4Geeks Academy

Explotación de Pentesting en máquina vulnerable

Por: Juan Cervantes Simón

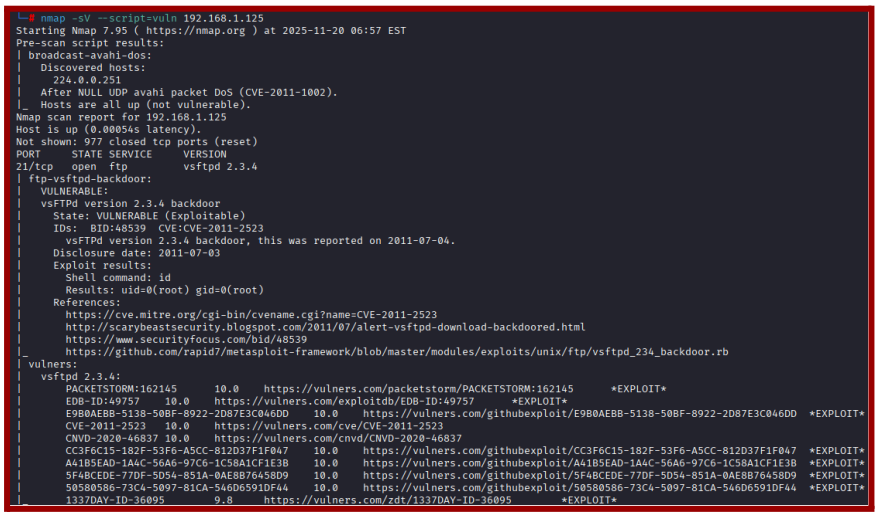
Índice

Resumen del Entorno

En este proyecto, se va a pasar a la explotación de vulnerabilidades por parte de una máquina vulnerable, ***Metasploitable***, con objetivo de descubrir y documentar los puntos débiles de la configuración presente en esta máquina que se aloja en la red local.

Escaneo de servicios

Habiendo identificado la dirección de la máquina metasploitable en anteriores actividades haciendo uso del comando ***nmap -sn 192.168.1.0/24***, ahora se va a disponer a buscar las vulnerabilidades en los servicios expuestos con ayuda del script propio de *nmap*, ***nmap -sV --script=vuln 192.168.1.125***:



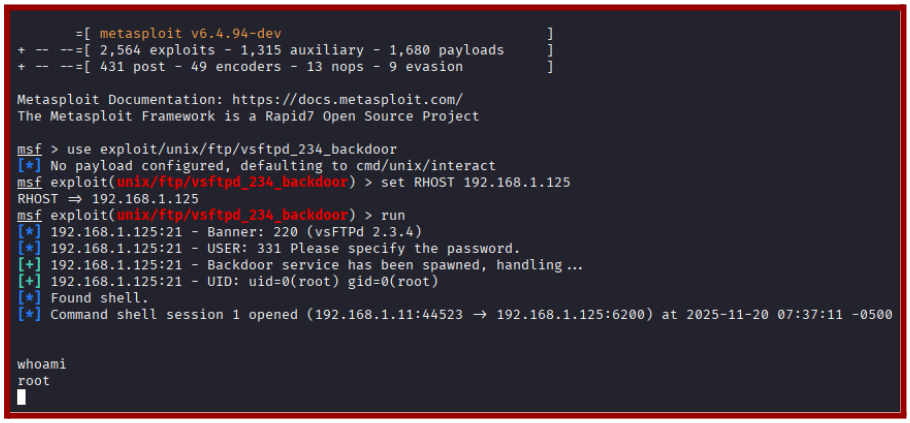
Aun siendo la salida muy extensa se puede apreciar que de las vulnerabilidades más graves se encuentra en el sistema de transferencia de ficheros que tiene la máquina ***FTPd***, y es que hay un exploit disponible que genera una puerta trasera en el sistema, por lo que se va a disponer de este exploit para tratar de conseguir esa puerta trasera.

Enumeración de servicios

Además del servicio **FTP**, también cuenta con **OpenSSH**, **SSLPoodle** y **VNC** como servicios de conexión remota, asimismo también tiene **phpMyAdmin**, para la gestión de base de datos, para las cuales se usa **postgreSQL** y **MySQL** como servicio de Base de Datos.

Vulnerabilidades detectadas y explotación

Siendo que la vulnerabilidad más grave es la puerta trasera encontrada en el servicio **vsFTPd**, por lo que, para usar correctamente el exploit, se va a usar el framework de metasploitable que Kali tiene incorporado, para ello, se accede al framework con el comando **msfconsole**, dentro de este, se selecciona el exploit de puerta trasera con ***use exploit/unix/ftp/vsftpd_234_backdoor***, finalmente para poder ejecutar la vulnerabilidad contra la máquina objetivo, ***set RHOST 192.168.1.125*** para apuntar a la *Metasploitable*, finalmente con ***run***, se ejecutará la vulnerabilidad contra la dirección especificada:



Gracias a esta ejecución, se ha podido iniciar una shell con valores de administración en la máquina objetivo, por lo que esta máquina puede calificarse correctamente como comprometida.

Recomendaciones para mitigación

Como se ha podido confirmar en este caso, esta vulnerabilidad está afectando al sistema porque está operando en una versión desactualizada en el protocolo, por lo que la mayor recomendación en este caso sería actualizar la versión del servicio usado a una más actual, pues se verifica en el CVE recogido para este exploit, que el las actualizaciones sucesivas este error ha sido corregido y no se ha vuelto a manifestar.
Adicionalmente y como buena práctica en lo sucesivo, siempre es recomendable mantener auditorías constantes, puesto que en estas se descubren vulnerabilidades nuevas más rápido, reduciendo el riesgo de explotación de las mismas por parte de terceros.

Conclusión

Con la exploración de esta máquina se ha puesto de manifiesto que, aún teniendo una estructura aparentemente segura, solo es necesario un único servicio vulnerable para comprometer un equipo, del mismo modo también se pone de manifiesto lo fácil que es que este tipo de errores pasen desapercibidos pese a su gravedad