Lab: Explotación de Vulnerabilidades

Fecha: 22/09/2025 Alumno/a: Facundo Caceres

Objetivo del ejercicio

El objetivo de intrusión al laboratorio facilitado por los profesores fue obtener permisos de administrador por la vulnerabilidad expuesta por el puerto 21 ftp (vsftpd 2.3.4).

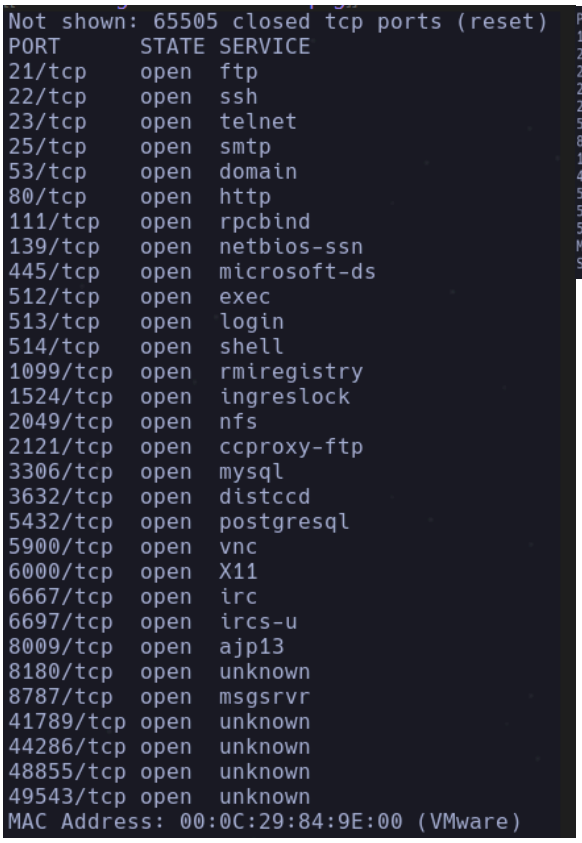
Alcance y reglas

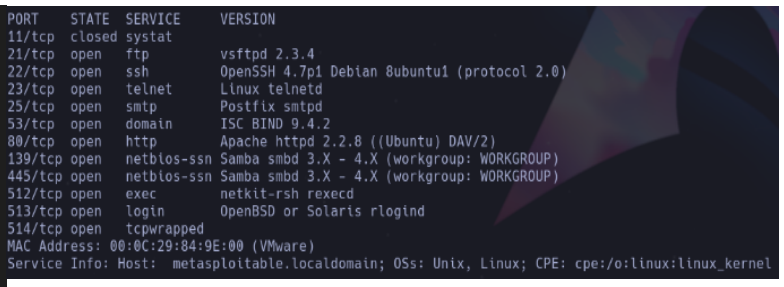
Entorno aislado (host-only/NAT), no atacar hosts fuera del lab, no usar credenciales reales. Indicar IP/host objetivo del laboratorio.

Procedimiento (paso a paso)

Primer paso: Reconocimiento

El primero paso fue un reconocimiento general de la máquina donde utilice un script automatizado de nmap el cual hace un escaneo rápido de todos los puertos(nmap -p- -T4 -n -v $target), en el cual me devuelve solo los puertos abiertos. Al ver que esta máquina presentaba varios puertos abiertos utilice un comando predefinido en el cual me dice que version de servicio corre por los puertos que le específico (nmap -sS -sV -T2 --scan-delay 1s -p $port $target)





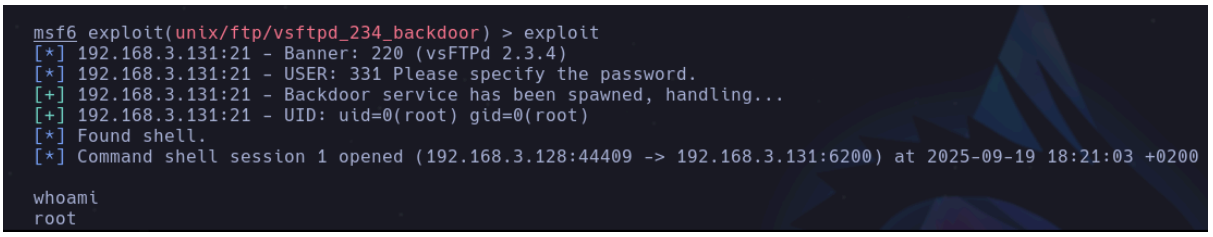
Segundo Paso: Búsqueda de vulnerabilidad

Teniendo en cuenta las versiones de los servicios que corren sobre esta maquina podemos ver que vulnerabilidad tienen, al tener tantos puertos abiertos y con versiones vulnerables me decante por el primer puerto que se nos muestra en el escaneo, el puerto 21 ftp (vsftpd 2.3.4) que presenta una conexión a una shell remota a través de una puerta trasera (backdoor)

Tercer paso: Explotación

Con la herramienta metasploit, podemos vulnerar este sistema medianamente fácil, lo primero que hacemos es abrirlo por consola con el comando msfconsole después buscamos la vulnerabilidad con search vsftpd en cual nos da como respuesta (exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent No VSFTPD v2.3.4 Backdoor Command Execution). Elegimos este exploit con (use exploit/unix/ftp/vsftpd 234 backdoor), después configuramos los parámetros con (set RHOSTS $target y set LPORT 21).

Una vez configurado todo podremos iniciar el exploit y dejar que este haga su trabajo, el comando para esto es (exploit) el cual nos devuelve una shell como el usuario root de la máquina víctima.



Impacto y clasificación

- Confidencialidad (C): ¿Se accede a datos? ¿Cuáles?
- Integridad (I): ¿Se pueden alterar datos o configuraciones?
- Disponibilidad (D): ¿Se degrada o interrumpe el servicio?

Como usuarios root podemos acceder a todos los datos y configuraciones del sistema, también podemos cambiar estas configuraciones y datos del sistema. Si así lo quisiéramos podríamos dejar inservible la máquina víctima por lo cual se considera una vulnerabilidad crítica.

Severidad estimada:Crítica (Baja/Media/Alta/Crítica)

Mitigación propuesta

El parche de actualización se puede descargar desde la página del proveedor.
Buscar una versión más nueva y segura de vsfptd.

Tiempo y obstáculos

Tiempo insumido: 20/30 min | Bloqueos encontrados y cómo los resolviste: Ningún bloqueo o dificultad encontrada, el procesos que más tiempo me llevó fue el reconocimiento pero una vez hecho este reconocimiento fue fácil acceder al sistema.

Reflexión final

Aprendí que al dedicar más tiempo en el reconocimiento puedo obtener un ingreso más facilitado ya que con los exploit y herramientas correctas se hace todo más rápido.
Sobre la máquina víctima lo que se podría hacer es: 1 si obligatoriamente necesita tener todos los puertos que vimos en el reconocimiento abiertos buscaría actualizar todos los servicios que corren por estos puertos, también podremos cambiar de puertos y no usar los predeterminados. 2 si no es obligatorio tener todos estos puertos abiertos cerraría los que no tendría que estar abiertos y también deberían actualizarse.