0. Introducción

Tengo que decir, que de esta máquina me siento especialmente orgulloso. Aunque no es muy compleja, fue mi primera máquina sin necesitar ningún writeup o pista. Vamos a ver como se resuelve.

1. Enumeración

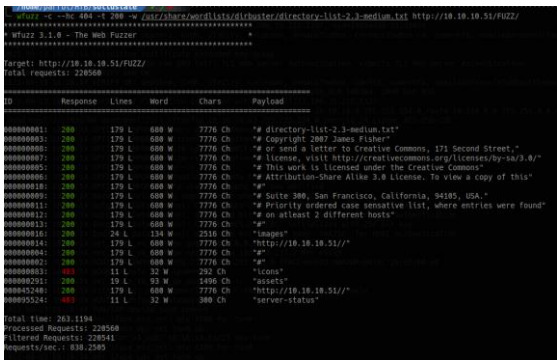
```
Nmap scan report for 10.10.10.51
Host is up (0.035s latency).

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.4p1 Debian 10+deb9u1 (protocol 2.0)
| ssh-hostkey:
|   2048 77:00:84:f5:78:b9:c7:d3:54:cf:71:2e:0d:52:6d:8b (RSA)
|   256 78:b8:3a:f6:60:19:06:91:f5:53:92:1d:3f:48:ed:53 (ECDSA)
|_  256 e4:45:e9:ed:07:4d:73:69:43:5a:12:70:9d:c4:af:76 (ED25519)
25/tcp   open  smtp    JAMES smtpd 2.3.2
|_smtp-commands: solidstate Hello nmap.scanme.org (10.10.14.63 [10.10.14.63])
80/tcp   open  http    Apache httpd 2.4.25 ((Debian))
|_http-title: Home - Solid State Security
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.25 (Debian)
110/tcp  open  pop3    JAMES pop3d 2.3.2
119/tcp  open  nntp    JAMES nntpd (posting ok)
4555/tcp open  rsip?
| fingerprint-strings:
|   GenericLines:
|     JAMES Remote Administration Tool 2.3.2
|     Please enter your login and password
|     Login id:
|     Password:
|     Login failed for
|     Login id:
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port4555-TCP:V=7.92%I=7%D=9/13%Time=6320AF87%P=x86_64-pc-linux-gnu%r(Ge
SF:nericLines,7C,"JAMES\x20Remote\x20Administration\x20Tool\x202\.3\.2\nPl
SF:ease\x20enter\x20your\x20login\x20and\x20password\nLogin\x20id:\nPasswo
SF:rd:\nLogin\x20failed\x20for\x20\nLogin\x20id:\n");
Service Info: Host: solidstate; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Sep 13 18:32:02 2022 -- 1 IP address (1 host up) scanned in 262.46 seconds
```

2. Análisis de vulnerabilidades.

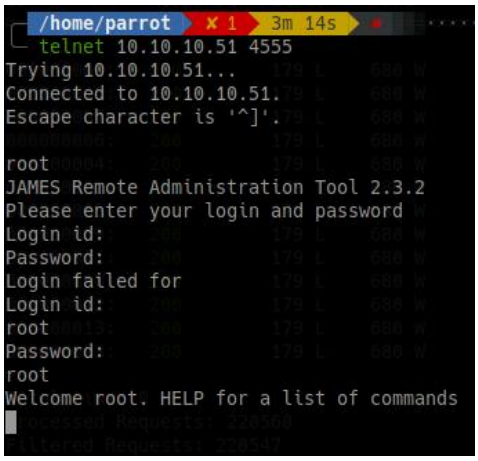
El puerto 22, que corresponde al servicio de SSH, lo vamos a obviar de momento, ya que no tenemos credenciales.

Vamos a seguir con el puerto 80, enumerando las tecnologías, que esta corriendo en la página web.

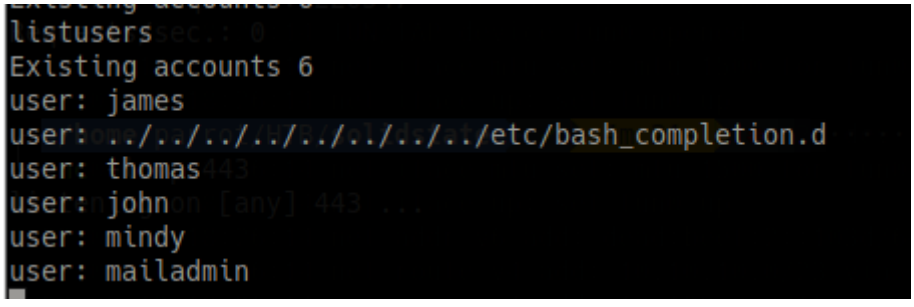
En principio, no vemos nada interesante en la web. Realizamos un wfuzz, que tampoco encuentra nada interesante.



Cambiamos un poco de vector de ataque y revisamos la parte de JAMES Remote Administration Tool. Googleando un poco (https://crimsonglow.ca/~kjiwa/2016/06/exploiting-apache-james-2.3.2.html) vemos que las credenciales por defecto, son root/root. Intentamos el acceso.



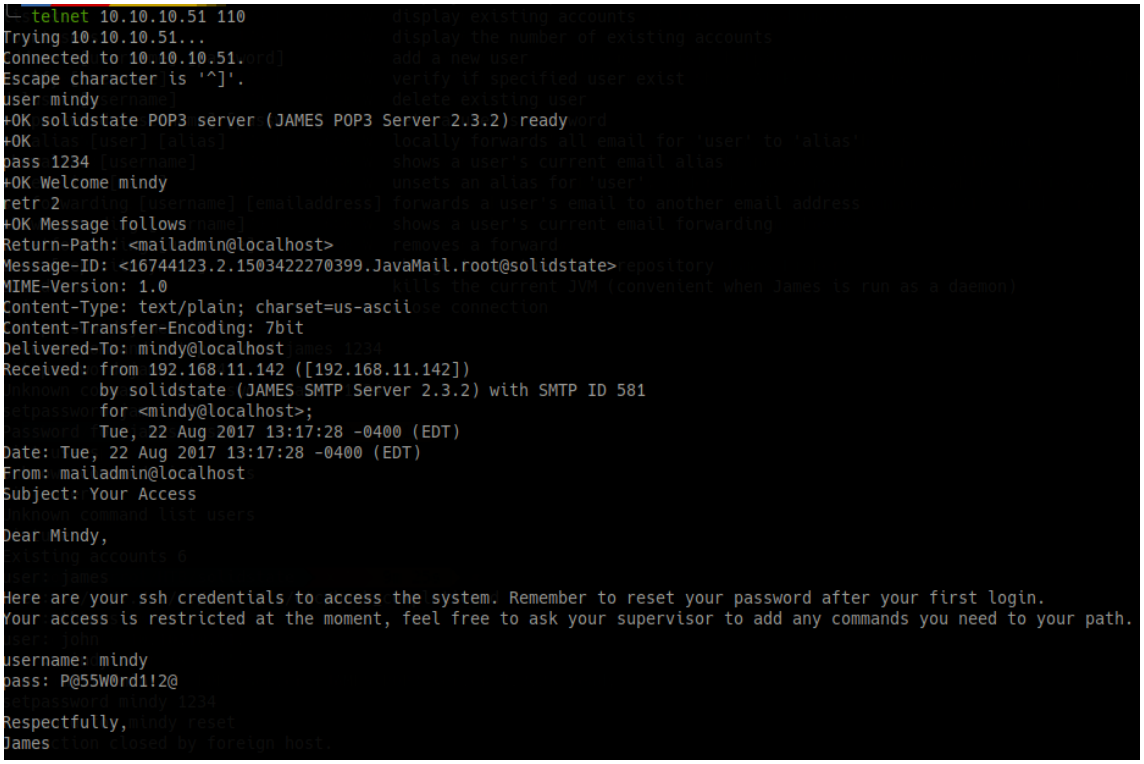
Podemos listar los usuarios actuales.



Adicionalmente, podemos cambiar la password a los distintos usuarios. Probamos primero con “james” e intentamos conectarnos al servicio de POP3. No vemos ningún correo.

Ahora, probamos con mindy. Vemos que tiene dos correos. ¡Pues a leer se ha dicho! El primer correo no vemos nada de interés.

En el segundo conseguimos unas credenciales.

