ASSIGNMENT - 2

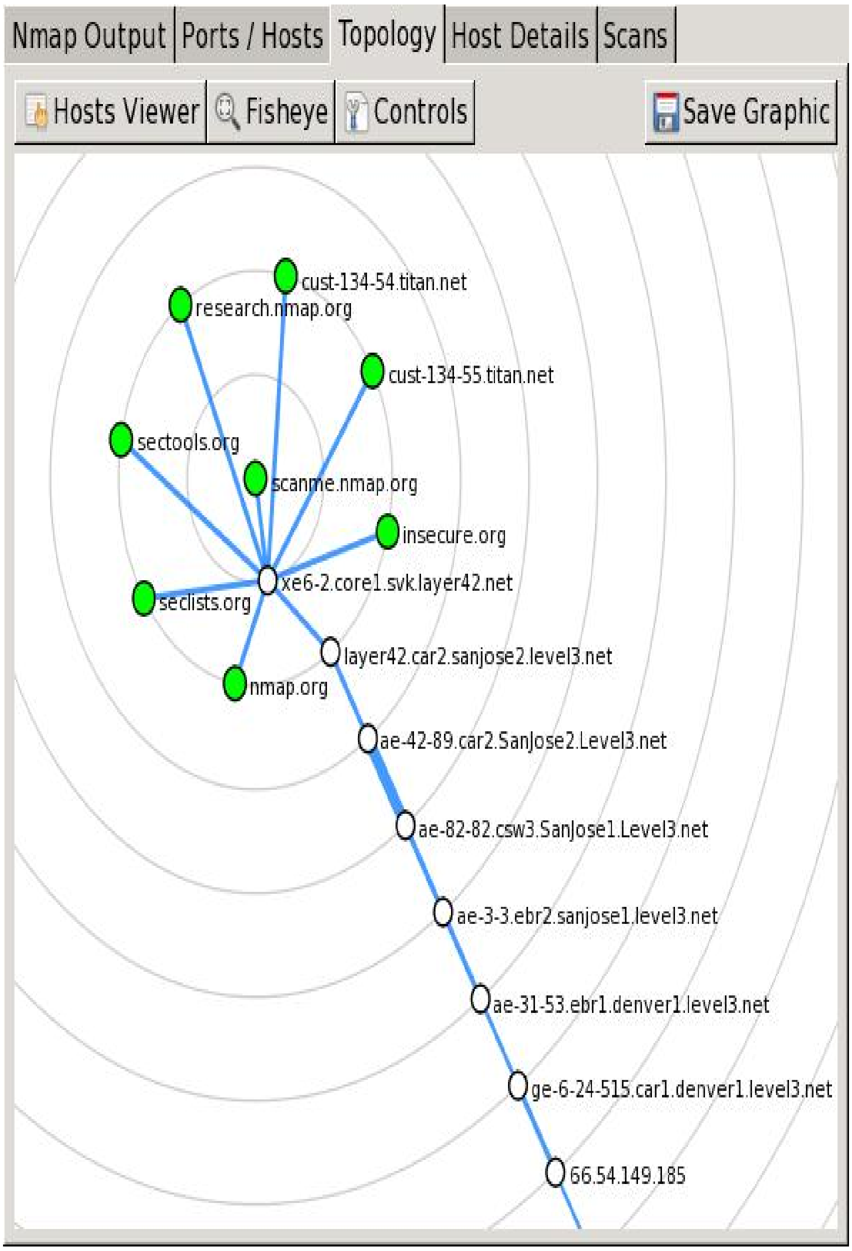
NAME : SANISETTY HEMA SAGAR

REG N0 : 21BCE7769

Certainly! Here are ten Kali Linux tools, each explained in detail, paragraph by paragraph:

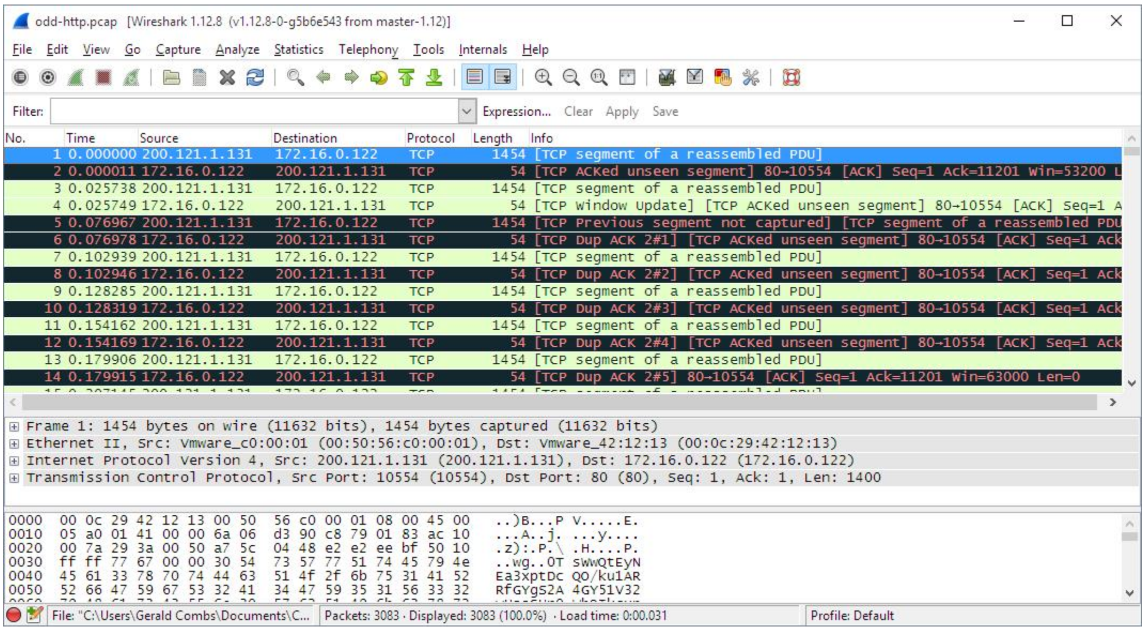
1. Nmap (Network Mapper):

Nmap is a versatile network scanning tool that serves as a Swiss army knife for network reconnaissance. It allows security professionals and ethical hackers to discover hosts, identify open ports, detect services, and even fingerprint operating systems. Nmap's scriptable capabilities make it highly adaptable for various scanning tasks, from basic network discovery to vulnerability assessment.


Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Hosts Viewer
Fisheye
Controls
Save Graphic
cust-134-54.titan.net
research.nmap.org
cust-134-55.titan.net
sectools.org
scanme.nmap.org
insecure.org
xe6-2.core1.svk.layer42.net
seclists.org
layer42.car2.sanjose2.level3.net
nmap.org
ae-42-89.car2.SanJose2.Level3.net
ae-82-82.csw3.SanJose1.Level3.net
ae-3-3.ebr2.sanjose1.level3.net
ae-31-53.ebr1.denver1.level3.net
ge-6-24-515.car1.denver1.level3.net
66.54.149.185

2. Wireshark:

Wireshark is an indispensable tool for deep packet inspection and network traffic analysis. It provides a graphical interface for capturing and dissecting network packets, making it easier to troubleshoot network issues, analyze protocols, and uncover potential security vulnerabilities. Security experts rely on Wireshark to gain insights into network communications and identify anomalies.



odd-http.pcap [Wireshark 1.12.8 (v1.12.8-0-g5b6e543 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
No.  Time     Source        Destination   Protocol Length Info
   1 0.000000 200.121.1.131 172.16.0.122  TCP      1454 [TCP segment of a reassembled PDU]
   2 0.000011 172.16.0.122  200.121.1.131 TCP        54 [TCP ACKed unseen segment] 80→10554 [ACK] Seq=1 Ack=11201 Win=53200 L
   3 0.025738 200.121.1.131 172.16.0.122  TCP      1454 [TCP segment of a reassembled PDU]
   4 0.025749 172.16.0.122  200.121.1.131 TCP        54 [TCP Window Update] [TCP ACKed unseen segment] 80→10554 [ACK] Seq=1 A
   5 0.076967 200.121.1.131 172.16.0.122  TCP      1454 [TCP Previous segment not captured] [TCP segment of a reassembled PDU
   6 0.076978 172.16.0.122  200.121.1.131 TCP        54 [TCP Dup ACK 2#1] [TCP ACKed unseen segment] 80→10554 [ACK] Seq=1 Ack
   7 0.102939 200.121.1.131 172.16.0.122  TCP      1454 [TCP segment of a reassembled PDU]
   8 0.102946 172.16.0.122  200.121.1.131 TCP        54 [TCP Dup ACK 2#2] [TCP ACKed unseen segment] 80→10554 [ACK] Seq=1 Ack
   9 0.128285 200.121.1.131 172.16.0.122  TCP      1454 [TCP segment of a reassembled PDU]
  10 0.128319 172.16.0.122  200.121.1.131 TCP        54 [TCP Dup ACK 2#3] [TCP ACKed unseen segment] 80→10554 [ACK] Seq=1 Ack
  11 0.154162 200.121.1.131 172.16.0.122  TCP      1454 [TCP segment of a reassembled PDU]
  12 0.154169 172.16.0.122  200.121.1.131 TCP        54 [TCP Dup ACK 2#4] [TCP ACKed unseen segment] 80→10554 [ACK] Seq=1 Ack
  13 0.179906 200.121.1.131 172.16.0.122  TCP      1454 [TCP segment of a reassembled PDU]
  14 0.179915 172.16.0.122  200.121.1.131 TCP        54 [TCP Dup ACK 2#5] 80→10554 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
```

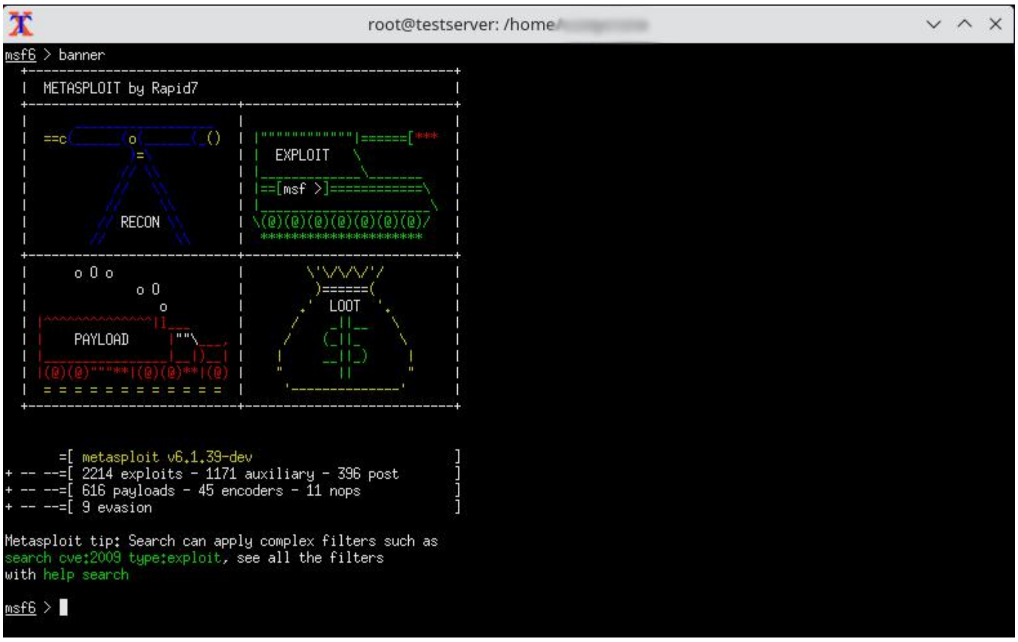
```
⊞ Frame 1: 1454 bytes on wire (11632 bits), 1454 bytes captured (11632 bits)
⊞ Ethernet II, Src: Vmware_c0:00:01 (00:50:56:c0:00:01), Dst: Vmware_42:12:13 (00:0c:29:42:12:13)
⊞ Internet Protocol Version 4, Src: 200.121.1.131 (200.121.1.131), Dst: 172.16.0.122 (172.16.0.122)
⊞ Transmission Control Protocol, Src Port: 10554 (10554), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 1400
```

