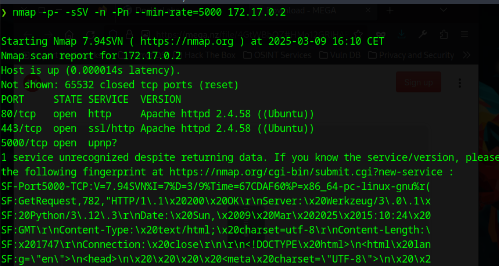
**WriteUp PingPong DockerLabs**



Francisco Javier García

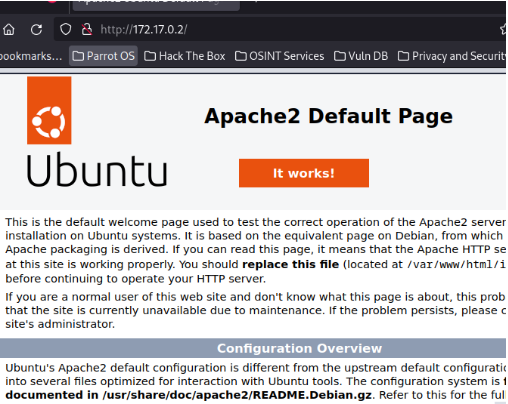
***Acceso al sistema***

Lo primero será escanear la máquina victima para ver que puertos y servicios tiene abiertos:

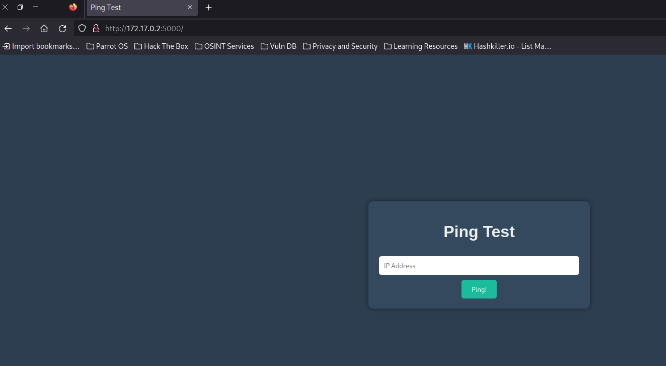


Podemos ver que tiene 3 puertos abiertos (80,443,5000).

Accedemos a los puertos “80” y “443” y nos aparece la default page de Apache:



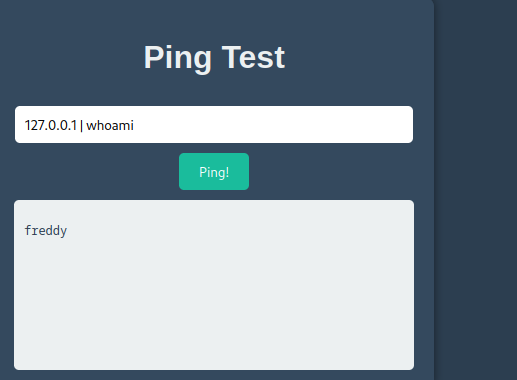
Después de un buen rato haciendo fuzzing y revisando el código fuente, pruebo a conectarme al puerto “5000” que si recordábamos, también lo tenia abierto, y para mi sorpresa puedo ver que es un panel para hacer ping:



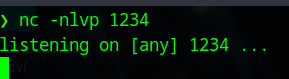
Pruebo a ejecutar el comando “whoami”, pero el servidor lo interpreta dentro del comando “ping -c 4”:



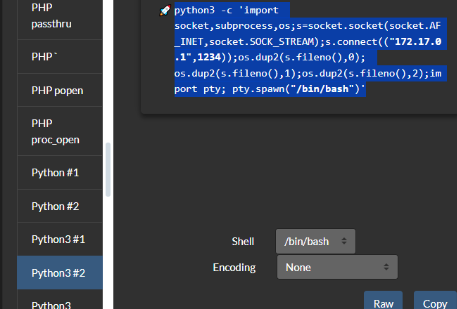
Sin embargo, después de probar un poco, consigo hacer que se ejecute el comando añadiendo un “|” delante de este:



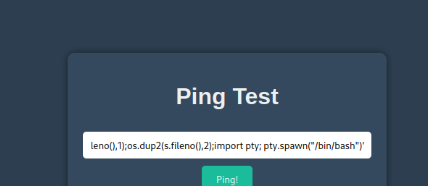
Sabiendo que así puedo hacer un bypass y ejecutar comandos en el servidor, me pondré a escuchar en mi localhost para conseguir una reverse shell:



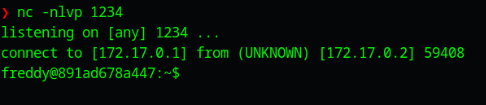
Después me meto en “[https://www.revshells.com](https://www.revshells.com/)” y elijo el payload. En mi caso, he elegido “Python3 #2”:



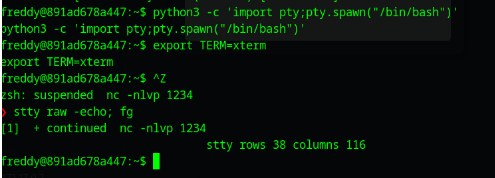
Luego vuelvo al servidor y ejecuto el payload:



Con esto ya tendríamos la reverse shell:



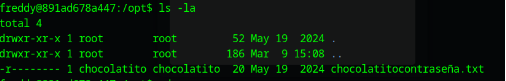
Lo siguiente que haríamos sería establecer una shell interactiva:



Navegando por el sistema, llego a “/opt” y encuentro un fichero llamado “chocolatitocontraseña.txt”:

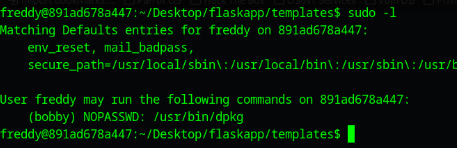


Intento leerlo, pero no puedo. Ya que no tengo permisos y solo puede leerlo el usuario “chocolatito”:



***Escalar privilegios***

Si pongo el comando “sudo -l” veo que puedo ejecutar como el usuario “bobby” el binario “dpkg”:

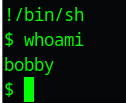


Esto lo puedo aprovechar para conseguir una shell como el usuario “bobby”.

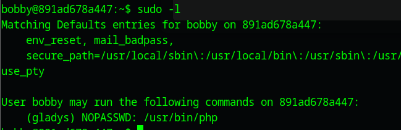
Para hacer eso, me fijo en la pagina “https://gtfobins.github.io”



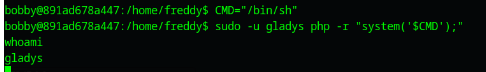
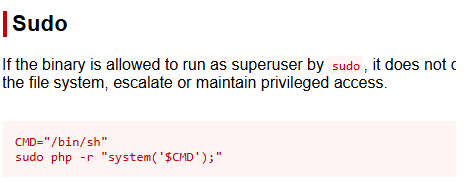
Siguiendo los pasos que aparecen, consigo una shell como el usuario “bobby”:



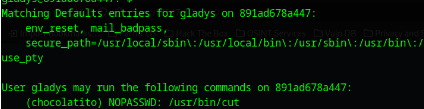
De nuevo, si ponemos “sudo -l” con el usuario bobby, vemos que podemos ejecutar como el usuario “gladys” el binario “php”:



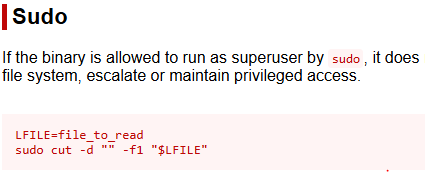
Nos apoyamos de gtfobins de nuevo para conseguir una shell como el usuario gladys:



Si con el usuario gladys, ponemos “sudo -l” podremos ver que podemos ejecutar el binario “cut” como el famoso usuario chocolatito:



Al igual que las otras veces, nos ayudamos de gtfobins :



Como vemos, podemos usar el binario “cut” para leer un fichero. Si recordamos, había un fichero en “/opt” llamado “chocolatitocontraseña.txt”, así que ese será el fichero que leamos:



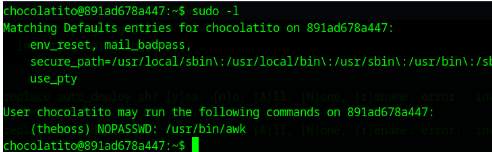
Ya tenemos las credenciales del usuario chocolatito.

“chocolatito:chocolatitopassword”

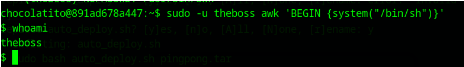
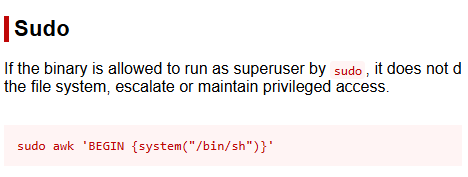
Accedemos a su cuenta con esas credenciales:



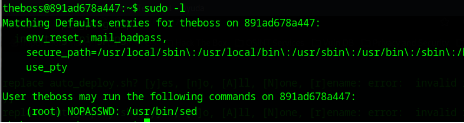
Siguiendo el patrón que teníamos, si ponemos “sudo -l” con el usuario chocolatito, veremos que podemos ejecutar el binario “awk” como el usuario “theboss”:



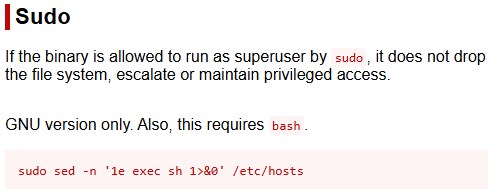
Nos ayudamos de gtfobins para saber como tener una shell con el usuario theboss:



Por ultimo, si con el usuario theboss ponemos el comando “sudo -l”, vemos que podemos ejecutar como root el binario “sed”:



Miramos en gtfobins como escalar privilegios para ser root con este binario:



Y ualah, ya seríamos el usuario root:



Con esto completaríamos la maquina PingPong de DockerLabs.