Capacidades Tecnicas, Legales y de Gestion Para Equipos Blue Team y Red Team

Cristian Alexander Vega Camacho

Asesor

Ever Luis Arroyo Baron

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Basicas, Tecnologia e Ingenieria - ECBTI

Especialización en Seguridad Informática

2024

Resumen

CyberFort Technologies es una organización líder en servicios de consultoría y asesoría en ciberseguridad, dirigida tanto a empresas del sector privado como a entidades gubernamentales. Tiene como objetivo formar equipos especializados de Blue Team y Red Team, con el propósito de fortalecer su postura de seguridad de su infraestructura tecnológica y mejorar su reputación en el mercado frente a sus clientes. Recientemente, la empresa llevó a cabo exhaustivas pruebas de pentesting en uno de sus activos de información más críticos, logrando identificar varias vulnerabilidades en un equipo que alberga una aplicación de gran valor estratégico para la organización. A partir de este análisis detallado, se formularon recomendaciones de seguridad específicas para mitigar los riesgos detectados y robustecer la infraestructura tecnológica.

Además, CyberFort Technologies desarrolló un conjunto integral de propuestas para la implementación de un sistema de contención y respuesta a incidentes informáticos. Estas propuestas incluyen la instalación de un firewall de última generación, la implementación de un sistema de detección y prevención de intrusiones (IDS/IPS), y la adopción de una plataforma de orquestación, automatización y respuesta de seguridad (SOAR). También se diseñaron metodologías eficaces para garantizar la protección continua de todos los activos de información. Todas estas actividades se llevaron a cabo en estricto cumplimiento de la legislación vigente y las normas relacionadas con la protección de datos personales, asegurando además el comportamiento ético de los profesionales que integran los equipos de Red Team y Blue Team en CyberFort Technologies.

***Palabras clave*:** firewall, Red Team, Blue Team, vulnerabilidades

Abstract

CyberFort Technologies is a leading organization in cybersecurity consulting and advisory services, targeting both private sector companies and government entities. Its goal is to build specialized Blue Team and Red Team units, aimed at strengthening the security posture of their technological infrastructure and improving their market reputation with clients. Recently, the company conducted extensive pentesting on one of its most critical information assets, successfully identifying several vulnerabilities in a system hosting an application of high strategic value to the organization. Following this detailed analysis, specific security recommendations were made to mitigate the identified risks and strengthen the technological infrastructure.

In addition, CyberFort Technologies developed a comprehensive set of proposals for the implementation of a containment and incident response system. These proposals include the installation of a next-generation firewall, the implementation of an Intrusion Detection and Prevention System (IDS/IPS), and the adoption of a Security Orchestration, Automation, and Response (SOAR) platform. Effective methodologies were also designed to ensure the continuous protection of all information assets. All these activities were carried out in strict compliance with current legislation and regulations related to personal data protection, while also ensuring the ethical conduct of the professionals who comprise the Red Team and Blue Team at CyberFort Technologies.

***Keywords*:** firewall, Red Team, Blue Team, vulnerabilities

Table of Contents

Lista de Tablas

Lista de Figuras

GLOSARIO

Backdoor: Es un malware elaborado para eludir las medidas de seguridad y poder acceder a un sistema, red o aplicación.

Blue Team: Es un grupo de expertos en ciberseguridad encargados de defender la infraestructura de una organización frente a los riesgos cibernéticos.

Dominio: Es un nombre único que identifica a un sitio web o una red en Internet.

Exploit: Es un programa o código que aprovecha una vulnerabilidad en un sistema, aplicación o red para realizar acciones no autorizadas.

Intrusión: Es un acceso no autorizado a un sistema, red o aplicación, generalmente con la intención de robar, alterar o destruir datos, o interrumpir el funcionamiento normal del sistema.

IP: (Protocolo de Internet) es una dirección única asignada a cada dispositivo conectado a una red que utiliza el Protocolo de Internet para comunicarse.

Meterpreter: Es una herramienta avanzada de post-explotación que forma parte del framework Metasploit. Se utiliza para interactuar con sistemas comprometidos, permitiendo a los atacantes ejecutar comandos.

Pentesting: Es un proceso en el que se simulan ataques cibernéticos controlados contra un sistema, red o aplicación para identificar y explotar vulnerabilidades.

Puerto: Es un punto de comunicación virtual que permite a los dispositivos y aplicaciones intercambiar datos a través de una red.

Ransomware: Es un tipo de malware que cifra los archivos de una víctima, bloqueando el acceso a ellos.

Red Team: Es un grupo de expertos en ciberseguridad que simula ataques reales para identificar y explotar vulnerabilidades en la infraestructura de una organización.

Shell: Es una interfaz que permite a los usuarios interactuar con el sistema operativo. Puede ser una interfaz de línea de comandos (CLI).

Vulnerabilidad: Es una debilidad o falla en un sistema, aplicación, red o proceso que puede ser explotada por atacantes para comprometer la seguridad.

Introducción

La conformación de equipos de Blue Team y Red Team es crucial para fortalecer la ciberseguridad en las organizaciones. Los equipos de Blue Team se encargan de la defensa, monitoreando y protegiendo los sistemas contra ataques cibernéticos. Su objetivo es detectar, responder y mitigar amenazas en tiempo real. Por otro lado, los equipos de Red Team simulan ataques reales para identificar vulnerabilidades y evaluar la efectividad de las defensas del Blue Team.

