Capacidades técnicas, legales y de gestión para equipos blue team y red team.

Luis Carlos Calderón Anacona

Universidad Nacional Abierta y a Distancia – UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en seguridad informática

Mayo 2025

Resumen.

Este reporte técnico ofrece un examen minucioso de las tareas llevadas a cabo en las fases 1 a 4, de acuerdo con las exigencias de CyberFort Technologies (Anexo 6 - Escenario 5). Se realizaron ensayos de intrusión que detectaron debilidades cruciales en sistemas anticuados, se valoraron elementos éticos y jurídicos en acuerdos, y se establecieron estrategias de contención eficaces. Los descubrimientos subrayan la importancia de robustecer las estrategias de Red Team y Blue Team, dando prioridad a la administración de parches, la supervisión proactiva con instrumentos como SIEM, y la formación del personal. Este documento proporciona sugerencias útiles para potenciar la posición de ciberseguridad de la entidad y respaldar la elección de especialistas en seguridad.

***Palabras clave*:** Red teams, Blue teams, SIEM, Ciberseguridad.

Abstract.

This white paper provides a thorough examination of the tasks performed in phases 1 through 4, in accordance with CyberFort Technologies' requirements (Exhibit 6 - Scenario 5). Penetration tests were conducted that identified critical weaknesses in outdated systems, ethical and legal elements in agreements were assessed, and effective containment strategies were planned.
The findings underscore the importance of strengthening Red Team and Blue Team strategies by prioritizing patch management, proactive monitoring with tools such as SIEM, and staff training. This document provides useful suggestions for strengthening the organization's cybersecurity posture and supporting the selection of security specialists.

***Keywords*:** Red team, Blue team, SIEM, Cybersecurity.

Índice

Lista de Figuras.

1. Glosario.

- **Red Team:** Equipo que simula ataques cibernéticos para detectar vulnerabilidades.
- **Blue Team:** Equipo encargado de defender y responder a incidentes de seguridad.
- **Pentesting:** Pruebas de penetración para evaluar la seguridad de sistemas.
- **SIEM:** Sistema de Gestión de Eventos e Información de Seguridad para monitoreo en tiempo real.
- **IDS/IPS:** Sistema de Detección/Prevención de Intrusos para identificar y bloquear amenazas.
- **MS17-010:** Vulnerabilidad en Windows (EternalBlue) explotada en ataques como WannaCry.
- **CIS Benchmarks:** Estándares de configuración segura para sistemas.
- **GPO:** Objetos de Política de Grupo para gestionar configuraciones en Windows.
- **Wazuh:** Herramienta SIEM de código abierto para análisis de seguridad.
- **Metasploit:** Plataforma para desarrollar y ejecutar exploits.

2. Introducción.

Este informe técnico tiene como objetivo principal consolidar y analizar los resultados de las actividades ejecutadas durante las Etapas 1 a 4, conforme a los lineamientos establecidos por CyberFort Technologies en el Anexo 6 - Escenario 5. Su propósito es evaluar la postura de ciberseguridad de la organización mediante la ejecución de pruebas controladas en entornos simulados, identificar vulnerabilidades críticas, y proponer estrategias específicas para optimizar las operaciones de los equipos Red Team y Blue Team. Además, se abordan aspectos éticos y legales que impactan las decisiones de seguridad, y se ofrecen recomendaciones prácticas para endurecer las defensas organizacionales frente a amenazas cibernéticas actuales.

El documento está diseñado para ser evaluado por analistas senior de seguridad de CyberFort Technologies, quienes seleccionarán a los expertos que integrarán está reconocida entidad. Por ello, se adopta un enfoque técnico riguroso, utilizando un lenguaje profesional y preciso, alineado con estándares de la industria como ISO 27001, NIST SP 800-53 y los CIS Controls. A lo largo del informe, se detallan los hallazgos de cada etapa, se justifican las recomendaciones con argumentos basados en evidencia y se concluye con aportes significativos al campo de la ciberseguridad.

3. Objetivos

3.1 Objetivo General.

Evaluar la postura de ciberseguridad de CyberFort Technologies mediante pruebas controladas, análisis ético-legal y medidas de contención, identificando vulnerabilidades y proponiendo mejoras en las estrategias de Red Team y Blue Team.

3.2 Objetivos Específicos.

- Configurar un entorno de pruebas que simule condiciones reales para evaluar estrategias ofensivas y defensivas.
- Analizar cláusulas contractuales desde una perspectiva ética y legal, identificando riesgos.
- Ejecutar pruebas de intrusión para detectar y explotar vulnerabilidades en sistemas desactualizados.
- Implementar y evaluar medidas de contención ante ataques simulados, optimizando la respuesta a incidentes.

4. Desarrollo.

4.1 Etapa 1: Conceptos: Equipos de Seguridad.

En esta etapa inicial, se estableció un entorno de pruebas utilizando VirtualBox como plataforma de virtualización. Se desplegaron dos máquinas virtuales: una con Windows 7 (IP: 10.0.2.15) y otra con Parrot OS, configuradas para simular una red organizacional. La comunicación entre ambas se validó mediante comandos como ipconfig en Windows y ping desde Parrot OS, asegurando conectividad en la red virtual (subred 10.0.2.0/24). Este banco de trabajo permitió replicar condiciones reales para evaluar estrategias ofensivas y defensivas.

Análisis:

La configuración de este entorno fue crucial para sentar las bases de las pruebas posteriores. Windows 7, un sistema operativo obsoleto desde 2020, se seleccionó intencionalmente para reflejar escenarios comunes en organizaciones que no actualizan su infraestructura, un riesgo documentado en el 2023 Verizon Data Breach Investigations Report, donde el 19% de los incidentes involucraron sistemas desactualizados. Por su parte, Parrot OS, con herramientas como Nmap y Metasploit preinstaladas, representó la perspectiva del Red Team, mientras que Windows permitió evaluar defensas del Blue Team.

Se destacó el rol complementario de ambos equipos debido a que el Red Team adopta un enfoque proactivo, identificando y explotando vulnerabilidades para simular ataques reales, mientras que el Blue Team se enfoca en la detección, contención y mitigación de incidentes. Esta colaboración es esencial, ya que, según MITRE

ATT&CK, las organizaciones que integran estas funciones reducen hasta un 30% el tiempo de respuesta a incidentes.

Relevancia Profesional:

Esta etapa subraya la importancia de entornos controlados para pruebas de seguridad, un estándar en metodologías como OSSTMM (Open Source Security Testing Methodology Manual), garantizando resultados reproducibles y éticamente responsables.

4.2 Etapa 2: Actuación Ética y Legal

Se realizó un análisis ético y legal basado en el "Anexo 3 - Acuerdo 1", identificando cláusulas que restringían la denuncia de actividades ilegales dentro de CyberFort Technologies. Por ejemplo:

Cláusula Primera: "La parte receptora se obliga a no divulgar [...] información confidencial o sobre procesos ilegales."

Cláusula Cuarta: "No denunciar ante las autoridades actividades sospechosas de espionaje."

Estas disposiciones se evaluaron frente a la legislación colombiana y principios éticos profesionales.

Análisis:

Las cláusulas contravienen la Ley 1273 de 2009 de Colombia, que protege la integridad de datos y sistemas (Art. 269A: acceso abusivo; Art. 269F: violación de datos personales), y la Ley 1581 de 2012, que regula la protección de datos. Asimismo, el Código de Ética de COPNIA exige a los profesionales actuar con integridad y reportar conductas ilegales, un deber que supera cualquier acuerdo contractual. A nivel global, frameworks como el GDPR y el NIST Cybersecurity Framework refuerzan esta postura, penalizando la omisión de reportes de incidentes. Permitir tales restricciones no solo expone a la organización a riesgos legales (multas, sanciones), sino que compromete su reputación y confianza pública. Por ejemplo, el caso de Uber en 2016, donde ocultó un breach masivo, resultó en una multa de $148 millones, evidenciando las consecuencias de priorizar el silencio sobre la ética.

Relevancia Profesional:

Este análisis resalta la necesidad de alinear contratos con marcos legales y éticos, un aspecto crítico para profesionales de ciberseguridad que deben equilibrar confidencialidad con responsabilidad social.

4.3 Etapa 3: Ejecución de Pruebas de Intrusión

El Red Team ejecutó pruebas de penetración en un servidor Windows 7 vulnerable (IP: 10.3.208.115), siguiendo el Anexo 4 - Escenario 3. Las fases fueron:

Reconocimiento: nmap -sS -sV 10.3.208.115 identificó el puerto 53 (SMB) abierto.

Análisis de Vulnerabilidades: El script smb-vuln-ms17-010.nse confirmó la presencia de MS17-010 (EternalBlue).

Explotación: En Metasploit, el módulo exploit/windows/smb/ms17_010_eternalblue generó una sesión Meterpreter.

Post-Explotación: Se creó el usuario "Luis_Calderón" con net user "Luis_Calderón" Password123! /add, demostrando control total.

Análisis:

La vulnerabilidad MS17-010, explotada en ataques como WannaCry (2017), sigue siendo relevante en sistemas sin parches, como este Windows 7 sin soporte desde 2020. El éxito del ataque evidencia tres fallos críticos:

Falta de actualizaciones, violando el principio básico de gestión de parches.

Configuración insegura del protocolo SMB, un vector común según el MITRE ATT&CK (T1210).

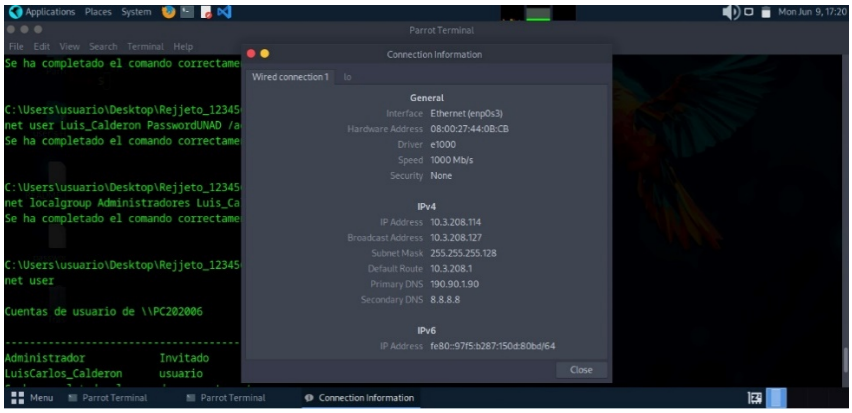
Ausencia de segmentación de red, permitiendo acceso irrestricto tras la explotación.

El impacto comprometió la confidencialidad (acceso a datos), integridad (modificación de cuentas) y disponibilidad (pantalla azul reportada), afectando los pilares de la tríada CIA. Esto subraya la necesidad de modernizar infraestructuras y aplicar controles proactivos.

Relevancia Profesional:

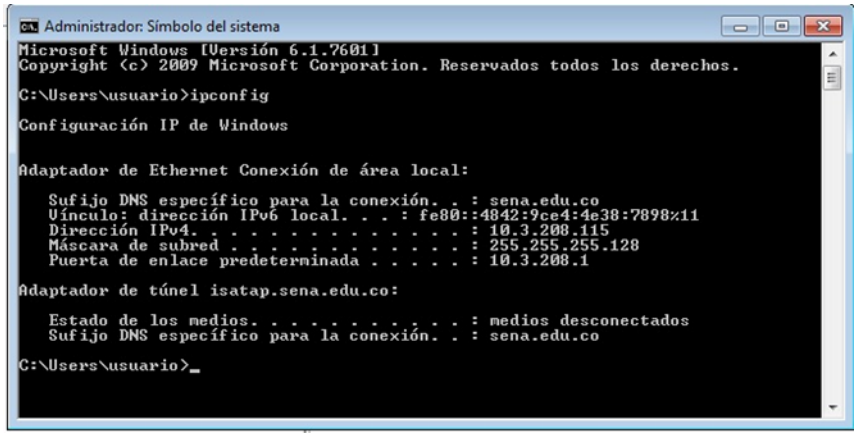
Las pruebas de intrusión son un estándar en la industria (e.g., OWASP, PTES), permitiendo identificar riesgos reales y justificar inversiones en seguridad ante stakeholders técnicos y ejecutivos.

