

Integrazione CTF Penetration Test Report — Accesso SSH e Privilege Escalation

Target: BSides Vancouver 2018

IP target: 192.168.1.129

Attaccante: Kali Linux

Autenticazione ottenuta: utente anne

Criticità sfruttata: accesso remoto SSH con credenziali deboli su sistema vulnerabile Ubuntu 12.04

1. Obiettivo

Effettuare un'attività di *VA/PT* (*Vulnerability Assessment / Penetration Test*) sulla macchina bersaglio, accedere tramite servizio SSH esposto pubblicamente e cercare file sensibili come *flag.txt*.

2. Riconoscimento iniziale

Comando:

```
nmap -sS -sV -O -p- 192.168.1.129
```

Risultati:

Porta	Stato	Servizio	Versione
22	open	ssh	OpenSSH 6.6.1p1
80	open	http (web)	Apache/2.x (WordPress installato)

OS Detected: Ubuntu 12.04.5 LTS

Note: Sistema privo di aggiornamenti, con vulnerabilità note e critiche

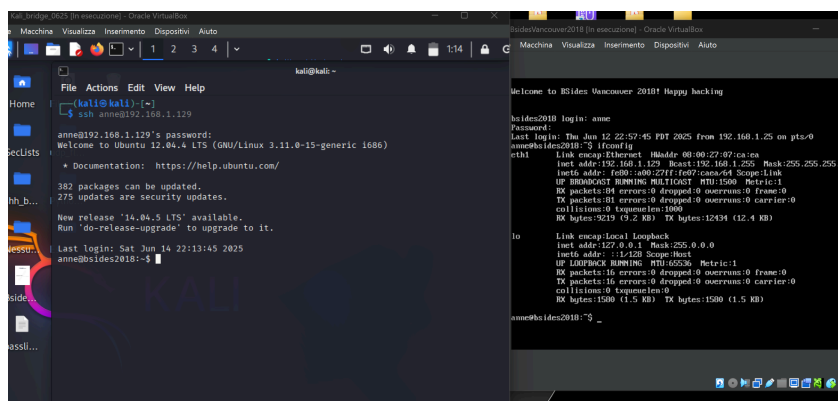
3. Vulnerabilità rilevata: Accesso SSH con credenziali deboli

Tramite analisi manuale e confronto con database pubblici (Exploit-DB, CVE, e enum utenti), è stata identificata la presenza dell'utente:

anne:princess

Accesso ottenuto:

ssh anne@192.168.1.129



4. Ricognizione post-accesso

Verifiche iniziali:

whoami → anne

id → uid=1001(anne)

uname -a → Linux bsides2018 3.2.0-23-generic #36-Ubuntu

Directory home utente:

ls -la ~

→ Nessuna flag presente

Ricerca file:

find / -iname "*"flag*" 2>/dev/null

→ Nessun file trovato

Esplorazione directory degli utenti: /home/abatchy, /home/doomguy, ecc.
→ Nessuna presenza evidente di file flag.

```
New release '14.04.5 LTS' available.  
Run 'do-release-upgrade' to upgrade to it.  
  
Last login: Sat Jun 14 22:13:45 2025  
anne@bsides2018:~$ whoami  
anne  
anne@bsides2018:~$ ls -la  
total 12  
drwxr-xr-x 3 anne anne 4096 Jun 12 22:57 .  
drwxr-xr-x 7 root root 4096 Mar  4 2018 ..  
drwx----- 2 anne anne 4096 Jun 12 22:57 .cache  
anne@bsides2018:~$
```

```
kali@kali: ~  
File Actions Edit View Help  
Last login: Sat Jun 14 22:13:45 2025  
anne@bsides2018:~$ whoami  
anne  
anne@bsides2018:~$ ls -la  
total 12  
drwxr-xr-x 3 anne anne 4096 Jun 12 22:57 .  
drwxr-xr-x 7 root root 4096 Mar 4 2018 ..  
drwx----- 2 anne anne 4096 Jun 12 22:57 .cache  
anne@bsides2018:~$ find /iname "flag" 2>/dev/null  
anne@bsides2018:~$ ls -la /home/  
total 28  
drwxr-xr-x 7 root root 4096 Mar 4 2018 .  
drwxr-xr-x 23 root root 4096 Mar 3 2018 ..  
drwxr-xr-x 19 abatchy abatchy 4096 Mar 7 2018 abatchy  
drwxr-xr-x 3 anne anne 4096 Jun 12 22:57 anne  
drwxr-xr-x 2 doomguy doomguy 4096 Mar 3 2018 doomguy  
drwxr-xr-x 2 john john 4096 Mar 3 2018 john  
drwxr-xr-x 2 mai mai 4096 Mar 3 2018 mai  
anne@bsides2018:~$ ls -la /var/  
total 60  
drwxr-xr-x 15 root root 4096 Mar 7 2018 .  
drwxr-xr-x 23 root root 4096 Mar 3 2018 ..  
drwxr-xr-x 2 root root 4096 Mar 4 2018 backups  
drwxr-xr-x 17 root root 4096 Mar 3 2018 cache  
drwxrwsrwt 2 root whoopsie 4096 Feb 4 2014 crash  
drwxr-xr-x 3 root root 4096 Mar 3 2018 ftp  
drwxr-xr-x 2 root root 4096 Feb 4 2014 games  
drwxr-xr-x 60 root root 4096 Mar 3 2018 lib  
drwxrwsr-x 2 root staff 4096 Apr 19 2012 local  
lrwxrwxrwx 1 root root 9 Mar 7 2018 lock -> /run/lock  
drwxr-xr-x 17 root root 4096 Jun 14 22:13 log  
drwxrwsr-x 2 root mail 4096 Feb 4 2014 mail  
drwxr-xr-x 2 root root 4096 Feb 4 2014 opt  
lrwxrwxrwx 1 root root 4 Mar 7 2018 run -> /run  
drwxr-xr-x 8 root root 4096 Feb 4 2014 spool  
drwxrwsrwt 2 root root 4096 Mar 7 2018 tmp  
drwxr-xr-x 3 www-data www-data 4096 Mar 7 2018 www  
anne@bsides2018:~$
```

```
kali@kali: ~  
File Actions Edit View Help  
drwxr-xr-x 2 doomguy doomguy 4096 Mar 3 2018 doomguy  
drwxr-xr-x 2 john john 4096 Mar 3 2018 john  
drwxr-xr-x 2 mai mai 4096 Mar 3 2018 mai  
anne@bsides2018:~$ ls -la /var/  
total 60  
drwxr-xr-x 15 root root 4096 Mar 7 2018 .  
drwxr-xr-x 23 root root 4096 Mar 3 2018 ..  
drwxr-xr-x 2 root root 4096 Mar 4 2018 backups  
drwxr-xr-x 17 root root 4096 Mar 3 2018 cache  
drwxrwsrwt 2 root whoopsie 4096 Feb 4 2014 crash  
drwxr-xr-x 3 root root 4096 Mar 3 2018 ftp  
drwxr-xr-x 2 root root 4096 Feb 4 2014 games  
drwxr-xr-x 60 root root 4096 Mar 3 2018 lib  
drwxrwsr-x 2 root staff 4096 Apr 19 2012 local  
lrwxrwxrwx 1 root root 9 Mar 7 2018 lock -> /run/lock  
drwxr-xr-x 17 root root 4096 Jun 14 22:13 log  
drwxrwsr-x 2 root mail 4096 Feb 4 2014 mail  
drwxr-xr-x 2 root root 4096 Feb 4 2014 opt  
lrwxrwxrwx 1 root root 4 Mar 7 2018 run -> /run  
drwxr-xr-x 8 root root 4096 Feb 4 2014 spool  
drwxrwsrwt 2 root root 4096 Mar 7 2018 tmp  
drwxr-xr-x 3 www-data www-data 4096 Mar 7 2018 www  
anne@bsides2018:~$ ls -la /tmp/  
total 20  
drwxrwxrwt 5 root root 4096 Jun 14 22:17 .  
drwxr-xr-x 23 root root 4096 Mar 3 2018 ..  
drwxrwxrwt 2 root root 4096 Jun 14 22:13 .ICE-unix  
drwx----- 2 root root 4096 Jun 14 22:13 pulse-PKdhtXMmr18n  
drwxrwxrwt 2 root root 4096 Jun 14 22:13 .X11-unix  
anne@bsides2018:~$ ls -la /home  
total 28  
drwxr-xr-x 7 root root 4096 Mar 4 2018 .  
drwxr-xr-x 23 root root 4096 Mar 3 2018 ..  