Esta dinámica de ataque y defensa permite a las organizaciones mejorar continuamente sus estrategias de seguridad, identificar puntos débiles y desarrollar respuestas más efectivas ante incidentes. La colaboración entre Blue Team y Red Team es esencial para crear un entorno de ciberseguridad robusto y resiliente.

En el siguiente informe se presentará un análisis detallado de las pruebas de intrusión realizadas para la organización CyberFort Technologies como también de las recomendaciones de seguridad propuestas para mitigar los riesgos cibernéticos identificados y las estrategias de seguridad enfocadas a prevenir futuros incidentes cibernéticos.

Objetivos

Objetivo General

Elaborar un informe técnico detallado para la organización CyberFort Technologies, con el propósito de establecer los resultados de las pruebas de pentesting realizadas y las recomendaciones de seguridad elaboradas para mitigar los riesgos cibernéticos.

Objetivos Específicos

Analizar y explicar los resultados de la prueba de pentesting realizada a la organización CyberFort Technologies.

Establecer recomendaciones y estrategias de seguridad enfocadas a fortalecer la seguridad de la infraestructura tecnológica.

Formular las conclusiones, posterior a las actividades realizadas previamente.

ANALISIS LEGAL CYBERFORT TECHNOLOGIES – ACUERDO DE CONFIDENCIALIDAD

Este informe inicial tiene como propósito informar a la gerencia de CyberFort Technologies sobre las irregularidades encontradas en el acuerdo de confidencialidad elaborado por el abogado de la empresa. Se han identificado varias cláusulas que presentan aspectos no éticos y/o ilegales, las cuales se detallan a continuación.

Cláusula Primera: La cláusula que menciona "La información confidencial o sobre procesos ilegales dentro de CyberFort Technologies" fomenta el encubrimiento de actividades ilícitas, lo cual es contrario a los deberes éticos de un profesional en ingeniería.

Cláusula Segunda (Definición de información confidencial): Incluir actividades ilegales como "datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos" dentro de la definición de información confidencial es problemático, ya que estas actividades no pueden ser protegidas por un acuerdo de confidencialidad.

Cláusula Cuarta (Puntos 3, 4 y 9) – Obligaciones de la parte Receptora: Está cláusula prohíbe denunciar cualquier actividad sospechosa de espionaje o apropiación de información, lo cual es problemático. Según las leyes en Colombia, cualquier persona tiene el deber de reportar actividades ilegales a las autoridades competentes.

Cláusula Octava – Solución de Controversias: La cláusula que establece que "En caso de que la información ilegal o confidencial sea encontrada en manos del receptor, este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a CyberFort Technologies" exime a la empresa de cualquier responsabilidad legal, lo cual no es legalmente válido.

Artículos de la Ley 1273 Vulnerados

Artículo 269ª: Acceso abusivo a un sistema informático: La ejecución de actividades ilegales como el acceso indebido a sistemas informáticos vulnera este artículo[1]. La cláusula primera fomenta el encubrimiento de estos accesos no autorizados.

Artículo 269H: Circunstancias de agravación punitiva: Incentivar el encubrimiento de actos ilegales puede agravar las penas debido a las circunstancias que genera el incumplimiento del artículo 269ª.

Artículo 269C: Interceptación de datos informáticos: La definición de información confidencial que incluye "datos de chuzadas, interceptación de información" vulnera directamente este artículo.

[1] Policía. (2009). Ley 1273 [LEY_1273_2009].Policía. (pp. 1-4). https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos

Artículo 269F: Violación de datos personales: La prohibición de denunciar actividades ilegales atenta contra la apropiación de información confidencial[2] y puede generar sanciones y penas de prisión.

Las irregularidades detectadas en el acuerdo de confidencialidad de CyberFort Technologies representan un riesgo legal y ético significativo. Se recomienda revisar y modificar las cláusulas mencionadas para alinearlas con las legislaciones vigentes y los principios éticos profesionales.

EJERCICIO DE RED TEAM EJECUTADO

Debido a una fuga de información detectada en uno de los equipos de CyberFort Technologies, se llevó a cabo una prueba de pentesting para identificar la vulnerabilidad asociada con una de las aplicaciones instaladas en un sistema Windows. Esta prueba se realizó siguiendo las fases y metodologías establecidas por diversos marcos de trabajo en pentesting. A continuación, se presentan los resultados obtenidos en cada fase del proceso.

