

**INFORME EJECUTIVO – TÉCNICO**

**VULNERABILIDADES DETECTADAS**

**PUERTO 5900**

**SERVICIO VNC - VIRTUAL NETWORK COMPUTING**

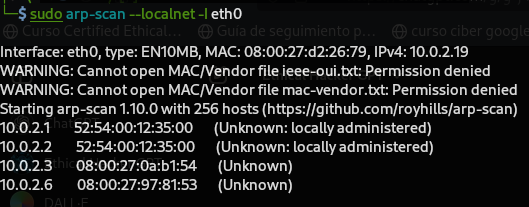
INTRODUCCION

En el presente informe se detalla el proceso llevado a cabo para explotar un servicio VNC () que opera en el puerto 5900 de la máquina objetivo “Metasploitable 2”, utilizándose una serie de herramientas, incluyendo Nmap, Metasploit y vncviewer, para identificar y explotar este servicio, resultando con el acceso completo al sistema con privilegios de root.

FASES DEL PROCESO DE EXPLOTACIÓN

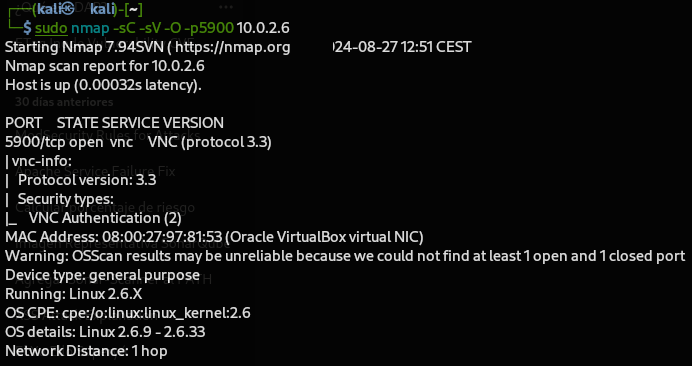
1. Identificación de la Dirección IP de la Máquina Objetivo

* Herramienta Utilizada: arp-scan y nmap
* Descripción: Se utilizaron ambas herramientas para escanear la red y determinar la dirección IP de la máquina objetivo, conocida como Metasploitable 2, siendo un paso es crucial para enfocar los esfuerzos de prueba de penetración en el host correcto.
* Resultado: La dirección IP de la máquina Metasploitable 2 se identificó como 10.0.2.6.



2. Escaneo de Servicios y Puertos Abiertos

* Herramienta Utilizada: nmap y db\_nmap
* Descripción: Después de iniciar una nueva workspace en Metasploit para almacenar y organizar los resultados, se ejecutó db\_nmap para obtener un escaneo detallado de los servicios y puertos abiertos en la máquina objetivo, al igual que se hizo previamente con nmap, identificando el sistema operativo en uso.
* Resultado: Se ha confirmado que el puerto 5900/TCP se encuentra abierto, ejecutando el servicio VNC, siendo un sistema que permite la visualización y control remoto de otro equipo a través de la red, usando el protocolo 3.3, teniendo activada la autenticación por contraseña antes de permitir el acceso remoto. El sistema operativo detectado fue Linux, correspondiente a la máquina Metasploitable 2.



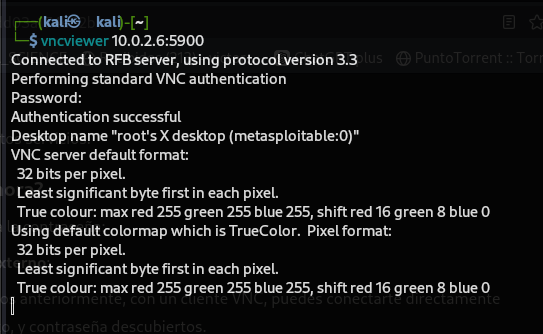
3. Búsqueda de Vulnerabilidades, Exploits Disponibles y Ejecución

