**BsidesVancouver2018**

Abbiamo un macchina ubuntu di cui non sappiamo nulla, né nomi degli users, né tantomeno le passwords, dobbiamo cercare di ottenere l’accesso Root.

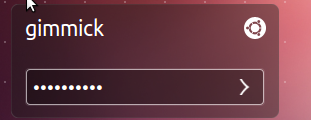
**Tentativo 1: editing del GRUB Boot Entry**

Dal menù GRUB iniziale, premendo “e”, possiamo editare le indicazioni di avvio.

Individuo la riga che specifica il kernel e le opzioni di avvio, sostituisco la modalità di avvio da read only (ro) con modalità read and write (rw)

Premendo f10 per avviare la macchina con i nuovi parametri.

Siamo ora entrati come root, ma a un livello bassissimo, tra le cose che possiamo fare da qui, c’è la possibilità di creare un nuovo utente con accessi di root.



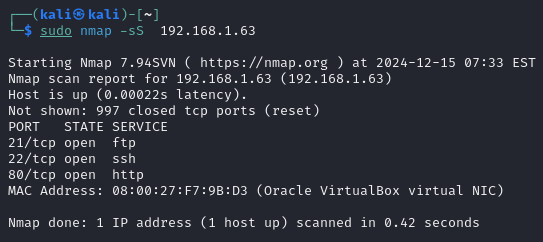
**Tentativo 2: sfruttamento ftp e brute force**

Assumiamo di non poter editare il Menù GRUB, ma di avere accesso fisico alla macchina e di poter entrare come guest.

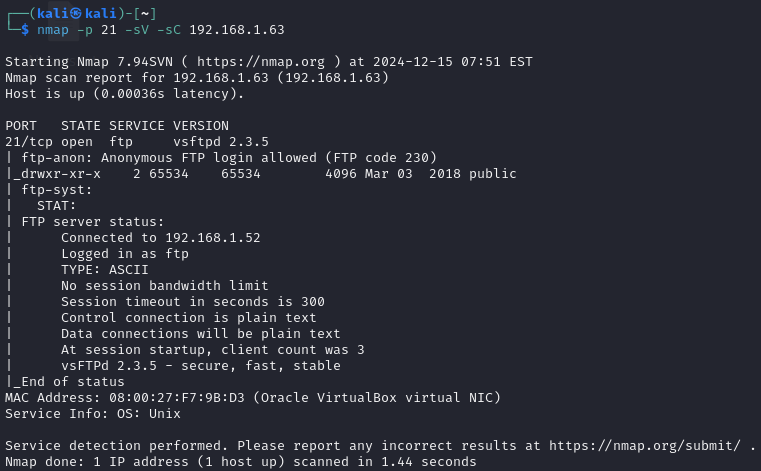
Ho lanciato un arp scan con nmap sulla mia Kali e ho individuato l’ip della macchina BsidesVancouver2018 (da qui in avanti chiamata target).

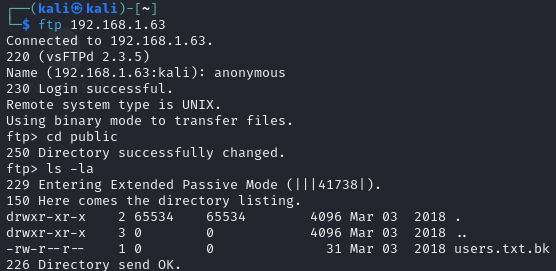
Comando: nmap -sn -PR 192.168.1.0/24

Conoscendo gli IP dei miei altri device, so che il target ha l’ip 192.168.1.53.

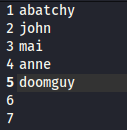
Da qui posso lanciare uno scan nmap per vedere quali sono le porte aperte.

Troviamo la 21, 22 e 80, scannerizziamo più a fondo la 21



Troviamo che la versione utilizzata è la vsftpd 2.3.5, facendo delle ricerche, scopro che permette di accedere in anonimato al server ftp, provo.

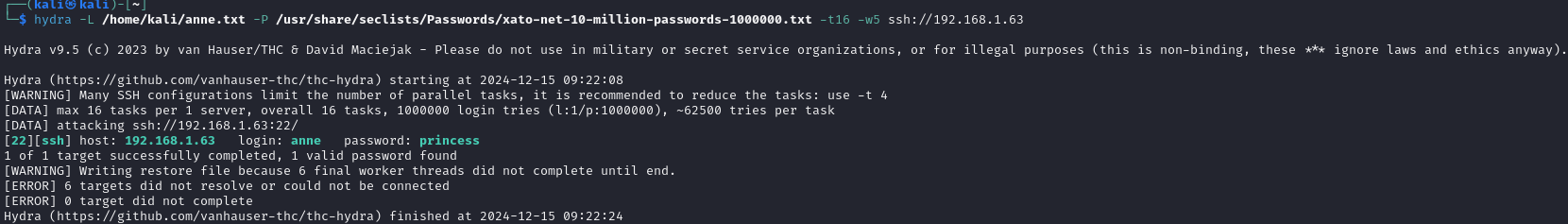
Come mostrato nell’immagine, posso muovermi nelle directories e controllare i file, trovo users.txt.bk

Provo a scaricarlo con il comando GET, ho il permesso di farlo, lo apro e trovo:

Abbiamo finalmente una lista di users.

Da qui provo a far crackare a hydra le password di accesso di ogni user.

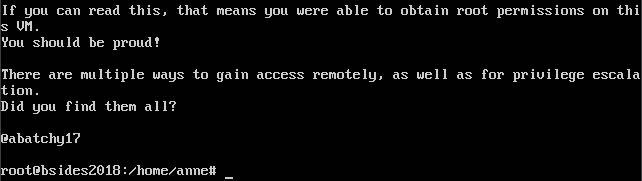
Provo sul servizio ssh.



Anne utilizza princess come password :(

Da qui basta semplicemente inserire le credenziali di anne nel target e cercar qualcosa di rilevante



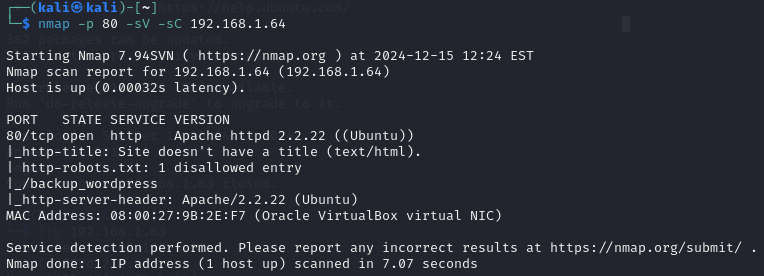
Ls evidenzia un file chiamato flag.txt, lo apro

Abbiamo trovato il nostro obbiettivo.

**Tentativo 3: work in progress**

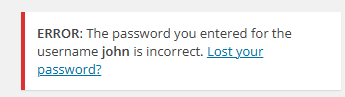
Assumiamo stavolta di non avere accesso fisico alcuno alla macchina.

Con l’IP della macchina, stavolta esploriamo la porta 80



Troviamo che la macchina ha una pagina wordpress, provo ad accedervi su <http://192.168.1.64/backup_wordpress>



Trovo questo, esplorando la pagina trovo una sezione di login, inserendo i vari users e password casuali, noto alcune differenze tra di loro: quando inserisco qualsiasi altro username, a prescindere dalla password, mi esce scritto di aver sbagliato il login, ma se provo con john, esce scritto che ho sbagliato solo la password, ne deduco che john è un user presente su questa pagina e da come leggo nella home, è un IT administrator, con probabili accessi profondi.

Qui è dove mi fermo. Ho provato a brute forzare con hydra l’user john, ma non so come configurarlo. Tutti gli altri exploit che ho ricercato richiedono di avere in qualche modo l’accesso al sito, ma non trovo modo di creare un nuovo user anche senza che esso sia amministratore.

Ipotesi conclusive:

Se riuscissi a trovare le credenziali di john, proverei a vedere se la pagina wordpress contiene dei file php per poter inserire una shell con cui prendere la reverse shell del target tramite netcat o l’uso di qualche codice python (da ricerche per gli altri tentativi, credo NetCat non sia presente nella macchina)

Qualora riuscissi ad avere accesso alla reverse shell proverei a cercare qualsiasi cosa che abbia accessi di root, che mi permetta di scrivere qualcosa, come un daemone o dei processi in corso, se così fosse, sarebbe facile da lì iniziare una connessione inversa da ascoltare con NetCat e trovare la flag da lì.