CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUE TEAM Y RED TEAM.

ESTUDIANTE

ANDRES FELIPE GARCES ESCOBAR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
2025

CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUE TEAM Y RED TEAM.

SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM

ESTUDIANTE

ANDRES FELIPE GARCES ESCOBAR

Tutor(a) o Director de Curso
LUIS FERNANDO ZAMBRANO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SANTA MARTA
2025

CONTENIDO

pág.

RESUMEN

Este informe detalla las estrategias diseñadas y aplicadas por los equipos Red Team y Blue Team durante los ejercicios prácticos planteados en los distintos escenarios del curso, abordando componentes técnicos, éticos y legales. Se identifican vulnerabilidades críticas, se explican las técnicas de ataque y defensa, y se brindan recomendaciones concretas para fortalecer la postura de seguridad organizacional.

GLOSARIO

Blue Team: Equipo defensivo encargado de detectar, contener y mitigar ataques.

Exploit: Código o técnica que aprovecha vulnerabilidades.

Malware: Software malicioso diseñado para infiltrarse o dañar sistemas.

PoC: Prueba de concepto para demostrar la explotación de una vulnerabilidad.

Red Team: Equipo ofensivo que simula ataques para identificar vulnerabilidades.

SIEM: Sistema de Gestión de Información y Eventos de Seguridad.

INTRODUCCIÓN

La ciberseguridad es una disciplina que requiere enfoques ofensivos y defensivos coordinados. Este informe presenta las estrategias y tácticas aplicadas por los equipos Red Team y Blue Team, bajo los escenarios de prueba definidos por CyberFort Technologies. Se abordan desde las técnicas empleadas para explotar vulnerabilidades, hasta las defensas implementadas para mitigar ataques, integrando además un análisis ético y legal necesario para comprender el alcance completo de las operaciones de ciberseguridad.

OBJETIVOS

- **OBJETIVO GENERAL**

Analizar y documentar las estrategias implementadas por los equipos Red Team y Blue Team para fortalecer la seguridad organizacional.

- **OBJETIVOS ESPECÍFICOS**

1. Identificar las principales vulnerabilidades explotadas durante los ejercicios Red Team.
2. Describir detalladamente las tácticas defensivas aplicadas por el Blue Team.
3. Examinar las implicaciones éticas y legales en cada escenario.
4. Proponer recomendaciones para robustecer la infraestructura de seguridad.

DESARROLLO DEL INFORME

Actuación ética y legal – Etapa 2

Después de un análisis detallado del anexo 3, se llega a la conclusión de que en la cláusula primera no se establece ninguna prohibición de denunciar actos ilegales, pero sí se configura una coacción al firmante para encubrir delitos como el espionaje y el acceso abusivo a sistemas informáticos. Esto va en contra del deber ciudadano de denunciar actos delictivos, además de vulnerar múltiples artículos del Código Penal. También, en la cláusula octava, se observa una exención de responsabilidad para CyberFort, donde claramente se intenta anular la responsabilidad penal de la empresa incluso en caso de participación en delitos, lo cual no es jurídicamente válido ni éticamente aceptable. Además se establece una confidencialidad sobre actos ilegales, lo que contradice de forma notoria la Ley 1273 de 2009 y los principios básicos del derecho penal y ético, ya que los delitos no pueden estar protegidos por cláusulas de confidencialidad.

En relación con la Ley 1273 de 2009, se identifican vulneraciones a varios artículos, incluyendo el Art. 269A (Acceso abusivo a un sistema informático), dado que en la cláusula mencionada se obliga a no denunciar estos accesos, implicando un encubrimiento. Además, se vulnera el Art. 269E (Violación de datos personales), ya que se obliga a no denunciar actividades que vulneran datos de terceros, incurriendo así en complicidad pasiva. Finalmente, también se ve comprometido el Art. 269F (Uso de software malicioso), ya que el encubrimiento de software malicioso utilizado en CyberFort puede considerarse como complicidad en el delito informático.

Frente a la pregunta de si, existiendo estos procesos poco confiables en el anexo 3, aplicaría al trabajo en CyberFort Technologies, que ofrece un sueldo de $15.000.000 de pesos colombianos mensuales y contrato vitalicio, la respuesta es negativa. Como experto en ciberseguridad y bajo el Código de Ética de COPNIA, que establece que los ingenieros deben actuar con responsabilidad, transparencia y respeto por las normas jurídicas y sociales, aceptar o aplicar a este contrato iría en contra del deber de proteger los intereses públicos y respetar el orden legal. Esto comprometería mi integridad profesional y me convertiría en cómplice de los delitos informáticos mencionados. Ni el salario elevado ni el contrato vitalicio justificarían ceder ante cláusulas ilegales e inmorales.

Analizando el caso problema en el anexo 7, considero que las empresas de ciberseguridad deben tener acceso limitado y explícitamente autorizado a la información sensible de sus clientes durante una auditoría de seguridad. Este acceso debe estar sustentado por un contrato claro, contar con el consentimiento previo del cliente y ser registrado y supervisado por auditores externos. Y también, para evitar que los empleados utilicen herramientas avanzadas de análisis forense con fines no autorizados o éticamente cuestionables, es fundamental implementar auditorías internas y externas periódicas, asegurar que los registros de todas las acciones forenses sean inalterables mediante cadenas de custodias y separar las funciones entre quienes auditan y quienes analizan los datos.

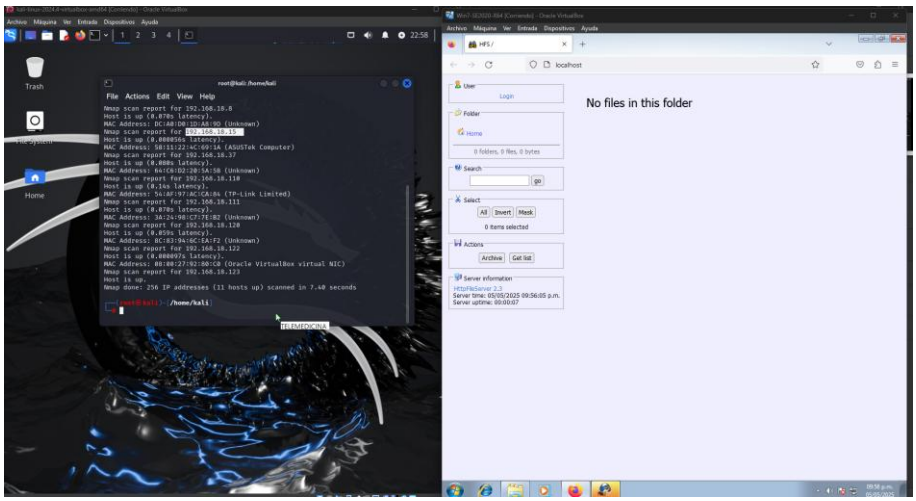
De aquí, podemos decir que el gobierno o/y organizaciones que descubran que una empresa de ciberseguridad contratada ha cometido actos de ciberespionaje deben actuar con contundencia, cancelando el contrato de inmediato, interponer denuncias penales, crear listas negras de proveedores inseguros y emitir comunicados públicos para restaurar la confianza y asegurar que estos hechos no se repitan.