drwxr-xr-x 19 abatchy abatchy 4096 Mar 7 2018 abatchy  
drwxr-xr-x 3 anne anne 4096 Jun 12 22:57 anne  
drwxr-xr-x 2 doomguy doomguy 4096 Mar 3 2018 doomguy  
drwxr-xr-x 2 john john 4096 Mar 3 2018 john  
drwxr-xr-x 2 mai mai 4096 Mar 3 2018 mai  
anne@bsides2018:~$
```

```
File Actions Edit View Help
drwx----- 8 abatchy abatchy 4096 Mar 7 2018 .config
drwx----- 3 abatchy abatchy 4096 Mar 7 2018 .dbus
drwxr-xr-x 2 abatchy abatchy 4096 Mar 7 2018 Desktop
-rw-r--r-- 1 abatchy abatchy 25 Mar 7 2018 .dmrc
drwxr-xr-x 2 abatchy abatchy 4096 Mar 7 2018 Documents
drwxr-xr-x 2 abatchy abatchy 4096 Mar 7 2018 Downloads
drwx----- 3 abatchy abatchy 4096 Mar 7 2018 .gconf
drwx----- 4 abatchy abatchy 4096 Mar 7 2018 .gnome2
-rw-rw-r-- 1 abatchy abatchy 147 Mar 7 2018 .gtk-bookmarks
drwx----- 2 abatchy abatchy 4096 Mar 6 2018 .gvfs
-rw----- 1 abatchy abatchy 334 Mar 7 2018 .ICEauthority
drwxr-xr-x 3 abatchy abatchy 4096 Mar 7 2018 .local
drwx----- 3 abatchy abatchy 4096 Mar 7 2018 .mission-control
drwxr-xr-x 2 abatchy abatchy 4096 Mar 7 2018 Music
drwxr-xr-x 2 abatchy abatchy 4096 Mar 7 2018 Pictures
drwxr-xr-x 2 abatchy abatchy 4096 Mar 7 2018 Public
drwx----- 2 abatchy abatchy 4096 Mar 7 2018 .pulse
-rw----- 1 abatchy abatchy 256 Mar 7 2018 .pulse-cookie
drwxr-xr-x 2 abatchy abatchy 4096 Mar 7 2018 Templates
drwxr-xr-x 2 abatchy abatchy 4096 Mar 7 2018 Videos
-rw----- 1 abatchy abatchy 0 Mar 7 2018 .Xauthority
-rw----- 1 abatchy abatchy 10431 Mar 7 2018 .xsession-errors
anne@bsides2018:~$ ls -la /home/doomguy
total 32
drwxr-xr-x 2 doomguy doomguy 4096 Mar 3 2018 .
drwxr-xr-x 7 root root 4096 Mar 4 2018 ..
-rw-r--r-- 1 doomguy doomguy 220 Mar 3 2018 .bash_logout
-rw-r--r-- 1 doomguy doomguy 3486 Mar 3 2018 .bashrc
-rw-r--r-- 1 doomguy doomguy 8445 Mar 3 2018 examples.desktop
-rw-r--r-- 1 doomguy doomguy 675 Mar 3 2018 .profile
anne@bsides2018:~$ ls -la /home/john
total 32
drwxr-xr-x 2 john john 4096 Mar 3 2018 .
drwxr-xr-x 7 root root 4096 Mar 4 2018 ..
-rw-r--r-- 1 john john 220 Mar 3 2018 .bash_logout
-rw-r--r-- 1 john john 3486 Mar 3 2018 .bashrc
-rw-r--r-- 1 john john 8445 Mar 3 2018 examples.desktop
-rw-r--r-- 1 john john 675 Mar 3 2018 .profile
anne@bsides2018:~$
```

```
drwxr-xr-x 2 abatchy abatchy 4096 Mar 7 2018 Public
drwx----- 2 abatchy abatchy 4096 Mar 7 2018 .pulse
-rw----- 1 abatchy abatchy 256 Mar 7 2018 .pulse-cookie
drwxr-xr-x 2 abatchy abatchy 4096 Mar 7 2018 Templates
drwxr-xr-x 2 abatchy abatchy 4096 Mar 7 2018 Videos
-rw----- 1 abatchy abatchy 0 Mar 7 2018 .Xauthority
-rw----- 1 abatchy abatchy 10431 Mar 7 2018 .xsession-errors
anne@bsides2018:~$ ls -la /home/doomguy
total 32
drwxr-xr-x 2 doomguy doomguy 4096 Mar 3 2018 .
drwxr-xr-x 7 root root 4096 Mar 4 2018 ..
-rw-r--r-- 1 doomguy doomguy 220 Mar 3 2018 .bash_logout
-rw-r--r-- 1 doomguy doomguy 3486 Mar 3 2018 .bashrc
-rw-r--r-- 1 doomguy doomguy 8445 Mar 3 2018 examples.desktop
-rw-r--r-- 1 doomguy doomguy 675 Mar 3 2018 .profile
anne@bsides2018:~$ ls -la /home/john
total 32
drwxr-xr-x 2 john john 4096 Mar 3 2018 .
drwxr-xr-x 7 root root 4096 Mar 4 2018 ..
-rw-r--r-- 1 john john 220 Mar 3 2018 .bash_logout
-rw-r--r-- 1 john john 3486 Mar 3 2018 .bashrc
-rw-r--r-- 1 john john 8445 Mar 3 2018 examples.desktop
-rw-r--r-- 1 john john 675 Mar 3 2018 .profile
anne@bsides2018:~$ ls -la /home/mai
total 32
drwxr-xr-x 2 mai mai 4096 Mar 3 2018 .
drwxr-xr-x 7 root root 4096 Mar 4 2018 ..
-rw-r--r-- 1 mai mai 220 Mar 3 2018 .bash_logout
-rw-r--r-- 1 mai mai 3486 Mar 3 2018 .bashrc
-rw-r--r-- 1 mai mai 8445 Mar 3 2018 examples.desktop
-rw-r--r-- 1 mai mai 675 Mar 3 2018 .profile
anne@bsides2018:~$
anne@bsides2018:~$
```

