Report: Esercizio sulla Riproduzione dell'Errore di Segmentazione in C

Introduzione

Nella lezione dedicata agli attacchi di sistema, abbiamo esplorato il concetto di buffer overflow, una vulnerabilità che si verifica quando i limiti dei buffer che accettano input utente non sono controllati adeguatamente. In questo esercizio, ho lavorato sulla riproduzione di un errore di segmentazione utilizzando un semplice programma in C.

Obiettivo

L'obiettivo dell'esercizio è stato quello di comprendere come un buffer overflow possa portare a un errore di segmentazione, scrivendo e modificando un programma in C che accetta input utente senza adeguati controlli sui limiti del buffer.

Ambiente di Lavoro

- **Sistema Operativo**: Kali Linux (VirtualBox VM, IP 192.168.1.111)
- **Editor di Testo**: Nano
- **Compilatore**: GCC

Procedura

1. **Avvio di Kali Linux** Ho avviato la mia macchina virtuale Kali Linux su VirtualBox.
2. **Apertura del Terminale** Ho aperto il terminale cliccando sull'icona del terminale nella barra superiore.
3. **Navigazione verso il Desktop** Ho eseguito il comando per spostarmi nella directory del desktop:

```
cd /home/kali/Desktop
```

4. **Creazione e Modifica del File C** Ho aperto l'editor di testo nano e creato un nuovo file chiamato BOF.c:

```
nano BOF.c
```

5. **Scrittura del Codice C** Ho inserito il seguente codice nel file BOF.c:

```
#include <stdio.h>

int main() {
```

```
    char buffer[30]; // Modificato a 30 per riprodurre l'errore di segmentazione

    printf("Si prega di inserire il nome utente:");
    scanf("%s", buffer);

    printf("Nome utente inserito: %s\n", buffer);

    return 0;
}
```

6. **Salvataggio e Chiusura del File** Ho salvato e chiuso il file premendo Ctrl + X, poi Y per confermare il salvataggio e infine Invio per confermare il nome del file.
7. **Compilazione del Codice C** Ho compilato il codice utilizzando gcc:

```
gcc -g BOF.c -o BOF
```

8. **Esecuzione del Programma** Ho eseguito il programma compilato:

```
./BOF
```

