SRI SHAKTHI INSTITUTE OF ENGINEERING AND TECHNOLOGY

COIMBATORE - 641062

POWERING THE YOUTH
EMPOWERING THE NATION

21CY512 - Vulnerability Assessment and Penetration Testing Laboratory

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

(CYBER SECURITY)

SRI SHAKTHI INSTITUTE OF ENGINEERING AND TECHNOLOGY

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

(CYBER SECURITY)

21CY512 – Vulnerability Assessment and Penetration Testing Laboratory

NAME: _____ **ROLL NO:** _____

CLASS: _____ **BRANCH:** _____

ACADEMIC YEAR: 2025 - 2026 **BATCH:** 2023 - 2027 **SEMESTER:** V

Certified and bonafide record of work done by ……...…….……

Place: Coimbatore

Date:

Staff In-Charge **Head of the Department**

University Register Number: ……...

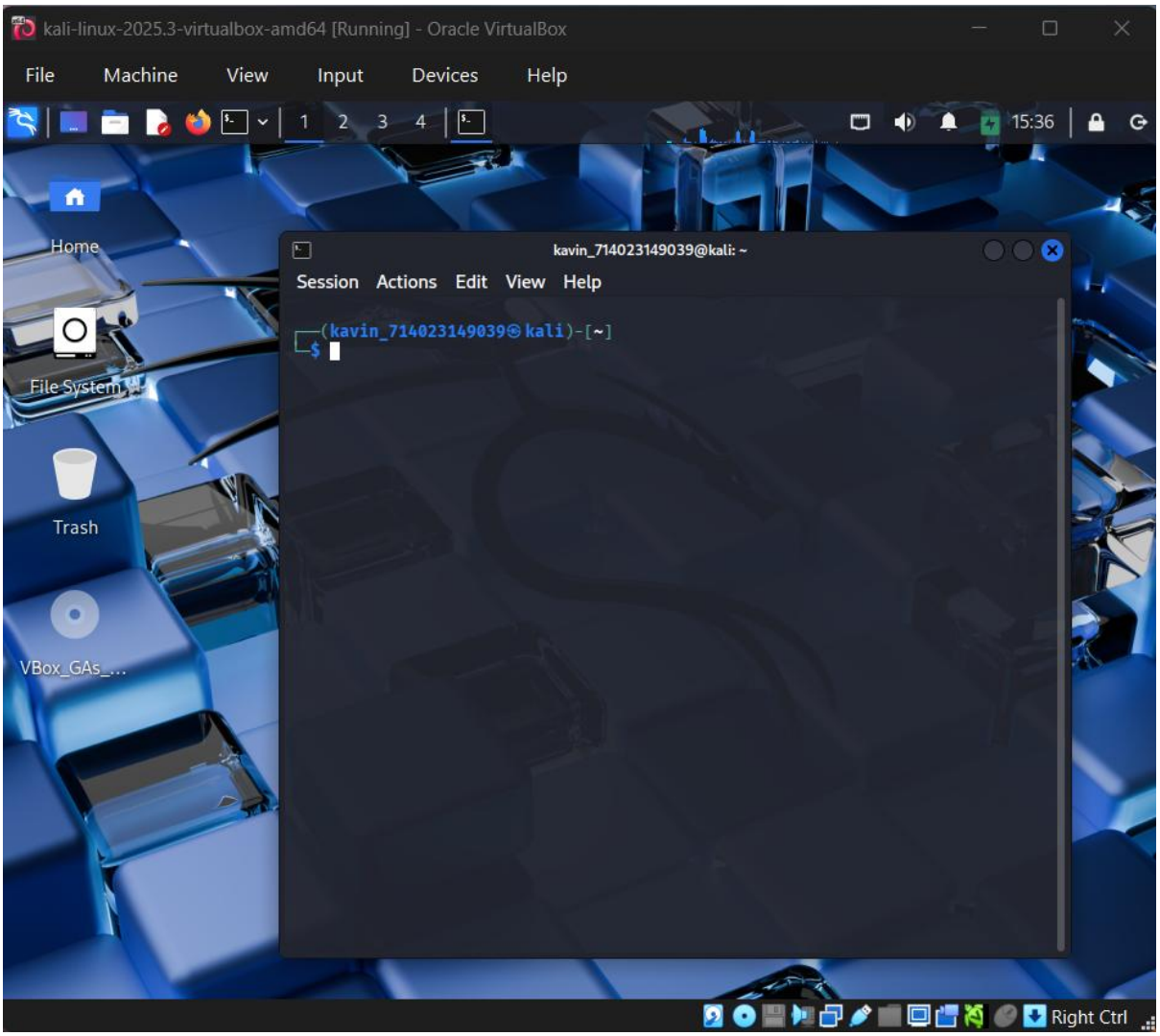
Submitted for the University Practical Examination held on ……..……

INTERNAL EXAMINER **EXTERNAL EXAMINER**

LIST OF EXPERIMENTS

S.NO	DATE	TITLE OF EXPERIMENT	MARK	SIGN
1	27.06.25	Installation of Kali Linux		
2	04.07.25	DNS Enumeration		
3	11.07.25	Open Port Scanning		
4	18.07.25	Password Guessing Tool to guess a Password		
5	25.07.25	Extract Password Hashes from Windows Machine		
6	01.08.25	Cracking Linux Passwords		
7	08.08.25	Experiments on SQL Injection – DVWA SQL Injections		
8	25.08.25	Packet Capturing and Analysis using Wireshark		
9	05.09.25	HTTP Eavesdropping using Wireshark		
10	12.09.25	Simulating Phishing Attack Scenario using SET		
11	23.09.25	Basic Vulnerability Scanning using NIKTO		
12	30.09.25	Cracking Password Hashes using John the Ripper		
13	07.10.25	Enumeration of Devices in a Local Network using ARP-SCAN		
14	14.10.25	Metasploit Framework		
15	24.1025	High Level and Low Level Penetration Test Reports		

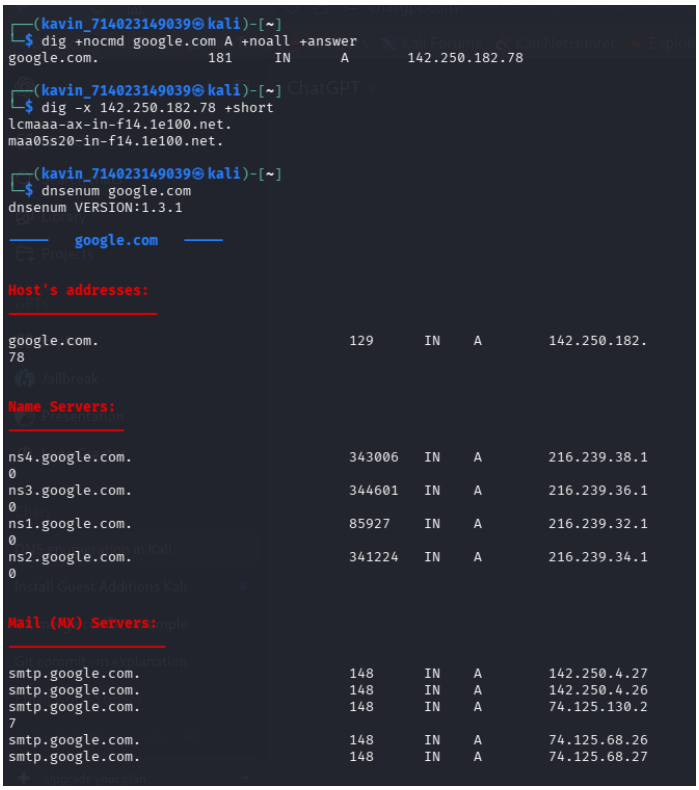
Output 1


kali-linux-2025.3-virtualbox-amd64 [Running] - Oracle VirtualBox
File
Machine
View
Input
Devices
Help
1
2
3
4
15:36
Home
File System
Trash
VBox_GAs_...
kavin_714023149039@kali: ~
Session
Actions
Edit
View
Help
(kavin_714023149039㉿kali)-[~]
$
Right Ctrl

Output 2.1

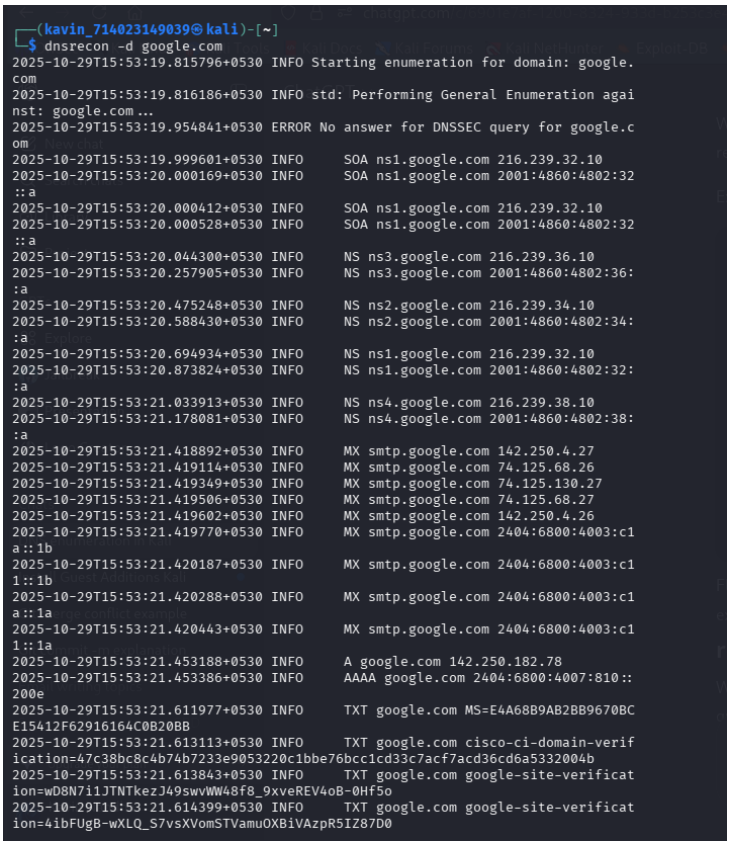
```
┌──(kavin_714023149039㉿kali)-[~]
└─$ nslookup
> server ns1.google.com
Default server: ns1.google.com
Address: 216.239.32.10#53
Default server: ns1.google.com
Address: 2001:4860:4802:32::a#53
> set type=any
> google.com
Server:         ns1.google.com
Address:        216.239.32.10#53

Name:   google.com
Address: 172.217.24.206
Name:   google.com
Address: 2404:6800:4007:83f::200e
google.com      text = "apple-domain-verification=30afIBcvSuDV2PLX"
google.com      nameserver = ns1.google.com.
google.com      text = "onetrust-domain-verification=de01ed21f2fa4d8781cbc3ff
b89cf4ef"
google.com      text = "MS=E4A68B9AB2BB9670BCE15412F62916164C0B20BB"
google.com
        origin = ns1.google.com
        mail addr = dns-admin.google.com
        serial = 824942276
        refresh = 900
        retry = 900
        expire = 1800
        minimum = 60
google.com      text = "docusign=05958488-4752-4ef2-95eb-aa7ba8a3bd0e"
google.com      text = "google-site-verification=4ibFUgB-wXLQ_S7vsXVomSTVamuO
XBiVAzpR5IZ87D0"
google.com      nameserver = ns4.google.com.
google.com      text = "docusign=1b0a6754-49b1-4db5-8540-d2c12664b289"
google.com      text = "cisco-ci-domain-verification=47c38bc8c4b74b7233e90532
20c1bbe76bcc1cd33c7acf7acd36cd6a5332004b"
google.com      text = "globalsign-smime-dv=CDYX+XFHUw2wml6/Gb8+59BsH31KzUr6c
1l2BPvqKX8="
google.com      text = "google-site-verification=wD8N7i1JTNTkezJ49swvWW48f8_9
xveREV4oB-0Hf5o"
google.com      rdata_65 = 1 . alpn="h2,h3"
google.com      nameserver = ns2.google.com.
google.com      rdata_257 = 0 issue "pki.goog"
google.com      text = "v=spf1 include:_spf.google.com ~all"
google.com      text = "facebook-domain-verification=22rm551cu4k0ab0bxsw536tl
ds4h95"
google.com      text = "google-site-verification=TV9-DBe4R80X4v0M4U_bd_J9cpOJ
M0nikft0jAgjmsQ"
google.com      nameserver = ns3.google.com.
google.com      mail exchanger = 10 smtp.google.com.
```

