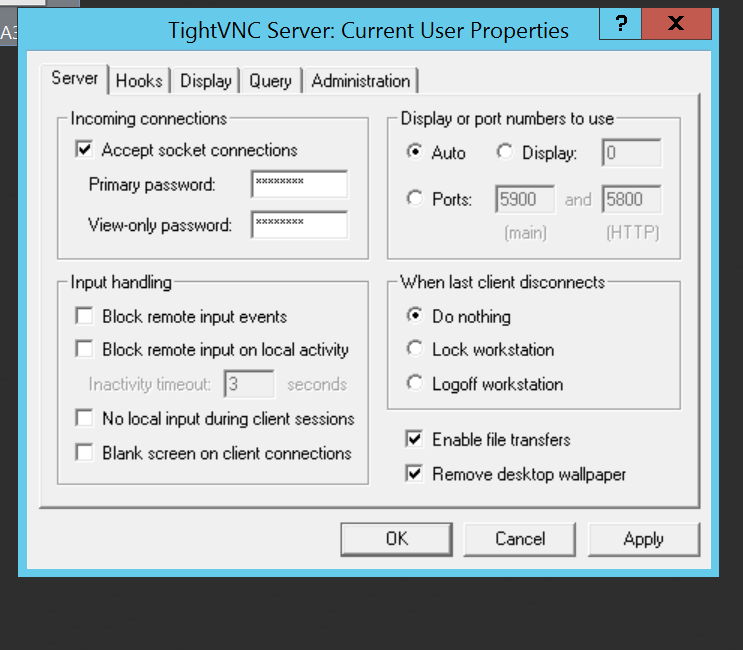
Øving 15 : Etisk hacking Exploiting

Setter opp TightVNC serveren setter passord:test123



Laster ned vncpwd kjører og finner passordet jeg satte på TightVNC

<https://www.raymond.cc/blog/download/did/232/>

Et bilde som inneholder tekst

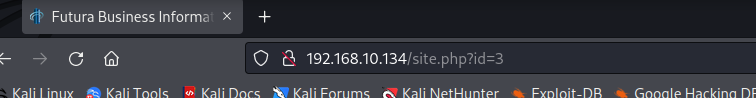
Automatisk generert beskrivelse

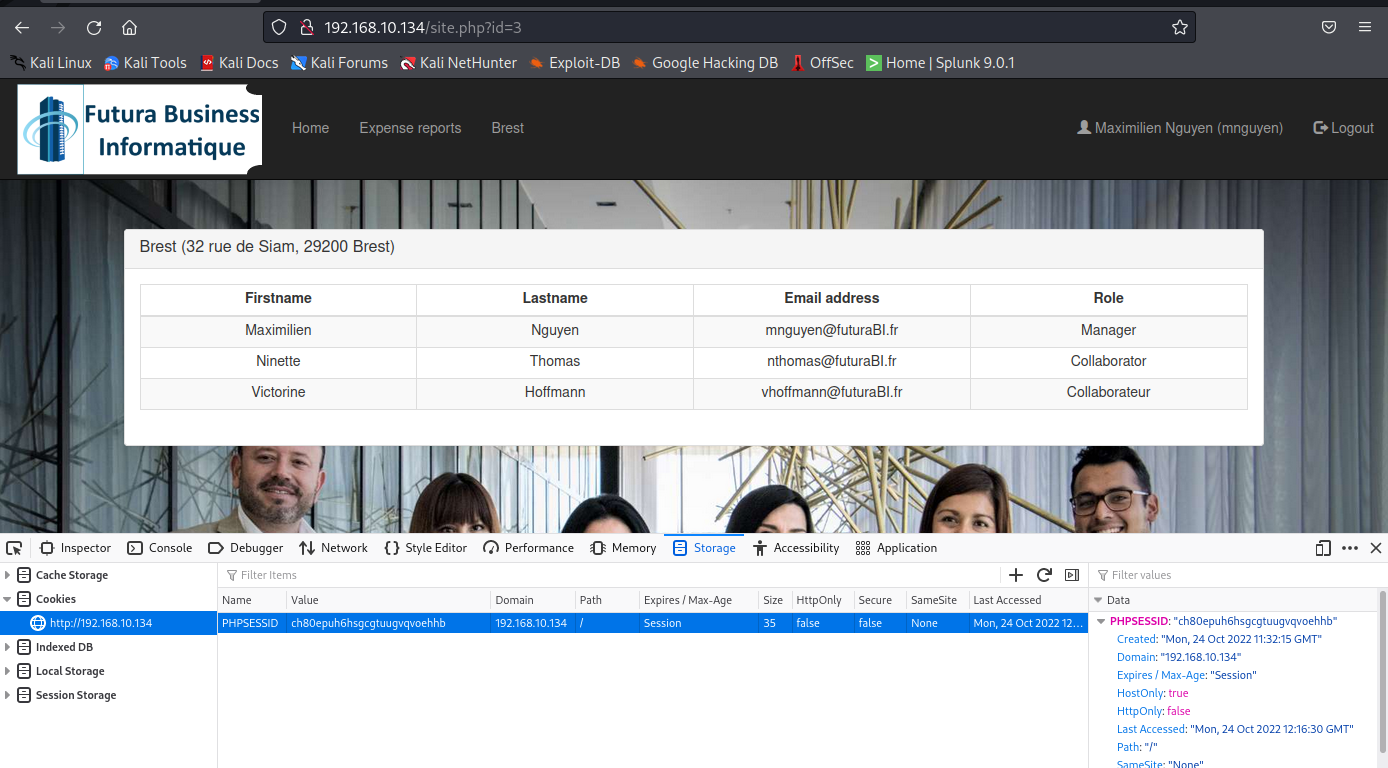
Kjører nmap mot ip adressen : 192.168.10.133 og får opp åpne porter