Fase de Reconocimiento y Análisis de Vulnerabilidades

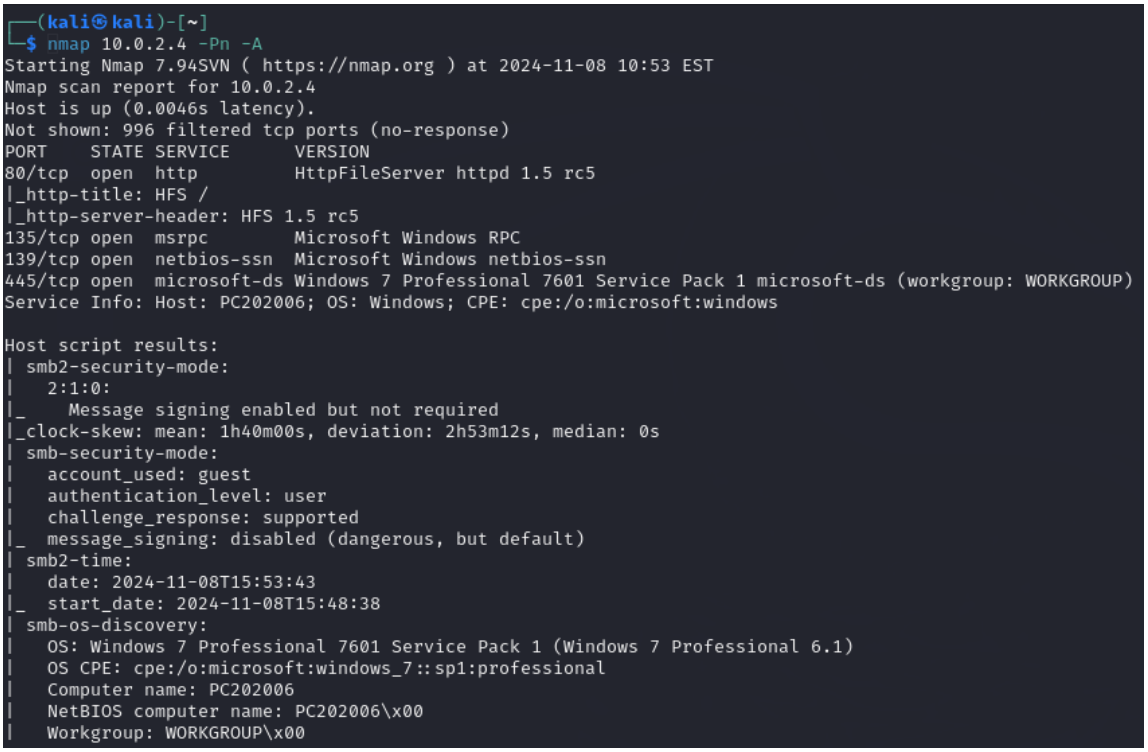
En la primera fase, se realizó un reconocimiento del equipo y un análisis de vulnerabilidades. Utilizando la herramienta nmap, se escaneó toda la red y se identificó la IP del

[2] Gobierno Digital. (2022). Decreto 338. https://gobiernodigital.mintic.gov.co/692/articles-238198_recurso_1.pdf

equipo Windows 7 (10.0.2.4). Se ejecutó el comando nmap 10.0.2.4 -Pn -A para identificar puertos y servicios abiertos, así como posibles vulnerabilidades[3]. Los resultados mostraron puertos abiertos: 135/tcp, 139/tcp, 445/tcp y 80/tcp. Se detectó una vulnerabilidad crítica en el puerto 445 (SMB), referenciada como "MS17-010", y varias vulnerabilidades en el puerto 80 (HTTP) asociadas a CVE-2007-6750 y CVE-2011-3192. Ver Figura 1.

Figura. 1

Escaneo de puertos



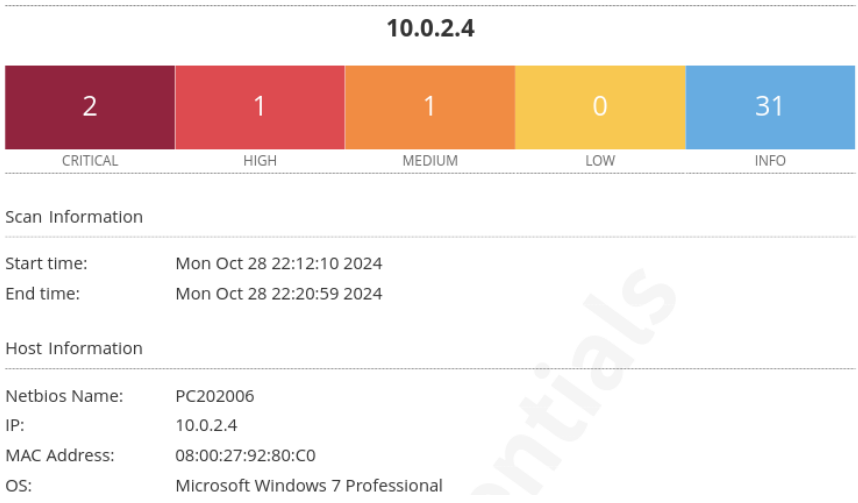
Fuente. Autoria Propia.

[3] Gerick Toro.(2008). Guía de referencia de Nmap. pp 1-49. Manual-de-uso-de-Nmap.pdf (riseup.net)

Para un análisis más detallado, se utilizó la herramienta Nessus, que identificó 2 vulnerabilidades críticas, 2 de alta categoría, 1 de baja categoría y 31 con información relacionada con el host. Entre las vulnerabilidades críticas, se destacó nuevamente la MS17-010 y fallas de seguridad en el protocolo HTTP del puerto 80. Ver figura 2.

Figura. 2

Reporte Nessus



Fuente. Autoria Propia

En la siguiente tabla se enumeran los puertos abiertos en el host, protocolos, servicios asociados y las vulnerabilidades identificadas en estos puertos.

Tabla 1

Vulnerabilidades identificadas.