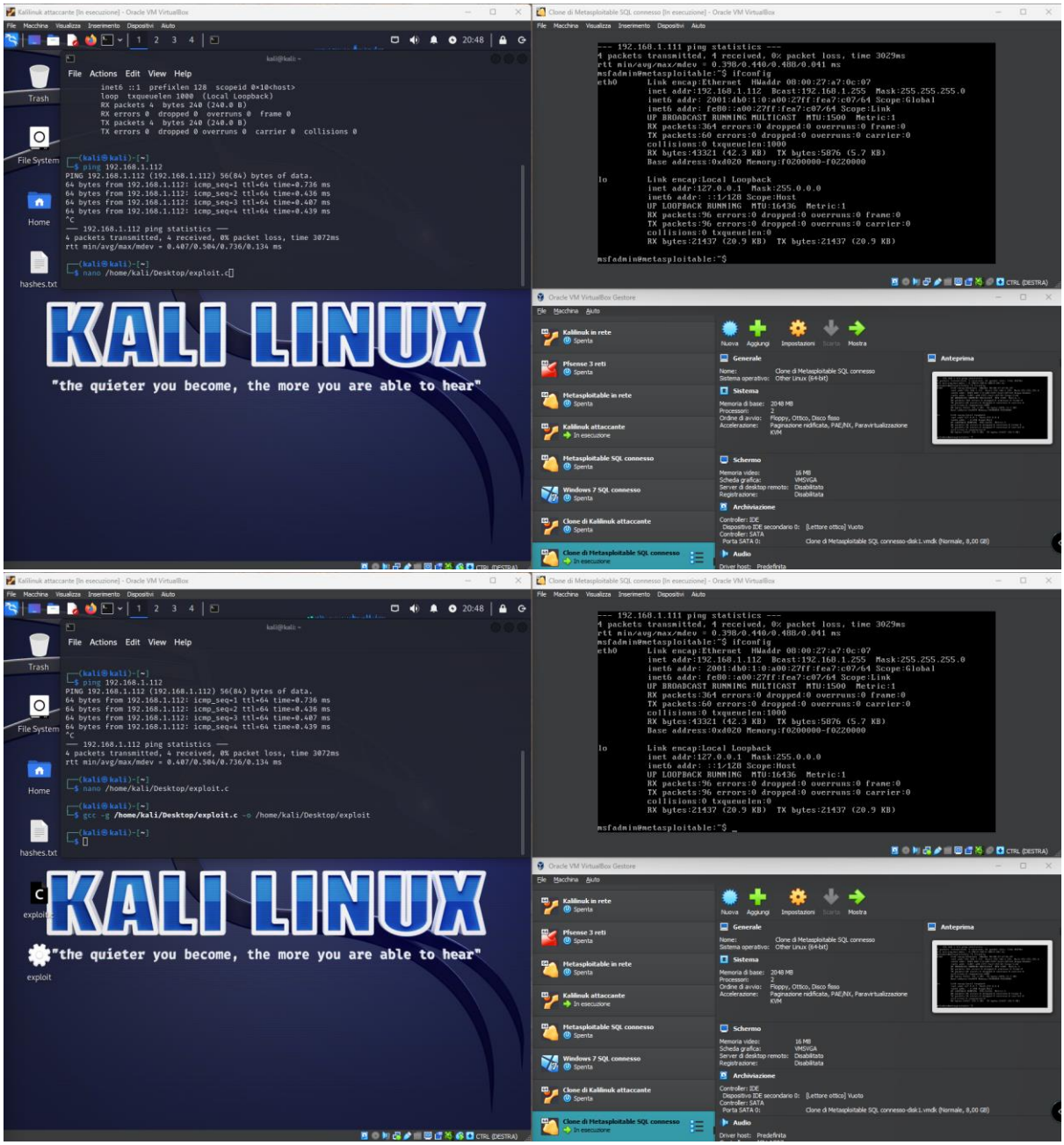
9. **Test dell'Overflow del Buffer** Ho inserito un nome utente di 10 caratteri, ad esempio abcdefghij, per verificare che il programma funzionasse correttamente. Successivamente, ho inserito un nome utente di 40 caratteri abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMN per verificare la presenza di un errore di segmentazione. Come previsto, il programma ha restituito un errore di segmentazione (segmentation fault), indicando che il programma ha tentato di accedere a una porzione di memoria non autorizzata.

