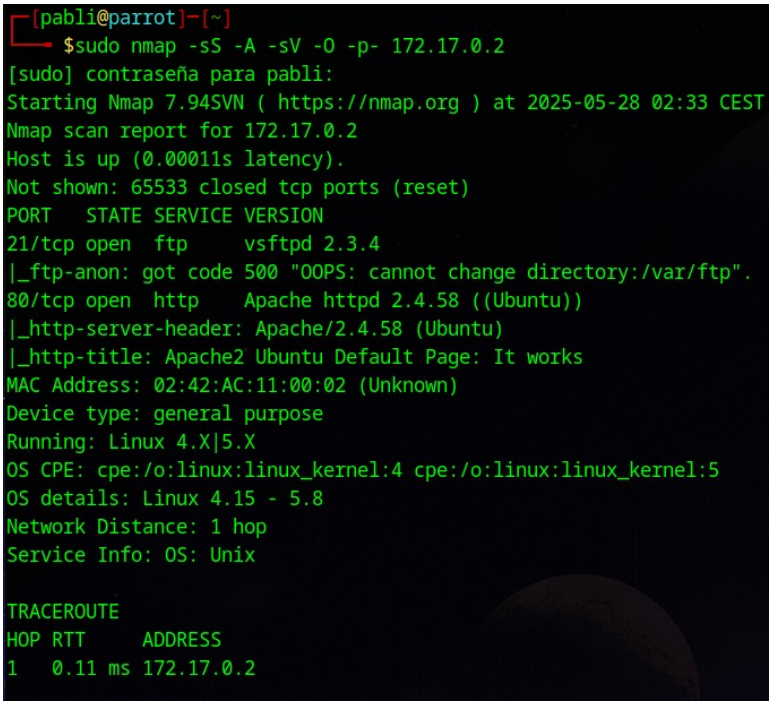
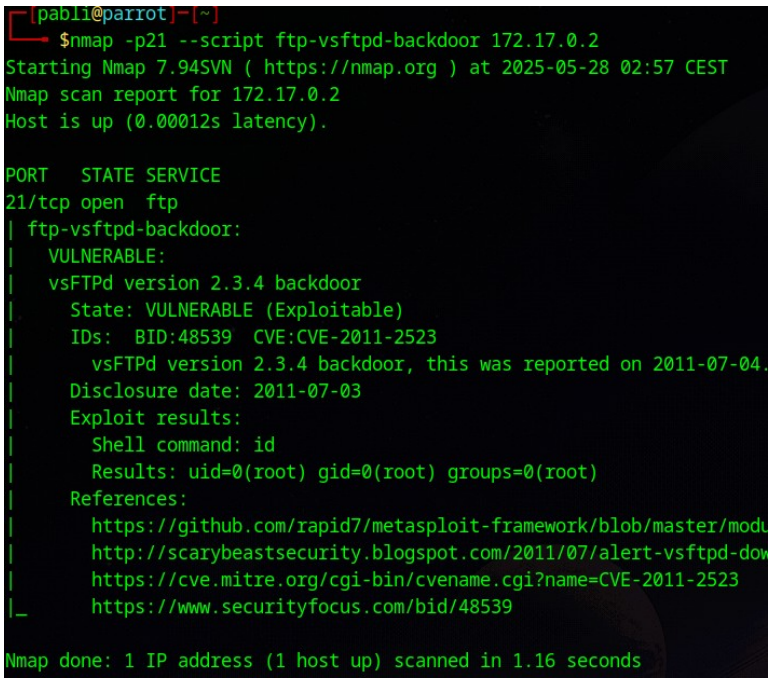
Dockerlabs
Máquina: tproot
Pablo José Pérez Díez

Escaneo inicial:




Observamos que tiene abierto el puerto 21 con FTP lo cual puede ser interesante, por lo tanto, buscamos Scripts NSE de nmap que nos puedan ayudar.

Utilizamos el siguiente Script:



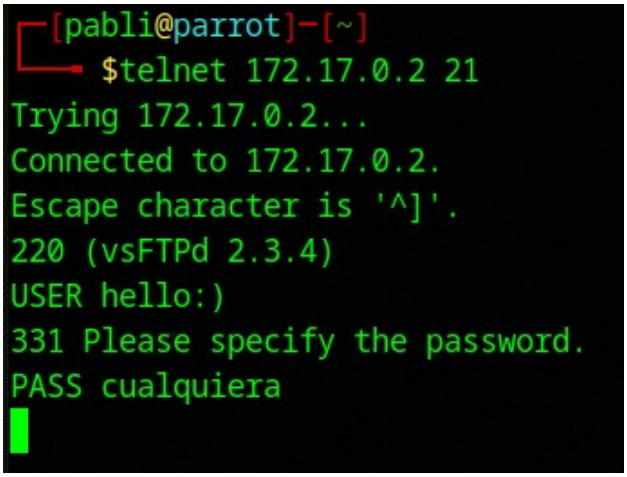
Como podemos ver el script ha explotado exitosamente la vulnerabilidad.
El exploit permite abrir una shell en el puerto 6200/tcp y entrar en el sistema.
Sin embargo, el script solo verifica la vulnerabilidad (ejecutando `id` y mostrando que eres root), pero no mantiene la conexión abierta.

**¿Cómo funciona esta vulnerabilidad?**

vsftpd 2.3.4 (un servidor FTP ) fue comprometido en 2011.
Los atacantes modificaron el código fuente e insertaron una backdoor.
Esta backdoor se activa cuando un usuario ingresa **`:)`** en su nombre.
Sin importar si ese usuario existe o no, asi que se puede usar cualquier nombre de usuario, lo importante es que incluya ":)" al final para activar la backdoor.

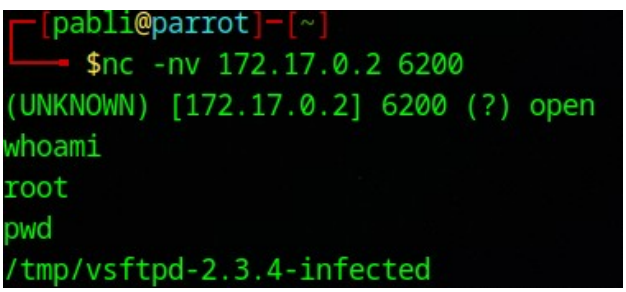
Es decir, se reconoce **`:)`** como trigger y ejecuta una función oculta que abre una shell bind (en el puerto 6200) con permisos de root.

Activamos la backdoor utilizando ":)" al insertar un nombre de usuario:

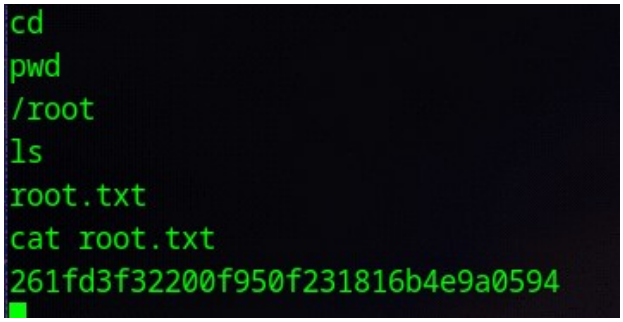



(La backdoor se activa al nivel del protocolo FTP, independientemente de la herramienta.
Por lo que se podría haber utilizado otras distintas, como por ejemplo netcat)

En este momento ya se ha abierto el puerto 6200 como podemos ver.
Nada más realizar la conexión ya tenemos una shell con privilegios de root:



Obtenemos la flag:




Otro ejemplo usando Netcat en vez de telnet: