to fortify their wireless networks against unauthorized access and potential breaches. In essence, Wifite is an indispensable resource for conducting controlled wireless assessments and strengthening the security posture of networks.



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

```
[ ]   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)-[~]
└─$ 
```

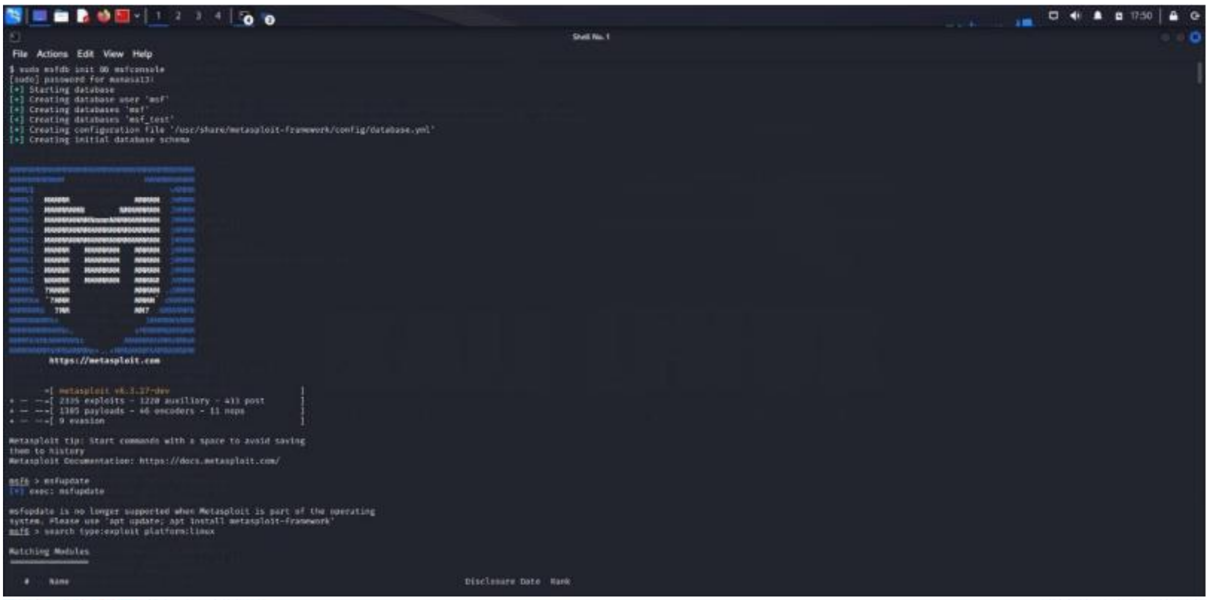
7. Reverse Engineering:
   For reverse engineering endeavors, two powerful tools, Clang and Ghidra, take center stage. Clang, an open-source C and C++ compiler front end, is an integral part of the LLVM project, excelling in parsing and compiling code. Meanwhile, Ghidra, a potent open-source reverse engineering framework developed by the NSA, provides a comprehensive suite of features for tasks like disassembly and decompilation. Together, Clang and Ghidra form a dynamic duo, equipping analysts, security professionals, and developers with the means to not only compile and analyze code but also to dissect and understand intricate software systems, making them indispensable assets in the realm of reverse engineering.



