CAPACIDADES TECNICAS, LEGALES Y DE GESTION PARA EQUIPOS BLUE TEAM Y RED TEAM

YENNIFER ANDREA VARGAS SANTOFIMIO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA “UNAD”
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
FLORENCIA, CAQUETÁ
2020

CAPACIDADES TECNICAS, LEGALES Y DE GESTION PARA EQUIPOS BLUE TEAM Y RED TEAM

YENNIFER ANDREA VARGAS SANTOFIMIO

Seminario Especializado

Director: JOHN FREDDY QUINTERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA “UNAD”
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
FLORENCIA, CAQUETÁ
2020

RESUMEN

En la actualidad la seguridad informática cumple un papel muy importante porque es un componente que permite brindar protección a la infraestructura de una organización para este caso es la red (LAN Y WLAN), equipo de cómputo, sistema operativo la cual permite crear y aplicar procesos y procedimientos para lograr garantizar la confidencialidad, integridad y disponibilidad de la información en un sistema y así poderles brindar seguridad a todas las personas que su información será protegida y manejada de una manera segura.

Mantener a una entidad sea pública o privada libre de riesgos informáticos es de vital importancia para disponer de un correcto funcionamiento de la infraestructura física y de los servicios que necesiten, es por ello que se deben implementar políticas de seguridad que promuevan el buen uso de todo lo que compone la BLUE TEAM, desde los dispositivos y mobiliario, hasta los servicios y el personal que la integran.

Todo esto analizando desde las vulnerabilidades que puedan poseer, los riesgos que se pueden presentar, hasta los ataques que se ejecuten (RED TEAM) que pongan en riesgo la integridad, disponibilidad y confidencialidad de la entidad, para posteriormente realizar planes de contingencia que eviten que un daño mayor pueda suceder, esto se hace con ayudas de herramienta de monitoreo de amenazas que dicen el problema como la posible solución.

INDICE

TABLA DE ILUSTRACIONES

Pag

TABLAS

GLOSARIO

HÁBEAS DATA: es un derecho constitucional que tiene todas las personas para solicitar, obtener información existente y eliminar o actualizar dicha información.

PENETRACION O PENTESTING: es una práctica utilizada para revisar la seguridad de red.

METAGOOFIL: Permite la obtener metadatos (todo tipo de archivo).

DNSENUM: Captura información sobre un dominio.

FIERCE: Escáner para enumerar las IP y los host para dominios.

NMAP: Permite escanear e identificar los servicios que se ejecutan en un equipo remoto.

OPENVAS SCANNER: Es un sistema que permite evaluar vulnerabilidades de seguridad en servidores y dispositivos de red.

RED TEAM: es un proceso de emulación de escenarios de amenazas que una empresa puede afrontar con el propósito de identificar las vulnerabilidades.

BLUE TEAM: es un grupo de seguridad que protege a la empresa de posibles ataques

COPNIA: Consejo Profesional Nacional de Ingeniería

BUGGLY: Establecimiento publico

METASPLOIT: Es un conjunto completo de herramientas utilizadas para probar la vulnerabilidad de los sistemas de información.

EXPLOIT: es un código que permite vulnerar la seguridad de un sistema y así lograr ingresar sin ningún problema

DASHBOARADS: es un tablero que proporciona vista de indicadores clave de rendimientos.

HARDENIZACIÓN: es el proceso de aseguramiento a un sistema mediante la reducción de vulnerabilidades

SIM: recopila datos, detallando informes a las personas a cargo de la seguridad de la información e informática de la empresa

INTRODUCCION

Hoy día el mundo gira al entorno de los sistemas de la información, se ha convertido en una pieza esencial para el funcionamiento vital de todas las organizaciones, donde se realizan procedimientos, se selecciona y se clasifica la información, permitiendo que las organizaciones manejen su información a través de redes de comunicación.

La normatividad vigente en Colombia sobre delitos informáticos y protección de datos personales ha sido poco a poco actualiza con el objetivo de aplicar el Artículo 15 de la Constitución Política, derecho adquirido por todos los colombianos, que es conocer, actualizar y rectificar los datos personales que reposa en base de datos, en archivo físico que se encuentran en las diferentes entidades públicas y privadas.

La tendencia a la conectividad trae consigo amenazas, vulnerabilidades y riesgos que a su vez generan la necesidad de protección de bienes y de la información, por ello es necesario, la publicación de las leyes para que todos los colombianos tengan conocimiento de sus derechos y deberes relacionado a la seguridad informática.

En el siguiente documento se presentará un informe detallado del procedimiento llevado a cabo en el Seminario especializado: equipos estratégicos en ciberseguridad: red team & blue team, siendo de gran importancia para evidenciar los resultados de vulnerabilidades y riesgos, las soluciones que se implementaron para corregirlos.

En la empresa se analizaron todos los componentes de la infraestructura física que hacen parte del Blue Team, estos se llaman activos y son los que pueden estar más expuestos a ciertas amenazas que posiblemente ocasionen daños graves. Es importante saber que se deben seguir todos los procesos de manera estricta para evitar posibles fallas ocasionadas por el mal manejo de los elementos involucrados en la red.

OBJETIVO GENERAL

Evaluar las acciones de los equipos Red Team y Blue Team de la organización WhiteHouse Security.

OBJETIVOS ESPECÍFICOS

- Identificar conceptos de seguridad
- Verificar procesos no éticos y legales en un acuerdo de trabajo
- Realizar pruebas de intrusión
- Contención de ataques informáticos

.

1. NORMATIVIDAD VIGENTE EN COLOMBIA

1.1. LEY 1266 DEL 31 DE DICIEMBRE DEL 2008

Por medio de la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en base de datos personales, en especial la financiera, crediticia, comercial, de servicios y la provenientes de tercero países y se dictan otras disposiciones

La Ley 1266 de 2008, es conocida como la Ley de Habeas Data, donde establece que toda persona tiene derecho a conocer, actualizar y rectificar la información que existe en entidades financieras y en base de datos, mediante el cual regula como se debe manejar los datos personales y demás derechos relacionados con la recolección, tratamiento y circulación de la información.