Figura 1: Dirección IP Parrot



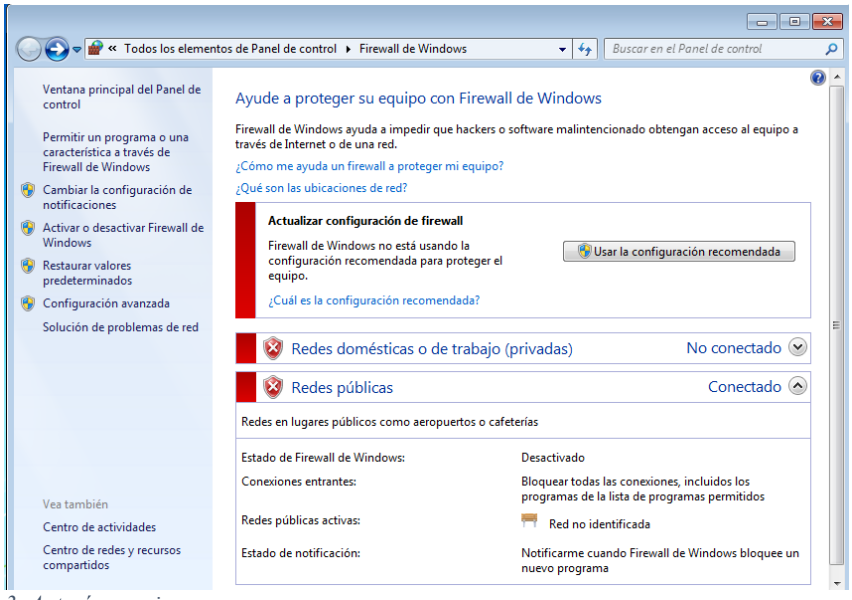
1. Autoría propia

Figura 2: Dirección IP Windows



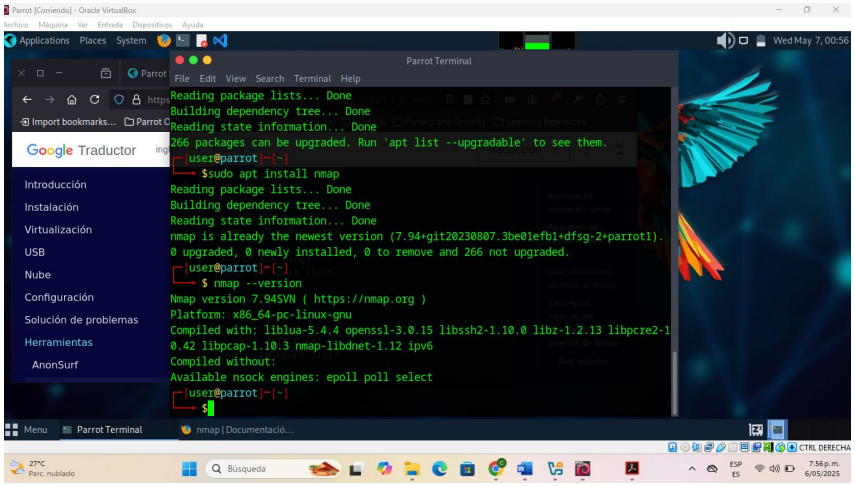
2. autoría propia

Figura 3: Firewalls



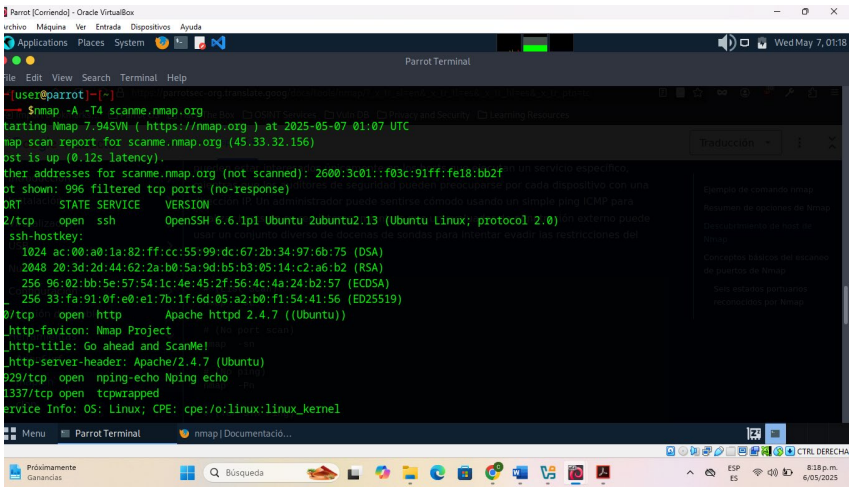
3. Autoría propia

Figura 4:Nmap



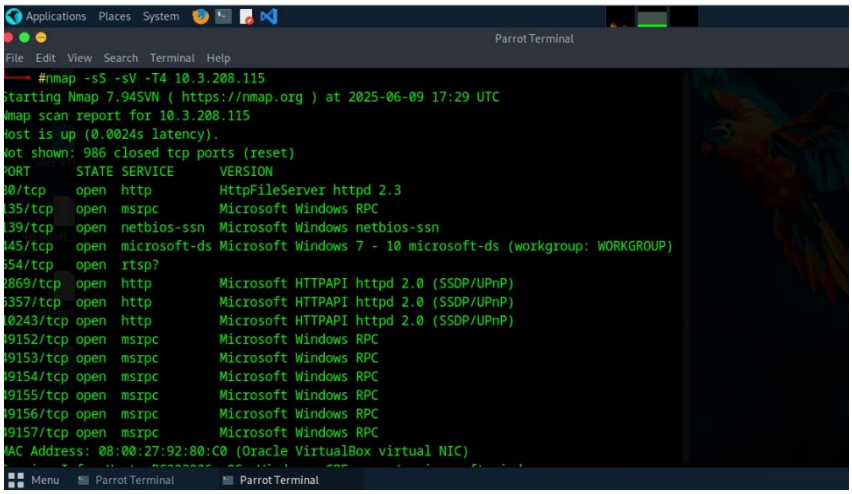
4. Autoría propia

Figura 5: código Nmap



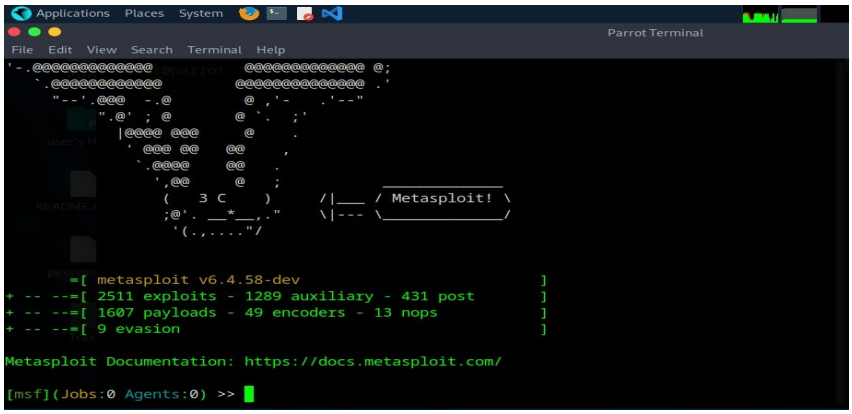
5. Autoría propia

Figura 6: Vulnerabilidades



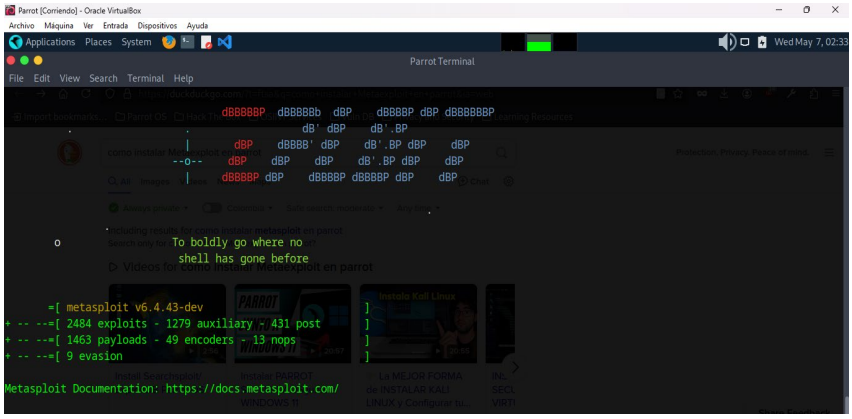
6. Autoría propia

Figura 7: Comando Metasploit



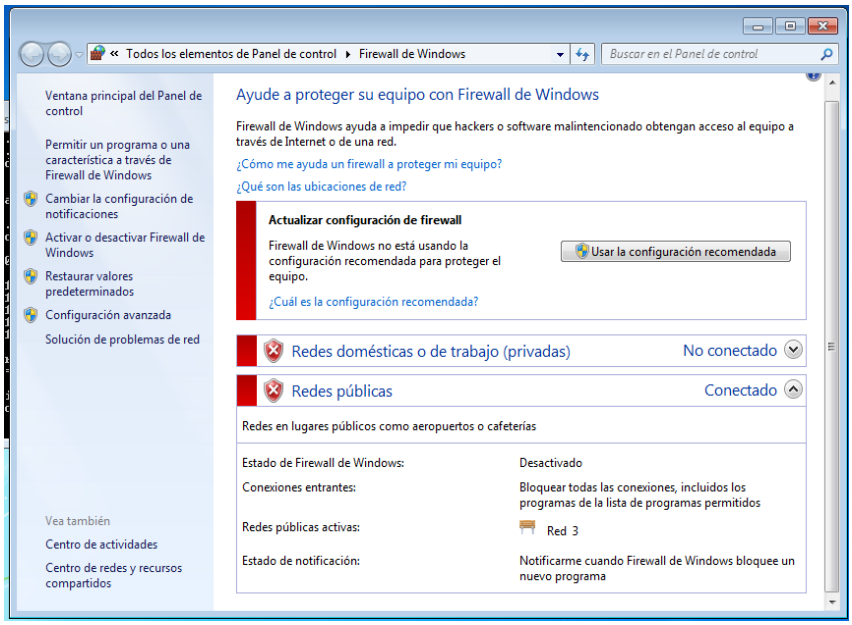
