RECONOCIMIENTO DE UNA MÁQUINA VULNERABLE METASPLOITABLE

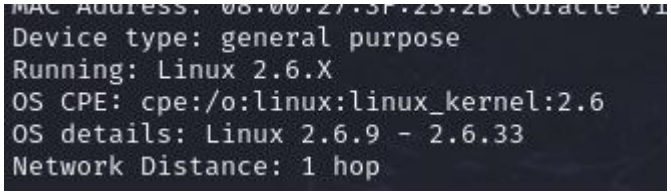
6 DE NOVIEMBRE DE 2024

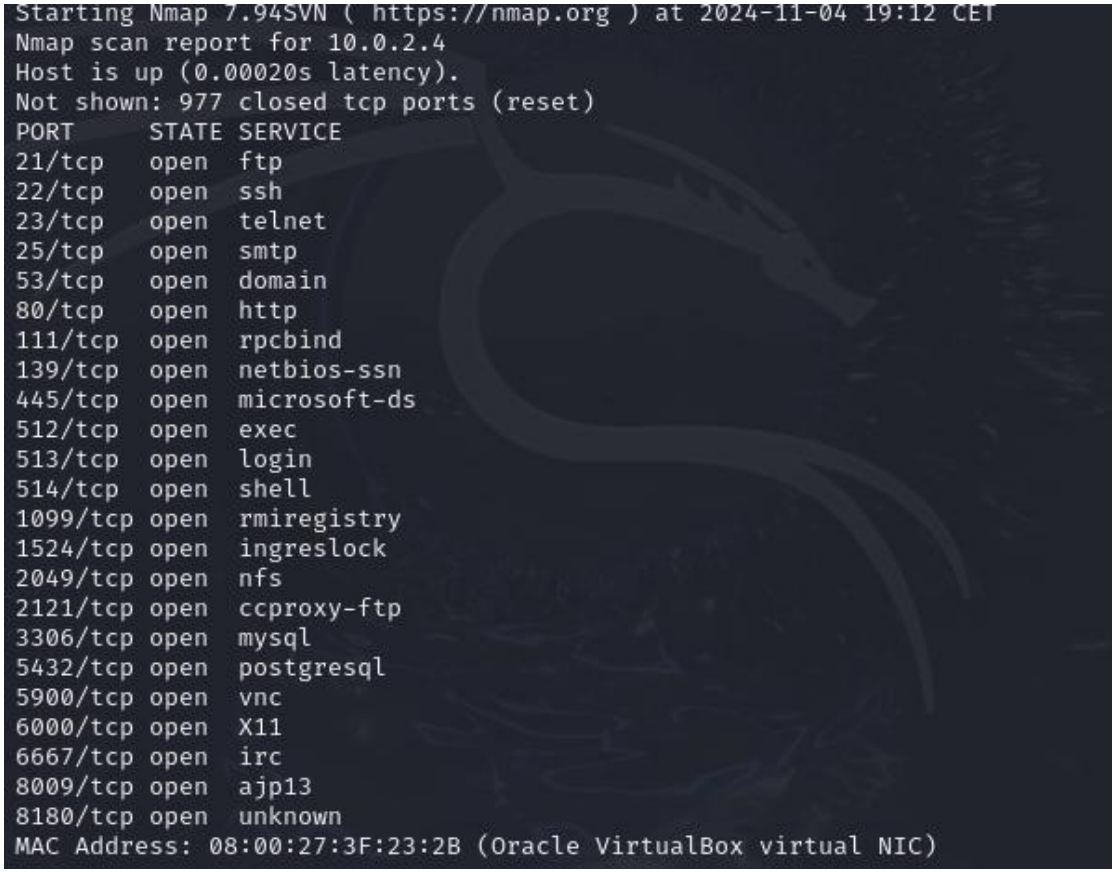
1. Objetivos y alcance

El objetivo de esta auditoría fue realizar un reconocimiento de vulnerabilidades en la maquina con el sistema operativo metasploitable. Se realizaran escaneos de red para buscar la dirección ip objetiva, escaneos sobre versiones y sistemas operativos, enumeración de puertos y servicios del objetivo.

2. Herramientas y técnicas utilizadas

Se utilizara nmap para realizar dicha auditoría. Se utilizó el comando **nmap -sS -sV -O -p- 10.0.2.4** para obtener una lista de puertos,servicios activos y sistema operativo.