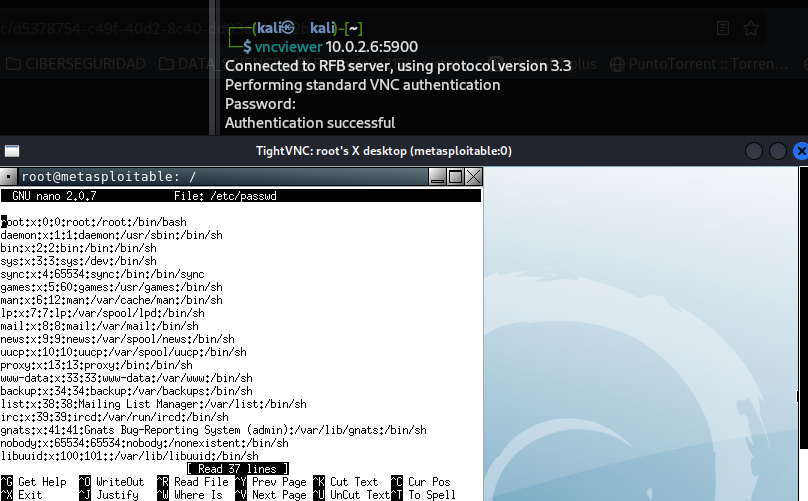
* Herramienta Utilizada: Metasploit
* Descripción: Se ha realizado una búsqueda en la base de datos de Metasploit para identificar cualquier exploit disponible que pudiera ser utilizado contra el servicio VNC en la versión 3.3. Sin embargo, no se encontró ningún exploit directo, pero encontrando un modulo auxiliar para conseguir las credenciales de acceso.
* Resultado: El módulo auxiliar (*vnc\_login*) pudo utilizarse para realizar un ataque de fuerza bruta contra el servicio, usando una lista predeterminada de contraseñas para ello, obteniendo finalmente las credenciales para acceso a la maquina atacada. La contraseña obtenida fue *“password*”, lo que indica una configuración débil y vulnerable.



4. Acceso al Sistema a través de VNC

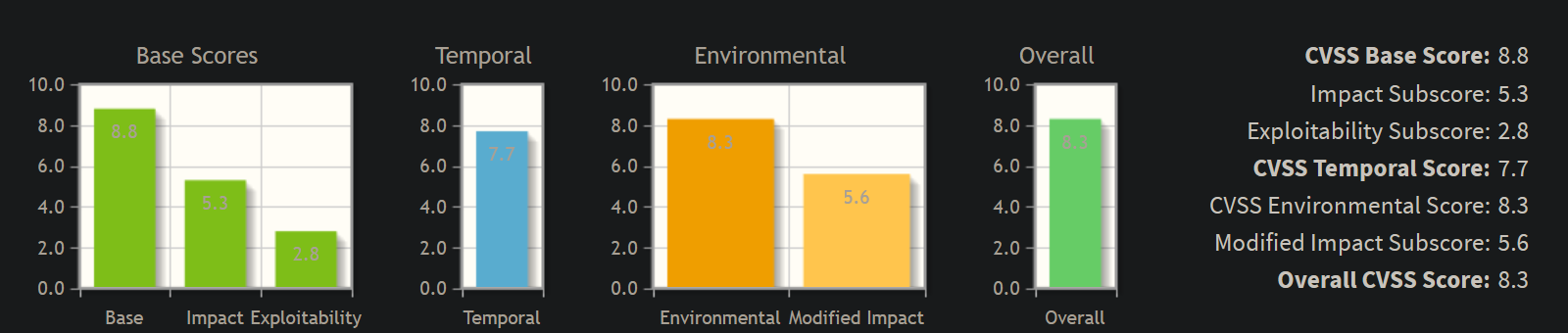
* Herramienta Utilizada: Cliente VNC (vncviewer)
* Descripción: Con la contraseña obtenida, se ha intentado buscar algún módulo de Metaexploit, para poder explotar la vulnerabilidad VNC con la contraseña obtenida con resultado infructuoso. Por ello, se ha utilizado el cliente externo VNC (vncviewer) para conectarse al servicio en la máquina objetivo.
* Resultado: Se ha logrado el acceso pleno al sistema objetivo como usuario root, permitiendo tomar el control total de la máquina.





5. Evaluación de la Vulnerabilidad según el NIST

* Herramienta Utilizada: CVSS (Sistema de Puntuación de Vulnerabilidad Común)
* Descripción: Se ha realizado una evaluación preliminar de la severidad de la vulnerabilidad explotada la calculadora del sistema CVSS del NIST.
* Resultado: La vulnerabilidad se ha evaluado con una puntuación aproximada de 8.3, lo que indica un alto riesgo debido a la facilidad con la que se pudo comprometer el sistema y la gravedad de las consecuencias.



CONCLUSIÓN

La identificación, explotación y análisis de esta vulnerabilidad resalta la importancia de una configuración adecuada y la necesidad de actualizar los servicios para evitar este tipo de compromisos en el sistema “Metaexploitable 2”. Además, la puntuación CVSS de 8.3 subraya la gravedad de la vulnerabilidad, confirmando que un atacante con acceso similar podría comprometer completamente el sistema, con graves consecuencias para la confidencialidad, integridad y disponibilidad de la red.

Este informe concluye que la máquina objetivo presenta vulnerabilidades críticas que deben ser abordadas de inmediato mediante la implementación de mejores prácticas de seguridad, incluyendo la actualización de software, el uso de contraseñas seguras y el cierre de puertos innecesarios.