Output 2.2



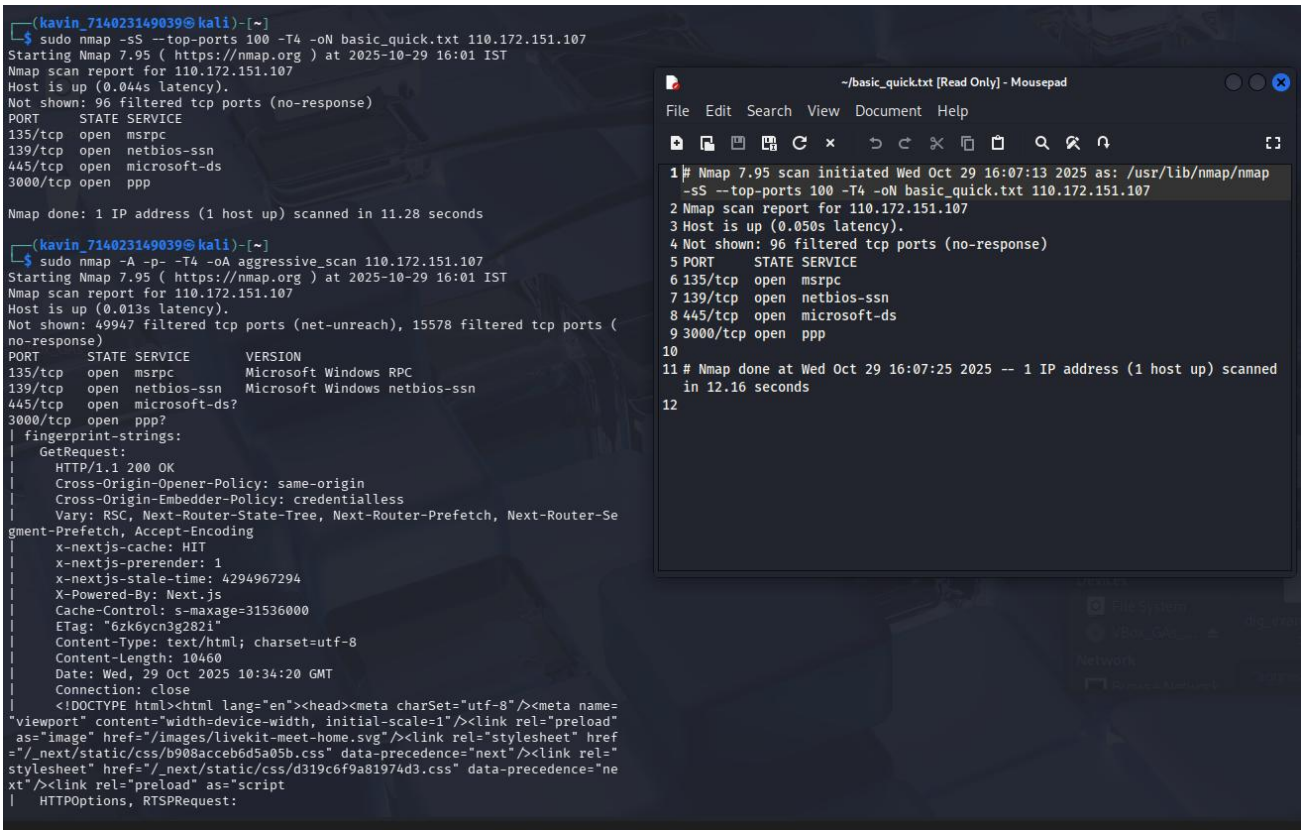
```
┌──(kavin_714023149039㉿kali)-[~]
└─$ dig +nocmd google.com A +noall +answer
google.com.             181     IN      A       142.250.182.78

┌──(kavin_714023149039㉿kali)-[~]
└─$ dig -x 142.250.182.78 +short
lcmaaa-ax-in-f14.1e100.net.
maa05s20-in-f14.1e100.net.

┌──(kavin_714023149039㉿kali)-[~]
└─$ dnsenum google.com
dnsenum VERSION:1.3.1

-----   google.com   -----

Host's addresses:
__________________

google.com.                              129      IN    A        142.250.182.
78

Name Servers:
_____________

ns4.google.com.                          343006   IN    A        216.239.38.1
0
ns3.google.com.                          344601   IN    A        216.239.36.1
0
ns1.google.com.                          85927    IN    A        216.239.32.1
0
ns2.google.com.                          341224   IN    A        216.239.34.1
0

Mail (MX) Servers:
__________________

smtp.google.com.                         148      IN    A        142.250.4.27
smtp.google.com.                         148      IN    A        142.250.4.26
smtp.google.com.                         148      IN    A        74.125.130.2
7
smtp.google.com.                         148      IN    A        74.125.68.26
smtp.google.com.                         148      IN    A        74.125.68.27
```