```
0000  00 0c 29 42 12 13 00 50  56 c0 00 01 08 00 45 00   ..)B...P V.....E.
0010  05 a0 01 41 00 00 6a 06  d3 90 c8 79 01 83 ac 10   ...A..j. ...y....
0020  00 7a 29 3a 00 50 a7 5c  04 48 e2 e2 ee bf 50 10   .z):.P.\ .H....P.
0030  ff ff 77 67 00 00 30 54  73 57 77 51 74 45 79 4e   ..wg..0T sWwQtEyN
0040  45 61 33 78 70 74 44 63  51 4f 2f 6b 75 31 41 52   Ea3xptDc QO/ku1AR
0050  52 66 47 59 67 53 32 41  34 47 59 35 31 56 33 32   RfGYgS2A 4GY51V32
```

File: "C:\Users\Gerald Combs\Documents\C... Packets: 3083 · Displayed: 3083 (100.0%) · Load time: 0:00.031 Profile: Default

3. Metasploit Framework:

The Metasploit Framework is a comprehensive penetration testing and exploitation tool that empowers security professionals to find, exploit, and validate vulnerabilities in target systems. With its vast collection of exploits, payloads, and post-exploitation modules, Metasploit is a must-have for simulating real-world attacks, assessing system security, and hardening defenses.

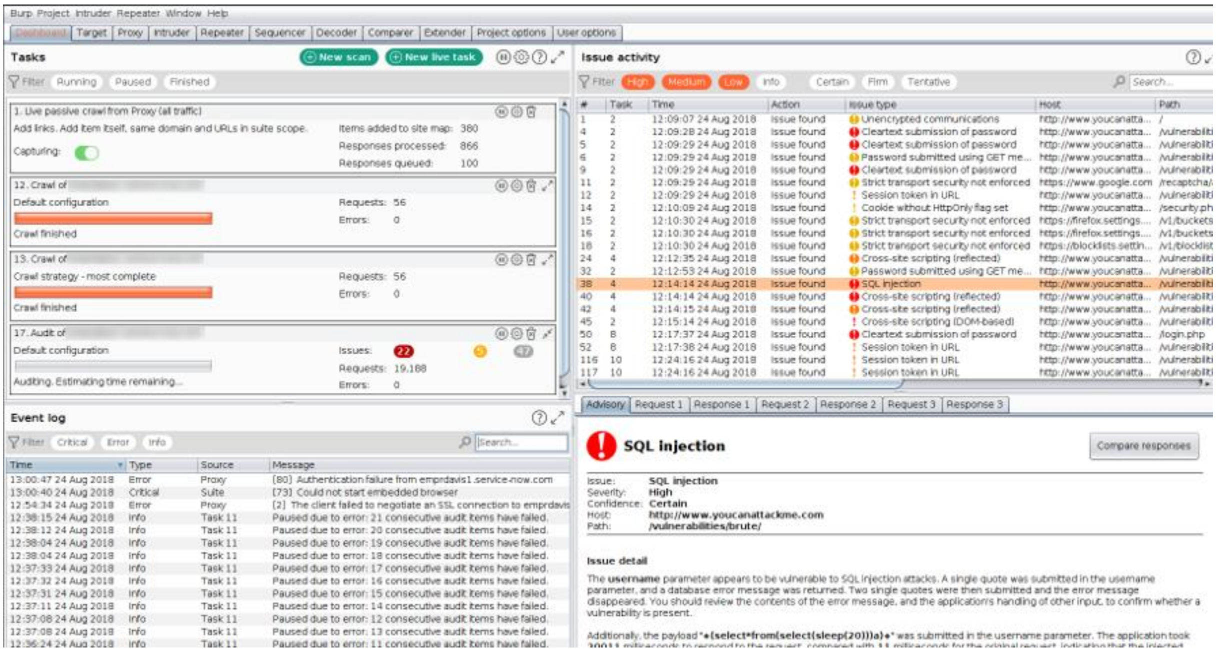


root@testserver: /home/[redacted]

```
msf6 > banner
 +-------------------------------------------------------+
 |  METASPLOIT by Rapid7                                 |
 +---------------------------+---------------------------+
 |      __________________   |                           |
 |  ==c(______(o(______(_()  | |""""""""""""|======[***  |
 |             )=\           | |  EXPLOIT   \            |
 |            // \\          | |_____________\_______    |
 |           //   \\         | |==[msf >]============\   |
 |          //     \\        | |______________________\  |
 |         // RECON \\       | \(@)(@)(@)(@)(@)(@)(@)/   |
 |        //         \\      |  *********************    |
 +---------------------------+---------------------------+
 |      o O o                |        \'\/\/\/'/         |
 |              o O          |         )======(          |
 |                 o         |       .'  LOOT  '.        |
 | |^^^^^^^^^^^^^^|l___      |      /    _||__   \       |
 | |    PAYLOAD     |""\___, |     /    (_||_     \      |
 | |________________|__|)__| |    |     __||_)     |     |
 | |(@)(@)"""**|(@)(@)**|(@) |    "       ||       "     |
 |  = = = = = = = = = = = =  |     '--------------'      |
 +---------------------------+---------------------------+


       =[ metasploit v6.1.39-dev                          ]
+ -- --=[ 2214 exploits - 1171 auxiliary - 396 post       ]
+ -- --=[ 616 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Search can apply complex filters such as
search cve:2009 type:exploit, see all the filters
with help search