7. Autoría propia

Figura 8: pentesting



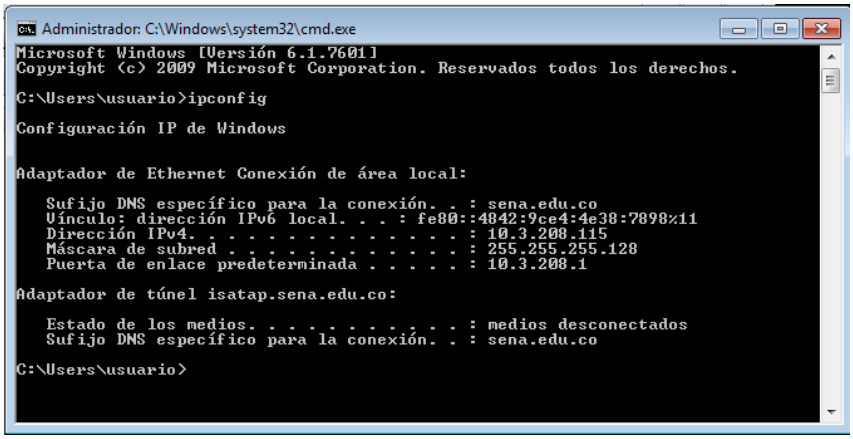
8. Autoría propia

Figura 9: firewall



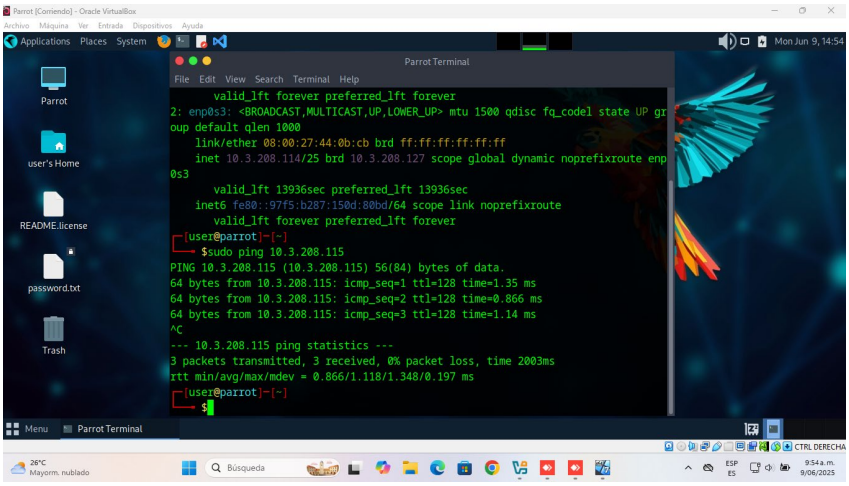
9.Autoría propia

Figura 10: Dirección IP de la maquina víctima con Windows 7



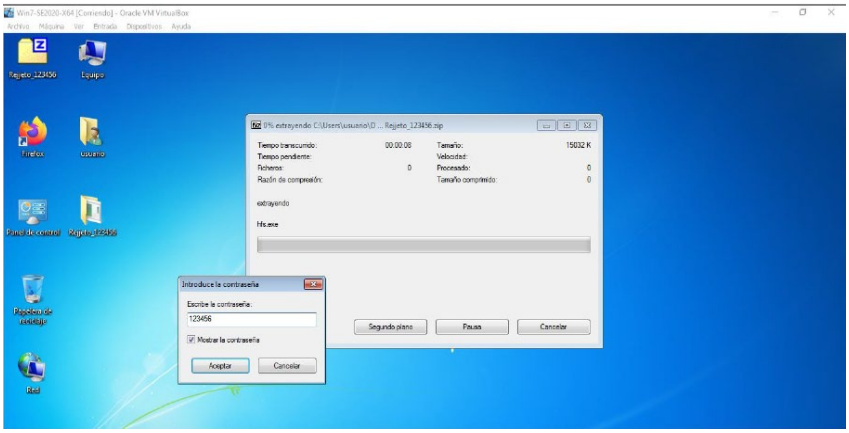
20. Autoría propia

Figura 11: Ping a windows



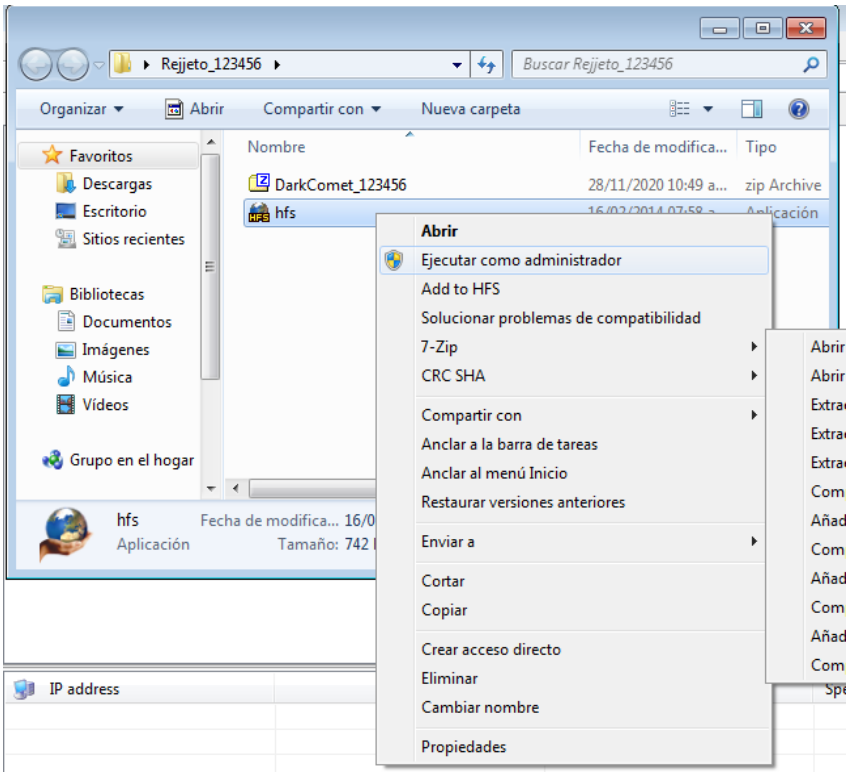
31. Autoría propia

Figura 12: Descompresión de programa Rejjeto para las pruebas de RCE



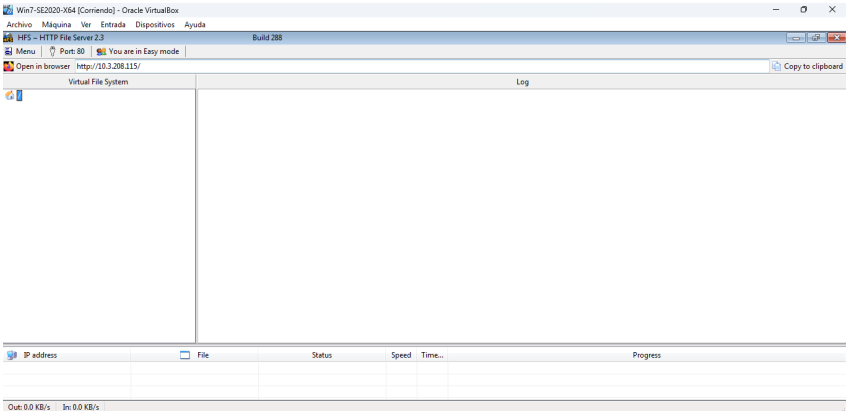
42. Autoría propia

Figura 13: Apertura de Programa Rejjeto para inicio de pruebas.



