

BSIDES VANCOUVER 2018

-In questo esercizio andremo ad ottenere in permessi di root in questa macchina,tutto tramite i mezzi che abbiamo imparato ad utilizzare nel peercorso
-i principali mezzi e ho utilizzato sono: Nmap,Dirb,Wpscan,Ssh e per terminare Hydra.

Scheda Server DHCP

☐ Configura scheda automaticamente

☒ Configura scheda manualmente

Indirizzo IPv4: 192.168.158.4

Maschera di rete IPv4: 255.255.255.0

Indirizzo IPv6: fe80::57f1:845:2f33:ac55

Lunghezza prefisso IPv6: 64

-Ho aperto il terminale su kali ed ho pingato l'ip creato precedentemente, una volta visto che funziona ho lanciato il comando "nmap2 per andare a vedere le porte tcp aperte nella macchina bersaglio.

Una volta terminata la scansione ho trovato 3 porte aperte, la 21, la 22 e la porta 80

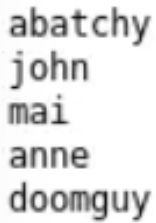
-Come prima cosa ho creato un scheda solo host per poter dare un ip alla macchina

```
(kali@kali)-[~]
$ ping 192.168.158.4
PING 192.168.158.4 (192.168.158.4) 56(84) bytes of data.
64 bytes from 192.168.158.4: icmp_seq=1 ttl=127 time=95.2 ms
64 bytes from 192.168.158.4: icmp_seq=2 ttl=127 time=4.29 ms
64 bytes from 192.168.158.4: icmp_seq=3 ttl=127 time=3.40 ms
64 bytes from 192.168.158.4: icmp_seq=4 ttl=127 time=3.57 ms
^S64 bytes from 192.168.158.4: icmp_seq=5 ttl=127 time=1.49 ms
64 bytes from 192.168.158.4: icmp_seq=6 ttl=127 time=2.06 ms
^C
  192.168.158.4 ping statistics:
  6 packets transmitted, 6 received, 0% packet loss, time 5170ms
 rtt min/avg/max/mdev = 1.486/18.337/95.213/34.392 ms
```

```
(kali@kali)-[~]
$ sudo nmap -A -Pn -p- 192.168.158.4 -oN all_tcp.nmap
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-01 11:05 EDT
█
```

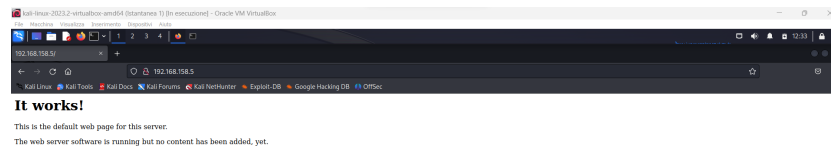
TEXT

-Cercando nel browser ,sfruttando la vulnerabilità nella porta 21, troveremo la cartella "public" dove saranno elencati i nomi utente



```
abatchy
john
mai
anne
doomguy
```

-Cercando solamente l'ip sul web browser il risultato sarà questo



-Una volta terminata la prima fase, inizieremo la parte di enumerazione.

-Arrivati a questo punto, io ho utilizzato il comando "dirb" per vedere se eventualmente ci fossero stati dei file/cartelle nascoste
in particolare io ho utilizzato questo comando qua:
`dirb http://192.168.158.4/ /usr/share/dirb/wordlists/common.txt -o dirb.log`

-Poi ho utilizzato "wpscan" per vedere i vari utenti di wordpress.
E ne ho trovati due Admin e john, ed il comando che utilizzato è questo:
`wpscan --url http://192.168.158.4/backup_wordpress/ --enumerate u > wpsan_users.log 2>&1`

-Un'altra funzionalità di "wpscan" e di poter fare il brute force delle password tramite delle liste di parole più comuni.

io ho utilizzato questa
:SecLists/Passwords/Common-Credentials/10k-most-common.
txt

andando a scoprire che la password di jhon è <enigma>

-Una volta terminato il tutto, andremo a sfruttare la vulnerabilità nella porta 22, cercando i metodi di autenticazione tramite il comando "ssh" e i nomi che avevamo trovato nella cartella public in precedenza.

Una volta provati tutti gli username noteremo che tutti quanti appartengono a "anne" richiederanno la password pubblica, mentre per accedere con l'utente "anne" sarà richiesta una password.

Quindi andremo a fare un'altro brute force per ottenere la password ssh di anne, però stavolta useremo "hydra" con un'altra lista delle parole più usate.

time hydra -l anne -P /usr/share/wordlists/rockyou.txt 192.168.158.4 ssh

-Dopo aver usato il comando sopracitato, il risultato sarà che la password di "anne" sarà "princess".

Quindi andremo ad utilizzare queste credenziali per accedere tramite ssh, e noteremo che l'utente anne appartiene al gruppo "sudo" quindi ha la possibilità di ottenere i permessi di root.