msf6 > █
```

4. Burp Suite:

Burp Suite is a renowned web application security testing tool that combines scanning, crawling, and manual testing capabilities. Security experts use it to identify and validate vulnerabilities in web applications, such as SQL injection, cross-site scripting (XSS), and security misconfigurations. Burp Suite's user-friendly interface simplifies the process of finding and remediating web application security issues.


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Tasks
New scan
New live task
Filter Running Paused Finished
Issue activity
Filter High Medium Low Info Certain Firm Tentative
Search...
Event log
Filter Critical Error Info
Search...
Advisory Request 1 Response 1 Request 2 Response 2 Request 3 Response 3
Compare responses

1. Live passive crawl from Proxy (all traffic)
Add links. Add item itself, same domain and URLs in suite scope.
Capturing:
Items added to site map: 380
Responses processed: 866
Responses queued: 100

12. Crawl of [redacted]
Default configuration
Crawl finished
Requests: 56
Errors: 0

13. Crawl of [redacted]
Crawl strategy - most complete
Crawl finished
Requests: 56
Errors: 0

17. Audit of [redacted]
Default configuration
Auditing. Estimating time remaining...
Issues: 22 47
Requests: 19,188
Errors: 0

#	Task	Time	Action	Issue type	Host	Path
1	2	12:09:07 24 Aug 2018	Issue found	Unencrypted communications	http://www.youcanatta...	/
4	2	12:09:28 24 Aug 2018	Issue found	Cleartext submission of password	http://www.youcanatta...	/vulnerabiliti
5	2	12:09:29 24 Aug 2018	Issue found	Cleartext submission of password	http://www.youcanatta...	/vulnerabiliti
6	2	12:09:29 24 Aug 2018	Issue found	Password submitted using GET me...	http://www.youcanatta...	/vulnerabiliti
9	2	12:09:29 24 Aug 2018	Issue found	Cleartext submission of password	http://www.youcanatta...	/vulnerabiliti
11	2	12:09:29 24 Aug 2018	Issue found	Strict transport security not enforced	https://www.google.com	/recaptcha/
12	2	12:09:29 24 Aug 2018	Issue found	Session token in URL	http://www.youcanatta...	/vulnerabiliti
14	2	12:10:09 24 Aug 2018	Issue found	Cookie without HttpOnly flag set	http://www.youcanatta...	/security.ph
15	2	12:10:30 24 Aug 2018	Issue found	Strict transport security not enforced	https://firefox.settings....	/v1/buckets
16	2	12:10:30 24 Aug 2018	Issue found	Strict transport security not enforced	https://firefox.settings....	/v1/buckets
18	2	12:10:30 24 Aug 2018	Issue found	Strict transport security not enforced	https://blocklists.settin...	/v1/blocklist
24	4	12:12:35 24 Aug 2018	Issue found	Cross-site scripting (reflected)	http://www.youcanatta...	/vulnerabiliti
32	2	12:12:53 24 Aug 2018	Issue found	Password submitted using GET me...	http://www.youcanatta...	/vulnerabiliti
38	4	12:14:14 24 Aug 2018	Issue found	SQL injection	http://www.youcanatta...	/vulnerabiliti
40	4	12:14:14 24 Aug 2018	Issue found	Cross-site scripting (reflected)	http://www.youcanatta...	/vulnerabiliti
42	4	12:14:15 24 Aug 2018	Issue found	Cross-site scripting (reflected)	http://www.youcanatta...	/vulnerabiliti
45	2	12:15:14 24 Aug 2018	Issue found	Cross-site scripting (DOM-based)	http://www.youcanatta...	/vulnerabiliti
50	8	12:17:37 24 Aug 2018	Issue found	Cleartext submission of password	http://www.youcanatta...	/login.php
52	8	12:17:38 24 Aug 2018	Issue found	Session token in URL	http://www.youcanatta...	/vulnerabiliti
116	10	12:24:16 24 Aug 2018	Issue found	Session token in URL	http://www.youcanatta...	/vulnerabiliti
117	10	12:24:16 24 Aug 2018	Issue found	Session token in URL	http://www.youcanatta...	/vulnerabiliti

Time	Type	Source	Message
13:00:47 24 Aug 2018	Error	Proxy	[80] Authentication failure from emprdavis1.service-now.com
13:00:40 24 Aug 2018	Critical	Suite	[73] Could not start embedded browser
12:54:34 24 Aug 2018	Error	Proxy	[2] The client failed to negotiate an SSL connection to emprdavis
12:38:15 24 Aug 2018	Info	Task 11	Paused due to error: 21 consecutive audit items have failed.
12:38:12 24 Aug 2018	Info	Task 11	Paused due to error: 20 consecutive audit items have failed.
12:38:04 24 Aug 2018	Info	Task 11	Paused due to error: 19 consecutive audit items have failed.
12:38:04 24 Aug 2018	Info	Task 11	Paused due to error: 18 consecutive audit items have failed.
12:37:33 24 Aug 2018	Info	Task 11	Paused due to error: 17 consecutive audit items have failed.
12:37:32 24 Aug 2018	Info	Task 11	Paused due to error: 16 consecutive audit items have failed.
12:37:31 24 Aug 2018	Info	Task 11	Paused due to error: 15 consecutive audit items have failed.
12:37:11 24 Aug 2018	Info	Task 11	Paused due to error: 14 consecutive audit items have failed.
12:37:08 24 Aug 2018	Info	Task 11	Paused due to error: 12 consecutive audit items have failed.
12:37:08 24 Aug 2018	Info	Task 11	Paused due to error: 13 consecutive audit items have failed.
12:36:24 24 Aug 2018	Info	Task 11	Paused due to error: 11 consecutive audit items have failed.

SQL injection

Issue: **SQL injection**
Severity: **High**
Confidence: **Certain**
Host: **http://www.youcanattackme.com**
Path: **/vulnerabilities/brute/**

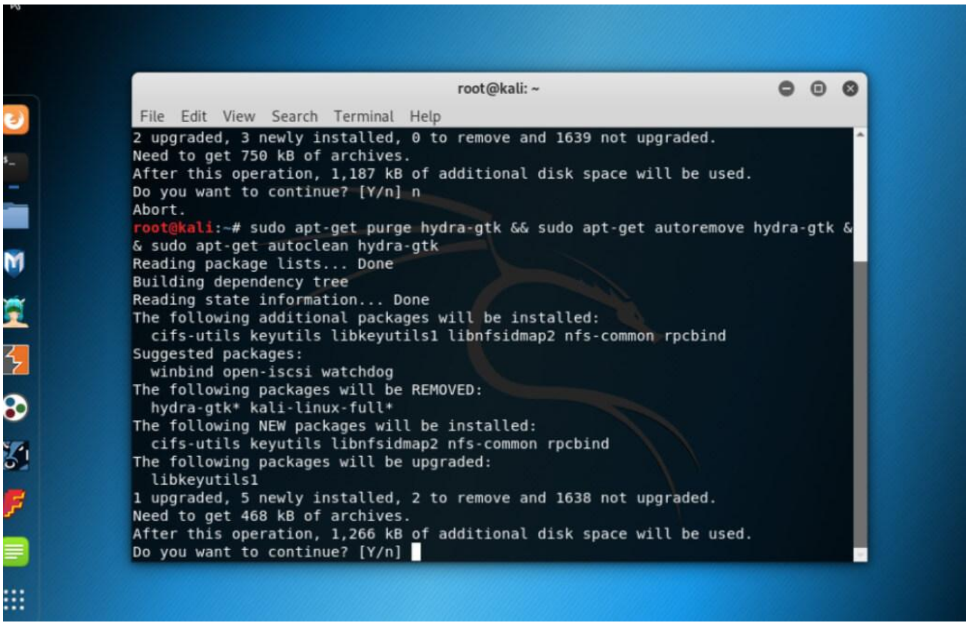
Issue detail

The **username** parameter appears to be vulnerable to SQL injection attacks. A single quote was submitted in the username parameter, and a database error message was returned. Two single quotes were then submitted and the error message disappeared. You should review the contents of the error message, and the application's handling of other input, to confirm whether a vulnerability is present.

Additionally, the payload **"+(select*from(select(sleep(20)))a)+"** was submitted in the username parameter. The application took 20011 milliseconds to respond to the request, compared with 11 milliseconds for the original request, indicating that the injected

5. Hydra:

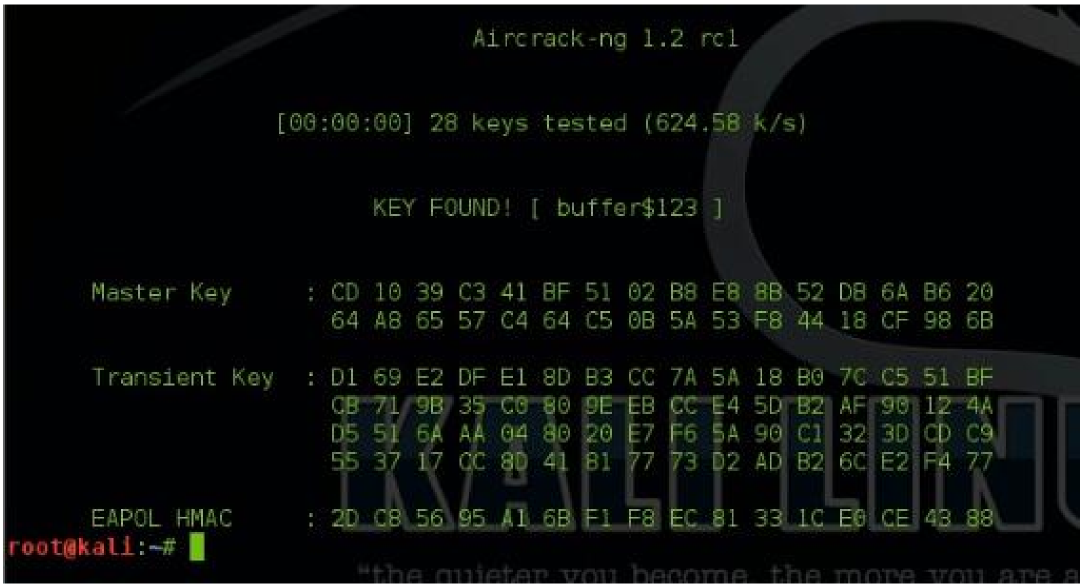
Hydra is a potent password-cracking tool known for its versatility and effectiveness. It supports various protocols, enabling security professionals to conduct dictionary and brute-force attacks against services like SSH, FTP, RDP, and more. Hydra is an essential tool for identifying weak or easily guessable passwords and strengthening authentication mechanisms.



