Black Box

Pentest Epicode

Valutazione delle vulnerabilità Penetration Test

Julio Armando Villanueva Carrion

04 nov 2025

Sommario Esecutivo

Questo report presenta i risultati di un'attività completa di Vulnerability Assessment e Penetration Testing (VA/PT) condotta sull'ambiente target rappresentato dalla macchina virtuale BSides Vancouver 2018.
L'analisi ha evidenziato diverse vulnerabilità ad alto impatto, che hanno consentito il compromesso totale del sistema e l'ottenimento di privilegi di amministratore (root) attraverso due distinti vettori di attacco indipendenti.

Scope

Di seguito l'IP del target:

- 192.168.56.101

Vulnerabilità a colpo d'occhio

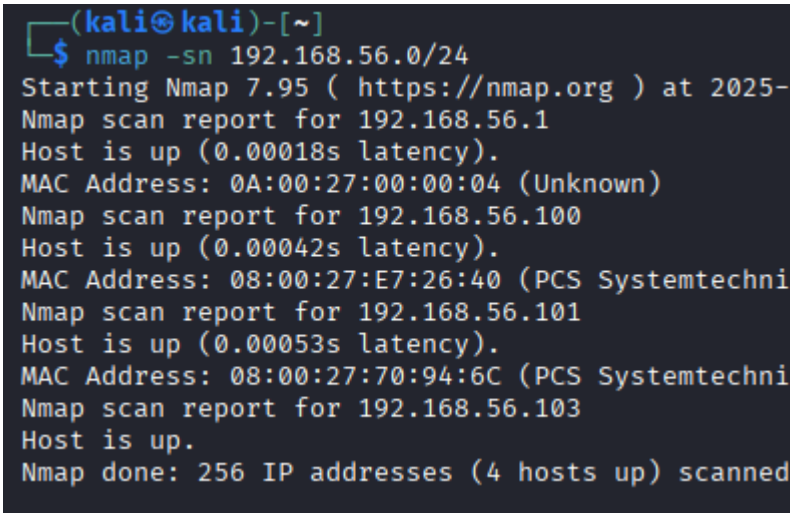
Tabella delle vulnerabilità identificate:

Vulnerability Name	Severity	Count
Attacco Brute Force SSH	Critico	1
Configurazione Errata Privilegi Sudo	Critico	1
Cron Job Root Scrivibile	Critico	1
Accesso FTP Anonimo	Alto	1

File users esposto	Medio	1
Total Vulnerabilities Found		5

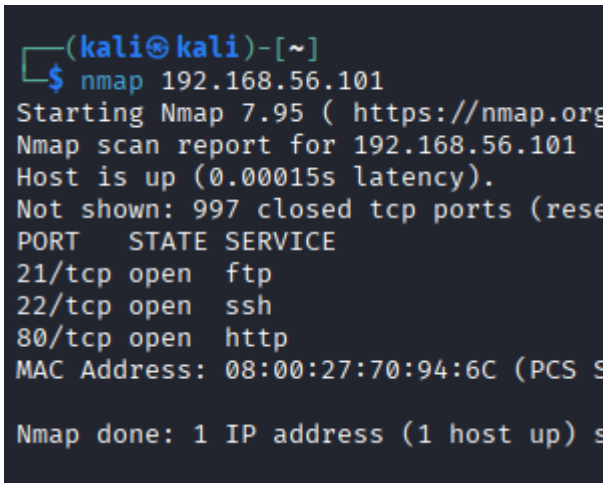
Azioni preliminari

Per verificare l'ip della Black Box ho lanciato il comando dhctl per avviare il DHCP e con ip a ho notato che avevo sia l'ip impostato (rete interna) che un altro ip (scheda solo host) ovvero 192.168.56.100, quindi con ciò ho verificato gli host attivi dentro la rete 192.168.56.0/24 con il comando nmap –sn 192.168.56.0/24



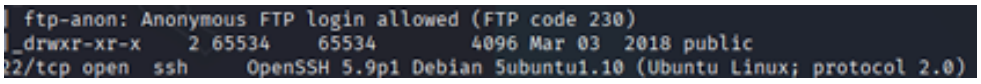
Fase di Scansione - Enumerazione

Verificando la connessione con l'ip 192.168.56.101, comando ping, ho fatto la scansione con nmap per vedere quali servizi sono attivi:



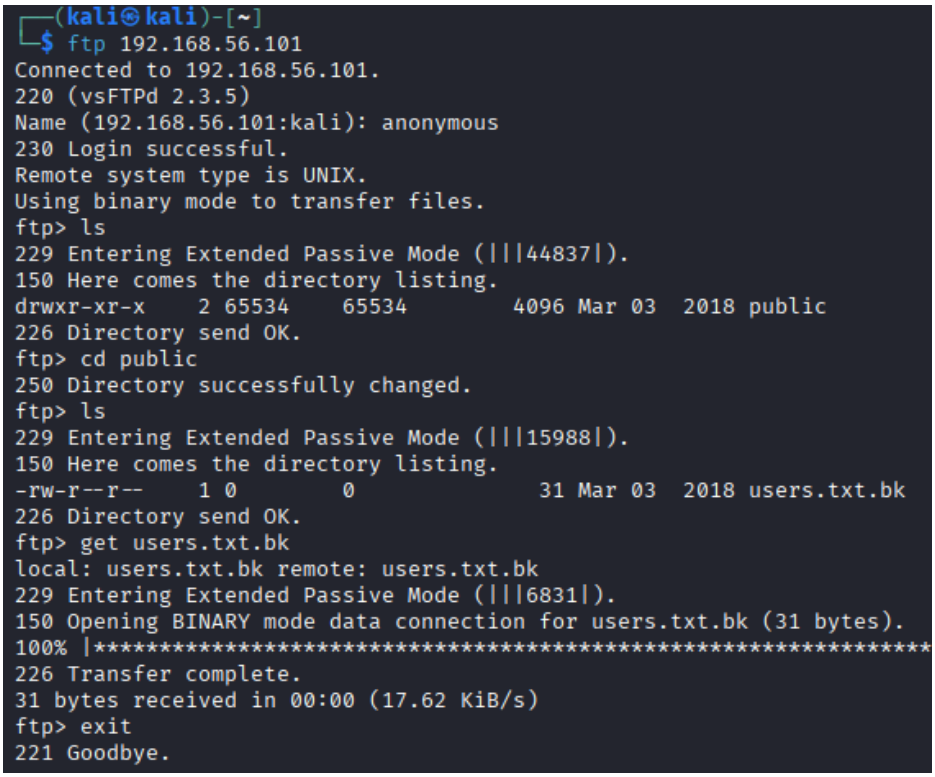
In questo caso come possiamo vedere ci sono 3 servizi attivi: FTP – porta 21, SSH – porta 22 e HTTP – porta 80

Facendo una scansione più profonda con nmap –A 192.168.56.101 possiamo verificare che il servizio ftp si può accedere come Anonymous



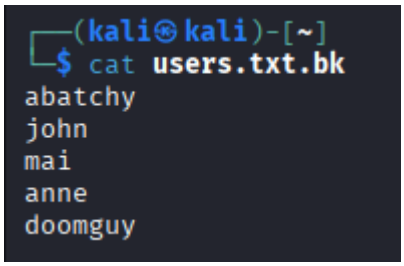
Penetration test

Identificato la vulnerabilità, sfruttiamola facendo l'accesso sul servizio ftp

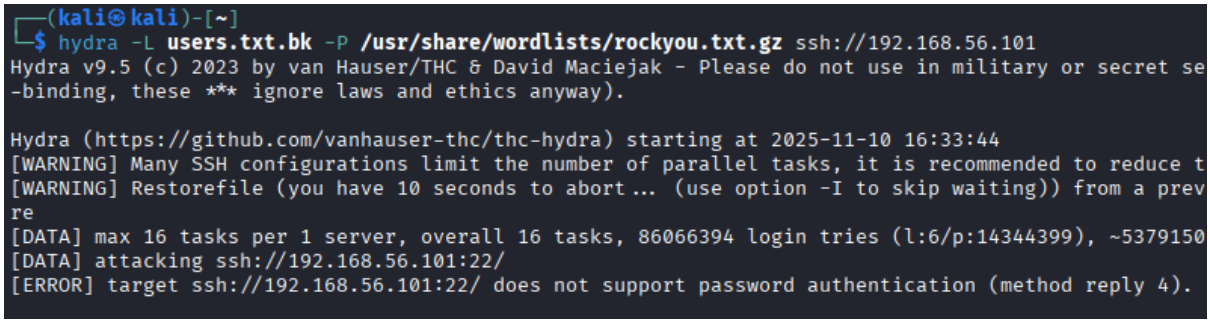


Si fa l'accesso login come anonymous, appena dentro possiamo usare ls per verificare che file ci sono all'interno. SI può notare che c'è una directory public, entriamo con il comando cd e dentro esso possiamo vedere che c'è un file TXT denominato users.txt.bk. Scarichiamolo con il comando get.