La Ley estable que:

- Todo entidad pública o privada no puede realizar ningún reporte negativo en el historial crediticio sin previo aviso.

- Establece los procedimientos para realizar un trámite de reclamo ante la entidad pública y privada

- El incumplimiento de esta ley la Superintendencia de Industria y Comercio y Superintendencia Financiera interpondrá sanciones como multas, suspensión de las actividades y cierre o clausura de las actividades de los bancos de datos.

1.2. LEY 1273 DEL 5 DE ENERO DEL 2009

“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”

La Ley 1273 de 2009 estableció diferentes delitos, con el objetivo de lograr proteger la información y datos de los colombianos, en la cual estableció penas de prisión de treinta y seis hasta ciento veinte meses y multas de cien hasta mil quinientos salarios minimis legales.

Establecido el delito como una conducta concerniente con el manejo de datos personales que están almacenados en base de datos de una entidad pública o

privada, la presente ley tiene como propósito de garantizar la protección a la información personal y así poder garantizar el derecho a la integridad.

Establecido los siguientes tenores como Acceso abusivo a un sistema informático, Obstaculización ilegítima de sistema informático o red de telecomunicación, Interceptación de datos informáticos, Daño informático, Uso de software malicioso, Violación de datos personales, Suplantación de sitios web para capturar datos personales, Hurto por medios informáticos y semejantes, Transferencia no consentida de activos

Todo colombiano puede efectuar denuncias ante el ente regulador si le están vulnerado su derecho a la integridad.

1.3. LEY 1581 DEL 17 DE OCTUBRE DEL 2012

"Por la cual se dictan disposiciones generales para la protección de datos personales"

La ley 1581 tiene como propósito aplicar el Artículo 15 de la Constitución Política, derecho adquirido por los Colombianos, que es conocer, actualizar y rectificar los datos personales reposados en base de datos, en archivo físico que se encuentran en las diferentes entidades públicas y privadas.

La Ley 1581 implementa medidas y políticas de seguridad, nombra la Superintendencia de Industria y comercio como ente regulador, una empresa cuando maneja Base de Datos deben registrarla, informar y garantizar la privacidad de los clientes, solo podrán utilizar la información autorizada y así evitar Demandas, Sanciones y Multas.

Las entidades deben solicitar previa autorización para manejar datos sensibles como origen étnico, partido político, historia clínica, orientación sexual, datos biométricos y datos de menores de edad, una vez se establezca que se está vulnerando su derecho constitucional puede interponer la Acción de tutela.

1.4. DECRETO 1377 DEL 27 DE JUNIO DEL 2013

Por el cual se reglamenta parcialmente la Ley 1587 de 2012

Tiene como propósito de realizar modificaciones y aclaraciones a la Ley 1581 de 2012, donde permite establecer con claridad algunos conceptos a la hora de identificar el tipo de dato, recolección de datos, autorización para el tratamiento de datos sensible, políticas de tratamiento a la información, el ejercicio de los derechos del titular, transferencia de la información y la responsabilidad frente al manejo de la información.

2. PRUEBAS DE PENETRACION O PENTESTING

Es una técnica que se utiliza para evaluar la seguridad de red, que se trata en realizar pruebas contra los mecanismos existentes de defensas en lo que se está analizando, para obtener resultados en las pruebas se debe realizar un análisis absoluto de los dispositivos tanto digitales y físicos, lo que se pretende con estas prueba es comprobar cuál es el comportamiento de los mecanismos de defensa, detectar las vulnerabilidades, fallas en los controles de seguridad y las brechas que existen, para ello se debe someter el sistema a medidas extremas.

La mayoría de las empresas presentan incidentes como la fuga de la información, accesos no autorizados, perdida de datos que se podría haberse evitado, en cuanto hubieran reforzado la protección en su debido momento.

2.1. FASES DE UNA PRUEBA DE PENETRACION

2.1.1. FASE DE CONTACTO

Es la fase inicial donde se realiza el contacto directo con el cliente para acordar como se va a realizar la prueba de penetración, aspectos como los servicios que se van a incluir, establecer los objetivos de la prueba, los puntos críticos de la empresa, se les explica el daño que se presentaría en caso de un ataque y por último se debe realizar una autorización por escrito.

2.1.2. FASE DE RECOLECCIÓN DE INFORMACIÓN

En esta fase se debe trabajar en el reconocimiento de la empresa, recopilar toda la información necesaria para hacer el trabajo y obtener los resultados esperados, se debe identificar toda la infraestructura posible como los sistemas, programas y demás que se requiera, es muy importante seguir la actividad de la empresa en las redes sociales para lograr información y así poder realizar el test de penetración

2.1.3. FASE DE MODELADO DE AMENAZA

De acuerdo a la información obtenida se debe definir una estrategia para realizar la prueba de penetración y establecer los objetivos para así poderlos cumplir sin tener un resultado inesperado.

2.1.4. FASE DE ANÁLISIS DE VULNERABILIDADES

En esta fase se debe estimar el éxito de la estrategia de penetración con la identificación las vulnerabilidades, se debe colocar en práctica las habilidades para realizar el test, identificando y haciendo uso de las herramientas más adecuadas para lograr el mayor éxito posible de acuerdo con los objetivos establecidos.

2.1.5. FASE DE EXPLOTACIÓN

En la presente fase tiene como objetivo obtener acceso a los sistemas y se ejecutan los exploits con las vulnerabilidades identificadas anteriormente, en caso de no poder ingresar se utilizarán las credenciales obtenidas.

2.1.6. FASE DE POST-EXPLOTACIÓN

Una vez se logra el acceso a los sistemas del cliente inicia la fase donde se demuestran las consecuencias de la brecha de seguridad que presenta la empresa, cuyo objetivo es conseguir el mayor nivel de privilegios, acceso a la red, acceder a los sistemas de información, identificar los datos y los servicios que se pueden vulnerar y lo más importante es demostrarle al cliente lo que puede llegar a obtener un intruso si logra ingresar al sistema.