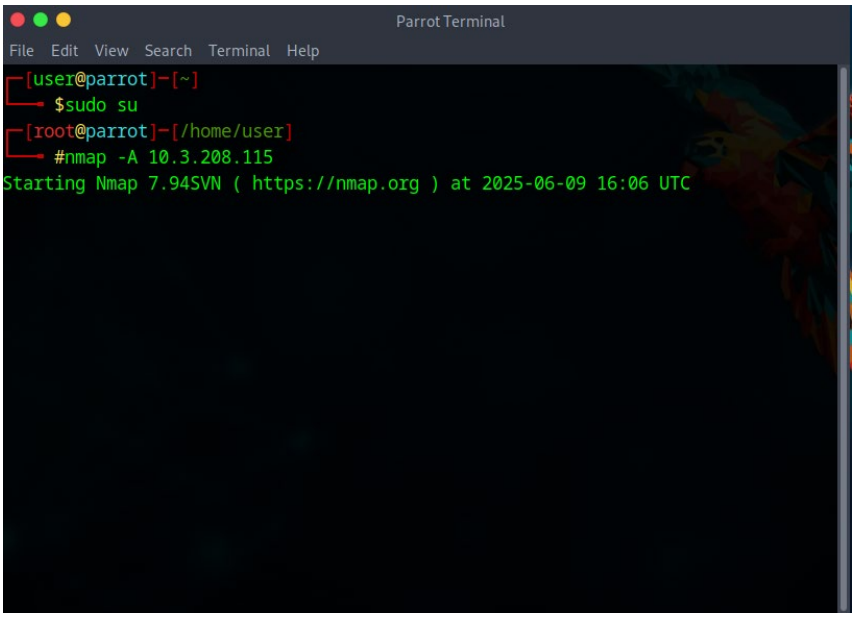
53. Autoría propia

Figura 14: Vista de la interfaz del programa Rejjeto HFS.



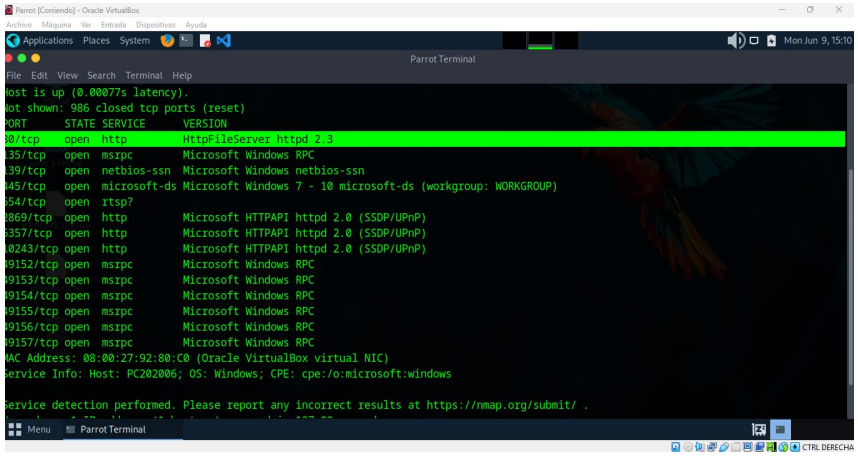
64. Autoría propia

Figura 15: Inicio de Nmap a la IP del host Victima para escaneo de Puertos.



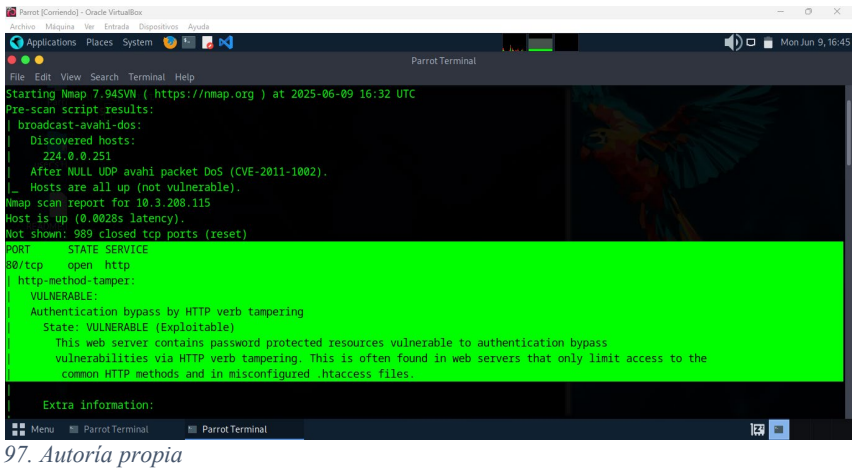
75. Autoría propia

Figura 16: Hallazgo de puerto 80 vulnerable con el servicio HttpFileServer 2.3 corriendo.



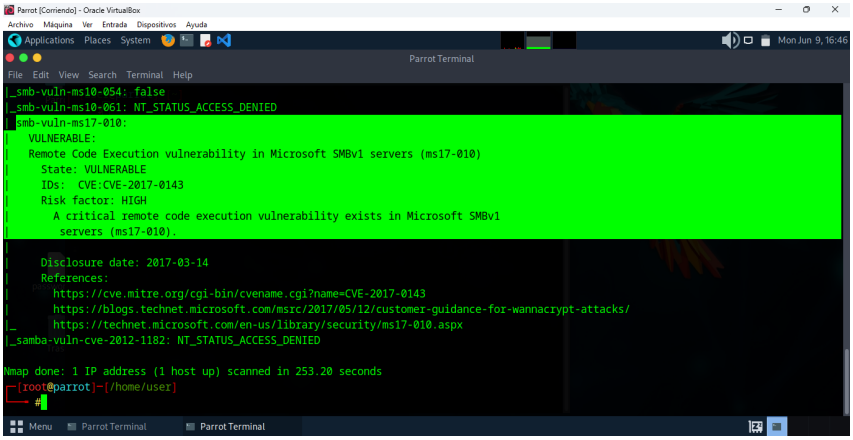
86. Autoría propia

Figura 17: Hallazgo de vulnerabilidad de puerto 80 servicio HttpFileServer 2.3 (Explotable).