Ejecución de pruebas de intrusión – Etapa 3.

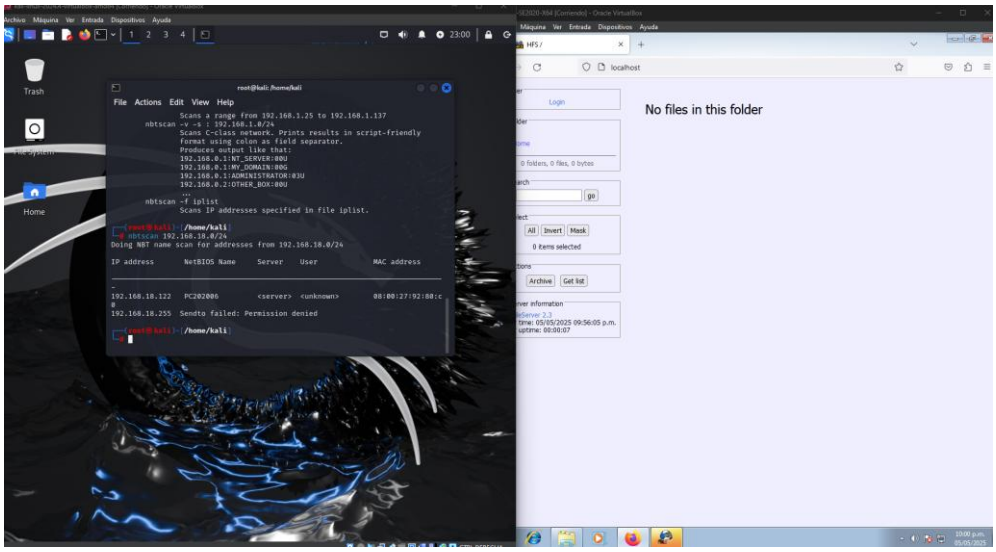
En esta etapa iniciamos el proceso de pruebas mediante dos maquinas y que explicare a continuación lo realizado:

Inicialmente ya hemos configurado nuestras maquinas virtuales para crear comunicación entre ellas.

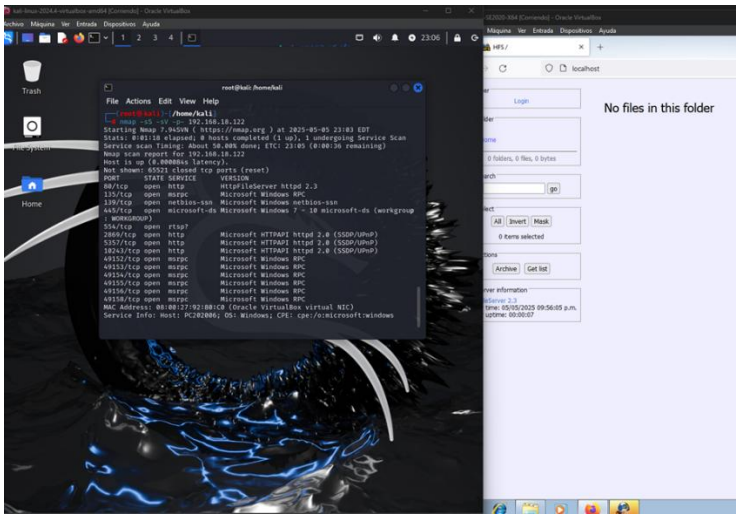
Ya después iniciamos a scanear la red con Nmap.



Aquí ya encontramos la IP de la máquina que necesitamos identificar. Con nbtscan buscamos el nombre de esta máquina. (Para esto se debe tener abierto Rejjeto ya que es aquí donde se abre la vulnerabilidad.)

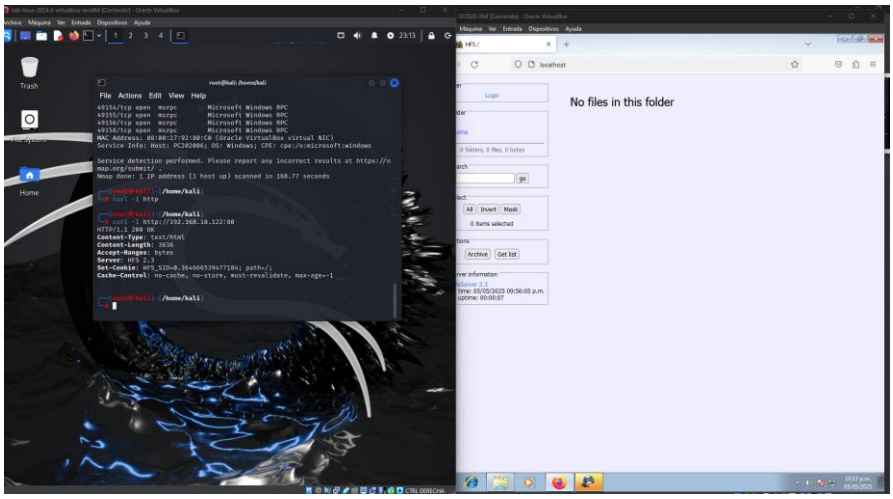


Observamos que el nombre de la maquina vulnerable es PC202006.