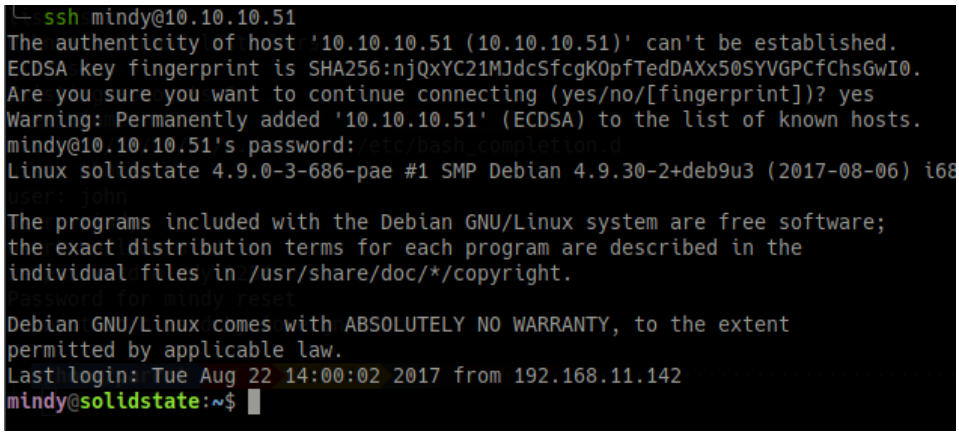


username: mindy

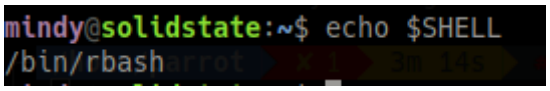
pass: P@55W0rd1!2@

3. Explotación y acceso

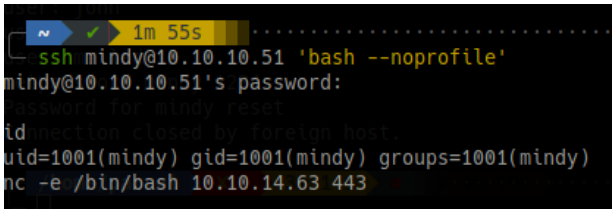
Vamos a probar si podemos conectarnos por SSH. Y efectivamente, ganamos acceso.



No podemos ejecutar sudo -l. Comprobamos si estamos ante una “restricted shell” y efectivamente.



Para escaparnos de esta “restricted shell”, lo realizamos de la siguiente forma:

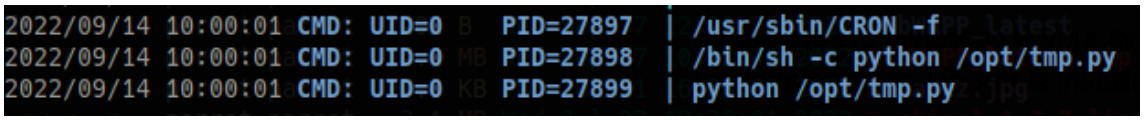


Realizamos el tratamiento de la TTY como siempre.

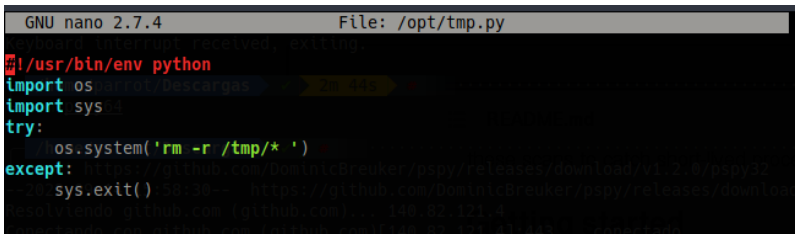
4. Escalada de privilegios.

Hacemos un reconocimiento de privilegios, permisos sobre ficheros, capabilities, etc. pero no vemos nada de interés. Nos descargamos el script pspy para hacer un seguimiento de los procesos corriendo en el sistema (https://github.com/DominicBreuker/pspy).

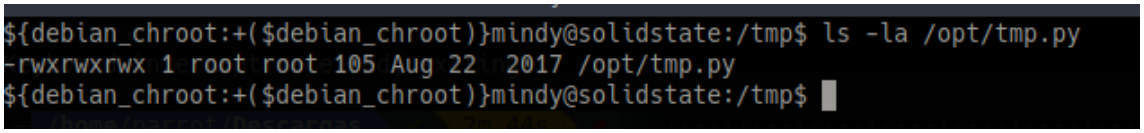
Nos llama la atención este proceso que ejecuta /opt/tmp.py con permisos de root.



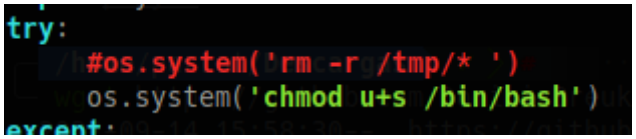
Vemos el contenido de dicho script y comprobamos que ejecuta un comando a nivel de sistema operativo.



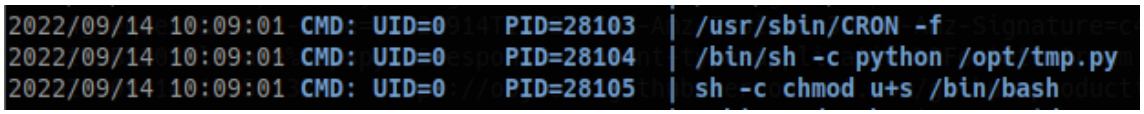
Revisando los permisos, vemos que tenemos permisos de escritura. ¡Qué regalo!



Pues nada, vamos a modificar el script para que añada permisos SUID sobre la bash.



Esperamos a que se ejecute el script.



Listo. Ya somos root.