Puerto	Servicio	Vulnerabilidad	CVE Asociado
135 /TCP	RPC	No detectada	No detectada
139 /TCP	NetBIOS	No detectada	No detectada
445 /TCP	SMBv1	smb-ms17-010 (Eternalblue, Wannacry, petya, eternalrocks)	CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE 2017-0148
80/TCP	HTTP (HFS)	DoS, Ejecución remota de comandos RCE	CVE-2007-6750 y CVE-2011-3192

Fase de Explotación

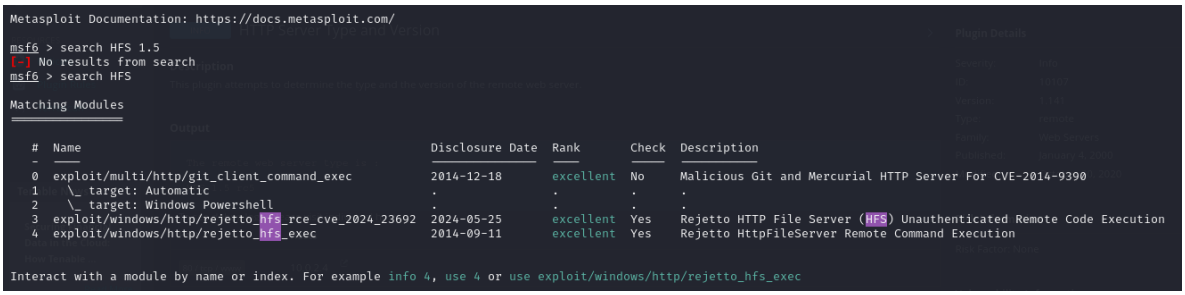
Explotación de la Vulnerabilidad HFS Rejetto (HTTP File Server): Se utilizó Metasploit para buscar y configurar el exploit apropiado para la aplicación HFS Rejetto (versión 1.5) en el puerto 80. Se identificaron dos exploits:

- ***exploit/windows/http/rejetto_hfs_rce_cve_2024_23692***
- ***exploit/windows/http/rejetto_hfs_exec***.

En la siguiente figura se ilustra los exploits identificados para la aplicación hfs, haciendo uso de la herramienta metasploit con el parámetro search

Figura. 3

Exploits Hfs



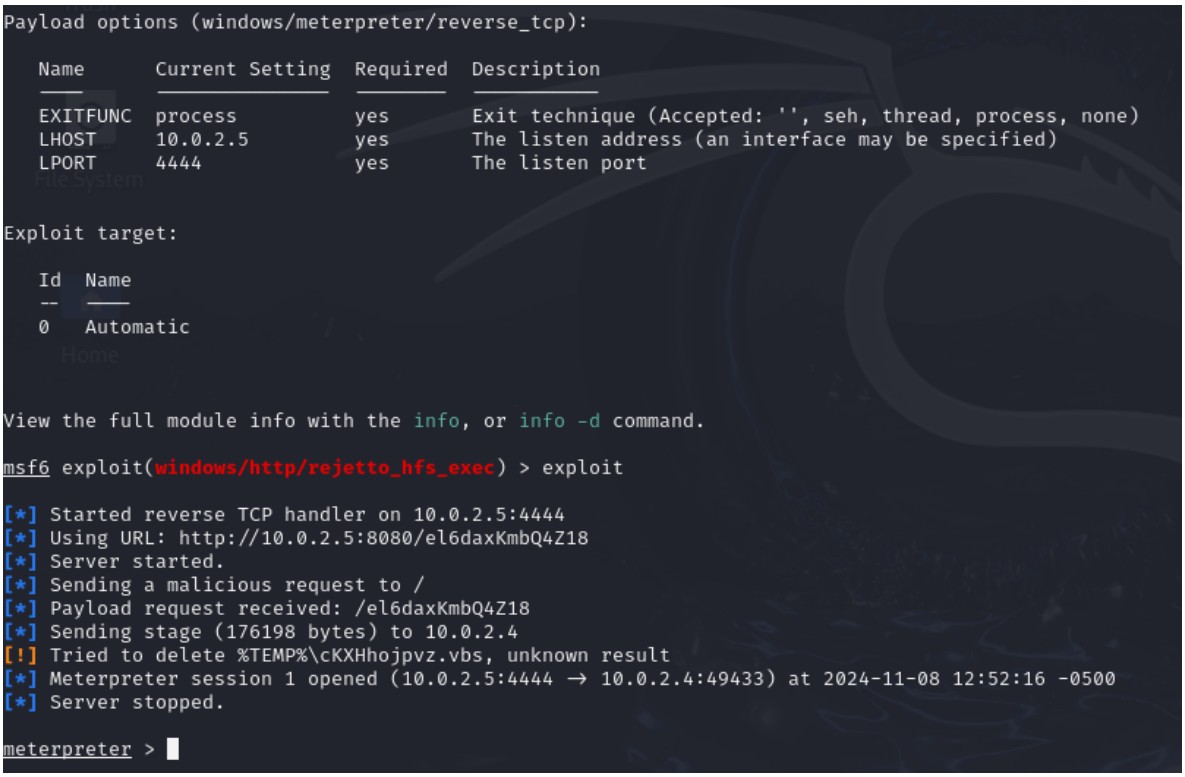
Fuente. Autoria Propia

Se configuró y ejecutó el exploit, logrando establecer una sesión remota mediante meterpreter y escalando privilegios para crear un usuario administrador[4]. Ver Figura 4.