Output 2.3

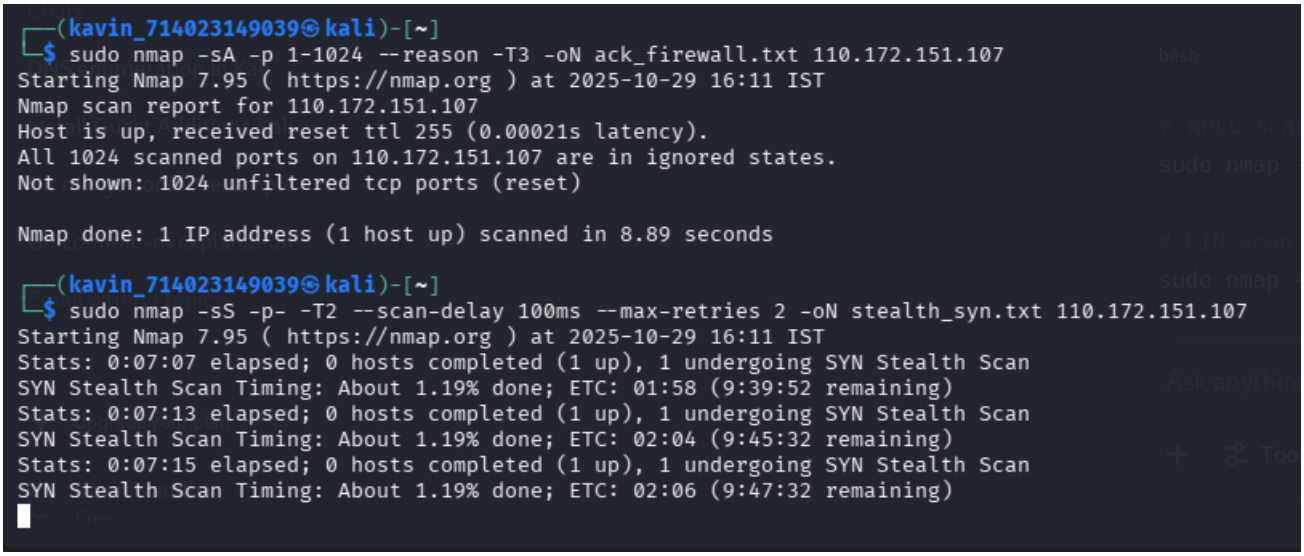


```
┌──(kavin_714023149039㉿kali)-[~]
└─$ dnsrecon -d google.com
2025-10-29T15:53:19.815796+0530 INFO Starting enumeration for domain: google.
com
2025-10-29T15:53:19.816186+0530 INFO std: Performing General Enumeration agai
nst: google.com...
2025-10-29T15:53:19.954841+0530 ERROR No answer for DNSSEC query for google.c
om
2025-10-29T15:53:19.999601+0530 INFO     SOA ns1.google.com 216.239.32.10
2025-10-29T15:53:20.000169+0530 INFO     SOA ns1.google.com 2001:4860:4802:32
::a
2025-10-29T15:53:20.000412+0530 INFO     SOA ns1.google.com 216.239.32.10
2025-10-29T15:53:20.000528+0530 INFO     SOA ns1.google.com 2001:4860:4802:32
::a
2025-10-29T15:53:20.044300+0530 INFO     NS ns3.google.com 216.239.36.10
2025-10-29T15:53:20.257905+0530 INFO     NS ns3.google.com 2001:4860:4802:36:
:a
2025-10-29T15:53:20.475248+0530 INFO     NS ns2.google.com 216.239.34.10
2025-10-29T15:53:20.588430+0530 INFO     NS ns2.google.com 2001:4860:4802:34:
:a
2025-10-29T15:53:20.694934+0530 INFO     NS ns1.google.com 216.239.32.10
2025-10-29T15:53:20.873824+0530 INFO     NS ns1.google.com 2001:4860:4802:32:
:a
2025-10-29T15:53:21.033913+0530 INFO     NS ns4.google.com 216.239.38.10
2025-10-29T15:53:21.178081+0530 INFO     NS ns4.google.com 2001:4860:4802:38:
:a
2025-10-29T15:53:21.418892+0530 INFO     MX smtp.google.com 142.250.4.27
2025-10-29T15:53:21.419114+0530 INFO     MX smtp.google.com 74.125.68.26
2025-10-29T15:53:21.419349+0530 INFO     MX smtp.google.com 74.125.130.27
2025-10-29T15:53:21.419506+0530 INFO     MX smtp.google.com 74.125.68.27
2025-10-29T15:53:21.419602+0530 INFO     MX smtp.google.com 142.250.4.26
2025-10-29T15:53:21.419770+0530 INFO     MX smtp.google.com 2404:6800:4003:c1
a::1b
2025-10-29T15:53:21.420187+0530 INFO     MX smtp.google.com 2404:6800:4003:c1
1::1b
2025-10-29T15:53:21.420288+0530 INFO     MX smtp.google.com 2404:6800:4003:c1
a::1a
2025-10-29T15:53:21.420443+0530 INFO     MX smtp.google.com 2404:6800:4003:c1
1::1a
2025-10-29T15:53:21.453188+0530 INFO     A google.com 142.250.182.78
2025-10-29T15:53:21.453386+0530 INFO     AAAA google.com 2404:6800:4007:810::
200e
2025-10-29T15:53:21.611977+0530 INFO     TXT google.com MS=E4A68B9AB2BB9670BC
E15412F62916164C0B20BB
2025-10-29T15:53:21.613113+0530 INFO     TXT google.com cisco-ci-domain-verif
ication=47c38bc8c4b74b7233e9053220c1bbe76bcc1cd33c7acf7acd36cd6a5332004b
2025-10-29T15:53:21.613843+0530 INFO     TXT google.com google-site-verificat
ion=wD8N7i1JTNTkezJ49swvWW48f8_9xveREV4oB-0Hf5o
2025-10-29T15:53:21.614399+0530 INFO     TXT google.com google-site-verificat
ion=4ibFUgB-wXLQ_S7vsXVomSTVamuOXBiVAzpR5IZ87D0
```

Output 3.1



Output 3.2



Output 4

```
┌──(kavin_714023149039㉿kali)-[/var/www/html/dvwa/config]
└─$ hydra -l admin -P /usr/share/wordlists/rockyou.txt localhost http-post-fo
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
cs anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-30 09:
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1
[DATA] attacking http-post-form://localhost:80/dvwa/login.php:username=^USER^
[80][http-post-form] host: localhost   login: admin   password: 123456
[80][http-post-form] host: localhost   login: admin   password: 12345
[80][http-post-form] host: localhost   login: admin   password: 1234567
[80][http-post-form] host: localhost   login: admin   password: password
[80][http-post-form] host: localhost   login: admin   password: nicole
[80][http-post-form] host: localhost   login: admin   password: 123456789
[80][http-post-form] host: localhost   login: admin   password: iloveyou
[80][http-post-form] host: localhost   login: admin   password: princess
[80][http-post-form] host: localhost   login: admin   password: rockyou
[80][http-post-form] host: localhost   login: admin   password: 12345678
[80][http-post-form] host: localhost   login: admin   password: babygirl
[80][http-post-form] host: localhost   login: admin   password: monkey
[80][http-post-form] host: localhost   login: admin   password: daniel
[80][http-post-form] host: localhost   login: admin   password: abc123
[80][http-post-form] host: localhost   login: admin   password: jessica
[80][http-post-form] host: localhost   login: admin   password: lovely
1 of 1 target successfully completed, 16 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-10-30 09:
```

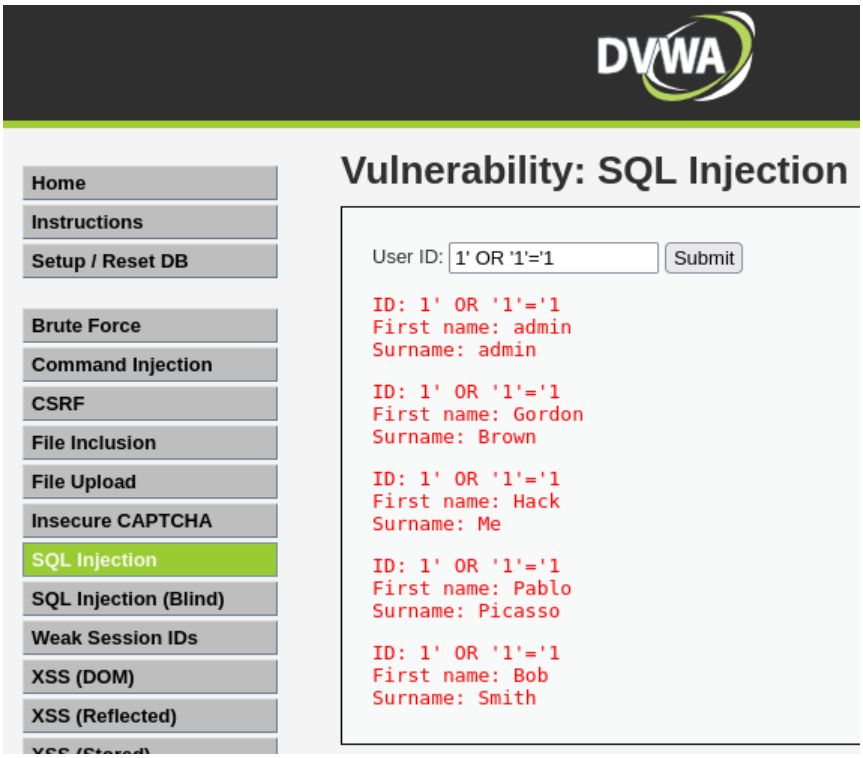
Output 5

```
┌──(kavin_714023149039㉿kali)-[~/Desktop]
└─$ samdump2 system sam
*disabled* Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae93
1b73c59d7e0c089c0:::
*disabled* Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d
7e0c089c0:::
*disabled* :503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c0
89c0:::
*disabled* :504:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c0
89c0:::
kavin:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:
::
*disabled* :1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c
089c0:::
```