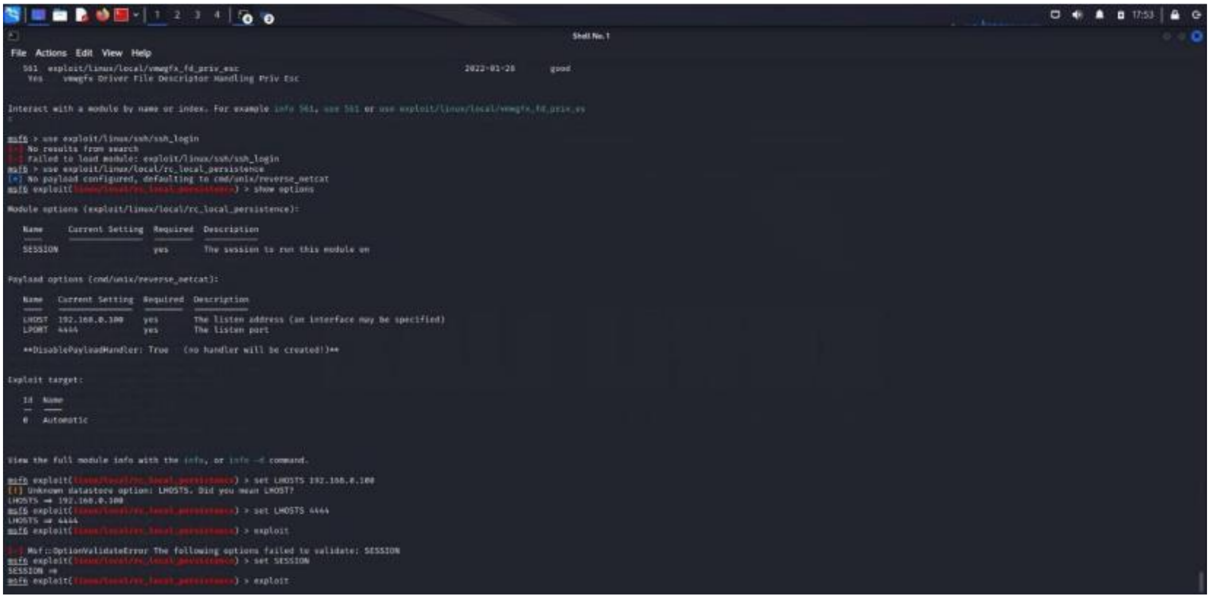
```
/* WARNING: Control flow encountered bad instruction data */

void UndefinedFunction_0006(char param_1)

{
  byte bVar1;
  char in_C;

  DAT_0003 = 0;
  bVar1 = func_0x733c();
  *(undefined *)(ushort)(byte)(param_1 + 100) = 0;
  in_C = bVar1 + 0xdf + in_C;
  DAT_3e68 = DAT_3e68 << 1 | 0x98 < bVar1;
  *(undefined *)(ushort)(byte)(param_1 + 0x20) = 0;
  DAT_2920 = DAT_2920 >> 1 | CARRY1((in_C + '\x82' + 'n') - (in_C == 7),DAT_0061) << 7;
                    /* WARNING: Bad instruction - Truncating control flow here */
  halt_baddata();
}
```

8. Exploitation Tools:
   The go-to tool for exploiting IP addresses is the Metasploit Framework. This widely adopted open-source penetration testing and exploitation tool is renowned for its comprehensive toolkit. It equips security professionals, penetration testers, and

ethical hackers with a suite of capabilities for pinpointing vulnerabilities, crafting and executing exploits, and executing thorough security assessments. The Metasploit Framework serves as an essential resource for evaluating and fortifying the security posture of both systems and applications, making it a cornerstone in the arsenals of those dedicated to safeguarding digital environments.



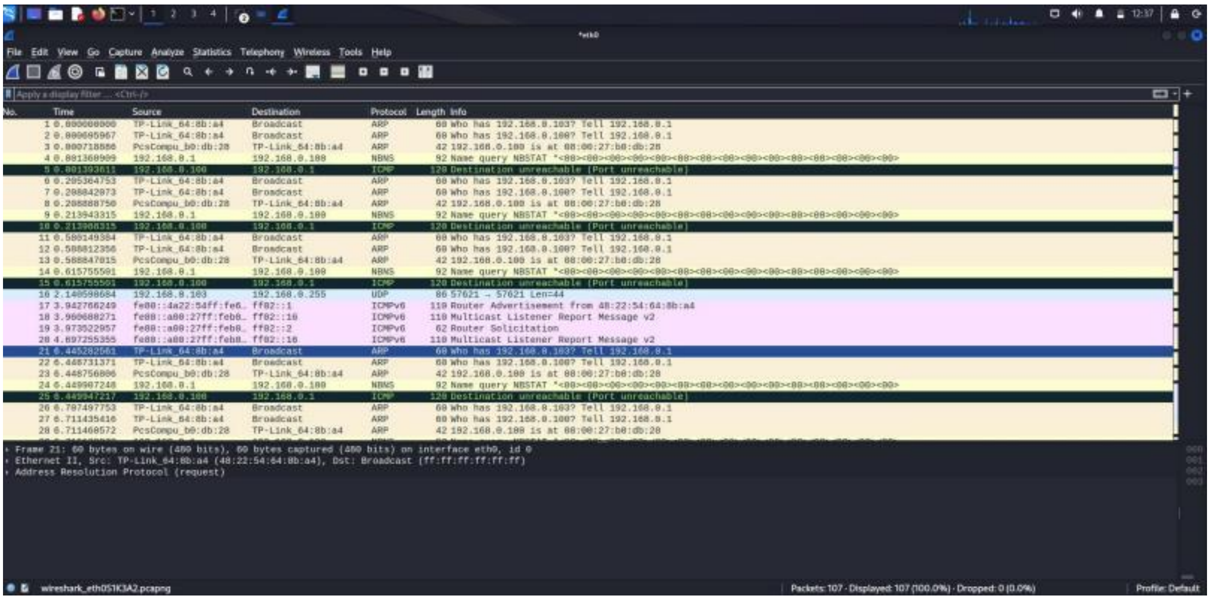
```
$ sudo msfdb init && msfconsole
[sudo] password for manasa13:
[+] Starting database
[+] Creating database user 'msf'
[+] Creating databases 'msf'
[+] Creating databases 'msf_test'
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'
[+] Creating initial database schema

        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
```