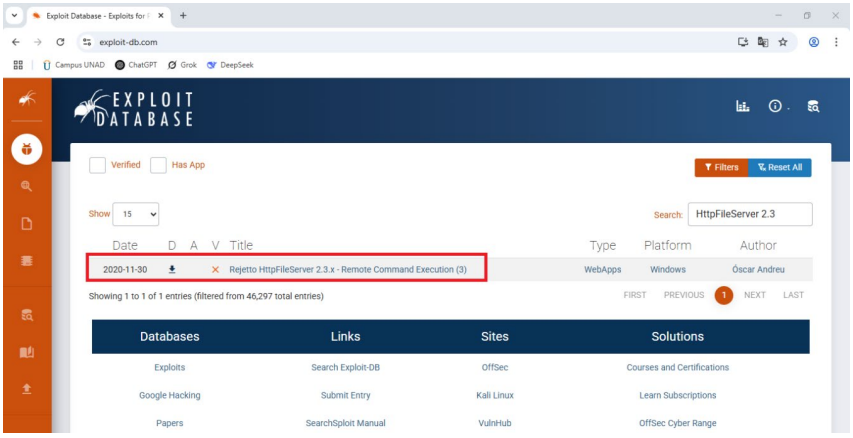
97. Autoría propia

Figura 18: Vulnerabilidad RCW en SMBv1 con CVE-2017-0143



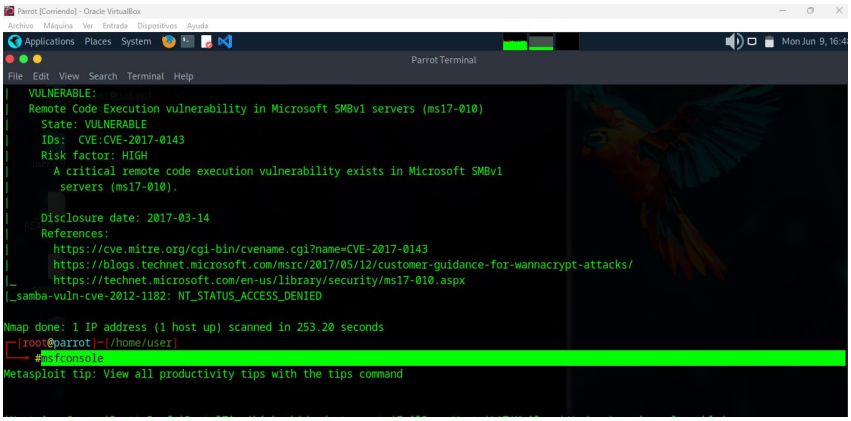
108. Autoría propia

Figura 19: Revisión de base de datos de exploits sobre servicio HttpFileServer 2.3.



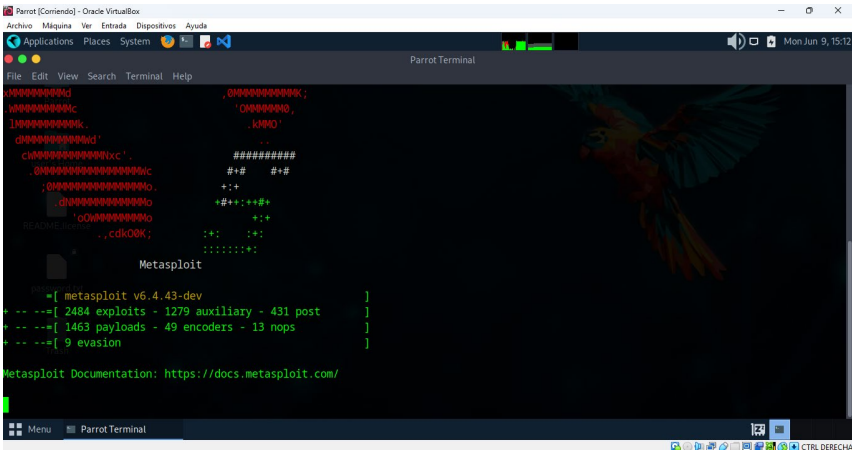
119. Autoría propia

Figura 20: Apertura de herramienta Metasploit para explotación de vulnerabilidad.



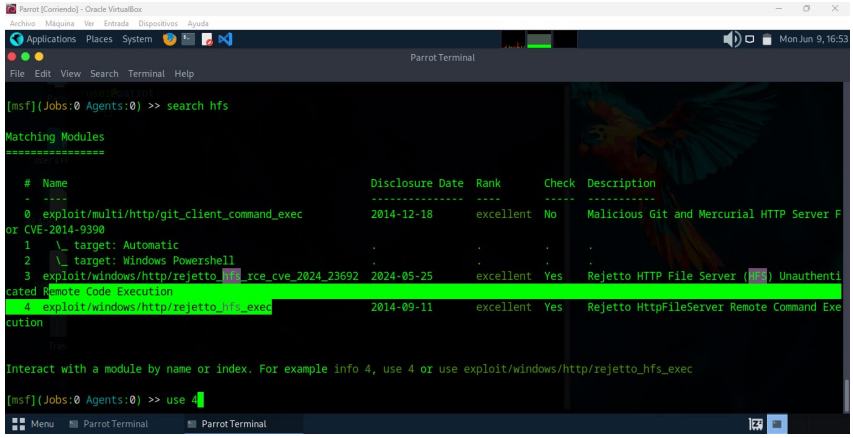
20. Autoría propia

Figura 21: Aplicación Metasploit corriendo.



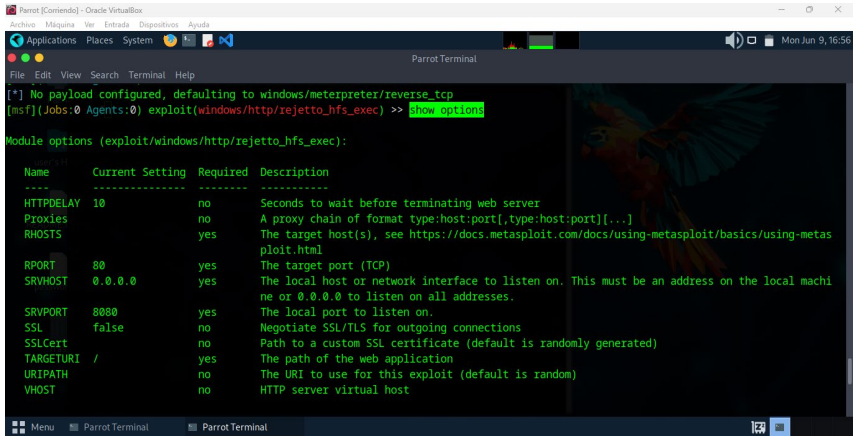
21. Autoría propia

Figura 22: Búsqueda con comando "Search" de exploits para "HFS" y uso de modulo 4.



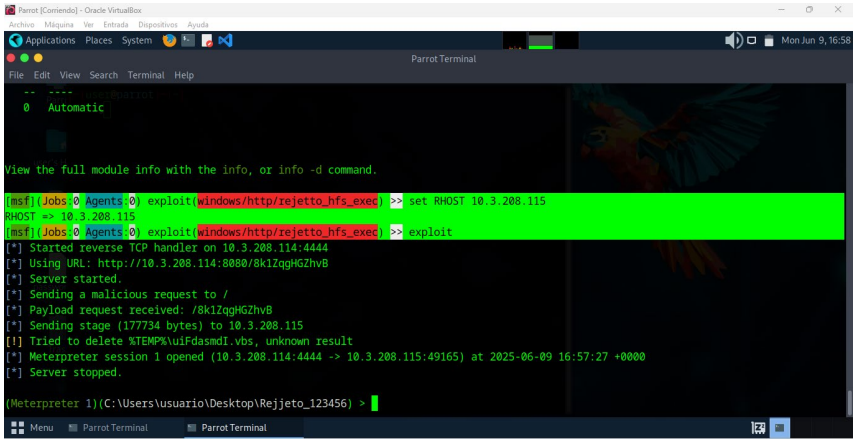
22. Autoría propia

Figura 23: Vista de configuración para establecer parámetros al Exploit.



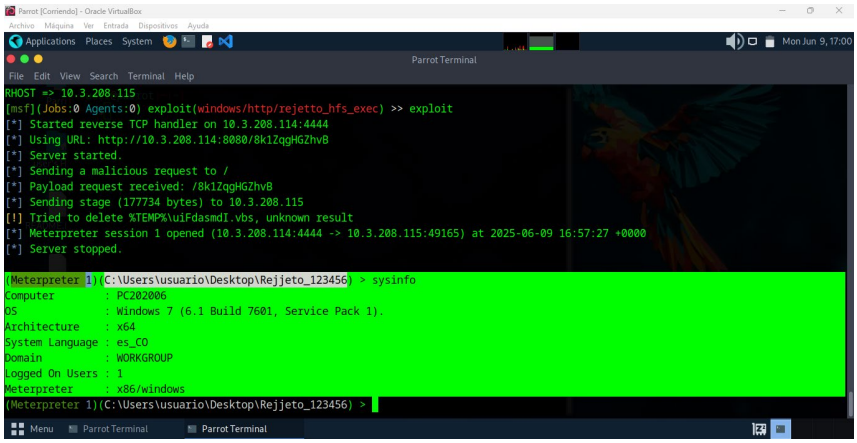
23. Autoría propia

Figura 24: Establecimiento de Host víctima y comando para iniciar el Exploit.



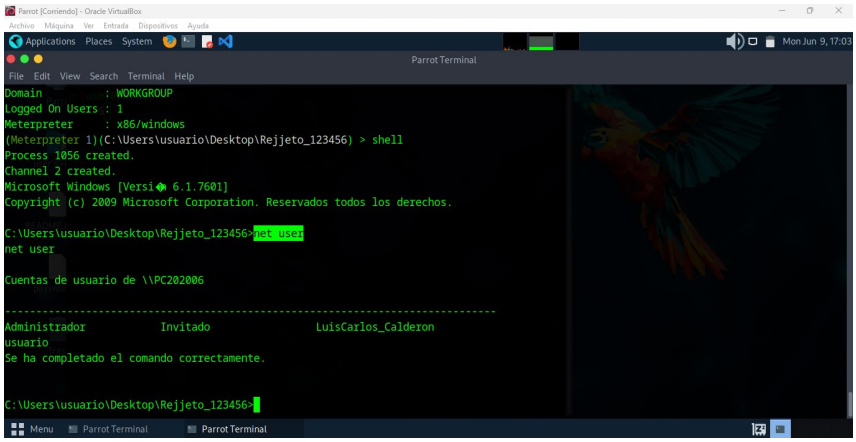
24. Autoría propia

Figura 25: Explotación exitosa y conexión a equipo remotamente, uso de comando de "Sysinfo"



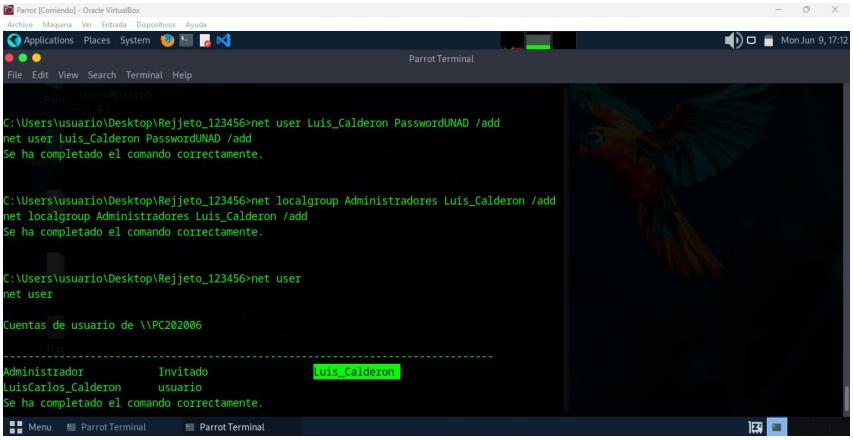
25. Autoría propia

Figura 26: Comando Shell para ejecutar comandos de sistema en la maquina Víctima y vista de usuario del sistema.



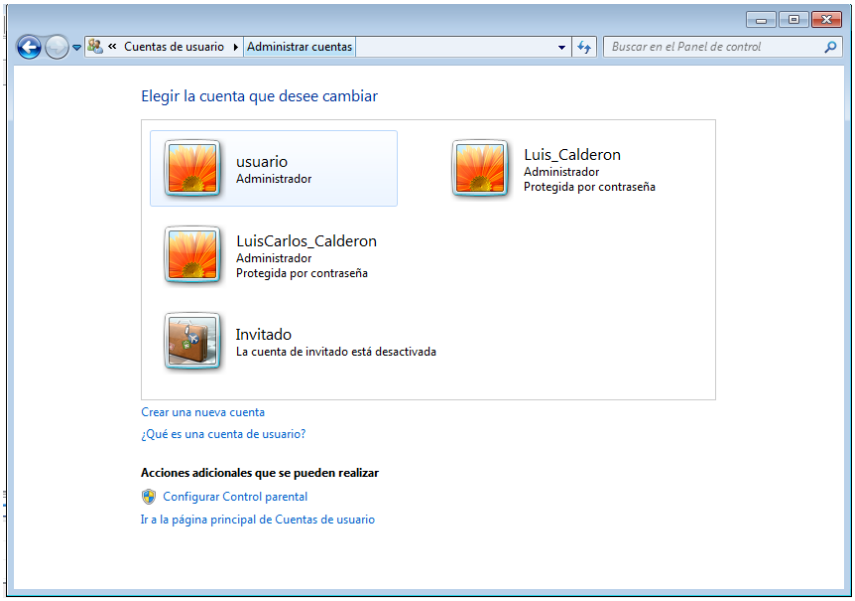
26. Autoría propia

Figura 27: usuario y contraseña Administrador.



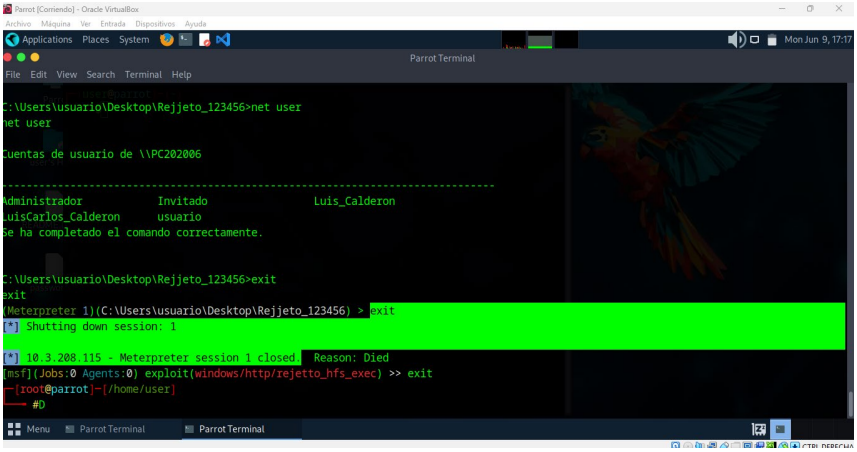
27. Autoría propia

Figura 28: Vista desde Windows 7 de cuenta creada desde Parrot.



28. Autoría propia

Figura 29: Cierre de sesión en maquina Parrot después de la creación del usuario administrador por RCE en vulnerabilidad de HttpFileServer 2.3 de Rejjeto.



29. Autoría propia

4.4 Etapa 4: Contención de Ataques Informáticos

El Blue Team respondió a un ataque simulado (Anexo 5 - Escenario 4) con:

Aislamiento: netsh interface set interface "Ethernet" disable desconectó el sistema comprometido.

Identificación: Process Explorer y netstat -ano detectaron procesos y conexiones anómalas.

Mitigación: Se bloquearon puertos con el firewall y se aplicó el parche MS17-010.

Monitoreo: Wazuh, configurado con reglas CIS Benchmarks, generó alertas en tiempo real.

Análisis:

La respuesta rápida evitó la propagación del ataque, alineándose con NIST SP 800-61, que prioriza contención sobre análisis inicial en incidentes críticos. Sin embargo, la dependencia de herramientas manuales como Process Explorer revela una brecha: la falta de un SIEM robusto retrasó la detección automatizada. Según IBM (2023), las organizaciones con monitoreo proactivo reducen el costo promedio de un breach de $4.24 millones a $2.9 millones.

El uso de CIS Benchmarks para hardening (e.g., desactivar SMBv1) es una práctica avalada por la industria, pero su implementación tardía en este caso permitió la explotación inicial. Esto refuerza la necesidad de defensas preventivas, no solo reactivas.

Relevancia Profesional:

Esta etapa demuestra la importancia de planes de respuesta a incidentes (IR) bien definidos y herramientas avanzadas, competencias esenciales para Blue Teams en entornos empresariales.

5. Recomendaciones para Estrategias.

5.1 Red Team

Reconocimiento Avanzado: Usar Shodan para mapear dispositivos expuestos y Maltego para correlacionar datos públicos (e.g., dominios, IPs).

El 60% de los breaches comienzan con reconocimiento pasivo (Verizon DBIR 2023), por lo que simular estas técnicas mejora la preparación organizacional.

Ingeniería Social: Ejecutar campañas de phishing con herramientas como SET (Social-Engineer Toolkit).

El 74% de los ataques involucran el factor humano (Verizon 2023), haciendo imprescindible evaluar esta debilidad.

Exploits Personalizados: Desarrollar payloads con Veil o Empire, eludiendo antivirus comerciales.

Las APT usan técnicas avanzadas; replicarlas prepara al Blue Team para amenazas sofisticadas.

5.2 Blue Team

SIEM Robusto: Implementar Wazuh o Splunk con reglas personalizadas para detectar TTPs específicas (e.g., EternalBlue).

La visibilidad en tiempo real reduce el MTTD (Mean Time to Detect) de días a horas (SANS 2023).

Auditorías Frecuentes: Realizar pentests trimestrales y escaneos con Nessus, basados en CIS Benchmarks.

La detección proactiva corrige vulnerabilidades antes de su explotación, un enfoque obligatorio en ISO 27001.

Capacitación: Entrenar al personal en identificación de phishing y uso seguro de credenciales.

Reducir errores humanos mitiga un vector primario de ataques (Verizon 2023).

Estas estrategias fortalecen la capacidad ofensiva y defensiva, asegurando una postura de seguridad integral.

6. Recomendaciones para fortalecer la Seguridad Organizacional.

6.1 Gestión de Parches:

Usar WSUS para aplicar parches críticos (e.g., MS17-010) en un plazo de 30 días tras su lanzamiento.

El 35% de los exploits ocurren en sistemas sin actualizar (NIST 2023), haciendo esto una prioridad básica.

6.2 Principio de Mínimo Privilegio:

Configurar GPOs para restringir permisos administrativos y auditar accesos con Event Viewer.

Limita el daño de cuentas comprometidas, un control clave en CIS v8.

6.3 Herramientas Avanzadas:

Desplegar Snort como IDS/IPS para filtrar tráfico malicioso en tiempo real.

Bloquear ataques en la capa de red reduce la carga en endpoints (SANS 2023).

6.4 Cifrado:

Implementar BitLocker para discos y TLS 1.3 para comunicaciones.

Proteger datos sensibles mitiga el impacto de breaches (IBM 2023).

6.5 Actualizaciones Constantes:

Migrar de Windows 7 a Windows 11, desechando sistemas sin soporte.

Los sistemas obsoletos son un riesgo inaceptable en 2024 (Microsoft 2023).

Estas medidas, alineadas con estándares globales, minimizan la superficie de ataque y aseguran resiliencia.

7. Conclusiones.

Durante el semillero en las Fases 1,2,3 y 4 demostramos que una seguridad eficaz necesita un balance entre el equipo de ataque (Red Team) y el de defensa (Blue Team). El uso de MS17-010 en un sistema anticuado evidenció la negligencia de no dar prioridad a las actualizaciones, mientras que la contención exitosa resaltó la importancia de respuestas rápidas y herramientas como Wazuh. La dimensión moral y jurídica confirma que la transparencia es incuestionable, en concordancia con normativas como la 1273 de 2009.

CyberFort Technologies tiene que implementar las sugerencias administrativas de parches, SIEM, formación con el fin de reducir riesgos y adherirse a normas internacionales. Esta perspectiva no solo resguarda a la organización, sino que también fomenta el progreso del saber en ciberseguridad, fomentando prácticas éticas y técnicas sólidas.

LINK DEL VIDEO SUSTENTACIÓN: https://somup.com/cThvnmMNpw

8. Referencias

Alba, M. (2022). Análisis de metodologías de pentesting, red team y simulación de adversarios. Recuperado de https://www.b-secure.co/blog/pentesting-red-team-y-simulacion- de-adversarios

Congreso de Colombia. (2009). Ley 1273 de 2009. Recuperado de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=35153

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

Intelequia. (2021). Red Team y Blue Team - Funciones y diferencias en ciberseguridad. Recuperado de https://intelequia.com/es/blog/post/red-team-y-blue-team-funciones-y- diferencias-5. La República. (2024). Los ataques cibernéticos serán el principal riesgo global para las empresas en 2024. Recuperado de https://www.larepublica.co/finanzas/los-ataques- ciberneticos-son-el-principal-riesgo-empresarial-global-para-2024-3783263

Ordoñez, W. (2023). Red Team, Blue Team y Purple Team: Guía completa sobre los equipos en ciberseguridad. Recuperado de https://www.grouphacking.com/ciberseguridad/hacking- etico/red-team-blue-team-y-purple-team-guia-completa-sobre-los-equipos-7. Zuluaga Mateus, J. C. (2017). Hacking ético basado en la metodología abierta de testeo de seguridad – OSSTMM, aplicado a la rama judicial, seccional Armenia [Tesis de grado, Universidad Nacional Abierta y a Distancia]. Repositorio UNAD. Recuperado de https://repository.unad.edu.co/handle/10596/17410

CIS. (2023). CIS Benchmarks. Recuperado de https://www.cisecurity.org/cis-benchmarks

Microsoft. (2023). Windows Defender Exploit Guard. Recuperado de https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender- atp/exploit-protection

Wazuh. (2023). Wazuh documentation. Recuperado de https://documentation.wazuh.com

Snort. (2023). Snort documentation. Recuperado de https://www.snort.org/documents

Volatility Foundation. (2023). Volatility documentation. Recuperado de https://www.volatilityfoundation.org

Sysinternals. (2023). Process Explorer. Recuperado de https://docs.microsoft.com/en- us/sysinternals/downloads/process-explorer

FTK Imager. (2023). FTK Imager documentation. Recuperado de https://accessdata.com/product-download/ftk-imager-version-4-5

NIST. (2012). NIST SP 800-61 Revision 2: Computer security incident handling guide. Recuperado de https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Center for Internet Security. (2023). CIS Controls v8. Retrieved from https://www.cisecurity.org/controls/v8/

National Institute of Standards and Technology. (2023). NIST Cybersecurity Framework. Retrieved from https://www.nist.gov/cyberframework

Microsoft. (2023). Security best practices for Windows 10. Retrieved from https://docs.microsoft.com/en-us/windows/security/threat-protection/overview

SANS Institute. (2023). Critical Security Controls. Retrieved from https://www.sans.org/critical-security-controls

MITRE. (2023). ATT&CK Framework. Retrieved from https://attack.mitre.org