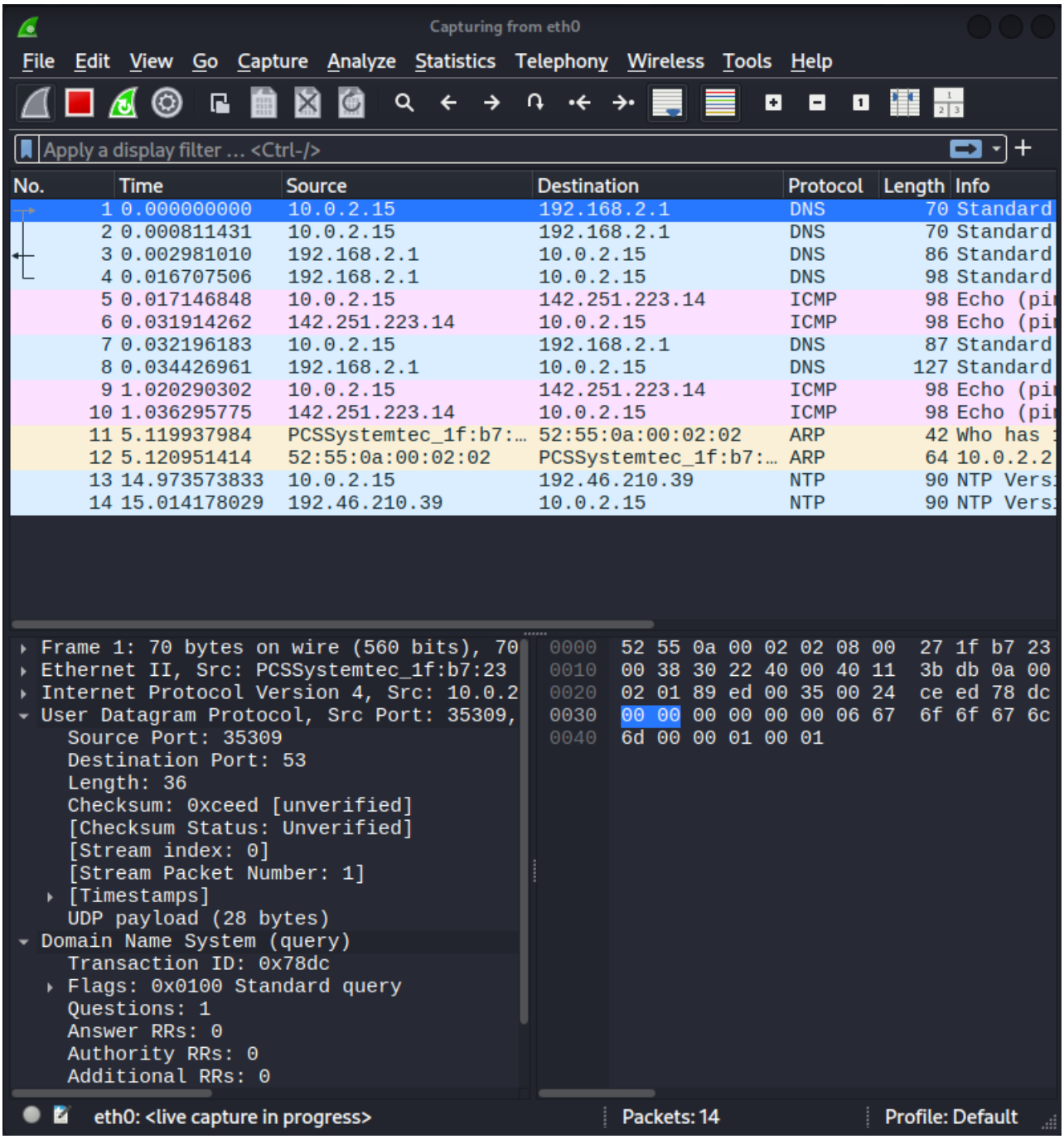
Output 6

```
┌──(kavin_7140231490398㉿kali)-[~/kavin_lab]
└─$ mkdir -p ~/kavin_lab
cd ~/kavin_lab

sudo cp /etc/passwd ./passwd.copy
sudo cp /etc/shadow ./shadow.copy

sudo grep '^kavin2:' ./shadow.copy > ./kavin2_shadow
grep '^kavin2:' ./passwd.copy > ./kavin2_passwd

unshadow ./kavin2_passwd ./kavin2_shadow > kavin2_unshadow.txt

cat kavin2_unshadow.txt
kavin2:$y$j9T$Yv6qZi4ropR8z1P.D.l9N.$cKVmvVaeIt1GRulrGxEY3HjAp

┌──(kavin_7140231490398㉿kali)-[~/kavin_lab]
└─$ john --format=crypt --wordlist=/usr/share/wordlists/rockyo
Using default input encoding: UTF-8
Loaded 1 password hash (crypt, generic crypt(3) [?/64])
No password hashes left to crack (see FAQ)

┌──(kavin_7140231490398㉿kali)-[~/kavin_lab]
└─$ john --show kavin2_unshadown.txt
stat: kavin2_unshadown.txt: No such file or directory

┌──(kavin_7140231490398㉿kali)-[~/kavin_lab]
└─$ john --show kavin2_unshadow.txt
kavin2:kavin:1004:1004::/home/kavin2:/bin/sh

1 password hash cracked, 0 left
```