[4] Guillén Zafra, J. L. (2017). Introducción al pentesting. https://diposit.ub.edu/dspace/handle/2445/124085

Figura. 4

Explotacion vulneranbilidad

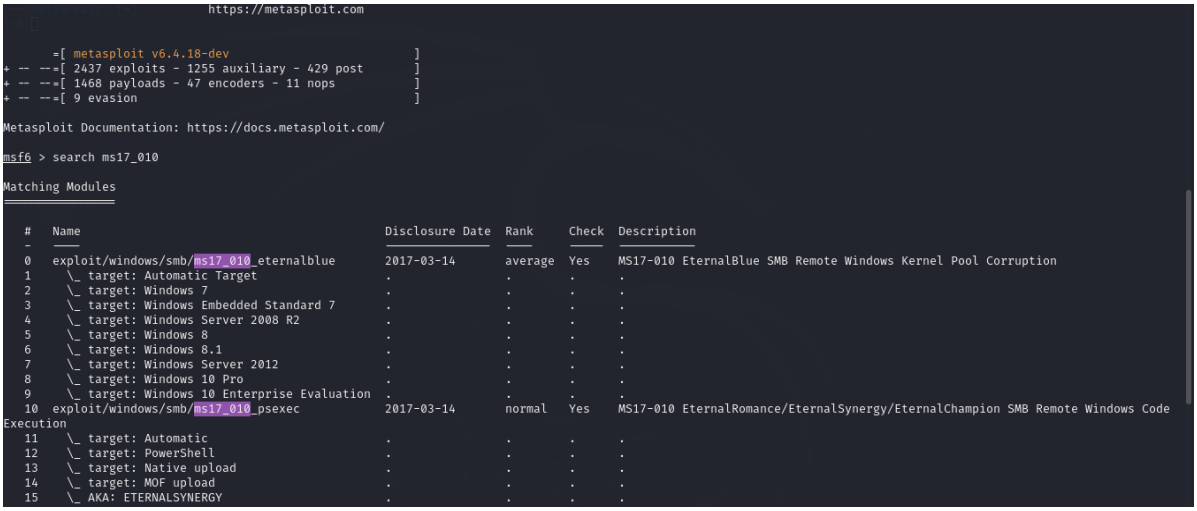


Fuente. Autoria Propia

Explotación de la Vulnerabilidad MS17-010 (Protocolo SMB): Se explotó la vulnerabilidad MS17-010 utilizando Metasploit. Se configuró el exploit ***exploit/windows/smb/ms17-010_eternalblue*** y se ejecutó, obteniendo una conexión por meterpreter y acceso a la Shell de Windows. Se creó un usuario administrador desde la Shell, manteniendo el control total sobre el host. Ver figura 5.

Figura. 5

Exploits SMB



Fuente. Autoria Propia

Fase de Post-Explotación

En la fase de post-explotación, se realizó un escalamiento de privilegios creando un usuario administrador desde la Shell de Windows. Esto permitió obtener y mantener el control total sobre el host. En la figura 6 se ilustra el usuario con privilegios de administrador creado en la maquina durante la fase de post-explotación.

Figura. 6

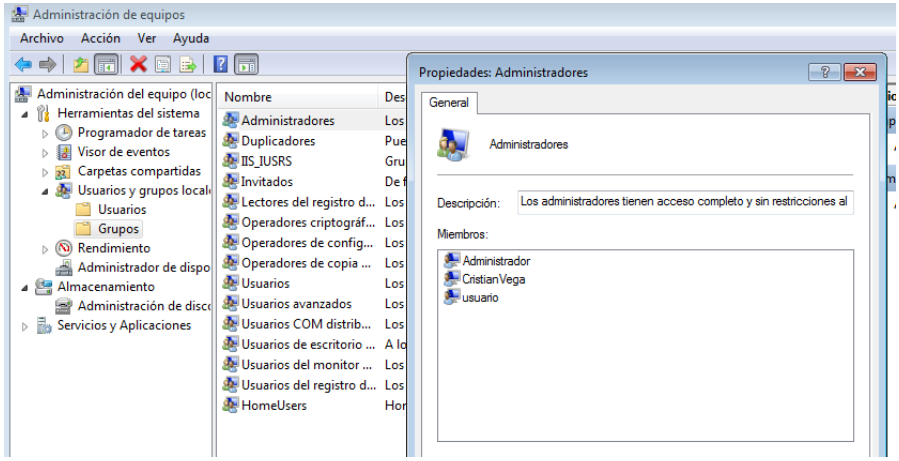
Elevacion de privilegios Shell de Windows

Fuente. Autoria Propia

Finalmente en la siguiente figura se evidencia desde el equipo Windows 7 los usuarios locales de la maquina y el usuario creado con privilegios de administrador durante la fase de post-explotacion. De acuerdo con este ejercicio de Red Team se puede determinar el nivel de impacto y riesgo que puede representar este equipo para la organización y la alta probabilidad de que un incidente cibernético se materialice, ocasionando una amenaza para la confidencialidad, integridad y disponibilidad de la información.

Figura. 7

Usuario Administrador



Fuente. Autoria Propia

BLUE TEAM: ESTRATEGIAS DE MITIGACION Y CONTENCION.