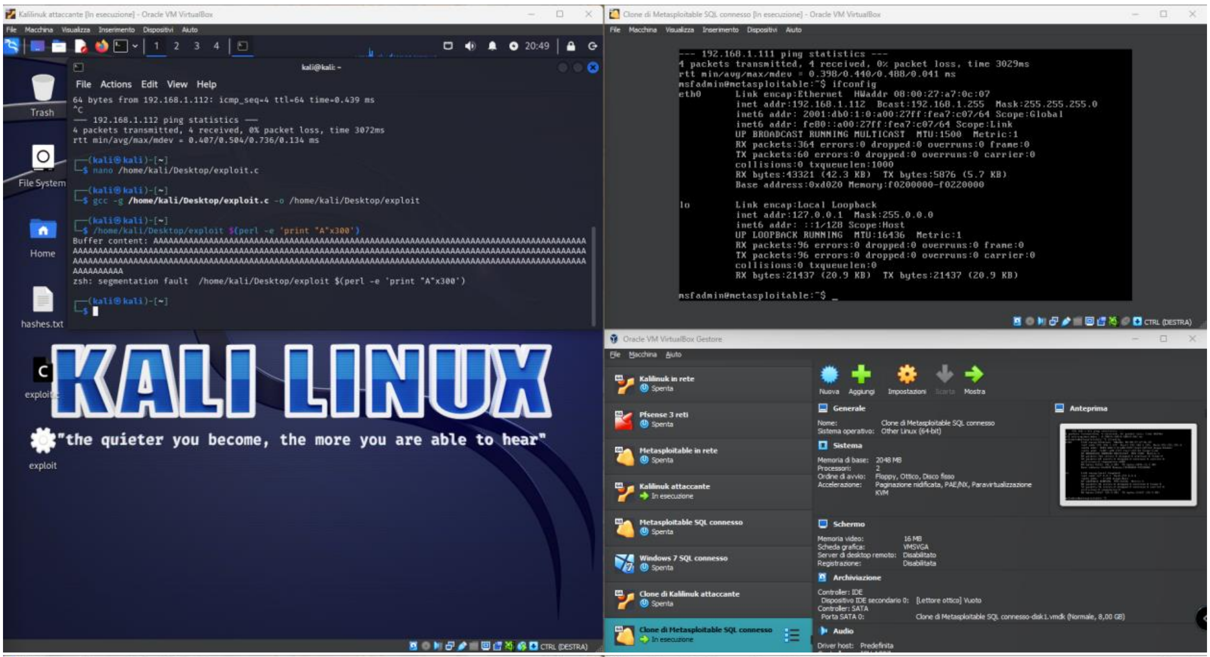
Conclusione

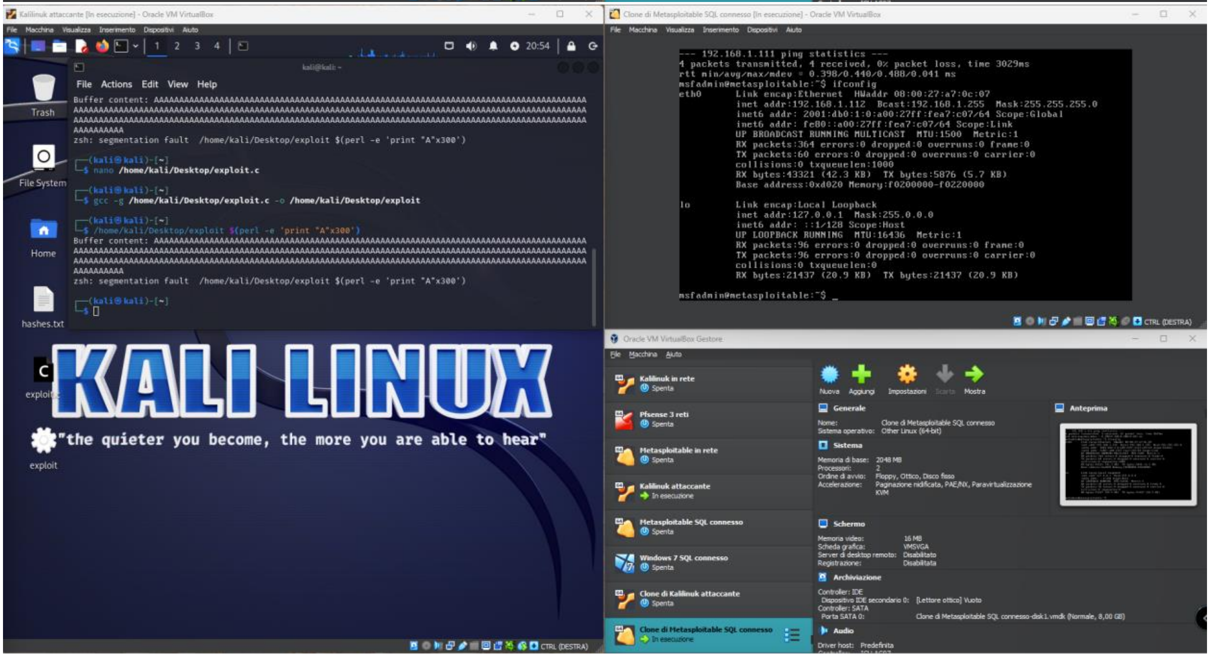
L'esercizio ha dimostrato come un buffer overflow possa causare un errore di segmentazione in un programma C. Aumentando la dimensione del buffer a 30 caratteri, ho potuto osservare come l'inserimento di un input superiore a questa dimensione causasse un errore di segmentazione, fornendo un chiaro esempio di come questa vulnerabilità possa essere sfruttata.

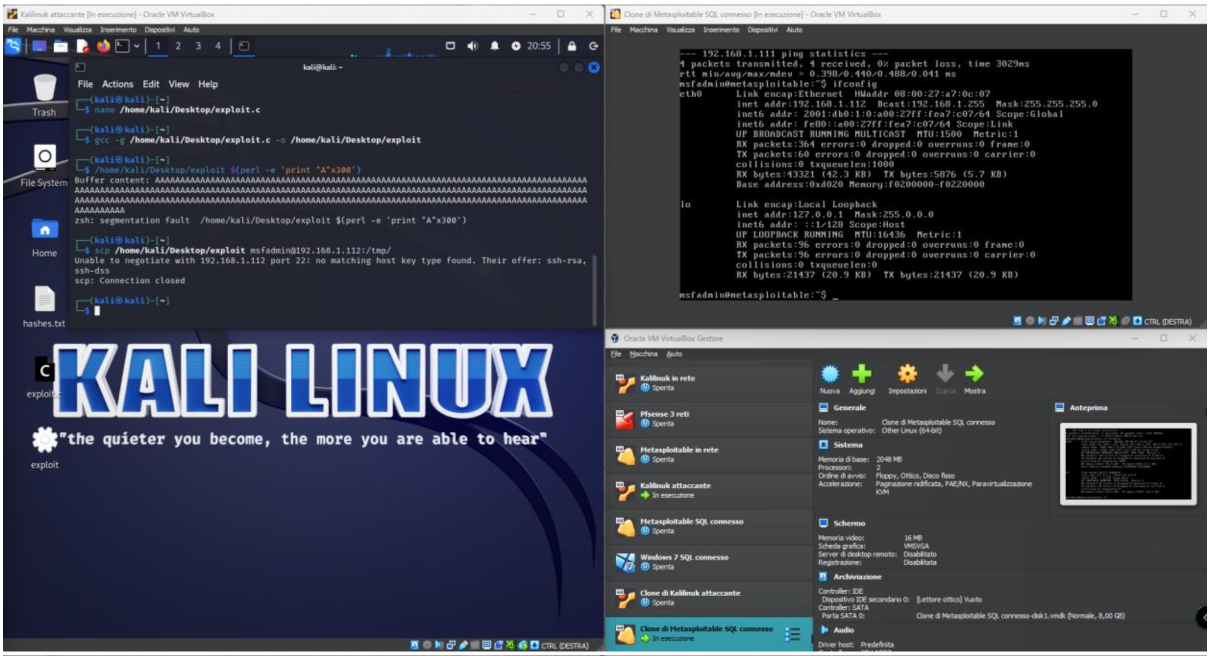
L'esperienza mi ha fornito una comprensione pratica dei concetti di buffer overflow e degli errori di segmentazione, evidenziando l'importanza di implementare adeguati controlli sui limiti dei buffer nei programmi.

