

ESERCITAZIONE WEEK 16 DAY 2



WI6D1 - Pratica (1) PDF

Esercizio
Traccia

Traccia:

Sulla base dell'esercizio visto in lezione teorica, utilizzare Kali per sfruttare la vulnerabilità relativa a Telnet con il modulo auxiliary telnet_version sulla macchina Metasploitable.

Requisito: Seguire gli step visti in lezione teorica. Prima, configurate l'IP della vostra Kali con 192.168.1.25 e l'IP della vostra Metasploitable con 192.168.1.40

Configurazione macchine:

```
(kali@kali)-[~]
$ ifconfig
eth0: flags=4163<UP, BROADCAST, RUNNING, MULTICAST> mtu 1500
    inet 192.168.1.25 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::a00:27ff:feeb:7ef5 prefixlen 64 scopeid 0<link>
    ether 08:00:27:cb:7e:f5 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 22 bytes 2844 (2.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP, LOOPBACK, RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0
    Link encap:Ethernet HWaddr 08:00:27:5c:1d:d1
    inet addr:192.168.1.40 Bcast:192.168.1.255 Mask:255.255.255.0
    inet6 addr: fe80::a00:27ff:fe5c:1dd1/64 Scope:Link
    UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
    RX packets:0 errors:0 dropped:0 overruns:0 frame:0
    TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:1000
    RX bytes:0 (0.0 B) TX bytes:9463 (9.2 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:186 errors:0 dropped:0 overruns:0 frame:0
    TX packets:186 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:0
```

Scansione nmap su target Metasploitable: è presente il servizio telnet in ascolto su porta 23 che trasmette su canale non cifrato. Ciò significa che un potenziale attaccante potrebbe sniffare la comunicazione e rubare informazioni sensibili come username, password ed i comandi scambiati tra client e server:

```
(kali@kali)-[~]
$ nmap -sV 192.168.1.40
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-20 13:41 EST
Nmap scan report for 192.168.1.40
Host is up (0.00045s latency).
Not shown: 977 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)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login?
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)
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
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Per sfruttare questa particolare vulnerabilità del servizio Telnet, si usa il modulo ausiliario **auxiliary/scanner/telnet/telnet_version**:

```

35 auxiliary/scanner/telnet/telnet_version
   normal No Telnet Service Banner Detection
36 auxiliary/scanner/telnet/telnet_encrypt_overflow
   normal No Telnet Service Encryption Key ID Overflow Detection
37 payload/cmd/unix/bind_busybox_telnetd
   normal No Unix Command Shell, Bind TCP (via BusyBox telnetd)
38 payload/cmd/unix/reverse
   normal No Unix Command Shell, Double Reverse TCP (telnet)
39 payload/cmd/unix/reverse_ssl_double_telnet
   normal No Unix Command Shell, Double Reverse TCP SSL (telnet)
40 payload/cmd/unix/reverse_bash_telnet_ssl
   normal No Unix Command Shell, Reverse TCP SSL (telnet)
41 exploit/linux/ssh/vyos_restricted_shell_privsc 2018-11-
05 great Yes VyOS restricted-shell Escape and Privilege Escalation
42 post/windows/gather/credentials/mremote
   normal No Windows Gather mRemote Saved Password Extraction

```

Interact with a module by name or index. For example `info 42`, use `42` or use `post/windows/gather/credentials/mremote`

```

msf6 > use auxiliary/scanner/telnet/telnet_version
msf6 auxiliary(scanner/telnet/telnet_version) >

```

Configurazione delle opzioni necessarie:

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

```
msf6 auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.1.40
rhosts => 192.168.1.40
msf6 auxiliary(scanner/telnet/telnet_version) > show options
```

Module options (auxiliary/scanner/telnet/telnet_version):

Name	Current Setting	Required	Description
PASSWORD		no	The password for the specified username
RHOSTS	192.168.1.40	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	23	yes	The target port (TCP)
THREADS	1	yes	The number of concurrent threads (max one per host)
TIMEOUT	30	yes	Timeout for the Telnet probe
USERNAME		no	The username to authenticate as

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

```
msf6 auxiliary(scanner/telnet/telnet_version) > |
```

Non serve in questo caso specificare alcun payload, quindi si procede con il comando exploit:

[illegible]

Sono così recuperati i dati di login.

Per verificare lo sfruttamento di questa vulnerabilità, possiamo accedere da kali al servizio Telnet:

