CYBER CRAFT

CYBERSECURITY SOLUTIONS

REPORTE TÉCNICO DE AUDITORIA DE SEGURIDAD

18 de abril de 2024

- Este informe técnico presenta un ejemplo simulado de evaluación de vulnerabilidades en un sistema informático, aplicado a una organización ficticia. Es importante destacar que este documento no debe ser considerado como una evaluación real ni debe ser utilizado para tomar decisiones operativas en entornos reales.

Consideraciones para el presente documento:

- **Propósito del informe:** El propósito de este documento es exclusivamente educativo, destinado a brindar a los estudiantes una comprensión práctica de los procesos de evaluación de vulnerabilidades en sistemas informáticos. Se enfoca en ilustrar técnicas, herramientas, y procedimientos empleados en este tipo de análisis, con el objetivo de fortalecer las habilidades y conocimientos en ciberseguridad.

- **Ámbito de aplicación**: Es importante mencionar que las vulnerabilidades y riesgos presentados en este informe son completamente ficticios y han sido diseñados con el único propósito de facilitar el aprendizaje y la práctica en un entorno controlado. Estos escenarios se pueden descargar, o utilizar en distintas plataformas.

- **Advertencia de uso**: Se advierte contra la utilización de este informe para cualquier propósito distinto al educativo mencionado anteriormente, No se debe intentar aplicar las técnicas, herramientas o información, expuesta en este documento en sistemas reales sin la supervisión y la autorización correspondiente de profesionales de ciberseguridad calificados.

- **Responsabilidad**: El autor de este informe no asume ninguna responsabilidad por el uso indebido o inapropiado de la información contenida en el mismo. Se insta a los lectores a utilizar este documento de manera ética y responsable.

Índice de contenido

Índice de Figuras

1. Objetivo

El propósito fundamental de la presente auditoría en el sistema MEOW es identificar y analizar exhaustivamente posibles puntos de vulnerabilidad. La meta primordial radica en la detección precisa de brechas en la seguridad informática que puedan comprometer la integridad, confidencialidad o disponibilidad de los datos y recursos del sistema MEOW.

Para lograr este cometido, se emplearán metodologías y herramientas especializadas con el fin de evaluar la robustez de las medidas de seguridad implementadas. Una vez recopilada la información pertinente sobre las vulnerabilidades potenciales, se proporcionará al equipo técnico un informe detallado que incluirá recomendaciones específicas para corregir las deficiencias detectadas. Este informe servirá como guía para la implementación de acciones correctivas, con el objetivo de fortalecer la postura de seguridad del sistema MEOW y mitigar los riesgos identificados.

2. Alcance

Esta auditoría se restringe a la ejecución de pruebas de intrusión exclusivamente en el segmento de red asignado, utilizando la conexión VPN proporcionada por HTB. El enfoque se centra específicamente en evaluar la seguridad del servicio Telnet. Es importante destacar que cualquier otra vulnerabilidad o riesgo de seguridad que no esté relacionado con este servicio no será abordado durante esta fase de prueba.

3. Metodología

La metodología utilizada se presenta en la Figura 3.1, la cual muestra las fases de la prueba. Es importante destacar, que no se realizó ninguna corrección o nueva implementación del sistema.

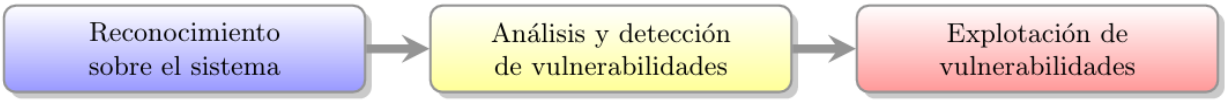

Figura 3.1 Metodología utilizada. Fuente [1]

3.1. Reconocimiento

El reconocimiento del equipo se llevó a cabo mediante una técnica TRACE-ICMP, como se muestra en la Figura 3.2, la cual sugiere que existe una alta probabilidad de que el sistema operativo ejecutado por el equipo objetivo esté basado en el kernel de Linux. Esta inferencia se deriva del valor TTL (Time to Live), el cual coincide con los parámetros típicos asociados a sistemas Linux.

```
┌─[us-starting-point-1-dhcp]─[10.10.15.25]─[isulgm@htb-
fjlytpfwta]─[~/Desktop/maquinas]
└──╼ [★]$ ping -c 1 10.129.87.30
PING 10.129.87.30 (10.129.87.30) 56(84) bytes of data.
64 bytes from 10.129.87.30: icmp_seq=1 ttl=63 time=8.35 ms

--- 10.129.87.30 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 8.350/8.350/8.350/0.000 ms
┌─[us-starting-point-1-dhcp]─[10.10.15.25]─[isulgm@htb-
fjlytpfwta]─[~/Desktop/maquinas]
└──╼ [★]$
```

Figura 3.2 TRACE ICMP desde el equipo del Analista. Fuente: Elaboración propia

3.2. Enumeración

La enumeración de los servicios y puertos se realizo mediante el escaneo de puertos con la herramienta NMAP, como se muestra en la Figura 3.3.

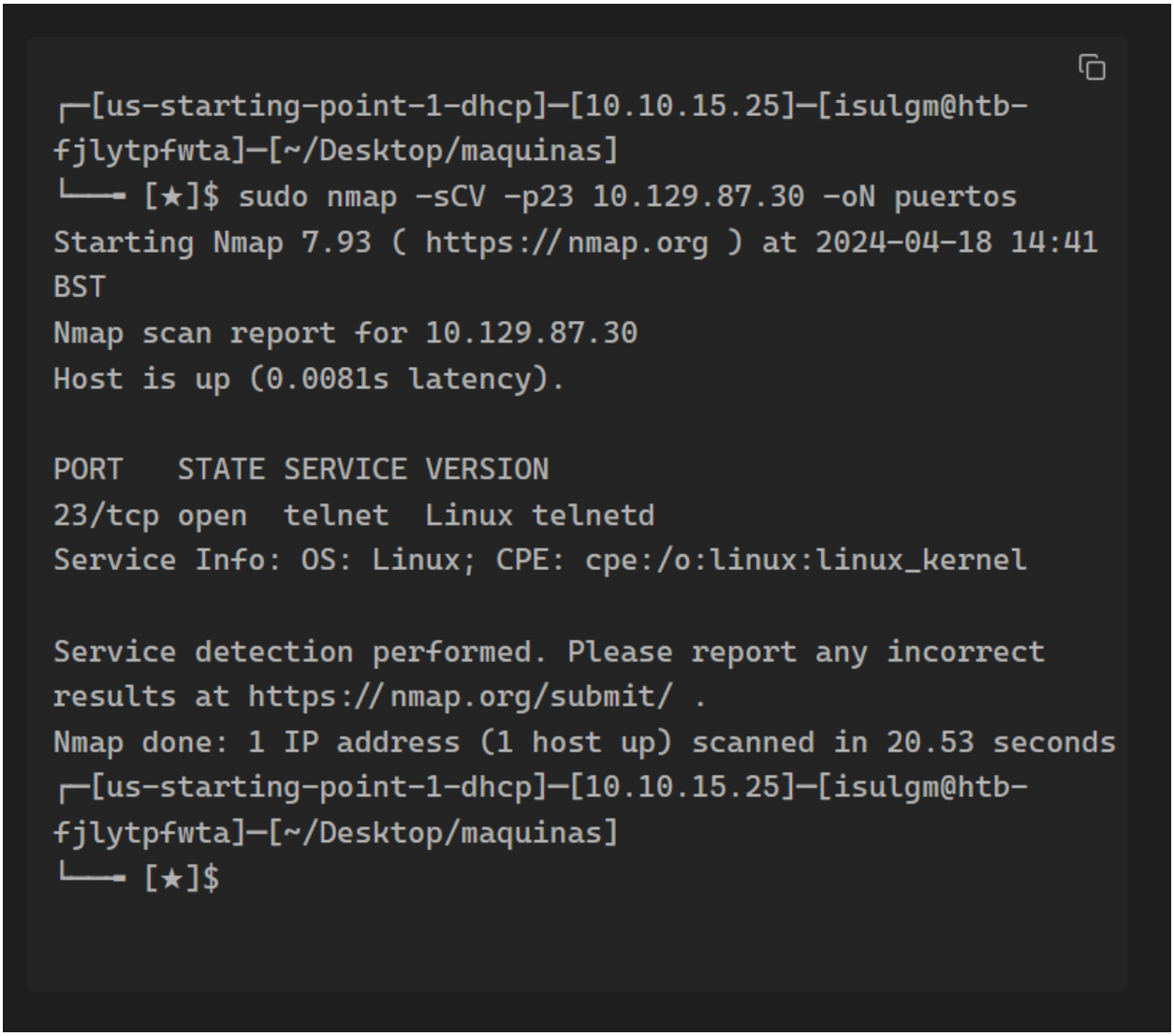

Figura 3.3 Escaneo con la herramienta NMAP. Fuente: Elaboración propia

Se detectaron posibles vulnerabilidades en el puerto 23, mediante el protocolo TCP, ejecutando el servicio TELNET.

3.3. Explotación

Para llevar a cabo la explotación de la vulnerabilidad, se realizó una exhaustiva investigación preliminar. Durante este proceso, se decidió probar con credenciales estándar de instalación en el área de autenticación del servicio Telnet desde la estación de trabajo del analista, como se ilustra en la Figura 3.4.

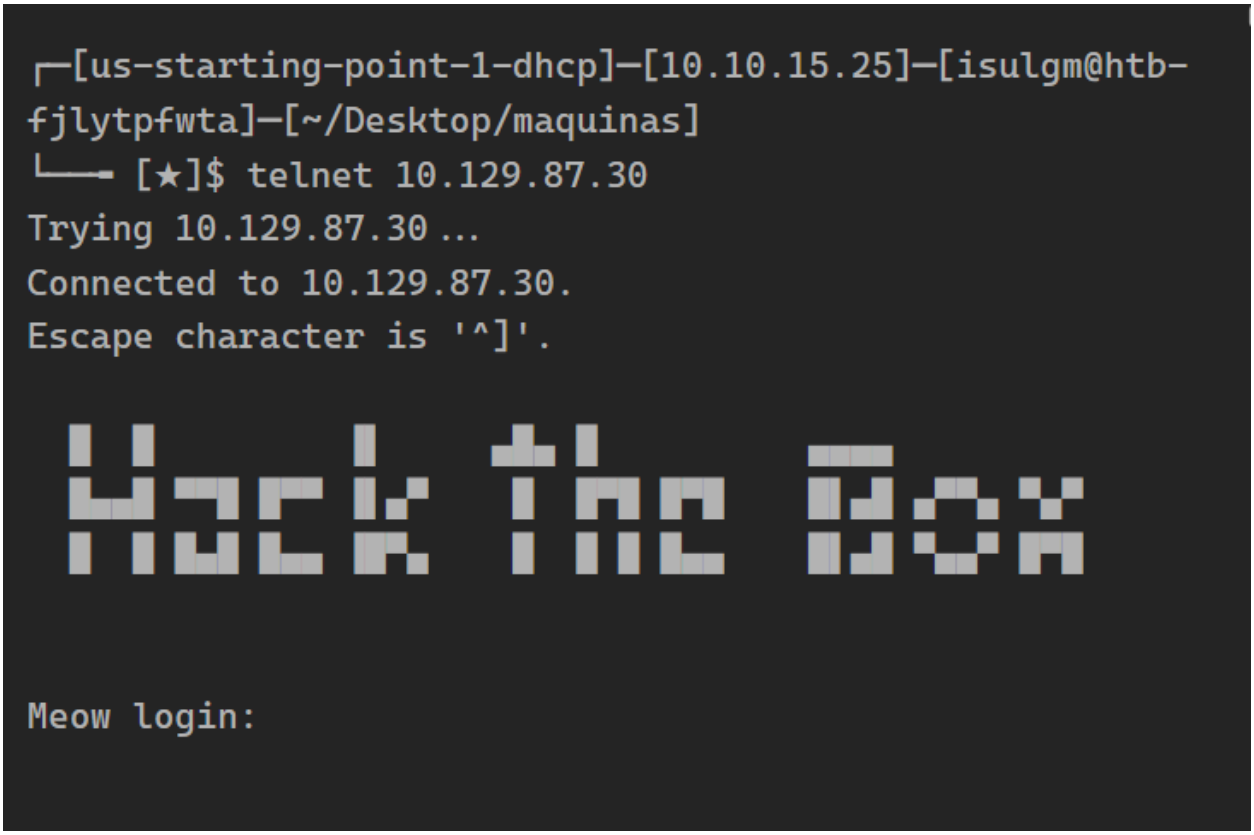

Figura 3.4 Login del servicio Telnet. Fuente: Elaboración propia

Las credenciales probadas fueron:

- Admin
- Adminstrator
- Meow
- Root

La contraseña que auténtico el servicio telnet, fue **ROOT**, lo que indica una vulnerabilidad critica para la organización.

3.4. Post-Explotación

Para está practica de auditoría, no se realizó una post explotación que requiera persistencia del equipo objetivo.

4. Recomendaciones

Con base en los hallazgos y análisis realizados, se emiten las siguientes recomendaciones dirigidas al equipo de sistemas, tecnologías de la información (TI) y responsables de los activos digitales:

- **Fortalecimiento de la Autenticación en el Servicio Telnet**: Se insta a configurar el servicio Telnet con medidas de autenticación más sólidas. Se sugiere emplear métodos de autenticación multifactoriales o certificados digitales para agregar capas adicionales de seguridad y mitigar los riesgos asociados con el acceso no autorizado.
- **Implementación de Políticas de Seguridad Rigurosas**: Se recomienda establecer políticas de seguridad claras y exhaustivas que regulen el acceso y la gestión de los servicios y recursos digitales. Estas políticas deben abordar aspectos como contraseñas seguras, controles de acceso basados en roles y monitoreo continuo de la actividad del sistema para detectar posibles intrusiones.
- **Actualizaciones y Parches de Seguridad**: Es esencial mantener actualizados todos los sistemas y aplicaciones, incluido el servicio Telnet, con los últimos parches de seguridad disponibles. Esto ayudará a cerrar posibles brechas de seguridad conocidas y garantizar la protección continua contra amenazas emergentes.
- **Capacitación y Concientización del Personal**: Se recomienda proporcionar capacitación periódica sobre buenas prácticas de seguridad informática al personal involucrado en la administración y el uso de los sistemas y servicios digitales. Esto incluye la importancia de utilizar contraseñas seguras, identificar y reportar posibles incidentes de seguridad, y seguir los procedimientos adecuados para mitigar riesgos.
- **Evaluación Regular de la Postura de Seguridad**: Se sugiere realizar evaluaciones periódicas de la seguridad de los sistemas y activos digitales para identificar y abordar proactivamente posibles vulnerabilidades. Esto puede incluir pruebas de penetración, auditorías de seguridad y análisis de riesgos para garantizar la robustez y la resiliencia del entorno digital.

Implementar estas recomendaciones ayudará a fortalecer la postura de seguridad de la infraestructura digital y mitigar los riesgos asociados con posibles vulnerabilidades en el servicio Telnet y otros activos críticos.

Conclusiones

La auditoría del sistema MEOW dentro de la infraestructura de la empresa HACK THE BOX representó un paso fundamental en la evaluación de la seguridad de la red. La conexión segura mediante VPN permitió llevar a cabo un análisis exhaustivo que abarcó desde el reconocimiento inicial del equipo y la red hasta el escaneo detallado y la enumeración de activos digitales.

Durante el proceso, se identificaron diversos puntos críticos que requieren atención inmediata. Específicamente, se determinó que el puerto 23, utilizado para el servicio Telnet, presenta un nivel de vulnerabilidad significativo debido a la ausencia de medidas de autenticación robustas. Esta vulnerabilidad potencial representa una brecha importante en la seguridad del sistema MEOW y, por extensión, en la integridad y confidencialidad de los datos alojados en la red.

Es crucial destacar que la detección de esta vulnerabilidad subraya la importancia de implementar medidas proactivas de seguridad, tales como autenticación multifactorial y políticas de acceso restrictivas, para mitigar riesgos y fortalecer la defensa contra posibles amenazas cibernéticas.

Además, este proceso de auditoría no solo identificó problemas específicos, sino que también resaltó la necesidad continua de realizar evaluaciones regulares de seguridad y de mantener actualizadas las defensas cibernéticas en un entorno en constante evolución.

Referencias

[1] Lugo S. (2024). Introducción al Ethical Hacking utilizando HTB.