En respuesta a las vulnerabilidades identificadas en el equipo Windows 7 , se presenta un informe detallado con las estrategias de mitigación recomendadas para garantizar la seguridad y continuidad operativa de CyberFort Technologies.

Actualizar el Sistema Operativo

- Descripción del Problema: La versión del sistema operativo Windows 7 ya no recibe soporte de Microsoft, lo que incrementa su vulnerabilidad a diversos ataques cibernéticos. La falta de actualizaciones de seguridad deja el sistema expuesto a exploits conocidos y nuevas amenazas.

- Acción Recomendada: Se recomienda actualizar todos los sistemas que aún operan con Windows 7 a la última versión de Windows disponible. Este proceso debe incluir la instalación de todos los parches de seguridad y actualizaciones críticas para asegurar que los sistemas estén protegidos contra las amenazas más recientes.

- Impacto Esperado: La actualización del sistema operativo reducirá significativamente el riesgo de ataques y mejorará la estabilidad y el rendimiento general de los sistemas.

Actualizar o Reemplazar HFS

- Descripción del Problema: La versión actual del HTTP File Server (HFS) utilizada en la infraestructura está obsoleta y no cumple con los estándares de seguridad modernos. Esto puede permitir a los atacantes explotar vulnerabilidades conocidas para comprometer el servidor.

- Acción Recomendada: Se recomienda actualizar HFS a su última versión disponible. Alternativamente, se puede considerar reemplazar HFS con un software o servidor HTTP más seguro y actualizado que cumpla con los requisitos de seguridad de la organización.

- Impacto Esperado: La actualización o reemplazo de HFS mejorará la seguridad del servidor, reduciendo el riesgo de explotación de vulnerabilidades y mejorando la eficiencia operativa.

Deshabilitar SMBv1

- Descripción del Problema: El protocolo SMBv1 es conocido por sus vulnerabilidades que permiten la ejecución de código remoto, lo que puede ser explotado por atacantes para tomar control de los sistemas.

- Acción Recomendada: Es crucial deshabilitar SMBv1 en todos los equipos y configurar SMBv3, que ofrece mejoras significativas en seguridad. Además, se deben configurar los parámetros de seguridad necesarios para evitar la ejecución de código remoto a través de la Shell de Windows.

- Impacto Esperado: La deshabilitación de SMBv1 y la implementación de SMBv3 fortalecerán la seguridad de la red, previniendo posibles ataques y mejorando la integridad de los datos.

Configurar un Firewall Perimetral

- Descripción del Problema: La falta de un firewall perimetral adecuado puede permitir el acceso no autorizado a la red de la organización, exponiendo los sistemas a ataques externos.

- Acción Recomendada: Se recomienda instalar o configurar un firewall de seguridad perimetral para gestionar los puertos abiertos y controlar el tráfico entrante no deseado. Este firewall debe ser capaz de bloquear intentos de acceso no autorizados y permitir solo el tráfico legítimo.

- Impacto Esperado: La implementación de un firewall perimetral mejorará la seguridad de la red, protegiendo los sistemas contra accesos no autorizados y ataques externos.

Implementar un Gestor de Parches de Seguridad

- Descripción del Problema: La gestión inadecuada de parches de seguridad puede dejar los sistemas vulnerables a exploits conocidos y nuevas amenazas.

- Acción Recomendada: Se debe configurar el servidor WSUS (Windows Server Update Services) para gestionar todos los parches de seguridad y actualizaciones en los equipos con sistemas Windows. Esto asegurará que todos los sistemas estén actualizados con las últimas correcciones de seguridad.

- Impacto Esperado: La implementación de un gestor de parches de seguridad garantizará que los sistemas estén protegidos contra vulnerabilidades conocidas, mejorando la seguridad general de la infraestructura.

Instalar y Usar Antivirus

- Descripción del Problema: La ausencia de un antivirus robusto puede permitir que actividades maliciosas pasen desapercibidas, comprometiendo la seguridad de los sistemas.

- Acción Recomendada: Es indispensable instalar un antivirus robusto que tenga la capacidad de analizar y detectar cualquier actividad maliciosa en los equipos de la

organización. Además, esta herramienta debe ser capaz de aislar los dispositivos infectados o comprometidos para evitar la propagación de malware.

- Impacto Esperado: La instalación y uso de un antivirus robusto mejorará la capacidad de detección y respuesta ante amenazas, protegiendo los sistemas contra infecciones y ataques.

Control de Acceso

- Descripción del Problema: La falta de políticas de control de acceso adecuadas puede permitir el acceso no autorizado a los sistemas y datos sensibles de la organización.

- Acción Recomendada: Se deben establecer políticas de control de acceso y administración de roles para las cuentas de usuario en los sistemas de la organización. Estas políticas deben alinearse con las recomendaciones establecidas por los diferentes estándares de seguridad.

- Impacto Esperado: La implementación de políticas de control de acceso mejorará la seguridad de los datos y sistemas, asegurando que solo el personal autorizado tenga acceso a información sensible.

Monitoreo de la Red

- Descripción del Problema: La falta de monitoreo en tiempo real puede permitir que actividades maliciosas pasen desapercibidas, comprometiendo la seguridad de la infraestructura.