2.1.7. FASE DE INFORME

En esta fase se elabora un informe donde se da a conocer los resultados de la prueba de penetración al cliente, mediante el cual se explica los riesgos a los que esta expuesto la empresa teniendo como referencia las vulnerabilidades encontradas, resaltando la seguridad que se encuentra establecida de manera exitosas, en los que exista fallas y el procedimiento a seguir para corregirlos, se tener en cuenta que se debe entregar dos informes uno ejecutivo y otro técnico, con el propósito de ser analizado e interpretado de mamera adecuada.

3. HERRAMIENTAS DE CIBERSEGURIDAD

- ✓ **METASPLOIT:** Es un conjunto completo de herramientas utilizadas para probar la vulnerabilidad de los sistemas de información, permitiendo la ejecución de exploits.
- ✓ **NMAP:** Es un programa que permite escanear e identificar los servicios que se ejecutan en un equipo remoto, la identificación de equipos activos, el sistema operativo en un equipo remoto.
- ✓ **OPENVAS:** Es un sistema que permite evaluar vulnerabilidades de seguridad en servidores y dispositivos de red, presta diferentes tipos de herramientas que permiten dar solución absoluta, potente de análisis y vulnerabilidades en la red.

- ✓ **EXPLOITDB:** Es un servicio en línea que contiene una base de datos de exploits, la cual los hackers suministran vulnerabilidades de aplicaciones y dan instrucciones de como las pueden utilizar y aprovechar al máximo.
- ✓ **CVE:** Es un sitio web donde encontramos una lista de vulnerabilidades conocidas donde se encuentra información relacionada a la vulnerabilidad como la versión de software afectadas, una posible solución y configurara para mitigar la vulnerabilidad.

4. ACUERDO DE CONFIDENCIALIDAD

4.1. ANALISIS PROPUESTA LABORAL

Como experta en ciberseguridad no aplicaría al trabajo en The WhiteHouse, teniendo en cuenta que COPNIA mediante Ley 842 del 2003 adopto el Código de Ética Profesional para los Ingenieros con el propósito de establecer los parámetros, conductas profesionales y así poderles garantizar a los ciudadanos una labor ética e intachable.

El Acuerdo de Confidencialidad de la empresa The WhiteHouse establece procesos ilegales y no ético que atenta a las conductas profesionales y se incumplen los siguientes Artículos del Código de ética profesional.

Tabla 1. Código de Ética Profesional

ARTICULO	NUMERAL	DESCRIPCION
31- Deberes Generales de los Profesionales	F	Como profesionales es nuestro deber de denunciar todo tipo de delito que se esté realizando en la empresa u entidad que nos encontremos laborando y realizar la entrega de las pruebas suficientes que comprueben el delito
34 - Prohibiciones especiales a los profesionales respecto de la sociedad	A	Como Ingenieros no debemos acceder a ningún trabajo que incurra a cualquier tipo de delitos establecidos por las Leyes Vigentes
35 - Deberes de los profesionales para con la dignidad de sus profesiones	B	Como profesionales íntegros debemos respetar y hacer respetar las leyes vigentes de nuestro país.

Fuente: Autor

5. OPERACIÓN ANDROMEDA BUGGLY

Fue una fachada legalmente constituida por el Ejercito para la creación del centro de inteligencia, pero todo lo que se realizaba en dichas instalaciones no era legal, de acuerdo a lo consultado Andrés Sepúlveda realizo interceptación ilegal a los negociadores de Paz que se encontraba en la Habana, políticos y funcionarios público, accedió a sistemas de información, utilizo software malicioso con el único propósito de obtener información confidencial.

Desde mi punto de vista, fue un caso bastante sonado en nuestro país, porque se evidencia el incumplimiento de los siguientes artículos de la Ley 1273 de 2009:

- 269A ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO
- 269C INTERCEPTACIÓN DE DATOS INFORMÁTICOS
- 269E USO DE SOFTWARE MALICIOSO
- 269F VIOLACIÓN DE DATOS PERSONALES

La Ley 1273 de 2009, establecido el delito como una conducta concerniente con el manejo de datos personales que están almacenados en base de datos de una entidad pública o privada, la presente ley tiene como propósito de garantizar la protección a la información personal y así poder garantizar el derecho a la integridad. Estableció penas de prisión de treinta y seis hasta ciento veinte meses y multas de cien hasta mil quinientos salarios mínimos legales.

El Consejo Profesional Nacional de Ingeniería – COPNIA, a través de la Ley 842 del 2003 adoptó el Código de ética profesional, donde se establece los deberes, prohibiciones de los profesionales y el régimen de inhabilidades e incompatibilidades, pero para este caso no es mucho lo que se aplica porque no era profesional, sino que era empírico había adquirido sus conocimientos de manera clandestino. Adquirir información confidencial sin tener la autorización correspondiente se está incurriendo a procesos no ético y legales.

6. EJECUCIÓN PRUEBAS DE INTRUSIÓN

6.1. BANCO DE TRABAJO

Se inicia a la instalación de:

- ✓ **INSTALACION DEL VIRTUALBOX**

- ✓ **PRIMERA MÁQUINA - WINDOWS 7 – 64 BIT**
- ✓ **SEGUNDA MAQUINA – WINDOWS 7**
- ✓ **TERCERA MÁQUINA – KALI LINUX**

Contemplando el laboratorio establecido frente al proceso de riesgos y vulnerabilidades del equipo Blue Team frente al Red Team se pueden establecer los siguientes ítems donde se demuestra los procedimientos ejecutados:

6.2. Ova win 7 x86 x64

Se utiliza herramientas de pentesting para verificar vulnerabilidades de servicios y puertos abiertos para ser utilizados como puertas traseras. En este caso se utilizó Kali Linux y herramientas de escaneo como Nmap.