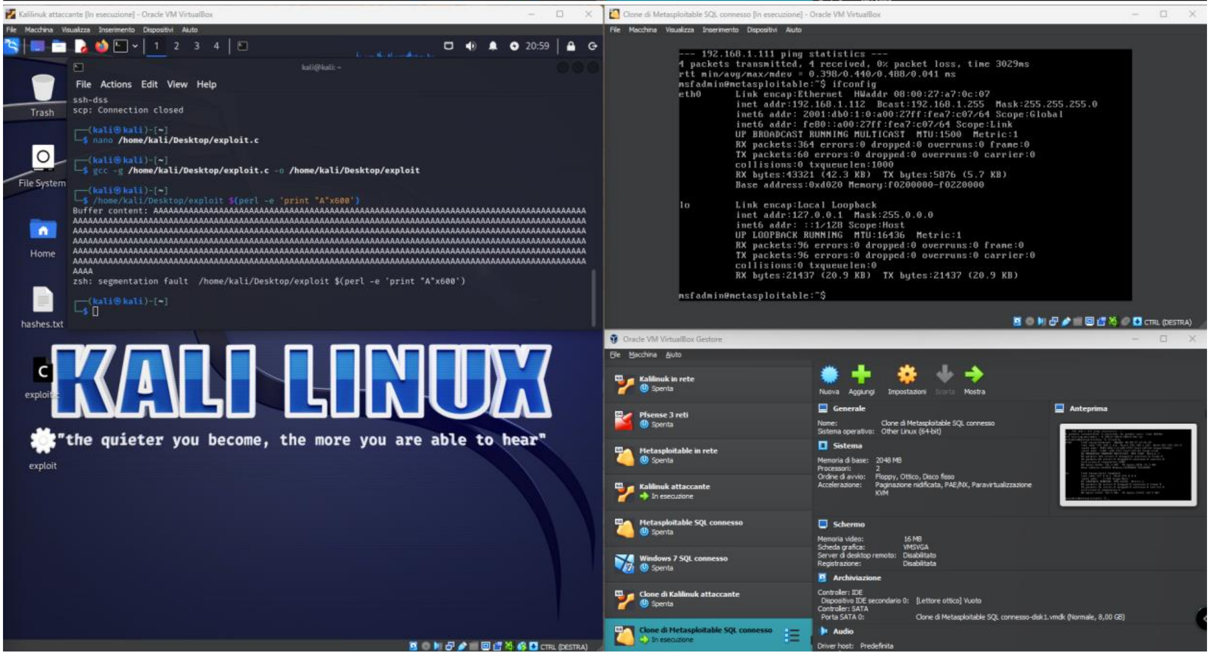
Screenshot


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


Kalilinuk attaccante [In esecuzione] - Oracle VM VirtualBox
kali@kali: ~
64 bytes from 192.168.1.112: icmp_seq=4 ttl=64 time=0.439 ms
^C
— 192.168.1.112 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3072ms
rtt min/avg/max/mdev = 0.407/0.504/0.736/0.134 ms
(kali㉿kali)-[~]
$ nano /home/kali/Desktop/exploit.c
(kali㉿kali)-[~]
$ gcc -g /home/kali/Desktop/exploit.c -o /home/kali/Desktop/exploit
(kali㉿kali)-[~]
$ /home/kali/Desktop/exploit $(perl -e 'print "A"x300')
Buffer content: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAA
zsh: segmentation fault /home/kali/Desktop/exploit $(perl -e 'print "A"x300')
(kali㉿kali)-[~]
$
KALI LINUX
"the quieter you become, the more you are able to hear"
Clone di Metasploitable SQL connesso [In esecuzione] - Oracle VM VirtualBox
--- 192.168.1.111 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3029ms
rtt min/avg/max/mdev = 0.398/0.440/0.488/0.041 ms
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:a7:0c:07
inet addr:192.168.1.112 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: 2001:db0:1:0:a00:27ff:fea7:c07/64 Scope:Global
inet6 addr: fe80::a00:27ff:fea7:c07/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:364 errors:0 dropped:0 overruns:0 frame:0
TX packets:60 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:43321 (42.3 KB) TX bytes:5876 (5.7 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:96 errors:0 dropped:0 overruns:0 frame:0
TX packets:96 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:21437 (20.9 KB) TX bytes:21437 (20.9 KB)
msfadmin@metasploitable:~$ _
Oracle VM VirtualBox Gestore
Kalilinuk in rete
Pfsense 3 reti
Metasploitable in rete
Kalilinuk attaccante
Metasploitable SQL connesso
Windows 7 SQL connesso
Clone di Kalilinuk attaccante
Clone di Metasploitable SQL connesso
Nome: Clone di Metasploitable SQL connesso
Sistema operativo: Other Linux (64-bit)
Memoria di base: 2048 MB