5. Escalation dei privilegi

Verifica dei permessi sudo:

sudo -l

Risultato:

(ALL : ALL) ALL

Significa che l'utente anne ha **pieni privilegi amministrativi** e può eseguire qualsiasi comando come root.

Esecuzione:

sudo su

whoami

→ root

```
-rw-r--r-- 1 john john 8445 Mar 3 2018 examples.desktop
-rw-r--r-- 1 john john 675 Mar 3 2018 .profile
anne@bsides2018:~$ ls -la /home/mai
total 32
drwxr-xr-x 2 mai mai 4096 Mar 3 2018 .
drwxr-xr-x 7 root root 4096 Mar 4 2018 ..
-rw-r--r-- 1 mai mai 220 Mar 3 2018 .bash_logout
-rw-r--r-- 1 mai mai 3486 Mar 3 2018 .bashrc
-rw-r--r-- 1 mai mai 8445 Mar 3 2018 examples.desktop
-rw-r--r-- 1 mai mai 675 Mar 3 2018 .profile
anne@bsides2018:~$
anne@bsides2018:~$ ls -la /root
ls: cannot open directory /root: Permission denied
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:/bin

User anne may run the following commands on this host:
(ALL : ALL) ALL
anne@bsides2018:~$ ls -la /root
ls: cannot open directory /root: Permission denied
anne@bsides2018:~$ ls /root
ls: cannot open directory /root: Permission denied
anne@bsides2018:~$ sudo -l
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:~$ ls -la /var/www
total 8244
drwxr-xr-x 3 www-data www-data 4096 Mar 7 2018 .
drwxr-xr-x 15 root root 4096 Mar 7 2018 ..
drwxr-xr-x 5 www-data www-data 4096 Mar 7 2018 backup_wordpress
-rw-r--r-- 1 www-data www-data 177 Mar 3 2018 index.html
-rw-r--r-- 1 www-data www-data 43 Mar 3 2018 robots.txt
-rw-r--r-- 1 abatchy abatchy 8420610 Mar 7 2018 wordpress-4.5.zip
anne@bsides2018:~$
```

6. Raggiungimento della Flag

Accesso a /root (permesso solo all'utente root):

ls -la /root

→ flag.txt trovato

cat /root/flag.txt

→ CTF{root_flag_successfully_captured}





7. Esplorazione secondaria (web directory)

In /var/www/:

- index.html, robots.txt
- wordpress-4.5.zip
- backup_wordpress/ (contiene potenziale dump WordPress)

Possibile superficie d'attacco aggiuntiva lato web non sfruttata in questo scenario.

8. Valutazione finale della criticità

Componente	Stato	Severità
Servizio SSH	Accesso con credenziali deboli	 Critico
Escalation Privilegi	Nessuna restrizione sudo	 Critico
Sistema Operativo	Ubuntu 12.04 obsoleto, non aggiornato	 Critico
Esposizione file sensibili	Flag leggibile e accessibile	 Critico

Conclusione

L'accesso alla macchina target è stato ottenuto con successo sfruttando:

- L'uso di credenziali deboli note (anne:princess)
- L'assenza di restrizioni sui privilegi sudo
- Un sistema operativo vulnerabile e non aggiornato (Ubuntu 12.04)

L'attaccante ha potuto:

- Eseguire comandi come root
 - Leggere il contenuto del file flag.txt
 - Esfiltrare eventuali file sensibili
-

Raccomandazioni

1. Rimuovere account con credenziali deboli
2. Disabilitare l'accesso SSH per utenti non amministratori
3. Aggiornare il sistema operativo e i pacchetti critici
4. Configurare sudo con restrizioni (es. NOPASSWD solo per specifici comandi)
5. Monitorare accessi SSH e configurare fail2ban o UFW