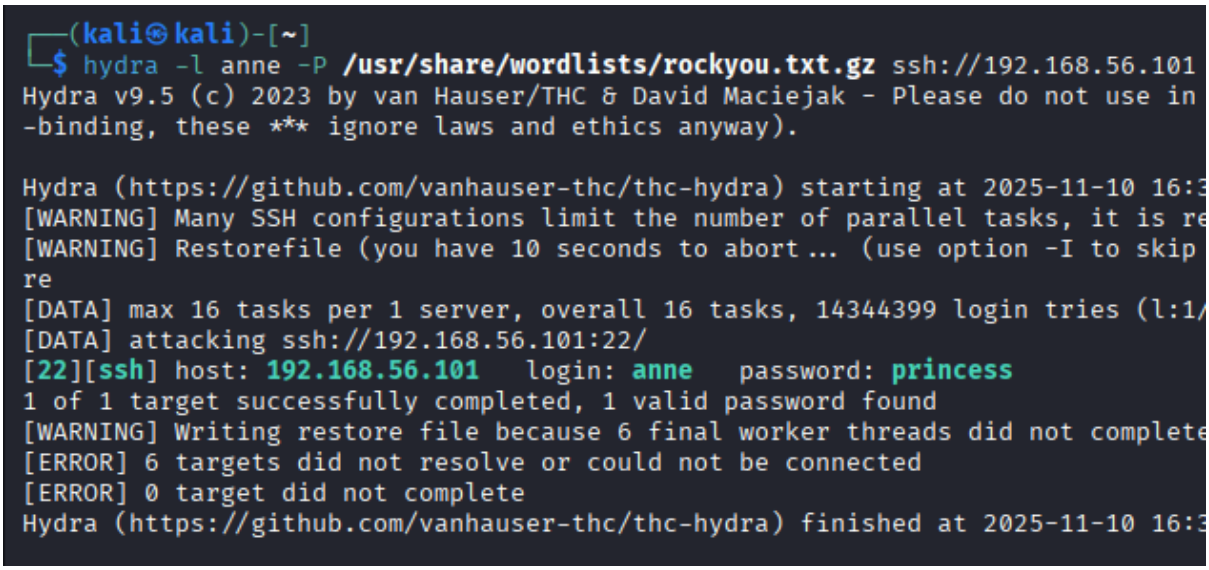
Viene scaricato su Download nella nostra Kali, quindi aprendo il terminal su Download e lanciando il comando cat users.txt.bk ci farà vedere il contenuto del file e in effetti possiamo vedere i nomi degli user, potrebbero essere l'username per accedere alla macchina Black Box.



Adesso che abbiamo gli username bisogna abbinarli a una password; quindi, ci facciamo aiutare con il comando hydra



Come possiamo vedere non riesce ad abbinare dato che la macchina non supporta password per l'autenticazione. Quindi per risolvere questo problema ho fatto la prova con tutti gli users fino a trovare l'unico user abbinato a una password ossia:



anne con password princess.

Trovato le credenziali posso accedere con SSH dalla Kali,

```
┌──(kali㉿kali)-[~]
└─$ ssh anne@192.168.56.101
The authenticity of host '192.168.56.101 (192.168.56.101)' can't be established.
ECDSA key fingerprint is SHA256:FhT9tr50Ps28yBw38pBWN+YEx5wCU/d8o1Ih22W4fyQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.101' (ECDSA) to the list of known hosts.
anne@192.168.56.101's password:
Welcome to Ubuntu 12.04.4 LTS (GNU/Linux 3.11.0-15-generic i686)

 * Documentation:  https://help.ubuntu.com/

382 packages can be updated.
275 updates are security updates.

New release '14.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Mon Nov 10 13:36:14 2025
anne@bsides2018:~$ sudo -l
[sudo] password for anne:
Matching Defaults entries for anne on this host:
    env_reset, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\

User anne may run the following commands on this host:
    (ALL : ALL) ALL
anne@bsides2018:~$ sudo su
root@bsides2018:/home/anne# cd
root@bsides2018:~# ls
flag.txt
root@bsides2018:~# cat flag.txt
Congratulations!

If you can read this, that means you were able to obtain root permissions on this VM.
You should be proud!

There are multiple ways to gain access remotely, as well as for privilege escalation.
Did you find them all?

@abatchy17
```

Per avere i permessi root è bastato lanciare il comando sudo –l, inserisco la password di anne e infine sudo su, cosi facendo ho ottenuto i permessi di root e facendo una ricerca, comando ls, ho trovato il flag.txt

Conclusioni:

L'obiettivo di ottenere privilegi amministrativi (root shell) sulla macchina target è stato raggiunto con successo. La compromissione è avvenuta attraverso diverse fasi, sfruttando criticità significative nella configurazione del sistema.

Questa esercitazione dimostra come l’intera catena di sicurezza possa fallire a causa di errori di configurazione evitabili. È prioritario rimuovere la direttiva di sudo (ALL: ALL) ALL concessa all’utente anne e disabilitare l’autenticazione tramite password, imponendo l’uso esclusivo di chiavi SSH. Infine, il recupero del flag finale nella directory /root/ conferma il completo controllo del sistema nel contesto della valutazione di sicurezza.