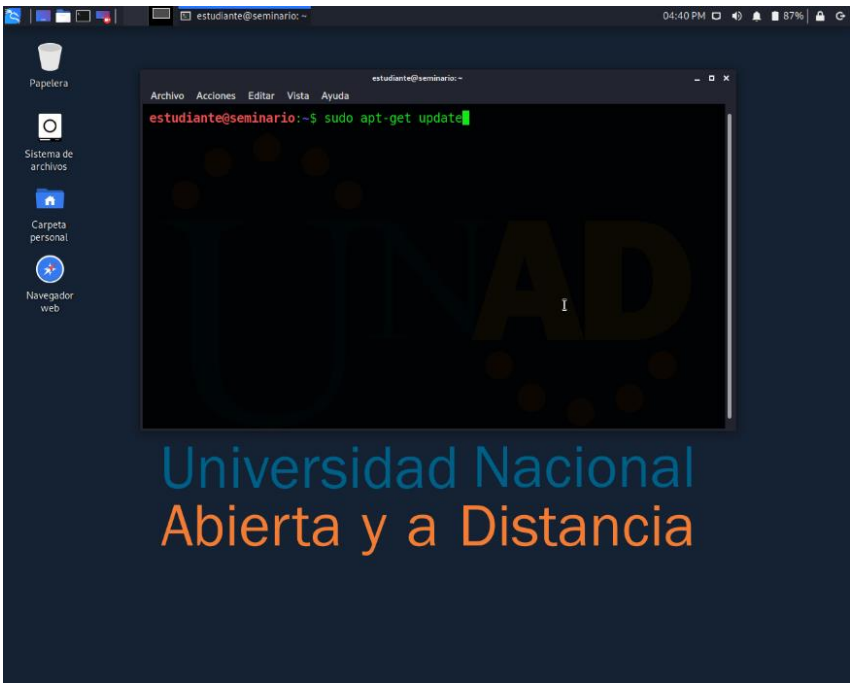


Ilustración 1. Ova win 7 x86 x64
Fuente: Autor

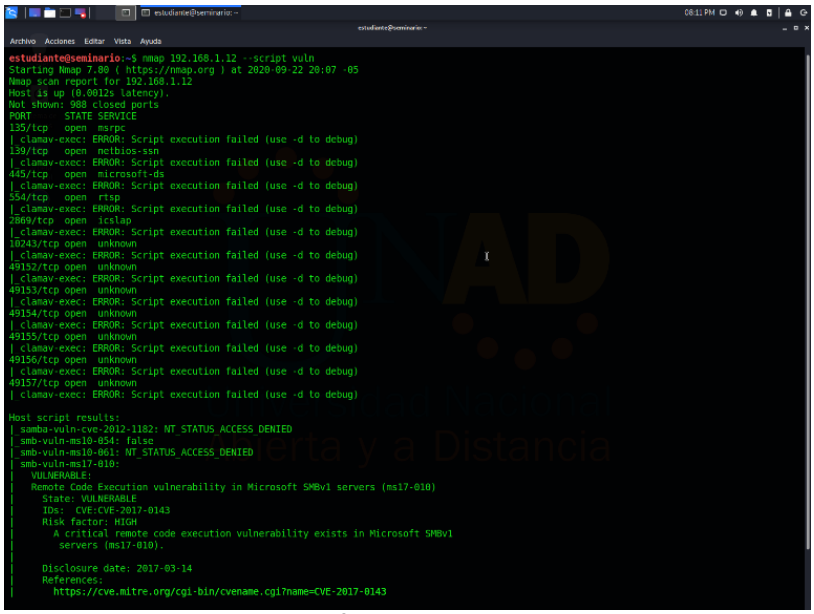


Ilustración 2. Comando nmap
Fuente: Autor

Se logra verificar el estado del escaneo del host víctima y detalla un resumen del estado encontrado:

Estado: Vulnerable

IDs: CVE:CVE-2017-0143 código de identificación de la vulnerabilidad
FACTOR DE RIESGO: ALTO
A CRITICAL REMOTE CODE EXECUTION VULNERABILITY EXISTS IN MICROSOFT SMBv1 SERVERS (ms17-010)

Ilustración 3. Comando msfconsole
Fuente: Autor

La vulnerabilidad encontrada ayuda a que por medio de exploit determinado para esa vulnerabilidad logre ingresar al sistema desde el CMD

Se ejecuta el comando RUN para iniciar con el metasploit se utiliza el comando use exploit/windows/smb/ms17_010_eternalblue para activar el payload eternalblue y lograr entrar al sistema de la víctima.

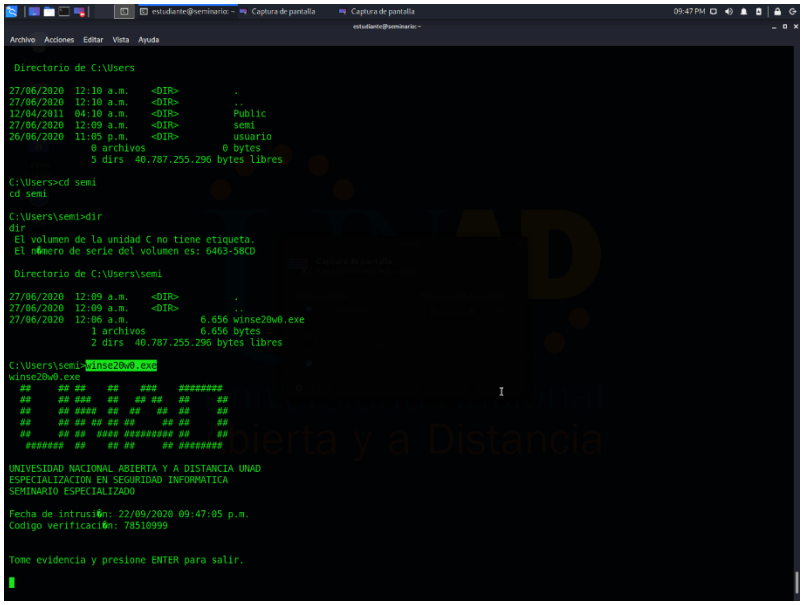


Ilustración 4. Comando winse20w0
Fuente: Autor

6.3. Ova Windows 7 32 bits

El exploit se completa, pero no se puede crear una sesión abierta para controlarlo, esto debido al procedimiento lanzado desde el equipo Intruso. En el host victima aparece un pantallazo azul generado por un error de sistema, ese error de sistema se genera cada vez que el exploit intenta generar un acuse de recibido del equipo víctima y sostener una sesión estable para ingresar.

El fallo de seguridad se debe a que el exploit por tratarse de un sistema operativo Windows 7 de 32 bits, el exploit inicialmente solo funciona con Windows a 64 bits.