```
2 upgraded, 3 newly installed, 0 to remove and 1639 not upgraded.
Need to get 750 kB of archives.
After this operation, 1,187 kB of additional disk space will be used.
Do you want to continue? [Y/n] n
Abort.
root@kali:~# sudo apt-get purge hydra-gtk && sudo apt-get autoremove hydra-gtk &
& sudo apt-get autoclean hydra-gtk
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  cifs-utils keyutils libkeyutils1 libnfsidmap2 nfs-common rpcbind
Suggested packages:
  winbind open-iscsi watchdog
The following packages will be REMOVED:
  hydra-gtk* kali-linux-full*
The following NEW packages will be installed:
  cifs-utils keyutils libnfsidmap2 nfs-common rpcbind
The following packages will be upgraded:
  libkeyutils1
1 upgraded, 5 newly installed, 2 to remove and 1638 not upgraded.
Need to get 468 kB of archives.
After this operation, 1,266 kB of additional disk space will be used.
Do you want to continue? [Y/n]
```

6. Aircrack-ng:

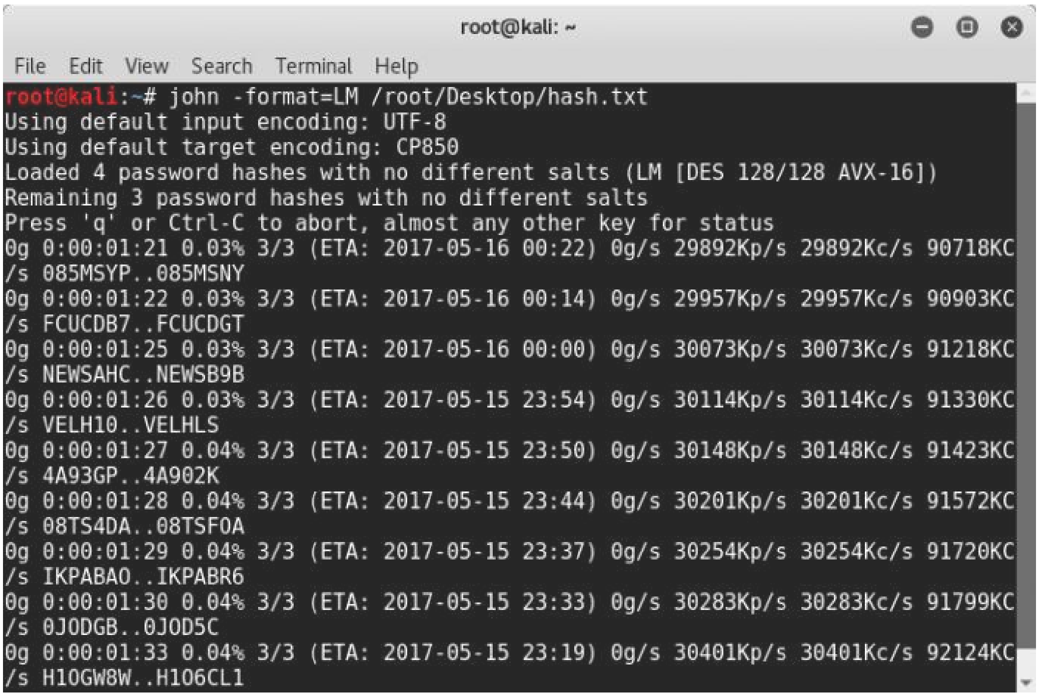
Aircrack-ng is a specialized suite of tools for assessing and securing Wi-Fi networks. It includes utilities for capturing wireless packets, performing WEP and WPA/WPA2 cracking, and conducting dictionary attacks on Wi-Fi passwords. Security testers use Aircrack-ng to evaluate the security of wireless networks and recommend improvements.



```
                              Aircrack-ng 1.2 rc1


                  [00:00:00] 28 keys tested (624.58 k/s)


                         KEY FOUND! [ buffer$123 ]


    Master Key     : CD 10 39 C3 41 BF 51 02 B8 E8 8B 52 D8 6A B6 20
                     64 A8 65 57 C4 64 C5 0B 5A 53 F8 44 18 CF 98 6B

    Transient Key  : D1 69 E2 DF E1 8D B3 CC 7A 5A 18 B0 7C C5 51 BF
                     CB 71 9B 35 C0 80 9E EB CC E4 5D B2 AF 90 12 4A
                     D5 51 6A AA 04 80 20 E7 F6 5A 90 C1 32 3D CD C9
                     55 37 17 CC 8D 41 81 77 73 D2 AD B2 6C E2 F4 77

    EAPOL HMAC     : 2D C8 56 95 A1 6B F1 F8 EC 81 33 1C E0 CE 43 88
root@kali:~# 
```

7. John the Ripper:

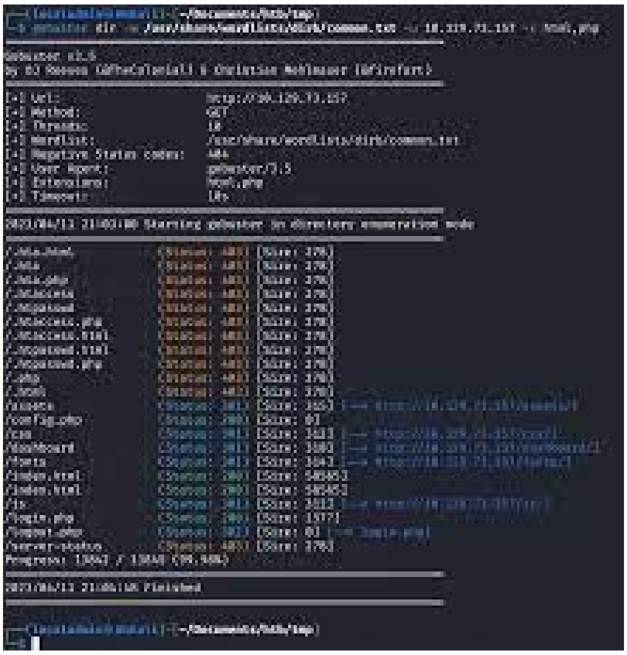
John the Ripper is a renowned password-cracking tool with a focus on Unix-based systems. It supports various password hash algorithms and can perform dictionary attacks and brute-force attacks on password hashes. This tool is indispensable for testing the strength of user passwords and enhancing overall security.



```
root@kali:~# john -format=LM /root/Desktop/hash.txt
Using default input encoding: UTF-8
Using default target encoding: CP850
Loaded 4 password hashes with no different salts (LM [DES 128/128 AVX-16])
Remaining 3 password hashes with no different salts
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:01:21 0.03% 3/3 (ETA: 2017-05-16 00:22) 0g/s 29892Kp/s 29892Kc/s 90718KC
/s 085MSYP..085MSNY
0g 0:00:01:22 0.03% 3/3 (ETA: 2017-05-16 00:14) 0g/s 29957Kp/s 29957Kc/s 90903KC
/s FCUCDB7..FCUCDGT
0g 0:00:01:25 0.03% 3/3 (ETA: 2017-05-16 00:00) 0g/s 30073Kp/s 30073Kc/s 91218KC
/s NEWSAHC..NEWSB9B
0g 0:00:01:26 0.03% 3/3 (ETA: 2017-05-15 23:54) 0g/s 30114Kp/s 30114Kc/s 91330KC
/s VELH10..VELHLS
0g 0:00:01:27 0.04% 3/3 (ETA: 2017-05-15 23:50) 0g/s 30148Kp/s 30148Kc/s 91423KC
/s 4A93GP..4A902K
0g 0:00:01:28 0.04% 3/3 (ETA: 2017-05-15 23:44) 0g/s 30201Kp/s 30201Kc/s 91572KC
/s 08TS4DA..08TSFOA
0g 0:00:01:29 0.04% 3/3 (ETA: 2017-05-15 23:37) 0g/s 30254Kp/s 30254Kc/s 91720KC
/s IKPABAO..IKPABR6
0g 0:00:01:30 0.04% 3/3 (ETA: 2017-05-15 23:33) 0g/s 30283Kp/s 30283Kc/s 91799KC
/s 0JODGB..0JOD5C
0g 0:00:01:33 0.04% 3/3 (ETA: 2017-05-15 23:19) 0g/s 30401Kp/s 30401Kc/s 92124KC
/s H10GW8W..H106CL1
```

8. Gobuster:

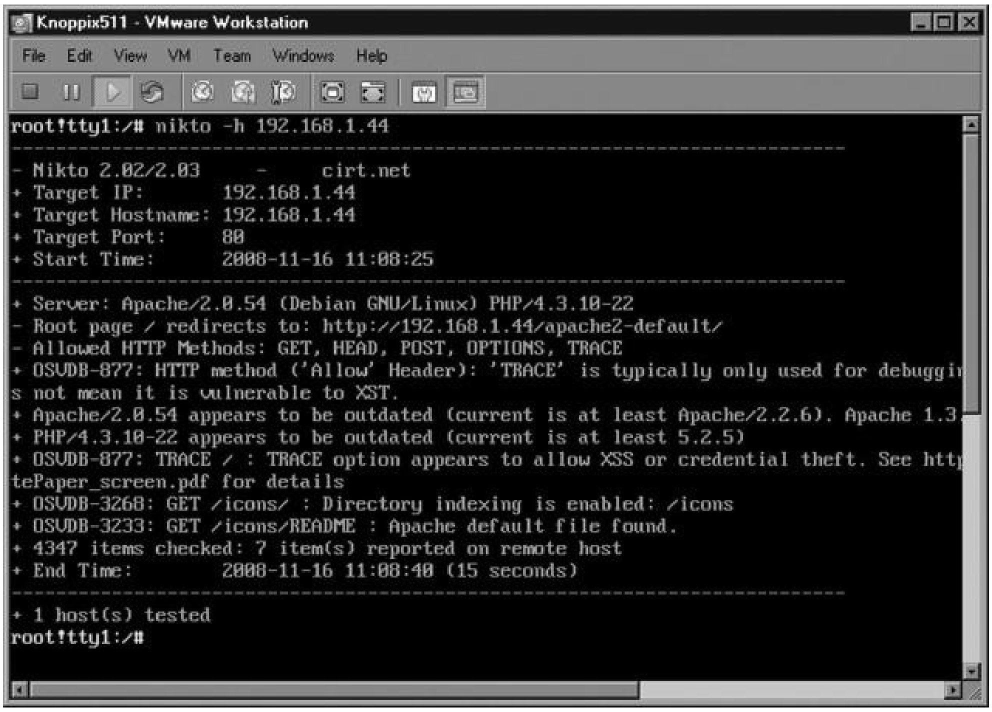
Gobuster is a directory and file brute-forcing tool designed for web application testing. Security professionals leverage it to discover hidden files and directories on web servers by systematically trying different paths and filenames. Gobuster aids in uncovering potential information leaks and security weaknesses.