Et bilde som inneholder tekst

Automatisk generert beskrivelse

**SQLMAP: Logg inn i kali (ikke host) gå inn i expenses reports siden**

****



**Trykk inspect i firefox linux -> storage også ligger SSID der (husk å bruke denne url er forkjellig fra maskin til maskin.**

**Skriver inn i kali terminalen:** sqlmap -u http://192.168.10.134/site.php?id=3 --dbs --cookie="PHPSESSID=ch80epuh6hsgcgtuugvqvoehhb" -T user --dump

Et bilde som inneholder tekst

Automatisk generert beskrivelse

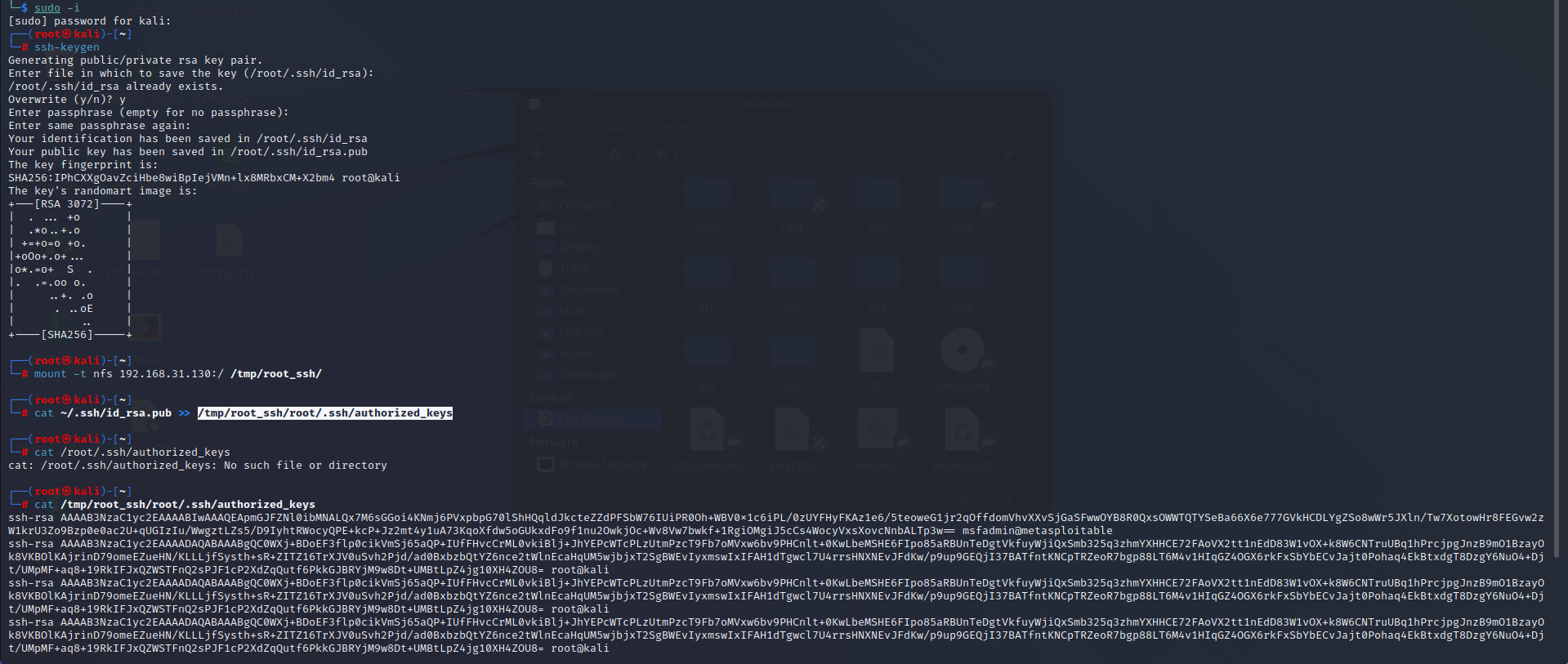
Et bilde som inneholder tekst

Automatisk generert beskrivelse

NSF del:

Et bilde som inneholder tekst

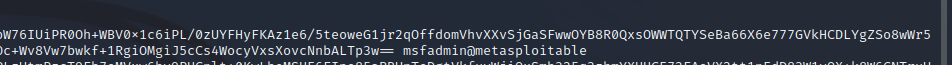
Automatisk generert beskrivelse



Et bilde som inneholder tekst

Automatisk generert beskrivelse

Det er lagt til et nytt nøkkel i root@kali dette er en indikasjon på at brukeren er innlogget