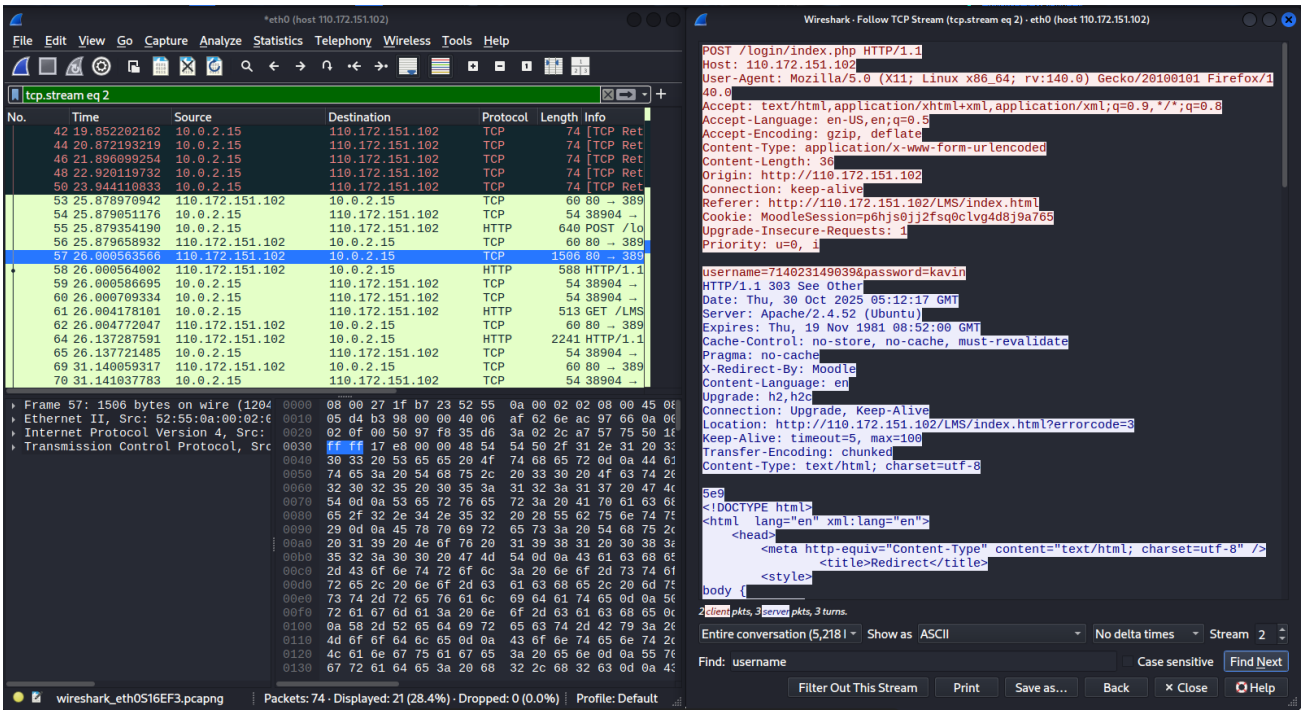
Output 7



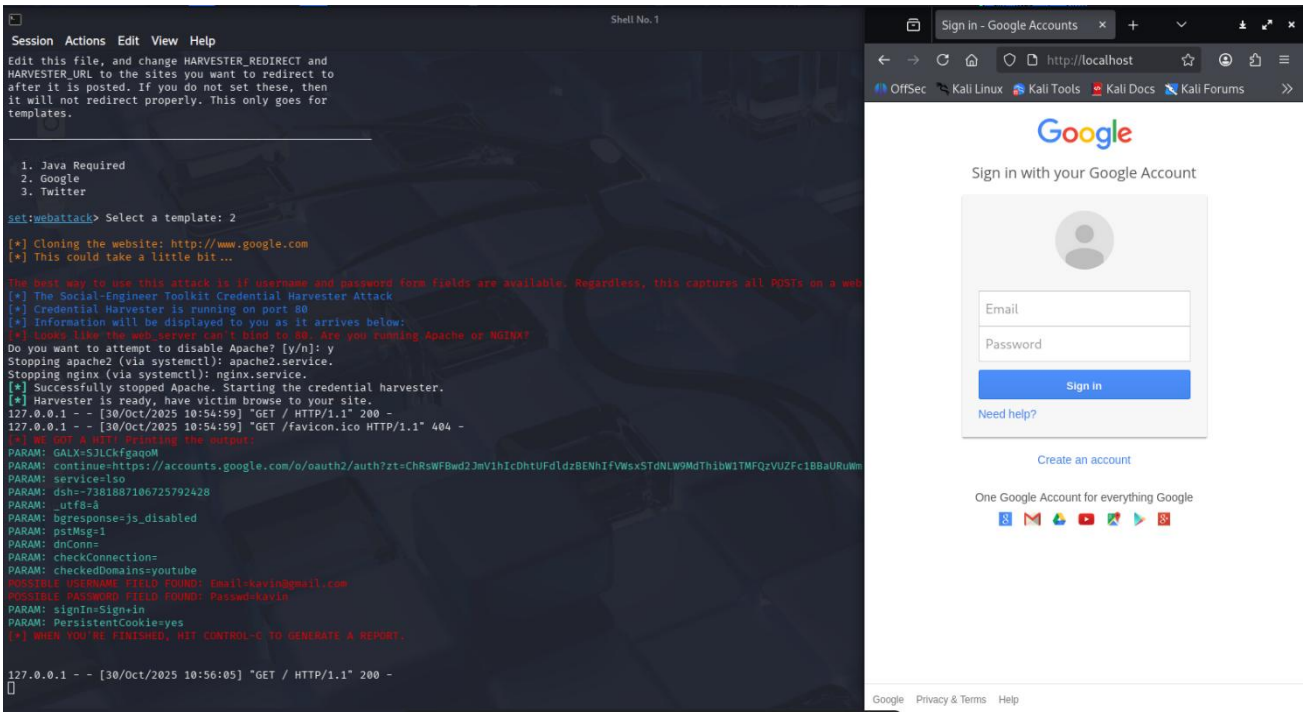
Output 8


Capturing from 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 10.0.2.15 192.168.2.1 DNS 70 Standard
2 0.000811431 10.0.2.15 192.168.2.1 DNS 70 Standard
3 0.002981010 192.168.2.1 10.0.2.15 DNS 86 Standard
4 0.016707506 192.168.2.1 10.0.2.15 DNS 98 Standard
5 0.017146848 10.0.2.15 142.251.223.14 ICMP 98 Echo (pi
6 0.031914262 142.251.223.14 10.0.2.15 ICMP 98 Echo (pi
7 0.032196183 10.0.2.15 192.168.2.1 DNS 87 Standard
8 0.034426961 192.168.2.1 10.0.2.15 DNS 127 Standard
9 1.020290302 10.0.2.15 142.251.223.14 ICMP 98 Echo (pi
10 1.036295775 142.251.223.14 10.0.2.15 ICMP 98 Echo (pi
11 5.119937984 PCSSystemtec_1f:b7:... 52:55:0a:00:02:02 ARP 42 Who has
12 5.120951414 52:55:0a:00:02:02 PCSSystemtec_1f:b7:... ARP 64 10.0.2.2
13 14.973573833 10.0.2.15 192.46.210.39 NTP 90 NTP Vers
14 15.014178029 192.46.210.39 10.0.2.15 NTP 90 NTP Vers
Frame 1: 70 bytes on wire (560 bits), 70
Ethernet II, Src: PCSSystemtec_1f:b7:23
Internet Protocol Version 4, Src: 10.0.2
User Datagram Protocol, Src Port: 35309,
Source Port: 35309
Destination Port: 53
Length: 36
Checksum: 0xceed [unverified]
[Checksum Status: Unverified]
[Stream index: 0]
[Stream Packet Number: 1]
[Timestamps]
UDP payload (28 bytes)
Domain Name System (query)
Transaction ID: 0x78dc
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
0000 52 55 0a 00 02 02 08 00 27 1f b7 23
0010 00 38 30 22 40 00 40 11 3b db 0a 00
0020 02 01 89 ed 00 35 00 24 ce ed 78 dc
0030 00 00 00 00 00 00 06 67 6f 6f 67 6c
0040 6d 00 00 01 00 01
eth0: <live capture in progress>
Packets: 14
Profile: Default

Output 9



Output 10



Output 11

```
┌──(kavin_714023149039㉿kali)-[~]
└─$ nikto -h http://110.172.151.102 -p 80 -o nikto_report.txt -Format txt
- Nikto v2.5.0
---------------------------------------------------------------------------
- ERROR: The -port option cannot be used with a full URI

┌──(kavin_714023149039㉿kali)-[~]
└─$ nikto -h http://110.172.151.102 -o nikto_report.txt -Format txt
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          110.172.151.102
+ Target Hostname:    110.172.151.102
+ Target Port:        80
+ Start Time:         2025-10-30 11:01:44 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.52 (Ubuntu)
+ /: Cookie MoodleSession created without the httponly flag. See: https://d
+ /: The anti-clickjacking X-Frame-Options header is not present. See: http
+ /: Uncommon header 'x-redirect-by' found, with contents: Moodle.
+ /: The X-Content-Type-Options header is not set. This could allow the use
ulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Root page / redirects to: http://110.172.151.102/login/index.php
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: The web server may reveal its internal or real IP in the Location head
-0649
+ Apache/2.4.52 appears to be outdated (current is at least Apache/2.4.54).

+ /config.php: PHP Config file may contain database IDs and passwords.
+ /admin/: Uncommon header 'x-accel-buffering' found, with contents: no.
+ /auth/: This might be interesting.
+ /backup/: Directory indexing found.
+ /backup/: This might be interesting.
+ /data/: This might be interesting.
+ /install/: Directory indexing found.
+ /install/: This might be interesting.
+ /lib/: This might be interesting.
+ /pix/: Directory indexing found.
+ /pix/: This might be interesting.
+ /user/: Uncommon header 'content-style-type' found, with contents: text/c
+ /user/: Uncommon header 'content-script-type' found, with contents: text/
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ Scan terminated: 5 error(s) and 19 item(s) reported on remote host
+ End Time:           2025-10-30 11:14:47 (GMT5.5) (783 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Output 12

```
┌──(kavin_714023149039㉿kali)-[~]
└─$ mkdir -p ~/john_sha512_lab

┌──(kavin_714023149039㉿kali)-[~]
└─$ cd john_sha512_lab/

┌──(kavin_714023149039㉿kali)-[~/john_sha512_lab]
└─$ mkpasswd -m sha-512 kavin > hashes.shadow

┌──(kavin_714023149039㉿kali)-[~/john_sha512_lab]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt --format=sha512crypy hashes.shadow
Unknown ciphertext format name requested

┌──(kavin_714023149039㉿kali)-[~/john_sha512_lab]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt --format=sha512crypt hashes.shadow
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:02 0.09% (ETA: 11:51:41) 0g/s 7207p/s 7207c/s 7207C/s donny..soybella
0g 0:00:00:04 0.17% (ETA: 11:53:04) 0g/s 7223p/s 7223c/s 7223C/s shalala..sammy10
kavin            (?)
1g 0:00:00:28 DONE (2025-10-30 11:14) 0.03479g/s 6965p/s 6965c/s 6965C/s kensley..jnjnjn
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

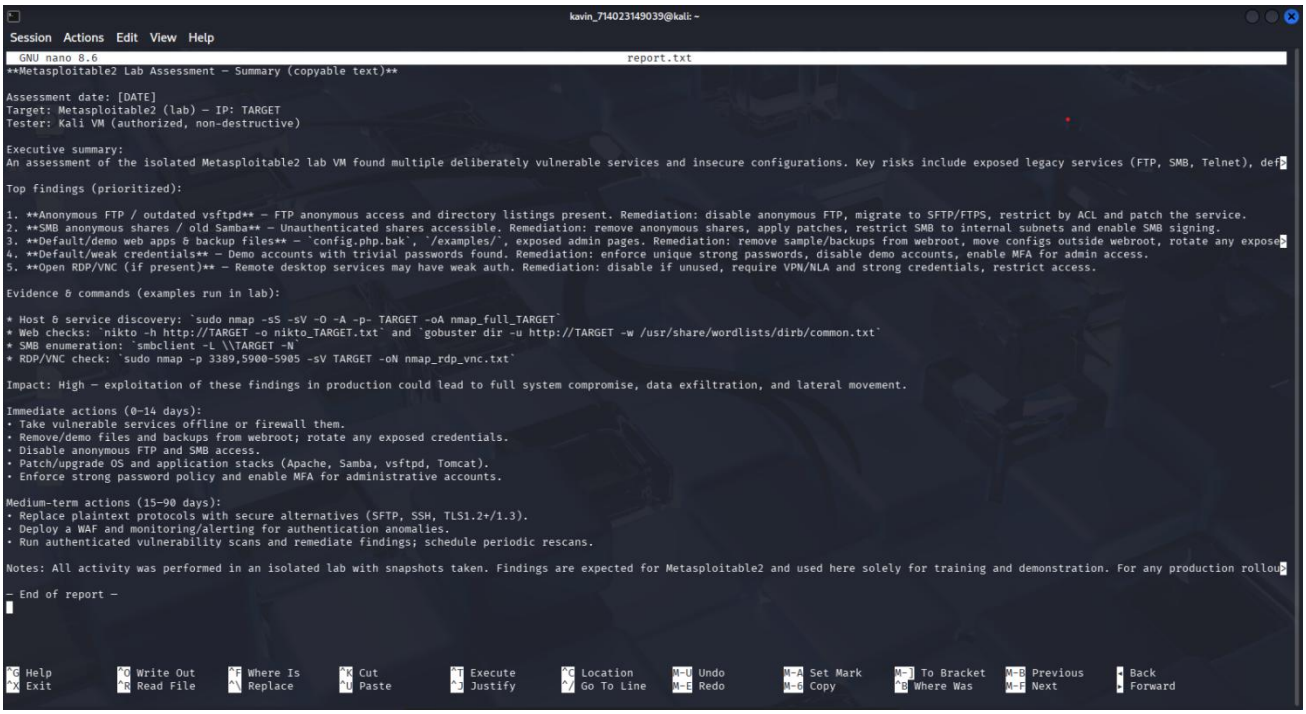
Output 13

```
┌──(kavin_714023149039㉿kali)-[~]
└─$ sudo arp-scan --localnet
Interface: eth0, type: EN10MB, MAC: 08:00:27:1f:b7:23, IPv4: 10.0.2.15
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
10.0.2.2        52:55:0a:00:02:02       (Unknown: locally administered)
10.0.2.3        52:55:0a:00:02:03       (Unknown: locally administered)

5 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.879 seconds (136.24 hosts/sec). 2 responded

┌──(kavin_714023149039㉿kali)-[~]
└─$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
10.0.2.2                 ether   52:55:0a:00:02:02   C                     eth0

┌──(kavin_714023149039㉿kali)-[~]
└─$ ip neigh show
10.0.2.2 dev eth0 lladdr 52:55:0a:00:02:02 REACHABLE
fd17:625c:f037:2::2 dev eth0 lladdr 52:56:00:00:00:02 router STALE
fe80::2 dev eth0 lladdr 52:56:00:00:00:02 router STALE
```

Output 14

```
┌──(kavin_714023149039㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Use sessions -1 to interact with the last opened session

 ______________________________________
/ it looks like you're trying to run a \
\ module                               /
 --------------------------------------
 \
  \
     __
    /  \
    |  |
    @  @
    |  |
    || |/
    || ||
    |\_/|
    \___/

       =[ metasploit v6.4.95-dev                          ]
+ -- --=[ 2,566 exploits - 1,315 auxiliary - 1,683 payloads     ]
+ -- --=[ 433 post - 49 encoders - 13 nops - 9 evasion          ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > use auxiliary/scanner/smb/smb_version
msf auxiliary(scanner/smb/smb_version) > set RHOSTS 110.172.151.107
RHOSTS ⇒ 110.172.151.107
msf auxiliary(scanner/smb/smb_version) > run
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.23/lib/rec
expression
[*] 110.172.151.107:445   - SMB Detected (versions:2, 3) (preferred dialect:SMB 3.
d:{bc4cd756-20fa-46eb-a151-3b84ec0505ff}) (authentication domain:TECHPARK2)
[+] 110.172.151.107:445   -   Host is running Version 10.0.26100 (likely Windows 1
[*] 110.172.151.107       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/smb/smb_version) > use auxiliary/scanner/http/http_version
msf auxiliary(scanner/http/http_version) > set RHOSTS 110.172.151.107
RHOSTS ⇒ 110.172.151.107
msf auxiliary(scanner/http/http_version) > run
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Output 15


kavin_714023149039@kali: ~
Session Actions Edit View Help
GNU nano 8.6 report.txt
Metasploitable2 Lab Assessment — Summary (copyable text)
Assessment date: [DATE]
Target: Metasploitable2 (lab) — IP: TARGET
Tester: Kali VM (authorized, non-destructive)
Executive summary:
An assessment of the isolated Metasploitable2 lab VM found multiple deliberately vulnerable services and insecure configurations. Key risks include exposed legacy services (FTP, SMB, Telnet), def
Top findings (prioritized):
1. **Anonymous FTP / outdated vsftpd** — FTP anonymous access and directory listings present. Remediation: disable anonymous FTP, migrate to SFTP/FTPS, restrict by ACL and patch the service.
2. **SMB anonymous shares / old Samba** — Unauthenticated shares accessible. Remediation: remove anonymous shares, apply patches, restrict SMB to internal subnets and enable SMB signing.
3. **Default/demo web apps & backup files** — `config.php.bak`, `/examples/`, exposed admin pages. Remediation: remove sample/backups from webroot, move configs outside webroot, rotate any expose
4. **Default/weak credentials** — Demo accounts with trivial passwords found. Remediation: enforce unique strong passwords, disable demo accounts, enable MFA for admin access.
5. **Open RDP/VNC (if present)** — Remote desktop services may have weak auth. Remediation: disable if unused, require VPN/NLA and strong credentials, restrict access.
Evidence & commands (examples run in lab):
* Host & service discovery: `sudo nmap -sS -sV -O -A -p- TARGET -oA nmap_full_TARGET`
* Web checks: `nikto -h http://TARGET -o nikto_TARGET.txt` and `gobuster dir -u http://TARGET -w /usr/share/wordlists/dirb/common.txt`
* SMB enumeration: `smbclient -L \\TARGET -N`
* RDP/VNC check: `sudo nmap -p 3389,5900-5905 -sV TARGET -oN nmap_rdp_vnc.txt`
Impact: High — exploitation of these findings in production could lead to full system compromise, data exfiltration, and lateral movement.
Immediate actions (0–14 days):
• Take vulnerable services offline or firewall them.
• Remove/demo files and backups from webroot; rotate any exposed credentials.
• Disable anonymous FTP and SMB access.
• Patch/upgrade OS and application stacks (Apache, Samba, vsftpd, Tomcat).
• Enforce strong password policy and enable MFA for administrative accounts.
Medium-term actions (15–90 days):
• Replace plaintext protocols with secure alternatives (SFTP, SSH, TLS1.2+/1.3).
• Deploy a WAF and monitoring/alerting for authentication anomalies.
• Run authenticated vulnerability scans and remediate findings; schedule periodic rescans.
Notes: All activity was performed in an isolated lab with snapshots taken. Findings are expected for Metasploitable2 and used here solely for training and demonstration. For any production rollou
— End of report —
^G Help ^O Write Out ^F Where Is ^K Cut ^T Execute ^C Location M-U Undo M-A Set Mark M-] To Bracket M-B Previous ^B Back
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo M-6 Copy ^Q Where Was M-F Next ^F Forward