```
┌──([illegible])-[~/Documents/htb/tmp]
└─$ gobuster dir -w /usr/share/wordlists/dirb/common.txt -u 10.129.73.157 -x html,php
===============================================================
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.129.73.157
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.5
[+] Extensions:              html,php
[+] Timeout:                 10s
===============================================================
2023/04/11 21:03:00 Starting gobuster in directory enumeration mode
===============================================================
/.hta.html            (Status: 403) [Size: 278]
/.hta                 (Status: 403) [Size: 278]
/.hta.php             (Status: 403) [Size: 278]
/.htaccess            (Status: 403) [Size: 278]
/.htpasswd            (Status: 403) [Size: 278]
/.htaccess.php        (Status: 403) [Size: 278]
/.htaccess.html       (Status: 403) [Size: 278]
/.htpasswd.html       (Status: 403) [Size: 278]
/.htpasswd.php        (Status: 403) [Size: 278]
/.php                 (Status: 403) [Size: 278]
/.html                (Status: 403) [Size: 278]
/assets               (Status: 301) [Size: 315] [--> http://10.129.73.157/assets/]
/config.php           (Status: 200) [Size: 0]
/css                  (Status: 301) [Size: 312] [--> http://10.129.73.157/css/]
/dashboard            (Status: 301) [Size: 318] [--> http://10.129.73.157/dashboard/]
/fonts                (Status: 301) [Size: 314] [--> http://10.129.73.157/fonts/]
/index.html           (Status: 200) [Size: 58565]
/index.html           (Status: 200) [Size: 58565]
/js                   (Status: 301) [Size: 311] [--> http://10.129.73.157/js/]
/login.php            (Status: 200) [Size: 1577]
/logout.php           (Status: 302) [Size: 0] [--> login.php]
/server-status        (Status: 403) [Size: 278]
Progress: 13842 / 13845 (99.98%)
===============================================================
2023/04/11 21:05:10 Finished
===============================================================

┌──([illegible])-[~/Documents/htb/tmp]
└─$
```

9. Nikto:

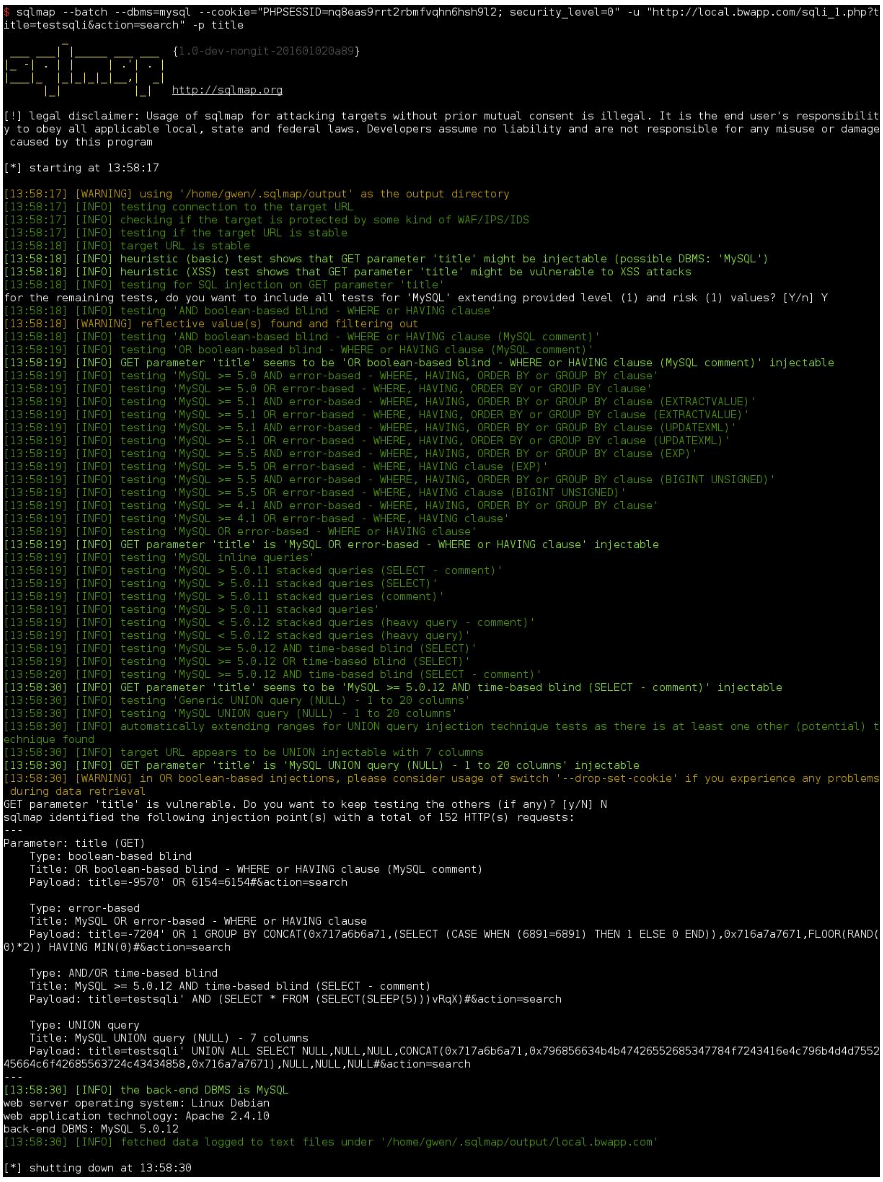
Nikto is a web server vulnerability scanner that specializes in identifying security issues in web applications and servers. It scans for known vulnerabilities, misconfigurations, and common security flaws, providing security teams with valuable insights into potential risks. Nikto is an essential tool for maintaining robust web application security.