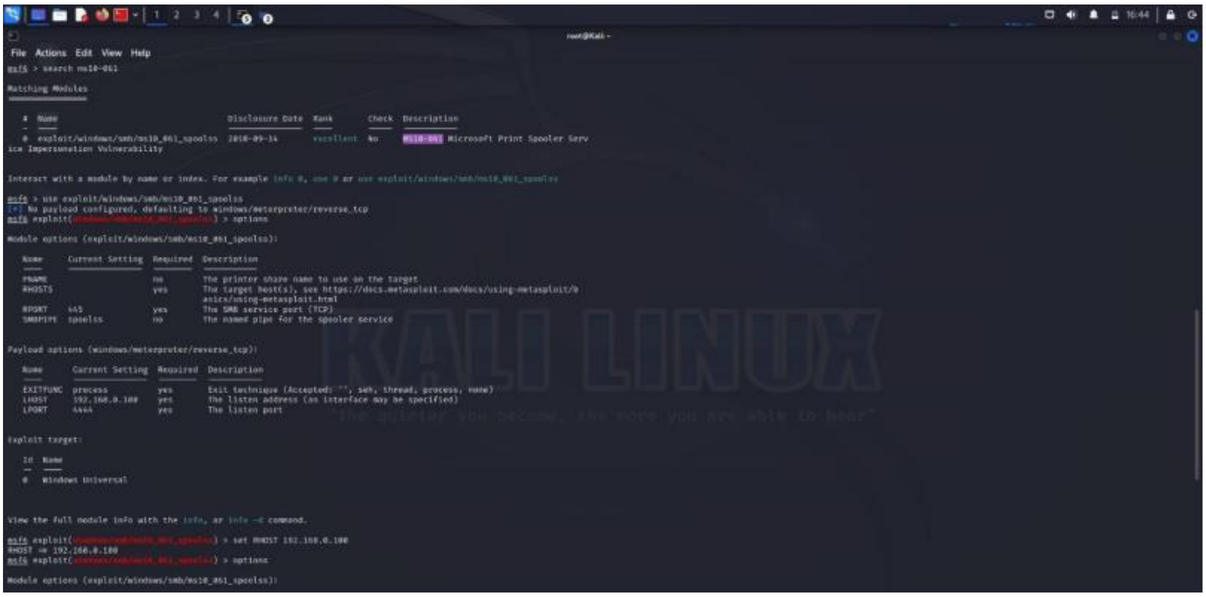
9. Sniffing and Spoofing:
   Wireshark is the go-to tool for exploring sniffing and spoofing activities. As a widely utilized open-source network protocol analyzer, Wireshark is primarily designed for in-depth network traffic analysis, although it can also be employed for network sniffing. It's crucial to emphasize that Wireshark is a legitimate and essential tool for network troubleshooting and security analysis, provided it is used responsibly, within legal frameworks, and adheres to ethical boundaries. Network administrators, security experts, and ethical hackers frequently leverage Wireshark for legitimate purposes, including monitoring network traffic, diagnosing network anomalies, and

conducting comprehensive network security assessments. This versatile tool remains a critical asset in safeguarding network integrity and ensuring its optimal performance.


*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 0.588149384   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 3.960688271   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 4.097255355   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 delving into post-exploitation activities, security professionals often turn to the potent tool known as Mimikatz. Recognized for its proficiency in extracting plaintext passwords, hashes, and various authentication credentials from system memory, Mimikatz is a go-to post-exploitation tool. It also excels in executing other post-exploitation tasks on Windows systems. While it is a crucial resource for security experts and penetration testers in assessing system vulnerabilities, it's important to acknowledge that Mimikatz is occasionally leveraged by malicious actors for both legitimate and nefarious purposes. This duality underscores the critical importance of responsible and ethical usage within the cybersecurity community.



```
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):
```