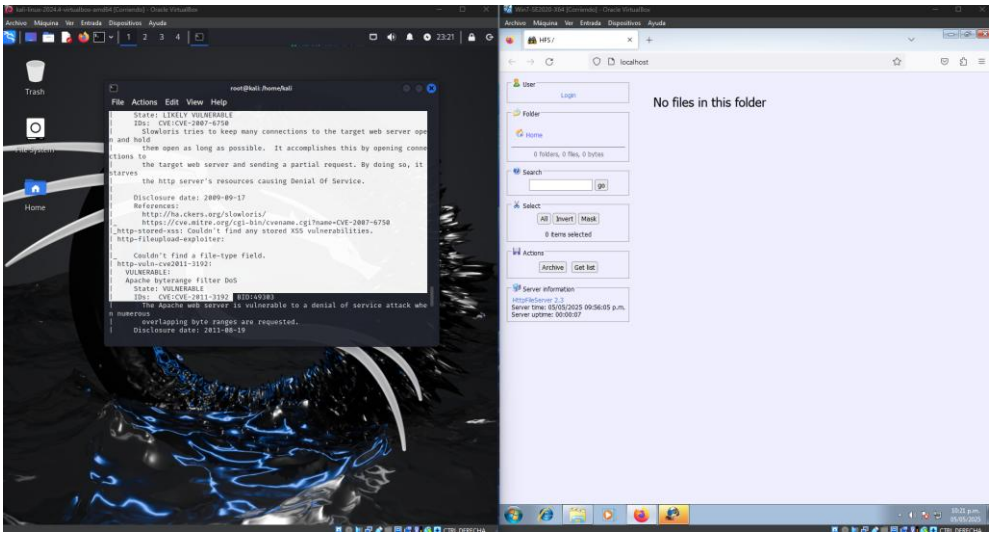


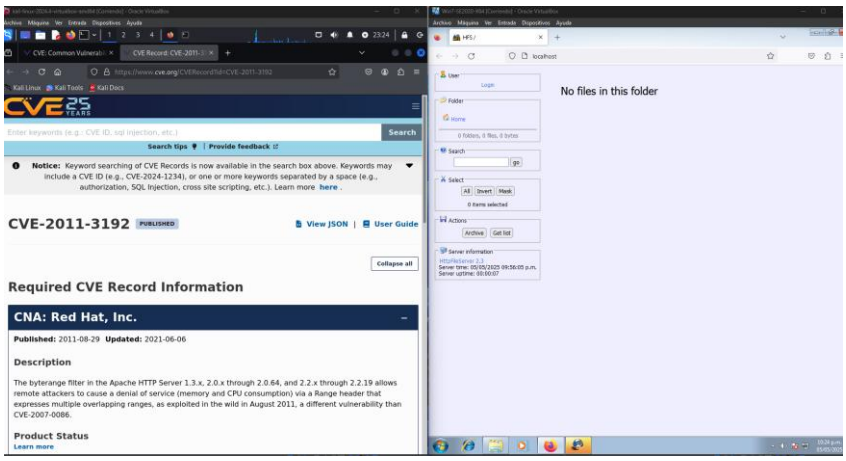
Despues utilizamos Nmap con el fin de scanear puertos y ver cual se encuentra vulnerable para explotar. Donde claramente encontramos el puerto 80 http. Siendo este donde trabajan los archivos de Rejjeto.

Ahora verificamos que la versión del rejjeto es 2.3, siendo vulnerable.

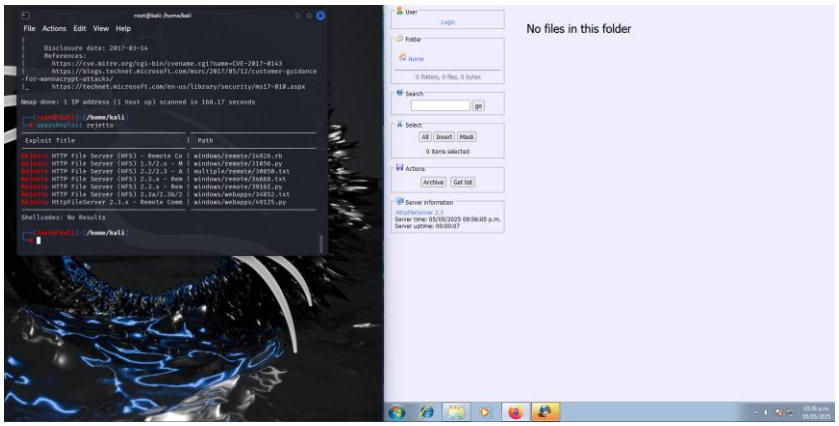


Despues ya con curl -I http:// 192.168.18.122:80 verificamos la vulnerabilidad CVE-2011-3192. Alli encontramos dos vulnerabilidades pero explotaremos la mencionada.

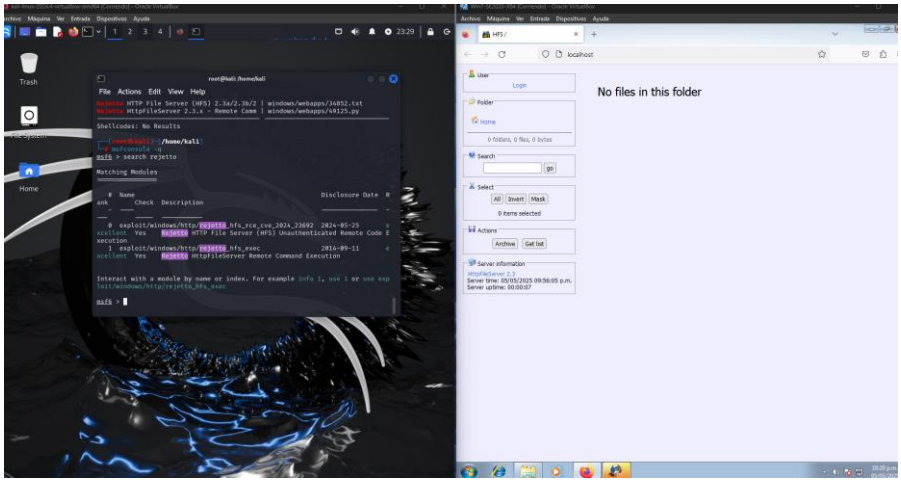


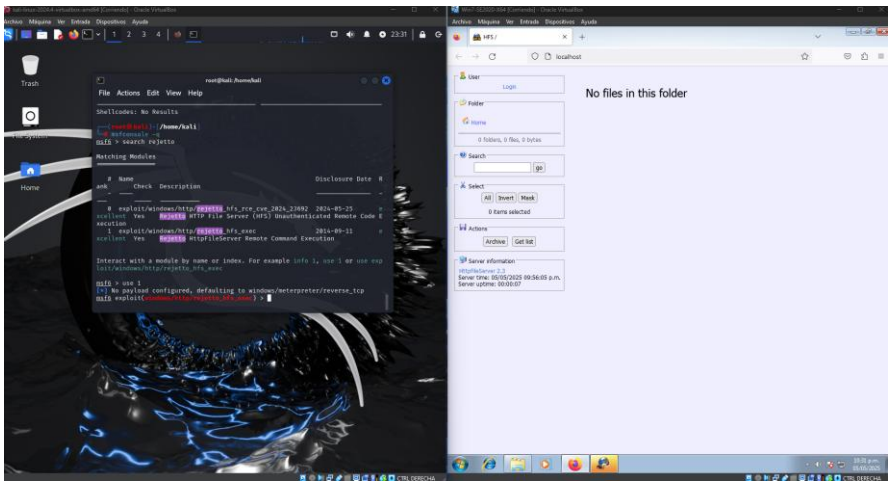


Ahora buscamos que exploit tenemos con rejjeto.

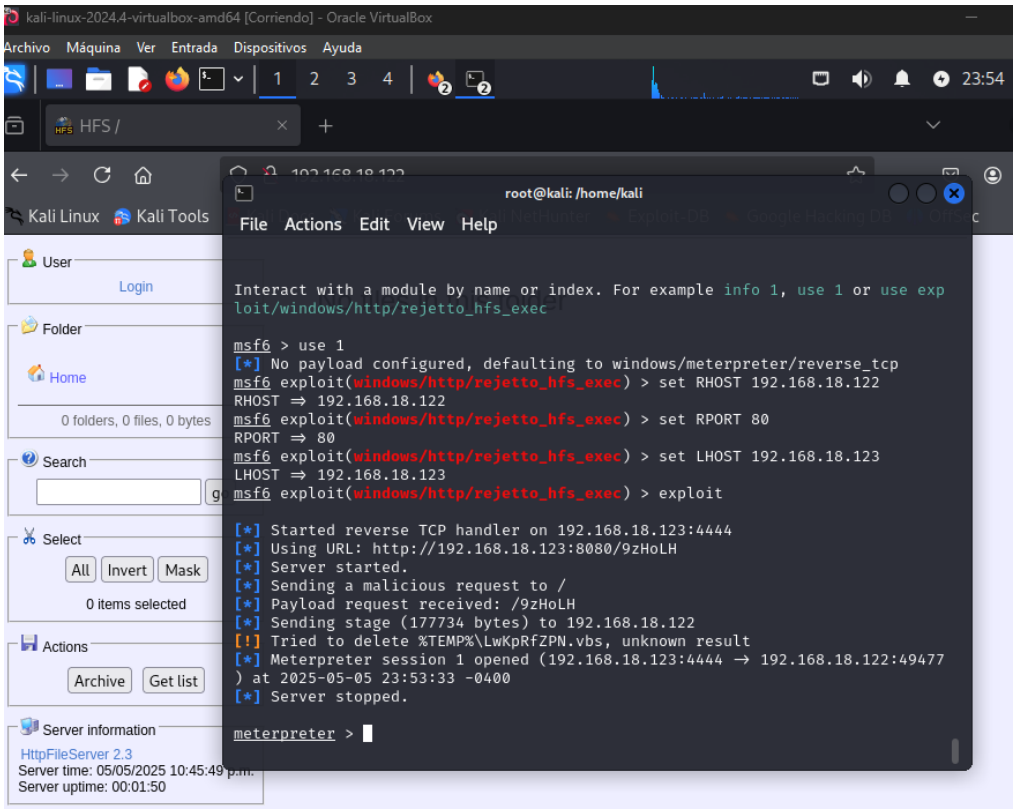


Encontramos 2 exploit. En el cual utilizaremos el “1”

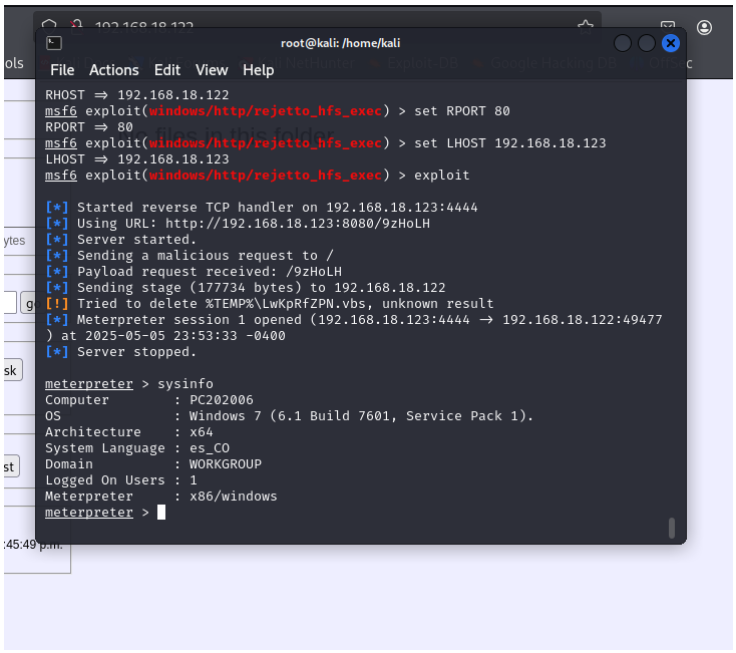




Configuramos payload.

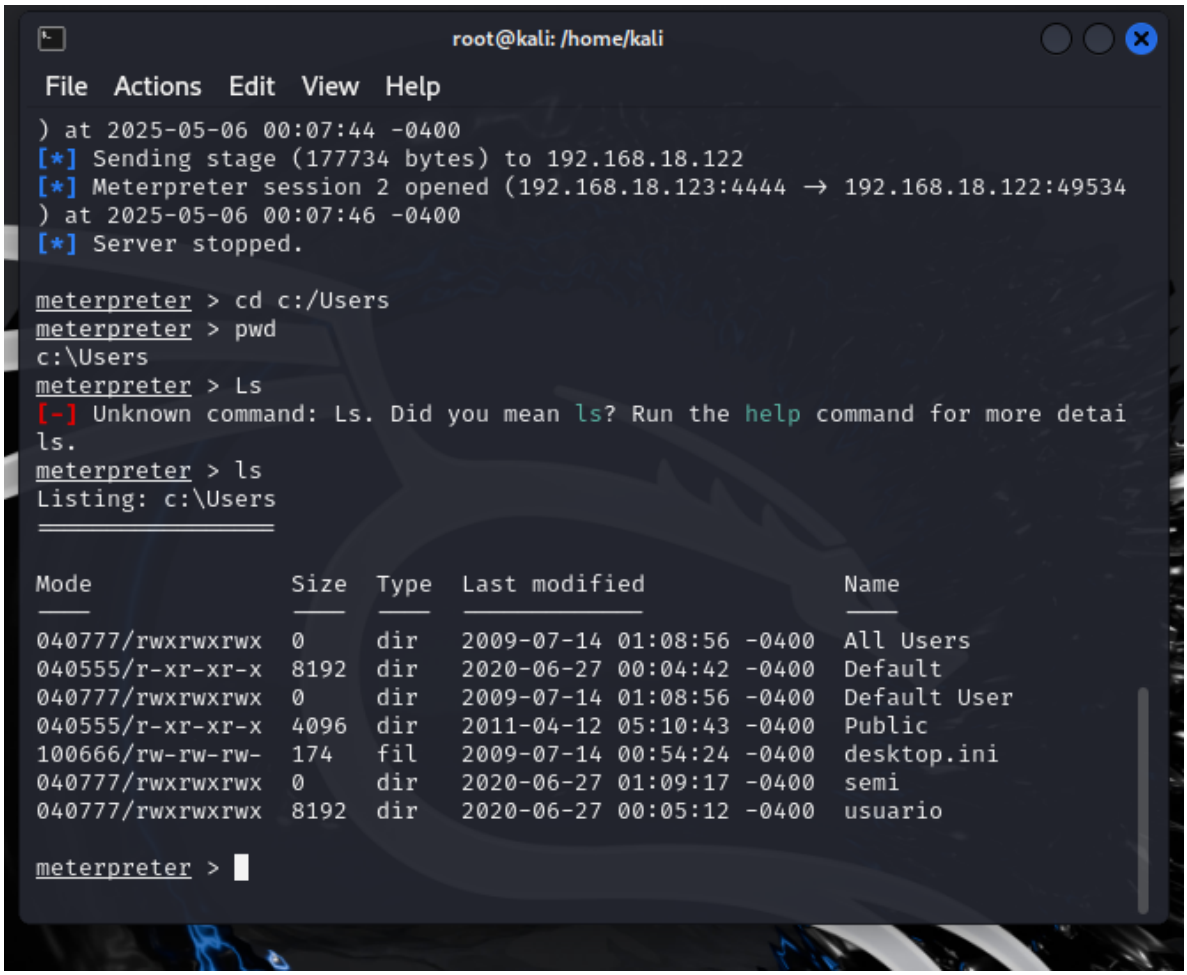


Abrimos la sesión y buscamos toda la info de la maquina iniciada.

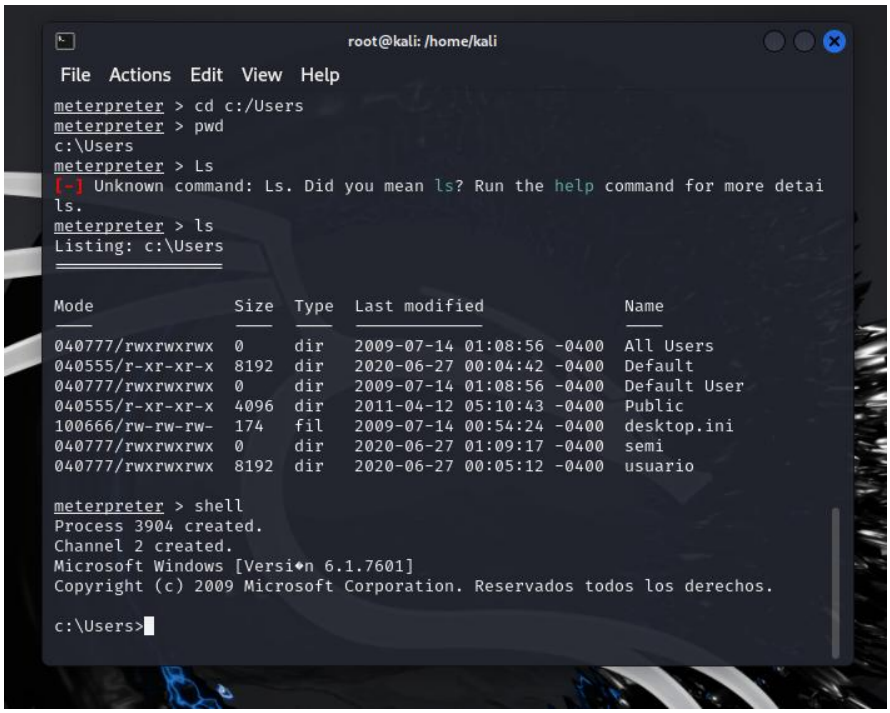


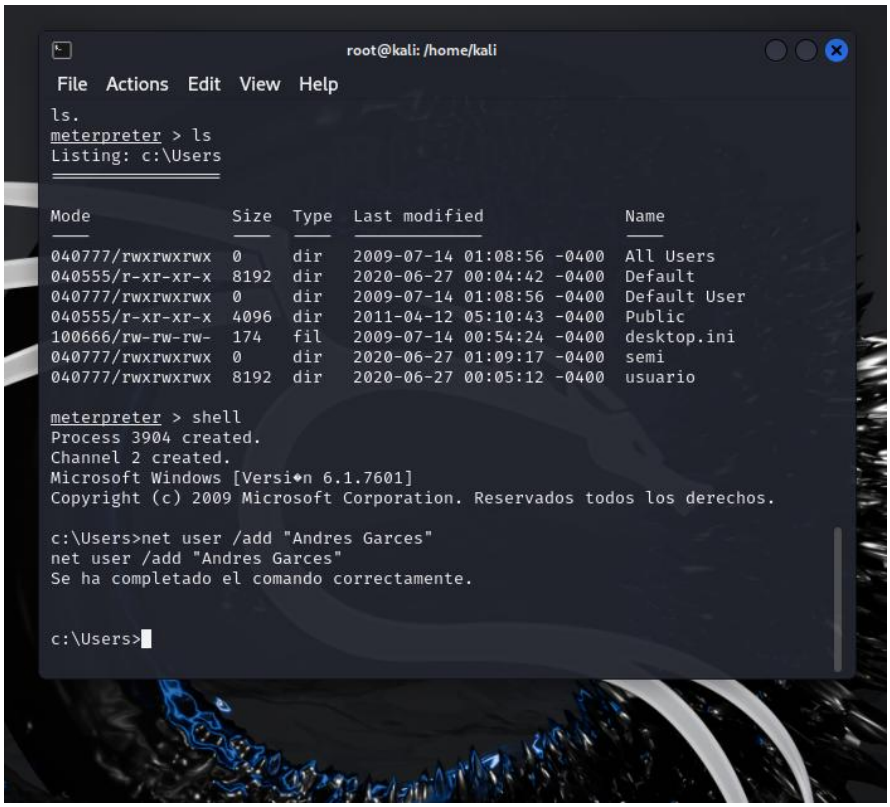
Al realizar la ya explotación iniciamos con la post explotación en la maquina.

Procedemos a ver la información de los usuarios.

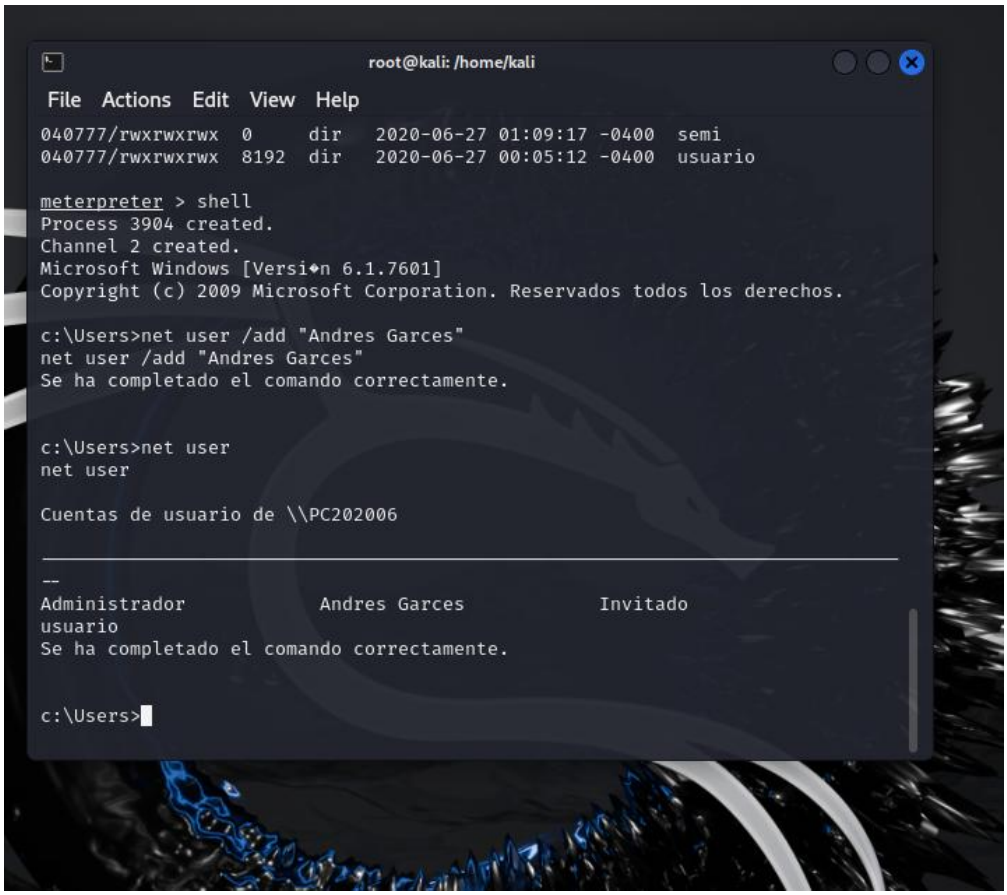


Abrimos consola Shell para proceder a crear el usuario administrador.

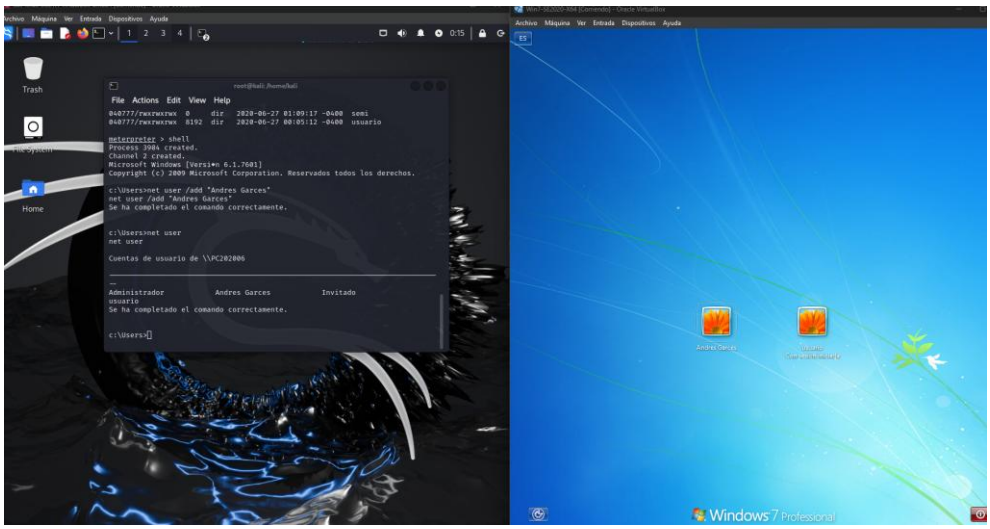


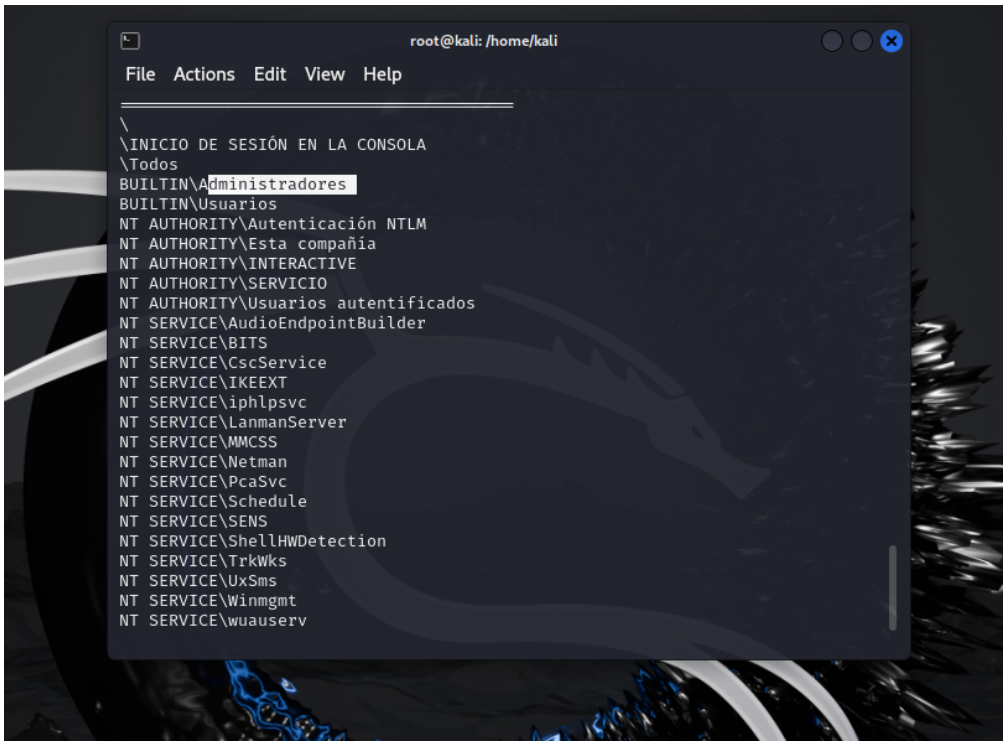


Creamos el usuario de manera exitosa “ Andres Garces”

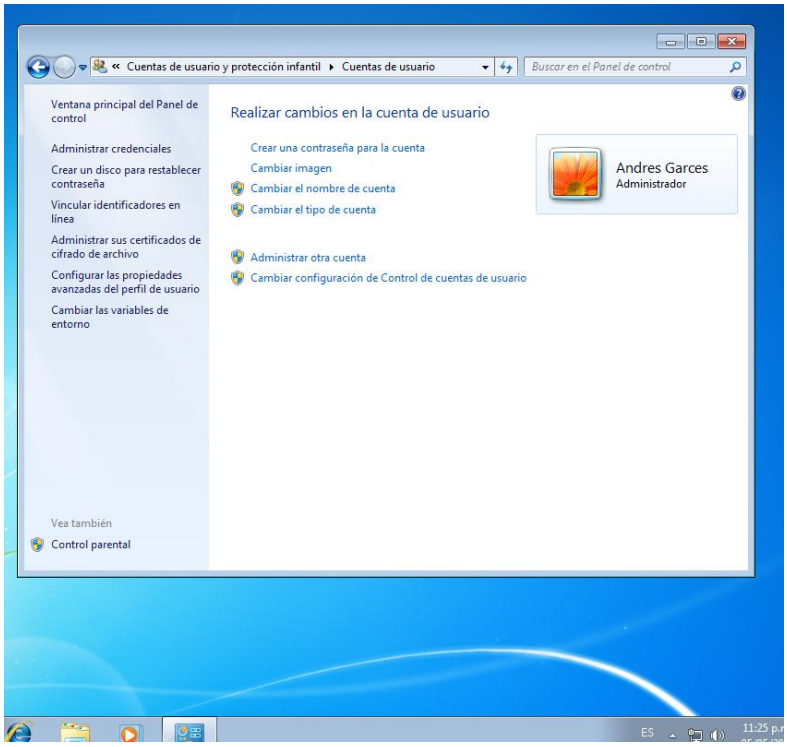


Verificamos en Windows.



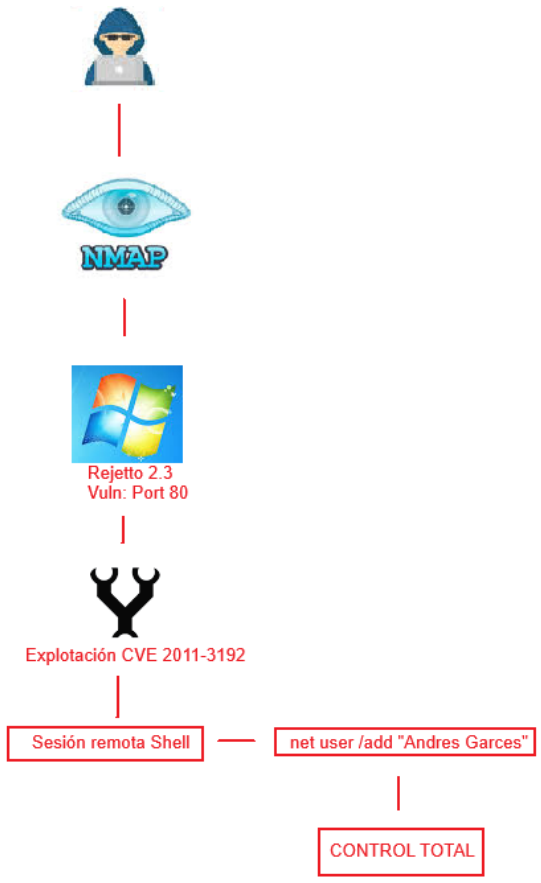


Agregamos el usuario a Administradores.



De aquí concluimos que se afecta a una máquina Windows al explotar una

vulnerabilidad conocida en un servidor web (en este caso, el software vulnerable se llama "Rejjeto", versión 2.3), lo que permite al atacante obtener acceso remoto y privilegiado. Al estar abierto el puerto 80 queda vulnerable la máquina, con la siguiente grafica explicare de una mejor manera:



Contención de ataques informáticos – Etapa 4.

Para contener un ataque en tiempo real, lo primero sería aislar la máquina comprometida de la red, ya sea desactivando la interfaz de red, desconectando el cable físico o la conexión Wi-Fi. Luego, se revisarían los procesos activos usando herramientas como Tasklist para identificar procesos sospechosos o sin firma, así como netstat -ano para verificar conexiones activas, puertos abiertos y posibles conexiones no autorizadas. Con

Wireshark se capturaría el tráfico de red para detectar patrones anómalos, y finalmente, se recolectarían los logs del sistema para rastrear el origen del ataque.

En cuanto a las acciones de hardenización para prevenir ataques, se implementarían:

- Aplicación de políticas de grupo (GPO) para restringir ejecución de scripts en carpetas temporales.
- Deshabilitación de servicios innecesarios que puedan ser explotables.
- Políticas de contraseñas robustas y autenticación multifactor.
- Software policies para bloquear aplicaciones no autorizadas.
- Actualizaciones regulares del sistema operativo y software.
- Eliminación de privilegios administrativos innecesarios.

Sobre las diferencias entre el Blue Team y el equipo de respuesta a incidentes, el Blue Team tiene una función proactiva y defensiva, dedicándose a la monitorización continua y configuración segura, mientras que el equipo de respuesta a incidentes actúa de forma reactiva, movilizándose solo cuando ocurre un incidente para contener, erradicar y recuperar.

Trabajar con el Center for Internet Security sería pertinente para el Blue Team, ya que permite establecer configuraciones seguras para sistemas operativos, dispositivos de red y aplicaciones, realizar auditorías de cumplimiento con estándares internacionales y reducir la superficie de ataque siguiendo buenas prácticas de ciberseguridad.

Un SIEM es una herramienta clave que recolecta, correlaciona y analiza registros generados por diferentes dispositivos y aplicaciones dentro de una infraestructura. Su función principal es generar alertas en tiempo real ante comportamientos sospechosos y facilitar análisis forense después de un incidente, ofreciendo visibilidad centralizada de la red y ayudando a cumplir normativas de seguridad. Un ejemplo de SIEM de código abierto es Wazuh, que permite funciones avanzadas de correlación en entornos Windows, Linux y en la nube.

Finalmente, tres herramientas esenciales para contener ataques informáticos son:

- Firewall, como UFW o IPTables en Linux, que permite establecer reglas para filtrar y bloquear tráfico sospechoso, denegar IPs no autorizadas, cerrar puertos innecesarios o restringir protocolos inseguros.
- Egress Filtering, usando soluciones como pfSense, que controla el tráfico saliente para impedir la comunicación de malware con servidores externos y evitar la exfiltración de datos.
- Sistemas de prevención de intrusiones (IDS/IPS), que permiten detectar y bloquear ataques en tiempo real, reduciendo el impacto y alcance de las amenazas.

Etapa 5.

El conjunto de acciones descritas muestra un enfoque integral para enfrentar amenazas de ciberseguridad, combinando respuestas inmediatas, con medidas preventivas como la hardenización del sistema, aplicación de políticas de seguridad y eliminación de privilegios innecesarios.

Además, se destaca la diferencia clara entre los roles del Blue y el equipo de respuesta a incidentes, resaltando que ambos son necesarios para mantener la seguridad organizacional. El uso de estándares como los del CIS y herramientas como los SIEM permite fortalecer la postura de seguridad, garantizando monitoreo continuo, generación de alertas y cumplimiento normativo.

CONCLUSIONES

- Las vulnerabilidades en aplicaciones comunes pueden comprometer sistemas críticos si no son gestionadas adecuadamente.
- Las acciones defensivas del Blue Team son fundamentales no solo para contener ataques, sino para evitar reincidencias.
- Los aspectos éticos y legales no pueden ignorarse en ninguna práctica de ciberseguridad; son la base para construir una cultura organizacional confiable.

RECOMENDACIONES

- Mantener inventarios actualizados de activos y vulnerabilidades.
- Capacitar regularmente a los equipos técnicos en ataques y defensas emergentes.
- Implementar controles éticos internos para reforzar el cumplimiento legal.
- Realizar pruebas periódicas Red/Blue Team para evaluar la resiliencia organizacional.

ASPECTOS QUE APORTAN AL DESARROLLO DE RED Y BLUE TEAM.

- Las prácticas del Red Team permiten identificar fallas antes de que sean explotadas por atacantes reales.
- Las actividades del Blue Team fortalecen las respuestas inmediatas y mejoran los mecanismos de recuperación.
- La colaboración entre ambos equipos genera un ciclo de aprendizaje continuo y mejora los estándares de seguridad.

RECOMENDACIONES PARA EL PLANTEAMIENTO DE ESTRATEGIAS QUE PERMITAN ENDURECER LOS ASPECTOS DE SEGURIDAD EN UNA ORGANIZACIÓN.

- Aplicar el principio de mínimo privilegio a todos los usuarios y servicios.
- Configurar sistemas de detección y respuesta ante incidentes (SIEM).
- Establecer políticas de parches y actualizaciones regulares.
- Fomentar una cultura organizacional enfocada en la seguridad y la ética.

CONCLUSIONES QUE PERMITAN LAS CONSTRUCCION DEL CONOCIMIENTO DESDE EL ENFOQUE DE LA CIBERSEGURIDAD.

La ciberseguridad no depende únicamente de herramientas tecnológicas, sino de estrategias integrales que incluyan prácticas ofensivas, defensivas y una estricta adherencia a principios éticos y legales. Las organizaciones que adoptan este enfoque integral están mejor preparadas para enfrentar amenazas avanzadas y proteger su infraestructura crítica.

VIDEO SUSTENTACION.

https://youtu.be/-tVnwXjxtLU

BIBLIOGRAFIA

CIS Security. (2020). CIS Center for Internet Security. CIS Benchmarks . https://www.cisecurity.org/cis-benchmarks/

CCN Cert. (2018). Guía de seguridad de las TIC (CCN-STIC-495) Seguridad en IPv6. CCN Cert. (pp. 10-29) . https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/1617-ccn-stic-495-seguridad-en-ipv6/file.html

Zambrano Hernández, Peña Hidalgo, H. J., & Cardenas Corral. (2024). Guía Para la Gestión y Clasificación de Incidentes de Ciberseguridad Abrir este documento utilizando ReadSpeaker docReader. Sello Editorial UNAD. https://selloeditorial.unad.edu.co/images/Documentos/ciberseguridad/Gu%C3%ADa_para_la_Gesti%C3%B3n_y_Clasificaci%C3%B3n_de_un_Incidentes_de_Ciberseguridad.pdf

Incibe. (2019). ¿Qué es el pentesting? Auditando la seguridad de tus sistemas . INCIBE. https://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditando-seguridad-tus-sistemas

Rajendran, J., Jyothi, V., & Karri, R. (2011). Blue team red team approach to hardware trust assessment. 2011 IEEE 29th International Conference on Computer Design (ICCD), 285-288 . https://doi.org/10.1109/ICCD.2011.6081410

Moreno, Patricio. (2015). Técnicas de detección de ataques en un sistema SIEM (Security Information and Event Management. Usfq. (pp. 31-63) Abrir este documento utilizando ReadSpeaker docReader. http://repositorio.usfq.edu.ec/bitstream/23000/4911/1/120801.pdf

Boek, A. J. R., & de León, C. A. N. (2011). De los delitos informáticos: Ley 1276 de 2009. In Manual de Derecho penal: Parte especial (pp. 624-641). Temis. https://dialnet.unirioja.es/servlet/articulo?codigo=4678589

Copnia. (2015). Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. Copnia. (pp. 3-26) . https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

Kotwani, B., Sawant, M. R., & Chopra, D. S. (2023). Red Teaming vs. Blue Teaming: A Comparative Analysis of CyberSecurity Strategies in the Digital Battlefield . INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT, 07(12), 1-11. https://doi.org/10.55041/IJSREM27675

Incibe. (2019). ¿Qué es el pentesting? Auditando la seguridad de tus sistemas . INCIBE. https://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditando-seguridad-tus-sistemas

PandaSecurity. (2018). Pentesting: Una herramienta muy valiosa para tu empresa. Panda Security Mediacenter . https://www.pandasecurity.com/spain/mediacenter/seguridad/pentesting-herramienta-empresa

Rapid7. (2012). Metasploitable 2 . (s. f.). Metasploit. https://metasploit.help.rapid7.com/docs/metasploitable-2

Revista Seguridad. (2018). Pruebas de penetración para principiantes: Explotando una vulnerabilidad con Metasploit Framework | Revista. Seguridad. https://revista.seguridad.unam.mx/numero-19/pruebas-de-penetraci%C3%B3n-para-

principiantes-explotando-una-vulnerabilidad-con-metasploit-fra

Diogenes, Y., & Ozkaya, E. (2018). Cybersecurity-attack and defense strategies: Infrastructure security with red team and blue team tactics. Packt Publishing Ltd. https://books.google.es/books?hl=es&lr=&id=pyZKDwAAQBAJ&oi=fnd&pg=PP1&dq=Blue+y+red+team&ots=VtFqFTsw3Z&sig=DV6w9HKbe6MoQipu97ayLhs9QHg#v=onepage&q=Blue%20y%20red%20team&f=false

Rajendran, J., Jyothi, V., & Karri, R. (2011, October). Blue team red team approach to hardware trust assessment. In 2011 IEEE 29th international conference on computer design (ICCD) (pp. 285-288). IEEE. https://ieeexplore.ieee.org/abstract/document/6081410