```
root!tty1:/# nikto -h 192.168.1.44
---------------------------------------------------------------------------
- Nikto 2.02/2.03     -     cirt.net
+ Target IP:       192.168.1.44
+ Target Hostname: 192.168.1.44
+ Target Port:     80
+ Start Time:      2008-11-16 11:08:25
---------------------------------------------------------------------------
+ Server: Apache/2.0.54 (Debian GNU/Linux) PHP/4.3.10-22
- Root page / redirects to: http://192.168.1.44/apache2-default/
- Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ OSVDB-877: HTTP method ('Allow' Header): 'TRACE' is typically only used for debuggi
s not mean it is vulnerable to XST.
+ Apache/2.0.54 appears to be outdated (current is at least Apache/2.2.6). Apache 1.3
+ PHP/4.3.10-22 appears to be outdated (current is at least 5.2.5)
+ OSVDB-877: TRACE / : TRACE option appears to allow XSS or credential theft. See htt
tePaper_screen.pdf for details
+ OSVDB-3268: GET /icons/ : Directory indexing is enabled: /icons
+ OSVDB-3233: GET /icons/README : Apache default file found.
+ 4347 items checked: 7 item(s) reported on remote host
+ End Time:        2008-11-16 11:08:40 (15 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
root!tty1:/#
```

10. SQLMap:

SQLMap is an automated SQL injection testing tool used to detect and exploit SQL injection vulnerabilities in web applications. Security professionals rely on SQLMap to automate the identification of SQL injection flaws, enabling them to assess database security comprehensively. It aids in finding and addressing critical vulnerabilities that could compromise data integrity and confidentiality.



```
$ sqlmap --batch --dbms=mysql --cookie="PHPSESSID=nq8eas9rrt2rbmfvqhn6hsh9l2; security_level=0" -u "http://local.bwapp.com/sqli_1.php?t
itle=testsqli&action=search" -p title
         _
 ___ ___| |_____ ___ ___  {1.0-dev-nongit-201601020a89}
|_ -| . | |     | .'| . |
|___|_  |_|_|_|_|__,|  _|
      |_|           |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibilit
y 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 at 13:58:17

[13:58:17] [WARNING] using '/home/gwen/.sqlmap/output' as the output directory
[13:58:17] [INFO] testing connection to the target URL
[13:58:17] [INFO] checking if the target is protected by some kind of WAF/IPS/IDS
[13:58:17] [INFO] testing if the target URL is stable
[13:58:18] [INFO] target URL is stable
[13:58:18] [INFO] heuristic (basic) test shows that GET parameter 'title' might be injectable (possible DBMS: 'MySQL')
[13:58:18] [INFO] heuristic (XSS) test shows that GET parameter 'title' might be vulnerable to XSS attacks
[13:58:18] [INFO] testing for SQL injection on GET parameter 'title'
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] Y
[13:58:18] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[13:58:18] [WARNING] reflective value(s) found and filtering out
[13:58:18] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[13:58:19] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[13:58:19] [INFO] GET parameter 'title' seems to be 'OR boolean-based blind - WHERE or HAVING clause (MySQL comment)' injectable
[13:58:19] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause'
[13:58:19] [INFO] testing 'MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause'
[13:58:19] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[13:58:19] [INFO] testing 'MySQL >= 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[13:58:19] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (UPDATEXML)'
[13:58:19] [INFO] testing 'MySQL >= 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (UPDATEXML)'
[13:58:19] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[13:58:19] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE, HAVING clause (EXP)'
[13:58:19] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[13:58:19] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE, HAVING clause (BIGINT UNSIGNED)'
[13:58:19] [INFO] testing 'MySQL >= 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause'
[13:58:19] [INFO] testing 'MySQL >= 4.1 OR error-based - WHERE, HAVING clause'
[13:58:19] [INFO] testing 'MySQL OR error-based - WHERE or HAVING clause'
[13:58:19] [INFO] GET parameter 'title' is 'MySQL OR error-based - WHERE or HAVING clause' injectable
[13:58:19] [INFO] testing 'MySQL inline queries'
[13:58:19] [INFO] testing 'MySQL > 5.0.11 stacked queries (SELECT - comment)'
[13:58:19] [INFO] testing 'MySQL > 5.0.11 stacked queries (SELECT)'
[13:58:19] [INFO] testing 'MySQL > 5.0.11 stacked queries (comment)'
[13:58:19] [INFO] testing 'MySQL > 5.0.11 stacked queries'
[13:58:19] [INFO] testing 'MySQL < 5.0.12 stacked queries (heavy query - comment)'
[13:58:19] [INFO] testing 'MySQL < 5.0.12 stacked queries (heavy query)'
[13:58:19] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (SELECT)'
[13:58:19] [INFO] testing 'MySQL >= 5.0.12 OR time-based blind (SELECT)'
[13:58:20] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (SELECT - comment)'
[13:58:30] [INFO] GET parameter 'title' seems to be 'MySQL >= 5.0.12 AND time-based blind (SELECT - comment)' injectable
[13:58:30] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[13:58:30] [INFO] testing 'MySQL UNION query (NULL) - 1 to 20 columns'
[13:58:30] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) t
echnique found
[13:58:30] [INFO] target URL appears to be UNION injectable with 7 columns
[13:58:30] [INFO] GET parameter 'title' is 'MySQL UNION query (NULL) - 1 to 20 columns' injectable
[13:58:30] [WARNING] in OR boolean-based injections, please consider usage of switch '--drop-set-cookie' if you experience any problems
 during data retrieval
GET parameter 'title' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 152 HTTP(s) requests:
---
Parameter: title (GET)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment)
    Payload: title=-9570' OR 6154=6154#&action=search

    Type: error-based
    Title: MySQL OR error-based - WHERE or HAVING clause
    Payload: title=-7204' OR 1 GROUP BY CONCAT(0x717a6b6a71,(SELECT (CASE WHEN (6891=6891) THEN 1 ELSE 0 END)),0x716a7a7671,FLOOR(RAND(
0)*2)) HAVING MIN(0)#&action=search

    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (SELECT - comment)
    Payload: title=testsqli' AND (SELECT * FROM (SELECT(SLEEP(5)))vRqX)#&action=search

    Type: UNION query
    Title: MySQL UNION query (NULL) - 7 columns
    Payload: title=testsqli' UNION ALL SELECT NULL,NULL,NULL,CONCAT(0x717a6b6a71,0x796856634b4b47426552685347784f7243416e4c796b4d4d7552
45664c6f42685563724c43434858,0x716a7a7671),NULL,NULL,NULL#&action=search
---
[13:58:30] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian
web application technology: Apache 2.4.10
back-end DBMS: MySQL 5.0.12
[13:58:30] [INFO] fetched data logged to text files under '/home/gwen/.sqlmap/output/local.bwapp.com'

[*] shutting down at 13:58:30
```

These ten Kali Linux tools are vital components of a security professional's toolkit, enabling them to conduct thorough security assessments, identify vulnerabilities, and enhance the overall security posture of systems and networks. Always remember to use these tools responsibly, with proper authorization and in compliance with ethical hacking guidelines and laws.