UNREALRCD del:

Starter msfconsole i linux

Et bilde som inneholder tekst

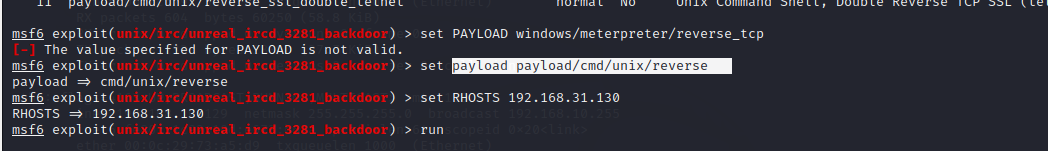
Automatisk generert beskrivelse

Set LHOST til kali IP adresse

Og sett payload til payload/cmd/unix/reverse **ellers så får man feilmelding**

Et bilde som inneholder tekst, datamaskin, skjermbilde

Automatisk generert beskrivelse



Et bilde som inneholder tekst

Automatisk generert beskrivelse

Et bilde som inneholder tekst

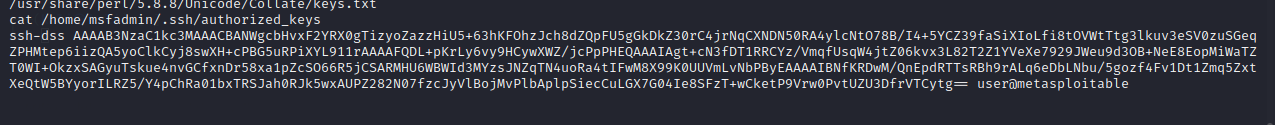
Automatisk generert beskrivelse

Et bilde som inneholder tekst

Automatisk generert beskrivelse

Blå- betyr at operasjonen kjører

Kjører kommandoene ovenfor som id , ls osv er inne i metasplod skriver cd.. for å gå ut av en bane osv locate keys for å finne authorized keys (leser av ssh nøklene)