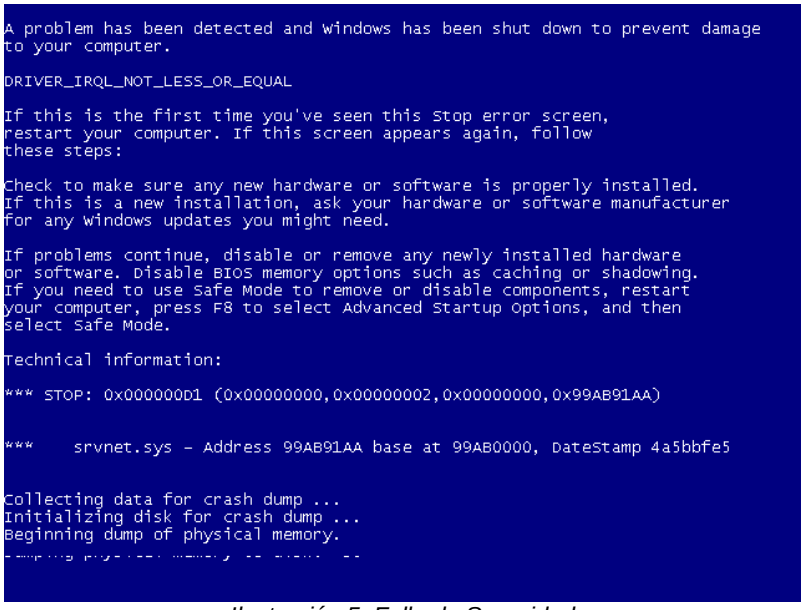


Ilustración 5. Falla de Seguridad
Fuente: Autor

7. CÓMO AFECTA EL ATAQUE A CADA UNA DE LAS MÁQUINAS

El ataque mediante el framework metasploit y el uso de paydloads para lograr penetrar en los dos sistemas operativos afecta a las maquinas gracias a la vulnerabilidad generada por la no actualización a tiempo de los sistemas de seguridad que Microsoft brinda constantemente a sus sistemas operativos. En el caso del host victima 192.168.1.11 lo afecta constantemente con problemas de seguridad en el sistema operativo generando reinicios constantes y pantallazo azul cada vez que se trata de ingresar mediante el exploit. El exploit se ejecuta correctamente, pero al tener ese constante problema generando reinicios en el sistema, no se logra crear una sesión estable para su intrusión.

El host victima 192.168.1.12 lo afecta de igual manera el exploit con la generación de un error del explorador de Windows, pero sin lograr abatir totalmente el sistema

y su reinicio. Completando la ejecución del exploit y la creación de una sesión de intrusión al sistema. La afectación es completa debido a que se tiene todo el control del host víctima.

Los dos sistemas son expuestos y se recomienda a la empresa instalar un sistema de seguridad con zona desmilitarizada DMZ para lograr retener al intruso y **lograr identificarlo de manera eficaz.**

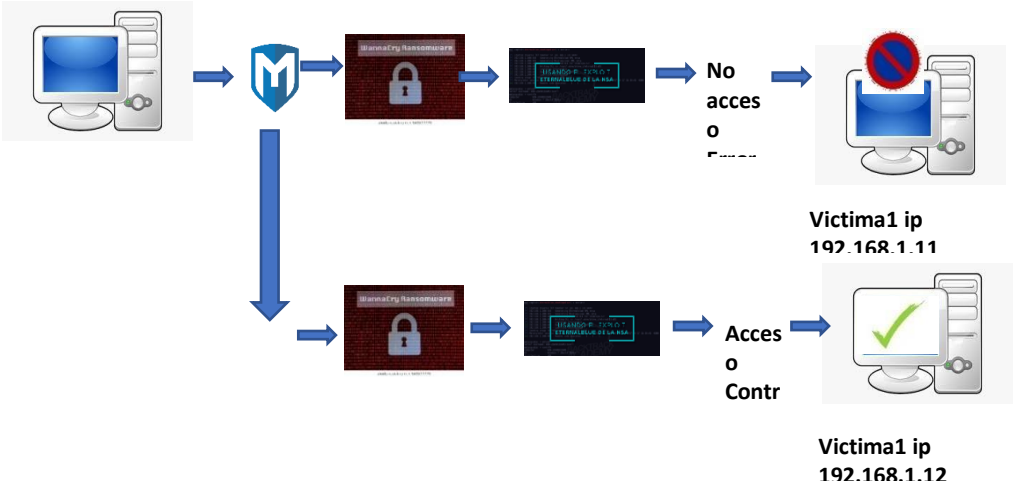


Ilustración 6. Proceso de Ataque
Fuente: Autor

8. ANALISIS DE RIESGOS Y VULNERABILIDADES

De acuerdo a la intrusión se necesita realizar un análisis de riesgos y vulnerabilidades para mitigar posibles y/o futuros problemas de ingresos no deseados al sistema.

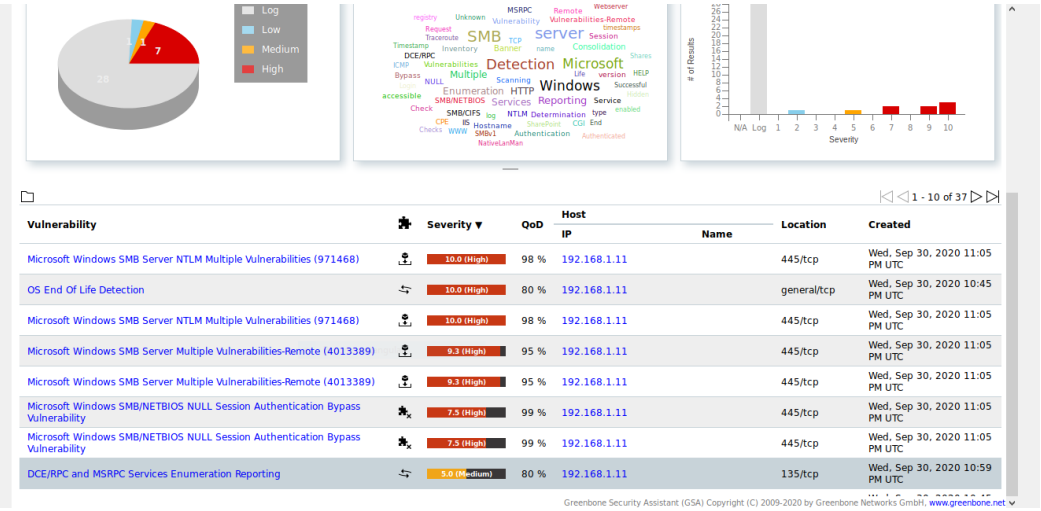
Para ello se utiliza nuevamente Kali Linux con una herramienta adicional que se puede instalar en cualquier Sistema operativo, sin embargo, como lo dije anteriormente se utiliza Kali Linux como Sistema operativo anfitrión.

Se realizan actualizaciones al sistema de Kali Linux y se procede con la instalación de OpenVas

Una vez ingresamos se inician los escaneos a las máquinas virtuales con problemas de vulnerabilidades.

8.1. ANALISIS DE VULNERABILIDADES

Se inicia el análisis de vulnerabilidades con OpenVas



1 - 10 of 37

Vulnerability	Severity ▼	QoD	Host IP	Host Name	Location	Created
Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)	10.0 (High)	98 %	192.168.1.11		445/tcp	Wed, Sep 30, 2020 11:05 PM UTC
OS End Of Life Detection	10.0 (High)	80 %	192.168.1.11		general/tcp	Wed, Sep 30, 2020 10:45 PM UTC
Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)	10.0 (High)	98 %	192.168.1.11		445/tcp	Wed, Sep 30, 2020 11:05 PM UTC
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)	9.3 (High)	95 %	192.168.1.11		445/tcp	Wed, Sep 30, 2020 11:05 PM UTC
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)	9.3 (High)	95 %	192.168.1.11		445/tcp	Wed, Sep 30, 2020 11:05 PM UTC
Microsoft Windows SMB/NETBIOS NULL Session Authentication Bypass Vulnerability	7.5 (High)	99 %	192.168.1.11		445/tcp	Wed, Sep 30, 2020 11:05 PM UTC
Microsoft Windows SMB/NETBIOS NULL Session Authentication Bypass Vulnerability	7.5 (High)	99 %	192.168.1.11		445/tcp	Wed, Sep 30, 2020 11:05 PM UTC
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80 %	192.168.1.11		135/tcp	Wed, Sep 30, 2020 10:59 PM UTC

Ilustración 7. Vulnerabilidades encontradas
Fuente: Autor

En este proceso se obtuvo como resultado por severidad y clase, 37 ítems.
7 altos, 1 medio, 1 bajo y 28 log

Se debe contemplar medidas de seguridad donde es necesario conocer la terminología utilizada para identificar y diferenciar los riesgo y vulnerabilidades que se presentan dentro del laboratorio.

- ✓ Integridad de los datos: que la información no valla ser modificado sin autorización previa de la persona.

- ✓ Autenticidad: es un mecanismo de verificación del personal que va manipular la información.

- ✓ La Confidencialidad: no divulgar la información y no permitir ser manipuladas por terceros.

- ✓ Disponibilidad: que debe estar disponible para el personal autorizado cuando se requiera.

8.1.2. VICTIMA 1

1. **Vulnerabilidades de Microsoft Windows SMB Server NTLM (971468)**

A este host le falta una actualización de seguridad crítica según Boletín de Microsoft MS10-012.

2. **Vulnerabilidad**

Detección de fin de vida útil del SO

- **Resumen**

El sistema operativo del host remoto ha llegado al final de su vida útil y debería no ser usado más.

3. **Vulnerabilidad**

Varias vulnerabilidades de Microsoft Windows SMB Server NTLM (971468)

- **Resumen**

A este host le falta una actualización de seguridad crítica según Boletín de Microsoft MS10-012.

4. **Vulnerabilidad**

Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)

- **Resumen**

A este host le falta una seguridad crítica se debe actualizar de acuerdo con el boletín de Microsoft MS17-010.

5. **Vulnerabilidad**

Vulnerabilidad de omisión de autenticación de sesión NULL SMB / NETBIOS de Microsoft Windows

- **Resumen**

El host ejecuta SMB / NETBIOS y es propenso a una autenticación y evitar la vulnerabilidad.

8.1.3. VICTIMA 2

De acuerdo a las vulnerabilidades del equipo ip victima 2 clase c 192.168.1.12/24 windows 7 64 bits, se logró identificar los siguientes patrones de vulnerabilidades que se consideran de mayor importancia:

1. **Vulnerabilidad:**

Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)

- **Resumen**

A este host le falta una seguridad crítica

Se debe actualizar de acuerdo con el boletín de Microsoft MS17-010.

2. **Vulnerabilidad:**

Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389) ...

OID: 1.3.6.1.4.1.25623.1.0.810676

Software / SO afectados

3. **Vulnerabilidad:**

Informes de enumeración de servicios DCE / RPC y MSRPC

- **Resumen**

Entorno de computación distribuida / Llamadas a procedimiento remoto (DCE / RPC) o servicios MSRPC en ejecución en el host remoto se puede enumerar conectándose en el puerto 135 y realizando las consultas correspondientes.

4. Vulnerabilidad:

Marcas de tiempo TCP

Se detectó que el host implementa RFC1323 / RFC7323.

Las siguientes marcas de tiempo se recuperaron con un retraso de 1 segundo entre ellas:

Paquete 1: 183212

Paquete 2: 183313

9. APLICACIÓN DE SOLUCIONES

- ✓ Se descarga la actualización de MS17-010 para reparar la vulnerabilidad EternalBlue y evitar ataque DoublePulsar.

- ✓ Se realiza la activación de firewall ya que estaba desactivado el servicio.

- ✓ Se realiza el cambio de configuración automático para un mejor manejo del update

- ✓ Se realiza la activación de Windows update, sin embargo, se informa que las actualizaciones de Windows 7 caducaron y no van a seguir teniendo soporte. Por lo tanto se recomienda que migren hacia una distribución de Linux o una nueva versión de Windows.

- ✓ La versión de uno de los Windows no recibe actualizaciones ya que es una versión HOME y el otro cliente es PRO. Las versiones de Windows 7 PRO y Windows 7 Enterprise tendrán actualizaciones hasta el 2023 ya que muchas empresas utilizan aun estos sistemas operativos.

- ✓ El cliente con sistema operativo Windows home no recibirá actualizaciones por medio de Windows update por lo tanto continuará vulnerable en red. Se recomienda migrar hacia otra distribución.
- ✓ Se actualizó el antivirus ya que no estaba funcional.

- ✓ Se instala ccleaner para eliminar registros que comprometan la seguridad del equipo de computo

- ✓ Se recomienda realizar copias de seguridad de acuerdo al protocolo de seguridad que se debe establecer en la empresa. Utilización de tecnología RAID, VPN, DMZ etc.

- ✓ Se descarga SAFETY para realizar un análisis de vulnerabilidades

- ✓ Tener sentido común y buenas prácticas con el uso del computador, utilización de memorias USB.

- ✓ Finalmente, se recomienda contar con un protocolo de seguridad para cualquier anomalía que perjudique la integridad de los datos de la empresa.

10. VIDEO DE SUSTENTACIÓN

Equipos Estratégicos En Ciberseguridad Red Team & Blue Team

http://youtu.be/UplRz1HRn_g?hd=1

CONCLUSIONES

Como profesionales debemos tener muy claro las Leyes Colombianas que nos permitan ser profesionales éticos y sobre todo no existe ninguna excusa para realizar procesos ilegales y no éticos.

Puedo concluir que nuestra profesión es muy importante, pero hay que utilizarla de manera legal, respectar las leyes vigentes y sobre todo adquirir valores que nos permitan ser éticos en todo el sentido de la palabra, no debemos utilizar nuestros conocimientos y habilidades para cometer algún tipo de delito.

Se debe implementar un plan de seguridad teniendo en cuenta la implementación de la norma ISO 27000 para que se pueda realizar reportes de manera oportuna por cada integrante de la empresa, ya que son activos potenciales de ésta y el manejo de información es vital desde cualquier perspectiva.

En espacios de mayor tamaño es necesario realizar un análisis más exhaustivo de todos los componentes que la integran, tal es el caso de la empresa, la cual cuenta con equipos variados y con equipos que pueden tener alto riesgo a sufrir ataques. Cada dispositivo cumple una función específica dentro de la empresa desde el cuidado y protección de los mismos hasta la prestación de servicios avanzados para ello es necesario que estos cuenten con los requerimientos mínimos para que su funcionamiento sea óptimo.

El mínimo descuido de seguridad en una empresa, por más básico que parezca puede ocasionar pérdidas millonarias y el fracaso de la empresa.

Para la realización del análisis de vulnerabilidades se utilizó una herramienta para el escaneo de las amenazas presentes en cada uno de los dispositivos de la empresa y encontrando diferentes vulnerabilidades que deben ser tenidas muy en cuenta.

Se detalló cada una de las vulnerabilidades encontradas y las soluciones que se establecen para su mitigación.

Las actualizaciones de software empresarial “pago” o “gratuito” se ve obligado a estar en la mira del personal de seguridad informática de la empresa para mantener un control mediante bitácoras que ayudan al autodiagnóstico de la información.

Contar con un perímetro de seguridad como una zona desmilitarizada y el uso de software y dispositivos como firewall, IDS o IPS ayudaran de manera positiva a controlar de una mejor manera cualquier problema de seguridad. De igual manera la implementación de ICLOUD en la empresa mitigaría exponencialmente los problemas de intrusión bajo respaldos completos en grandes porcentajes.

RECOMENDACIONES

Factor humano.

No existe restricción de acceso ya que el no manejan políticas de seguridad visibles, lo cual deja abiertas las puertas a externos, los cuales podrían poner en riesgo los bienes, la salud de funcionarios y demás personal.

Pérdida por robo o daño; se pueden presentar, incluso el hurto de un mouse, deja al equipo afectado medianamente inoperable. Por ello se recomienda el uso de bridas plásticas.

Ataques; puede ocurrir que un tercero, incluso un funcionario, con acceso a un punto de red o con la contraseña del wifi. Cambios, daños a los computadores, pérdida de información, virus y demás elementos maliciosos; los ataques, cambios en las computadoras, pérdidas y demás, pueden evitarse mediante auditorías, tanto interna como externa con el fin de diagnosticar y aconsejar los cambios pertinentes.

Es recomendable contar con todo el personal de la empresa capacitado frente a la ciberseguridad y temas a fines. (incluye personal administrativo)

Factor tecnológico

Bajas en el servicio eléctrico; éstas afectan directamente el quehacer de la empresa, para proteger los equipos y datos se recomienda el uso de UPS’s.

Servicio de internet; la carencia de este afecta directamente las actividades económicas de la empresa, ya que el 100% del tiempo se está utilizando con servicios SMB.

Fallos en los equipos; éstos pueden ser provocados por varios factores (fallos técnicos, actividad humana, factores ambientales).

Estar a la vanguardia de equipos tecnológicos y software administrativos ayudarán a realizar empalmes de sistemas de información para migrar de un sistema operativo a otro si se requiere.

Realizar o implementar cambios de infraestructura tecnológica para el uso adecuado de la información. Utilización de tecnología basada en RAID y manejo de la NUBE ayudará a salvaguardar la información.

Factor ambiental

Humedad; la humedad puede generar daños en los equipos, para evitarlo se puede utilizar un Higrómetro.

Temperatura; la temperatura, para el caso el “calor” puede afectar el funcionamiento de los equipos electrónicos, se recomienda el uso de termómetros.

Terremotos, fuego, meteoritos; éstos se dan de forma fortuita, para evitar la mayor

cantidad de posible de daños se debe actualizar el plan de contingencia y los mecanismos de evacuación.

BIBLIOGRAFIA

ACCENSIT. Análisis de vulnerabilidad informática: ¿En qué consiste?. [En línea]. Disponible en: https://www.accensit.com/blog/analisis-vulnerabilidad-informatica-en-que-consiste/

CAMBIO DIGITAL ONLINE. 12 principales herramientas de IDS/IPS. [En línea]. [Abril del 2020]. Disponible en: https://cambiodigital-ol.com/2020/04/12-principales-herramientas-de-ids-ips/

CATOIRA. Fernando. Pruebas de penetración para principiantes: explotando una vulnerabilidad con metasploit framework. [En línea]. Disponible en: https://revista.seguridad.unam.mx/numero-19/pruebas-de-penetraci%C3%B3n-para-principiantes-explotando-una-vulnerabilidad-con-metasploit-fra

CIBERSEGURIDAD.NET. Las fases de un test de penetración (Pentest) (Pentesting I). [En línea]. [23 de agosto de 2015]. Disponible en:https://www.cyberseguridad.net/index.php/455-las-fases-de-un-test-de-penetracion-pentest-pentesting-i

COPNIA. Código de Ética. [En línea]. Disponible en: https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

COPNIA. Ley 842 de 2003. [En línea].[Octubre del 2003]. Disponible en: https://www.copnia.gov.co/nuestra-entidad/normatividad/ley-842-de-2003

CVE. Historia. [En línea]. Disponible en: https://cve.mitre.org/about/history.html

EL ESPECTADOR. Caso Andrómeda y sus interrogantes [En línea].[Junio del 2018]. Disponible en: https://www.elespectador.com/noticias/judicial/caso-andromeda-y-sus-interrogantes/

EL ESPECTADOR. Los detalles de Andrómeda, según la Procuraduría**.** [En línea].[Junio del 2018]. Disponible en: https://www.elespectador.com/noticias/judicial/los-detalles-de-andromeda-segun-la-procuraduria/

EL TIEMPO. Fachada Andrómeda era legal, pero no todo lo que se hizo allí lo fue. [En línea].[Enero del 2015]. Disponible en: https://www.eltiempo.com/archivo/documento/CMS-15141236

INSECURE.ORG. ¿Las 75 Herramientas de Seguridad Más Usadas? [En línea]. Disponible en: https://insecure.org/tools/tools-es.html

INSTITUTO NACIONAL DE CIBERSEGURIDAD. Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian? [En línea]. [Marzo del 2017]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

KALI. Kali Linux: distribución de pruebas de penetración profesional. [En línea]. Disponible en: https://www.kali.org/docs/

KALI. Our Most Advanced Penetration Testing Distribution, Ever. [En línea]. Disponible en: https://www.kali.org/

MICROSOFT. Ciclo de vida de los productos y servicios. [En línea]. Disponible en: https://support.microsoft.com/enus/lifecycle/search?sort=PN&alpha=Windows%207&Filter=FilterNO

MICROSOFT. MS10-012: Vulnerabilidades en SMB Server podrían permitir la ejecución remota de código. [En línea]. [Abril del 2018]. Disponible en: http://support.microsoft.com/kb/971468

MICROSOFT. MS17-012: actualización de seguridad para Microsoft Windows: 14 de marzo de 2017. [En línea]. [Marzo del 2017]. Disponible en: https://support.microsoft.com/en-in/kb/4013078

MINTIC. Ley 1273. [En línea].[Enero del 2009]. Disponible en: https://www.mintic.gov.co/portal/inicio/3705:Ley-1273-de-2009

MINTIC. Ley 1273. [En línea].[Enero del 2009]. Disponible en: https://www.mintic.gov.co/portal/inicio/3705:Ley-1273-de-2009

NMAP. ORG. Nmap. [En línea]. Disponible en: https://nmap.org/

OLIVA, Juan. Explotando Vulnerabilidad MS17-010 o WannaCry. [En línea]. [Junio del 2017]. Disponible en: https://jroliva.net/2017/06/01/explotando-vulnerabilidad-wannacry-o-ms17-010/

OPEN WEBINARS. Introducción a los escaneres de vulnerabilidades. [En línea]. [Mayo del 2014]. https://openwebinars.net/blog/openvas-en-linux-explorando-nuestros-sistemas/

OPENVAS. OpenVAS - Escáner de evaluación de vulnerabilidad abierta. [En línea]. Disponible en: https://www.openvas.org/

PROGRAMA EN LINEA. ¿Qué es un Payload?. [En línea]. [Julio del 2019]. Disponible en: https://www.programaenlinea.net/que-es-un-payload/#:~:text=Meterpreter%3A%20Es%20un%20payload%20bastante,encuentran%20varias%20capas%20por%20encima

RAPI 7 METASPLOIT. Guía de inicio rápido. [En línea]. Disponible en: https://www.metasploit.com/

REGIMEN LEGAL DE BOGOTÁ D.C. Ley 1266de 2008 nivel nacional. [En línea] .[31 de diciembre del 2008]. Disponible en: https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34488

REVISTA HACKING ETICO. Fases del pentesting Aprende Como Hacer Auditoria de hacking a Empresas. [En línea]. Disponible en:https://www.revistahackingetico.com/2019/09/fases-del-pentesting-aprende-como-hacer.html

REVISTA. SEGURIDAD. Pruebas de penetración para principiantes: explotando una vulnerabilidad con metasploit framework. [En línea]. Disponible en: https://revista.seguridad.unam.mx/numero-19/pruebas-de-penetraci%C3%B3n-para-principiantes-explotando-una-vulnerabilidad-con-metasploit-fra

SECRETARIA SENADO. Ley estatutaria 1581 de 2012. [En línea]. [31 de agosto 2020]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

SISTEMA UNICO DE INFORMACION NORMATIVA. Decreto 1377 de 2013. [En línea]. [27 de junio de 2013]. Disponible en: http://www.suin-juriscol.gov.co/viewDocument.asp?id=1276081

WELIVESECURITY. ¿Sabes qué es un exploit y cómo funciona? [En línea]. [Octubre del 2014]. Disponible en: https://www.welivesecurity.com/la-es/2014/10/09/exploits-que-son-como-funcionan/

WELIVESECURITY. Cómo crear tu primer módulo para Metasploit. [En línea]. [Octubre del 2014]. Disponible en: https://www.welivesecurity.com/la-es/2014/10/17/como-crear-primer-modulo-metasploit/