- Acción Recomendada: Se recomienda la instalación de sistemas IDS/IPS (Intrusion Detection System/Intrusion Prevention System), SIEM (Security Information and Event Management), entre otros, para el monitoreo continuo de la infraestructura. Estos sistemas permitirán detectar y responder a anomalías en tiempo real[5].

- Impacto Esperado: El monitoreo continuo de la red mejorará la capacidad de detección y respuesta ante amenazas, protegiendo la infraestructura contra posibles intrusiones y ataques.

RECOMENDACIÓNES DE SEGURIDAD PARA LA CONTENCION Y RESPUESTA A INCIDENTES CIBERNETICOS EN TIEMPO REAL

Para mejorar la capacidad de respuesta ante incidentes de seguridad, se recomienda la instalación y configuración de las siguientes herramientas:

[5] Páez Sotomonte, B. O. (2020). Sistemas de detección de intrusiones: IDS vs sistemas de prevención de intrusiones: IPS. https://repository.unipiloto.edu.co/handle/20.500.12277/7427

Firewall de Nueva Generación (NGFW)

Descripción: Un NGFW ofrece protección avanzada contra amenazas, filtrando paquetes, controlando aplicaciones y utilizando inteligencia de amenazas[6].

Funciones Clave:

- Filtrado de paquetes y contenido.
- Control de aplicaciones.
- Actualización constante de firmas de malware.
- Gestión segura de VPN.

Beneficio: Proporciona una protección más detallada y efectiva contra amenazas avanzadas.

IDS/IPS (Sistemas de Detección y Prevención de Intrusos)

Descripción: Estas herramientas monitorean y protegen la red en tiempo real, detectando y bloqueando actividades sospechosas.

Funciones Clave:

- Monitoreo en tiempo real.
- Uso de bases de datos de firmas de ataques.

[6] Cortés Aldana, D. G. (2016). *Firewalls de nueva generación: la seguridad informática vanguardista* (Bachelor's thesis, Universidad Piloto de Colombia). https://repository.unipiloto.edu.co/handle/20.500.12277/2719

- Inteligencia artificial para detectar anomalías.

Beneficio: Mejoran la capacidad de detección y respuesta ante amenazas.

SOAR (Sistemas de Orquestación, Automatización y Respuesta de Seguridad)

Descripción: Un SOAR ayuda a gestionar y responder a incidentes de manera eficiente, automatizando tareas y coordinando herramientas de seguridad[7].

Funciones Clave:

- Integración de herramientas de seguridad.
- Automatización de tareas rutinarias.
- Gestión centralizada de incidentes.
- Priorización de eventos de seguridad.

Beneficio: Mejora la eficiencia y efectividad de las respuestas a incidentes.

[7] Medina, P. (2021). Plataformas SOAR. Respuesta orquestada y automatizada de la seguridad. https://www.lareferencia.info/vufind/Record/ES_2ce59a6e1ea3d7925eb8a172e72e1ca4

Conclusiones

La conformación de equipos de Blue Team y Red Team es indispensable en una organización debido a su capacidad para proporcionar una defensa integral contra amenazas cibernéticas. Los equipos de Blue Team se encargan de la defensa proactiva, monitoreando y protegiendo los sistemas de la organización, mientras que los equipos de Red Team adoptan un enfoque ofensivo, simulando ataques para identificar vulnerabilidades. Esta interacción fomenta una mejora continua de la seguridad, ya que los equipos de Red Team descubren fallos y debilidades, y los equipos de Blue Teams ajustan sus estrategias de defensa en consecuencia. Además, la simulación de ataques reales permite a la organización evaluar y mejorar sus planes de respuesta a incidentes, asegurando una preparación efectiva ante ataques reales. La presencia de estos equipos también aumenta la conciencia sobre la ciberseguridad dentro de la organización y proporciona oportunidades de capacitación práctica para el personal.

En resumen, la colaboración entre los equipos de Blue Team y Red Team es esencial para crear un entorno de seguridad robusto y resiliente, capaz de proteger a la organización contra una amplia gama de amenazas cibernéticas.

Recomendaciones

Planificar ejercicios de simulación de ataques cibernéticos periódicamente es fundamental para poder evaluar y mejorar los planes de respuesta ante posibles incidentes y fortalecer los controles de seguridad existentes en una organización

Establecer una interacción sinérgica entre los equipos de Blue Team y Red Team es primoridial para lograr una identificación y mitigación de riesgos mucho más efectiva y proactiva.

La implementación de herramientas informáticas sofisticadas y modernas en un entorno tecnológico, es vital para garantizar una proteccion más efectiva. Estas herramientas avanzadas permiten una detección y respuesta más rápida a las amenazas cibernéticas.

Es esencial establecer controles y estrategias de seguridad que estén alineados con las metodologías existentes y los estándares de seguridad reconocidos, además de facilitar el cumplimiento con las mejores prácticas y normativas del sector.

Es fundamental invertir en la capacitación y mejora continua del personal de seguridad en una organización. Esto asegura que el equipo esté siempre actualizado con las últimas amenazas y técnicas de defensa, fortaleciendo así la postura de seguridad y la capacidad de respuesta ante incidentes cibernéticos.

Referencias Bibliográficas

ACIEM. Código de Conducta. https://www.capacitacion.aciem.com.co/Etica/Cuaderno-Institucional-Etica-Ingenieria.pdf

Alonso Blanco, D. (2018). Análisis del exploit, EternalBlue. https://oa.upm.es/51939/

Arévalo Ticlla, S., Infante Girón, G., Valdivia Huamán, D., & Velásquez Rojas, J. (2014). Aprovechamiento de vulnerabilidades del sistema operativo Windows con la herramienta metasploit. https://repositorio.upn.edu.pe/handle/11537/2999

Avella-Coronado, J. D., Calderón-Barrios, L. F., & Mateus-Díaz, C. A. (2015). Guía metodológica para la gestión centralizada de registros de seguridad a través de un SIEM. https://repository.ucatolica.edu.co/handle/10983/2847

CIS. Implementation Guide. https://www.cisecurity.org/

Congreso Colombia. (2012). Ley 1581 de 2012. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Cortés Aldana, D. G. (2016). *Firewalls de nueva generación: la seguridad informática vanguardista* (Bachelor's thesis, Universidad Piloto de Colombia). https://repository.unipiloto.edu.co/handle/20.500.12277/2719

CVE. Mitre. https://cve.mitre.org/

de la Tejera, I. P., de la Tejera Chillón, N., Caballero, G. D. R., & Cano, S. D. Seguridad de la Información y Criterios Éticos en el uso de las Tecnologías Médicas. https://convencionsalud.sld.cu/index.php/convencionsalud22/2022/paper/viewFile/371/117

Función pública. (2018). Ley 1928 de 2018. https://www1.funcionpublica.gov.co/documents/34645357/34703567/Ley_1928_de_2018.pdf/f6402a0c-bf61-d150-0544-3f44753b5555?t=1560461998293

Gerick Toro.(2008). Guía de referencia de Nmap. pp 1-49. Manual-de-uso-de-Nmap.pdf (riseup.net)

Gobierno Digital. (2022). Decreto 338. https://gobiernodigital.mintic.gov.co/692/articles-238198_recurso_1.pdf

Guillén Zafra, J. L. (2017). Introducción al pentesting. https://diposit.ub.edu/dspace/handle/2445/124085

H Anderson. (2003). Introduction to nessus. pp 1-33. TutNessus.pdf (cryptomex.org)

LÓPEZ, M. R. E., & ARMENIA, Q. capacidades técnicas, legales y de gestión para equipos blueteam y redteam. https://core.ac.uk/download/pdf/421929867.pdf

Marchand-Niño, W. R., & Vega Ventocilla, E. J. Balanced Scorecard model for critical computer security controls according to the Center for Internet Security (CIS). https://alicia.concytec.gob.pe/vufind/Record/REVULIMA_b3d50c5cd82600a3550ffbe57c48209d

Martí Talón, R. M. (2016). *Desarrollo e implementacion practica de un pentest* (Doctoral dissertation, Universitat Politècnica de València). https://riunet.upv.es/handle/10251/70164

Medina, P. (2021). Plataformas SOAR. Respuesta orquestada y automatizada de la seguridad. https://www.lareferencia.info/vufind/Record/ES_2ce59a6e1ea3d7925eb8a172e72e1ca4

MINTIC. (2022). Políticas de Privacidad y Condiciones de Uso. https://www.mintic.gov.co/portal/inicio/Secciones-auxiliares/Politicas/2627:Politicas-de-Privacidad-y-Condiciones-de-Uso

Muñoz, M., & Rivas, L. (2015). Estado actual de equipos de respuesta a incidentes de seguridad informática. *RISTI: Iberian Journal on Information Systems & Technologies/Revista Ibérica de Sistemas e Tecnologias de Informação*. https://www.semanticscholar.org/paper/Estado-actual-de-equipos-de-respuesta-a-incidentes-Mu%C3%B1oz-Rivas/2cfa3c743f39189d6052b1816dd558c21c6a4355?p2df

NIST. Use of the common vulnerabilities and Exposures CVE. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-51.pdf

Núñez Alcalá, C. (2021). Penetration testing: auditoría profesional. https://openaccess.uoc.edu/handle/10609/132609

Páez Sotomonte, B. O. (2020). Sistemas de detección de intrusiones: IDS vs sistemas de prevención de intrusiones: IPS. https://repository.unipiloto.edu.co/handle/20.500.12277/7427

Policía. (2009). Ley 1273 [LEY_1273_2009].Policía. (pp. 1-4). https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos

Sain, G. La ciberseguridad como política de seguridad ciudadana. ciencias sociales. https://periferiaactiva.wordpress.com/wp-content/uploads/2024/07/narodowski-p-2024-pobreza-y-fragmentacion-en-asia-y-africa.-estudio-de-15-paises.pdf#page=157

Suárez, R. (2006). Mapeo de redes con Nmap. *Todo linux: la revista mensual para entusiastas de GNU/LINUX*, (63), 34-38. https://dialnet.unirioja.es/servlet/articulo?codigo=3227746

Zafra Guillen Luis. (2017). Introducción al pentesting. pp 5-18. memoria.pdf (ub.edu)

Zambrano Hernández, L. F. Capacidades técnicas, legales y de gestión para equipos blue team y red team. https://repository.unad.edu.co/handle/10596/62788

Anexos

Anexo A

Enlace Video

https://youtu.be/iHGeiExgk1w