Kalilinuk attaccante [In esecuzione] - Oracle VM VirtualBox
Buffer content: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAA
zsh: segmentation fault /home/kali/Desktop/exploit $(perl -e 'print "A"x300')
(kali㉿kali)-[~]
$ nano /home/kali/Desktop/exploit.c
(kali㉿kali)-[~]
$ gcc -g /home/kali/Desktop/exploit.c -o /home/kali/Desktop/exploit
(kali㉿kali)-[~]
$ /home/kali/Desktop/exploit $(perl -e 'print "A"x300')
Buffer content: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAA
zsh: segmentation fault /home/kali/Desktop/exploit $(perl -e 'print "A"x300')
(kali㉿kali)-[~]
$
KALI LINUX
"the quieter you become, the more you are able to hear"
Clone di Metasploitable SQL connesso [In esecuzione] - Oracle VM VirtualBox
--- 192.168.1.111 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3029ms
rtt min/avg/max/mdev = 0.398/0.440/0.488/0.041 ms
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:a7:0c:07
inet addr:192.168.1.112 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: 2001:db0:1:0:a00:27ff:fea7:c07/64 Scope:Global
inet6 addr: fe80::a00:27ff:fea7:c07/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:364 errors:0 dropped:0 overruns:0 frame:0
TX packets:60 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:43321 (42.3 KB) TX bytes:5876 (5.7 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:96 errors:0 dropped:0 overruns:0 frame:0
TX packets:96 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:21437 (20.9 KB) TX bytes:21437 (20.9 KB)
msfadmin@metasploitable:~$ _
Oracle VM VirtualBox Gestore
Clone di Metasploitable SQL connesso


Kalilinuk attaccante [In esecuzione] - Oracle VM VirtualBox
kali@kali: ~
┌──(kali㉿kali)-[~]
└─$ nano /home/kali/Desktop/exploit.c
┌──(kali㉿kali)-[~]
└─$ gcc -g /home/kali/Desktop/exploit.c -o /home/kali/Desktop/exploit
┌──(kali㉿kali)-[~]
└─$ /home/kali/Desktop/exploit $(perl -e 'print "A"x300')
zsh: segmentation fault /home/kali/Desktop/exploit $(perl -e 'print "A"x300')
┌──(kali㉿kali)-[~]
└─$ scp /home/kali/Desktop/exploit msfadmin@192.168.1.112:/tmp/
Unable to negotiate with 192.168.1.112 port 22: no matching host key type found. Their offer: ssh-rsa, ssh-dss
scp: Connection closed
KALI LINUX
"the quieter you become, the more you are able to hear"
Clone di Metasploitable SQL connesso [In esecuzione] - Oracle VM VirtualBox
--- 192.168.1.111 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3029ms
rtt min/avg/max/mdev = 0.398/0.440/0.488/0.041 ms
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:a7:0c:07
inet addr:192.168.1.112 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: 2001:db0:1:0:a00:27ff:fea7:c07/64 Scope:Global
inet6 addr: fe80::a00:27ff:fea7:c07/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:364 errors:0 dropped:0 overruns:0 frame:0
TX packets:60 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:43321 (42.3 KB) TX bytes:5876 (5.7 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:96 errors:0 dropped:0 overruns:0 frame:0
TX packets:96 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:21437 (20.9 KB) TX bytes:21437 (20.9 KB)
msfadmin@metasploitable:~$
Oracle VM VirtualBox Gestore
Kalilinuk in rete
Pfsense 3 reti
Metasploitable in rete
Kalilinuk attaccante
Metasploitable SQL connesso
Windows 7 SQL connesso
Clone di Kalilinuk attaccante
Clone di Metasploitable SQL connesso


Kalilinuk attaccante [In esecuzione] - Oracle VM VirtualBox
ssh-dss
scp: Connection closed
┌──(kali㉿kali)-[~]
└─$ nano /home/kali/Desktop/exploit.c
┌──(kali㉿kali)-[~]
└─$ gcc -g /home/kali/Desktop/exploit.c -o /home/kali/Desktop/exploit
┌──(kali㉿kali)-[~]
└─$ /home/kali/Desktop/exploit $(perl -e 'print "A"x600')
zsh: segmentation fault /home/kali/Desktop/exploit $(perl -e 'print "A"x600')
KALI LINUX
"the quieter you become, the more you are able to hear"
Clone di Metasploitable SQL connesso [In esecuzione] - Oracle VM VirtualBox
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:a7:0c:07
inet addr:192.168.1.112 Bcast:192.168.1.255 Mask:255.255.255.0
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
msfadmin@metasploitable:~$
Oracle VM VirtualBox Gestore