**Metasploit – VSFTP exploiting del:**

Starter msfconsole i linux

Et bilde som inneholder tekst

Automatisk generert beskrivelse

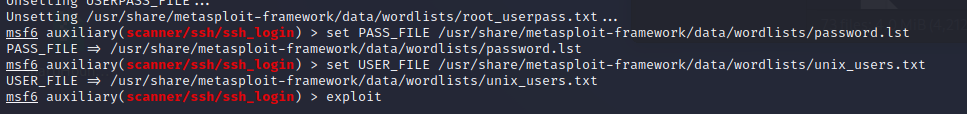
Et bilde som inneholder tekst

Automatisk generert beskrivelse

Et bilde som inneholder tekst

Automatisk generert beskrivelse

prøvde set USER\_FILE og PASS\_FILE til custom filer og deretter exploit (virker ikke dersom jeg brukte unset) prøver med en ny path



Et bilde som inneholder tekst

Automatisk generert beskrivelse

**Brute Force Del:**

Starter service postgressql og msfconsole

Et bilde som inneholder tekst

Automatisk generert beskrivelse

Et bilde som inneholder tekst, skjermbilde, overvåke, skjerm

Automatisk generert beskrivelse



Et bilde som inneholder tekst

Automatisk generert beskrivelse

Starter deretter brute-force med exploit kommandoen



Alternativt kan man sette usr\_file til mirai\_user.txt og tilsvarende for PASS\_FILE = mirai\_pass.txt og brute force , men det tar tid

Et bilde som inneholder tekst

Automatisk generert beskrivelse’

Finner bruker service pass:service . Når du logger deg inn med dette brukernavnet og passordet på metasploitable 2 virker det

Et bilde som inneholder tekst

Automatisk generert beskrivelse

Samme for user:user bruker dette og logger meg inn på user se under:

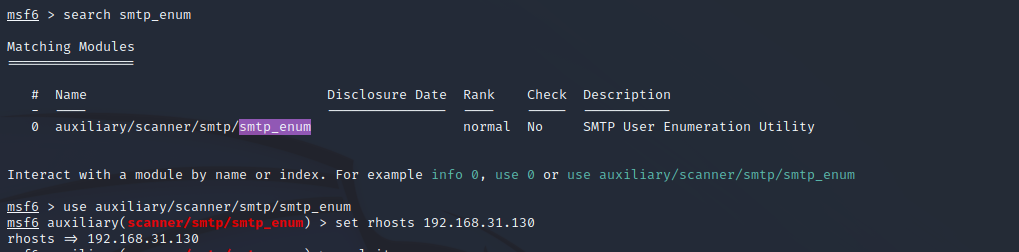
Et bilde som inneholder tekst

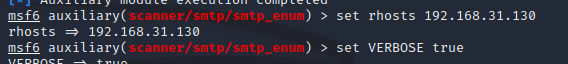
Automatisk generert beskrivelse

**Metasploit – enumerering av SMTP brukere del:**

**Et bilde som inneholder tekst

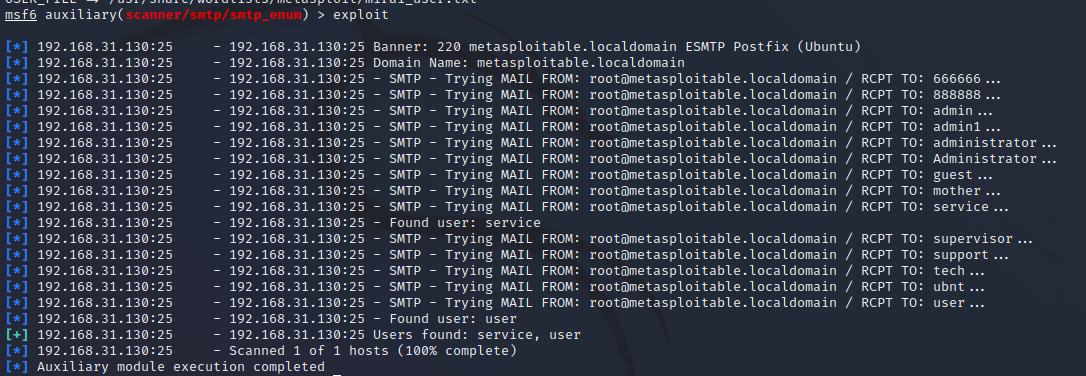
Automatisk generert beskrivelse**

****

****

****

**Kjører exploit kommandoen på msfconsole og får opp gyldige brukere : service og user**

****