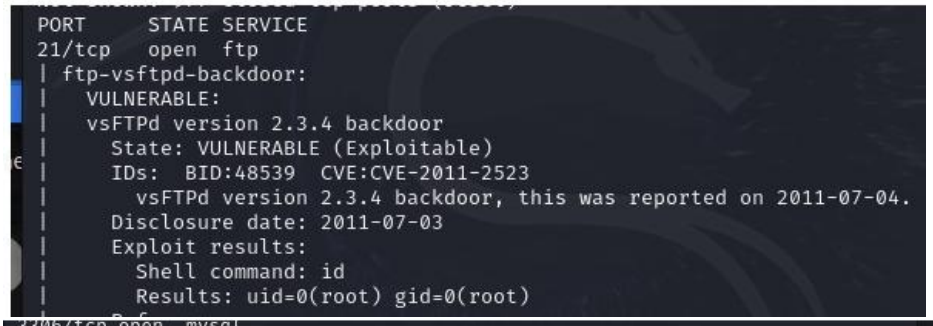


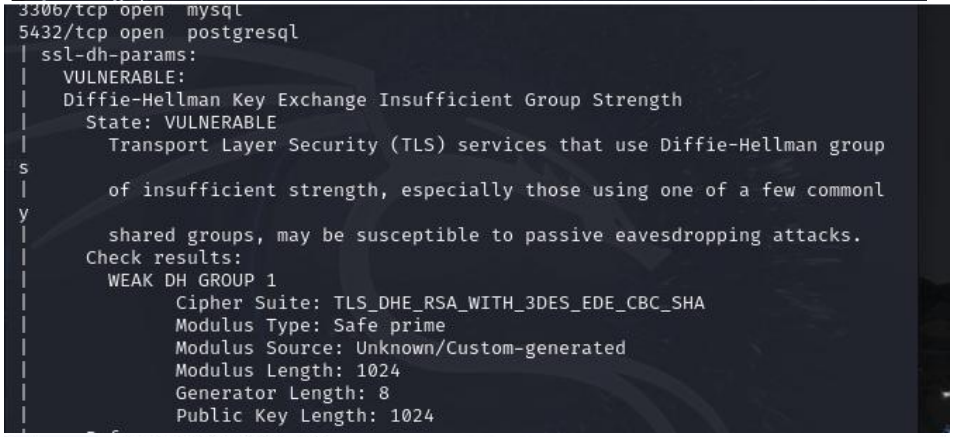


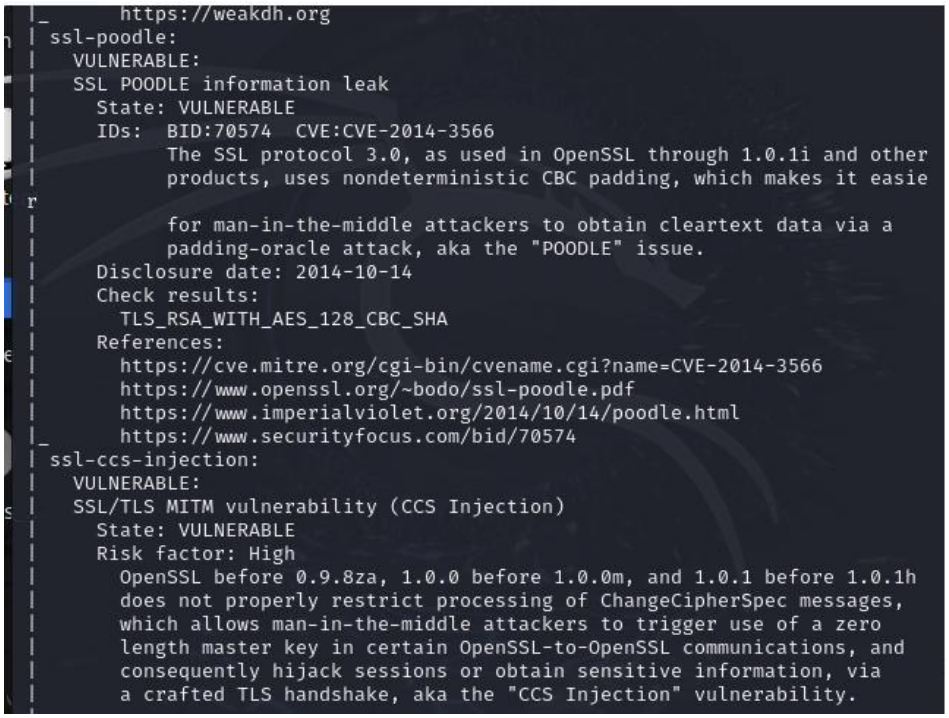
Se obtuvo una lista amplia de los puertos abiertos, sin embargo, no se obtuvieron versiones de los servicios corriendo en dichos puertos. Se detectó el sistema operativo Linux 2.6.9 - 2.6.33, lo cual es una información sensible para que un atacante pueda investigar posibles brechas en el sistema operativo.

3. Resultados de la vulnerabilidades

Para el escaneo de vulnerabilidades se ejecuto el script de nmap de vulnerabilidades comunes, utilizando el siguiente comando **nmap --script vuln -sS -p- 10.0.2.4**







La vulnerabilidad más peligrosa fue la encontrada en el puerto 21/tcp ftp con el CVE-2011-2553 con un riesgo critico(9.8). Esta vulnerabilidad permite que se ejecute una puerta trasera y se abra un shell en el puerto 6200/tcp. Lo cual garantiza acceso total al sistema de forma remota desde el ordenador atacante.

En el sistema pueden haber fugas de información debido a la vulnerabilidad CVE-2014-3566 en el puerto 5432/tcp esta vulnerabiliad en el protocolo SSL 3.0 en el OpenSSL permite que los atacantes realizar un ataque man-in-the-middle para obtener información no cifrada. Tiene un riesgo bajo (3.4) , sin embargo, no hay que ignorarla, la fuga de información puede contener datos sensible que puede llevar a un ataque mas peligroso.

4. Mitigación

Las recomendaciones para la mitigación de posibles ataques recae en mantener siempre los sistemas actualizados a la versiones más actuales. Para evitar una fuga de información através de un ataque de man in the middle se puede desactivar el soporte SSLv3 en las aplicaciones y en los servicios. Asegurar se obtener la versión más reciente de SSL/TLS para mejor encriptación.

La vulnerabilidad critica de ftp 21/tcp backdoor, se puede mitigar por completo actualizando a la versión mas recienten de VSFTPD y así evitar un control total de un usuario no autorizado.