


GUÍA DEL COMPONENTE PRÁCTICO DEL CURSO SEGURIDAD INFORMATICA

ACTIVIDAD PRÁCTICA 1 – FUNDAMENTOS DE SEGURIDAD INFORMATICA

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 1

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 auditoría.



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

TEMA: Fundamentos de Seguridad informática

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

- Definir las condiciones previas del sistema a revisar, seleccionar un sitio web
- Aplicar el análisis de vulnerabilidades con una herramienta 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 inter-operar 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 Esteganografia. (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.

3. HERRAMIENTAS NECESARIOS PARA LA PRÁCTICA

Virtual Virtualbox

ISO de Sistema Operativo Windows 7

Escáner de red, recomendable usar nmap y netscan

Nessus versión Home

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. Adicionalmente el tutor del curso brindara el acompañamiento en el desarrollo de la actividad a través de los recursos del aula.

Fecha de inicio de la actividad: 25 de Septiembre de 2016 a las 00:00 h

Fecha de finalización de la actividad: 05 de Octubre 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:

La máquina base debe contar con mínimo 4 Gb en memoria RAM, 30 Gb de espacio para asignar al disco de la máquina virtual.


5.1. PROCEDIMIENTO PARA REALIZAR LA PRACTICA

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.

1. Descargar Virtualbox de: <https://www.virtualbox.org/wiki/Downloads>, elegir la versión correspondiente a su sistema operativo.

Instalar la máquina virtual e instalar el sistema operativo Windows xp o Windows 7 por defecto. No es necesario instalar actualizaciones del sistema operativo. Revisar el anexo 1.

El controlador de tarjeta de red de la máquina virtual debe estar en Puente o Bridge.



Configurar los dos sistemas operativos en red, bajo el mismo segmento de red.

Hacer las pruebas de conectividad entre los dos sistemas operativos, máquina virtual y equipo base, documentando los resultados.


2. Instalar en el equipo base las herramientas para hacer el escaneo de red, pueden utilizar nmap, netscan, otras.


✓ Enlace para descarga de nmap:
<https://nmap.org/dist/nmap-7.12-setup.exe>

✓ Enlace de descarga de netscan:
<https://www.softperfect.com/products/networkscanner/>

Revisar los puertos abiertos, direcciones IP, direcciones físicas, recursos compartidos del sistema operativo Windows de la máquina virtual.

3. Descargar e instalar en el equipo base, la aplicación Nessus versión home, de <https://www.tenable.com/products/nessus/select-your-operating-system#> elija la versión Home, que es gratuita. Seleccionar el sistema operativo de acuerdo al hardware a 32 o 64 bits.





Instalar Nessus home, realizar un diagnóstico de vulnerabilidades al sistema operativo de la máquina virtual, a través de la dirección IP del equipo virtual.


Crear un Cuadro con las vulnerabilidades catalogadas como altas y críticas relacionar el respectivo CVE, lo pueden consultar en <https://cve.mitre.org/>

Plantear en el mismo cuadro la solución de las vulnerabilidades encontradas.

4. Realizar la revisión de efectividad por ataque mediante el uso de vulnerabilidades detectadas. Con la lista de vulnerabilidades, realizar la explotación de al menos una de las vulnerabilidades para verificar que se pueda hacer efectiva y no sea un falso positivo, haciendo la investigación necesaria para lograrlo. Documentar paso a paso el desarrollo.

6. 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 espaciado a 1,5
 - La estructura del documento debe contener:
- 

- Portada
- Introducción
- Objetivos
- Desarrollo de la práctica y describir paso a paso.
- Conclusiones.
- Bibliografía y referencias bibliográficas
- Todo el documento debe cumplir con las norma APA ver 6.

7. 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
COMPONENTE PRÁCTICO

Nombre del curso: SEGURIDAD INFORMATICA - 204039

Aspectos evaluados	Criterios de desempeño de la actividad individual Momento 1			P/ máxima
	Valoración alta	Valoración media	Valoración baja	
Creación del escenario de la práctica, máquina virtual y pruebas de conectividad	El estudiante creó el escenario de la práctica, la máquina virtual, configuración de red y pruebas de conectividad.	El estudiante realizó de forma parcialmente, el escenario de la práctica 1, la máquina virtual, configuración de red y pruebas de conectividad.	El estudiante no presentó sus aportes correspondientes. O No realizó la actividad.	6
	(Hasta 6puntos)	(Hasta 3 puntos)	(Hasta 0 puntos)	
Revisión de los puertos abiertos, direcciones IP, direcciones físicas, recursos compartidos del sistema operativo.	El estudiante realizó el diagnostico de los puertos abiertos, direcciones IP, direcciones físicas, recursos compartidos del sistema operativo. De manera satisfactoria con evidencias.	El estudiante realizó el diagnostico de manera parcial, de los puertos abiertos, direcciones IP, direcciones físicas, recursos compartidos del sistema operativo, o carece de algunas evidencias del proceso.	El estudiante no presentó sus aportes correspondientes. o No realizó la actividad.	6
	(Hasta 6 puntos)	(Hasta 3 puntos)	(Hasta 0	

			puntos)	
Diagnóstico de vulnerabilidades al sistema operativo de la máquina virtual	El estudiante realizó el diagnóstico de vulnerabilidades al sistema operativo de la máquina virtual de manera efectiva y creó el cuadro de resultados solicitado.	El estudiante realizó el diagnóstico de vulnerabilidades al sistema operativo de la máquina virtual de manera efectiva y creó el cuadro de resultados solicitado, manera parcial, o carece de información importante.	El estudiante no presentó sus aportes correspondientes. o No realizo la actividad.	6
	(Hasta 6 puntos)	(Hasta 3 puntos)	(Hasta 0 puntos)	
Prueba de explotación de vulnerabilidades	El estudiante realizó las pruebas de explotación de vulnerabilidades al sistema operativo de la máquina virtual de manera efectiva.	El estudiante realizó las pruebas de explotación de vulnerabilidades al sistema operativo de la máquina virtual, pero no logro la demostración.	El estudiante no presentó sus aportes correspondientes. O No realizo la actividad.	10
	(Hasta 10 puntos)	(Hasta 5 puntos)	(Hasta 0 puntos)	
Estructura del documento	El documento cumple con todas las condiciones de edición solicitadas y la norma APA ver 6.	El documento cumple parcialmente con las condiciones de edición	El estudiante no presentó aportes, o No realizó la	5

		solicitadas y la norma APA ver 6	actividad, o no cumple con lo mínimo solicitado para el documento.	
	(Hasta 5 puntos)	(Hasta 2 puntos)	(Hasta 0 puntos)	
TOTAL PUNTAJE DEL COMPONENTE PRÁCTICO				33



8. 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/adjuantos/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>



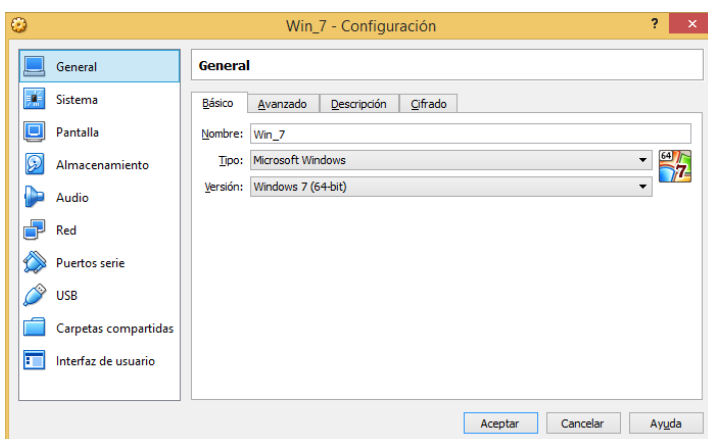
ANEXO 1 – Configuración sugerida para la máquina virtual

Anexo 2 Instalar Virtualbox

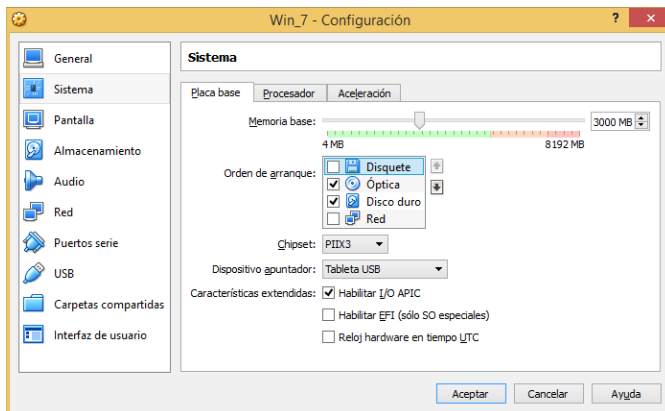
Descargar e instalar Virtualbox:

Crear una maquina nueva

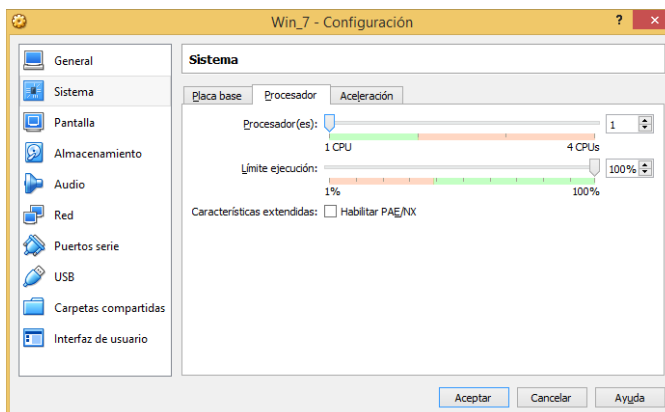
Tener en cuenta si el hardware es a 32 bits o a 64 bits.



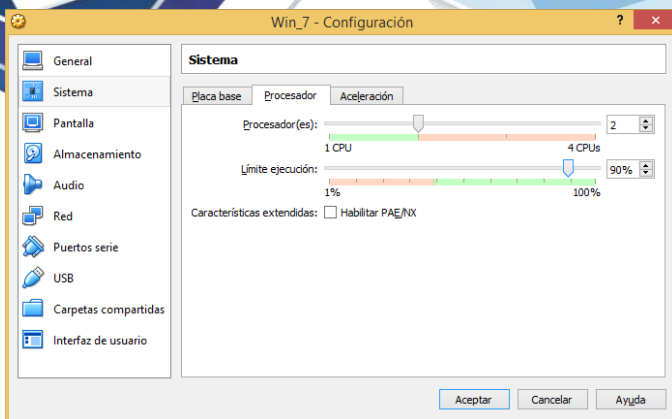
Asignar la memoria RAM debe ser suficiente y bien distribuida para que funcionen las dos máquinas. Se recomienda que el equipo base cuente con 4 GB en RAM, la distribuye 2,048 GB para la máquina virtual.



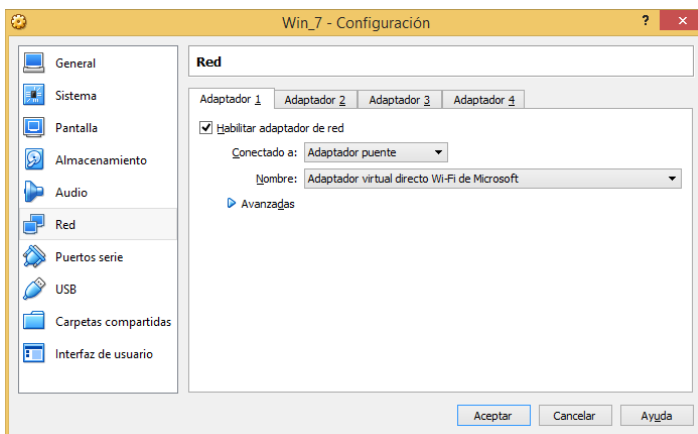
Si la maquina base es a 32 bits deben dejar 1 solo núcleo del procesador asignado.



Si es a 64 bits pueden asignar 2 núcleos del procesador.



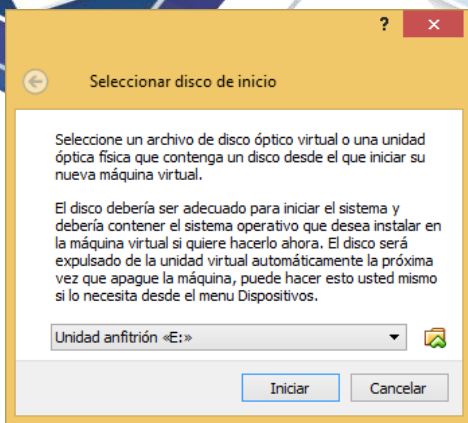
En Red, debe seleccionar Adaptador puente o Bridge Adapter



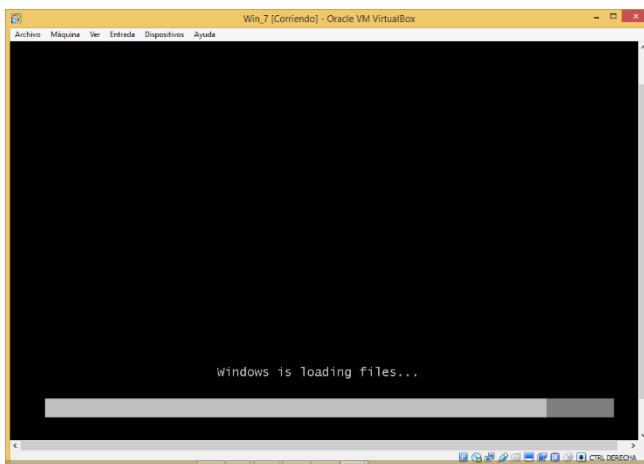
Las demás configuraciones se mantienen por defecto.

Iniciar la instalación de la máquina virtual creada.

Seleccionan el dispositivo donde tienen la ISO de Windows o el DVD de instalación.

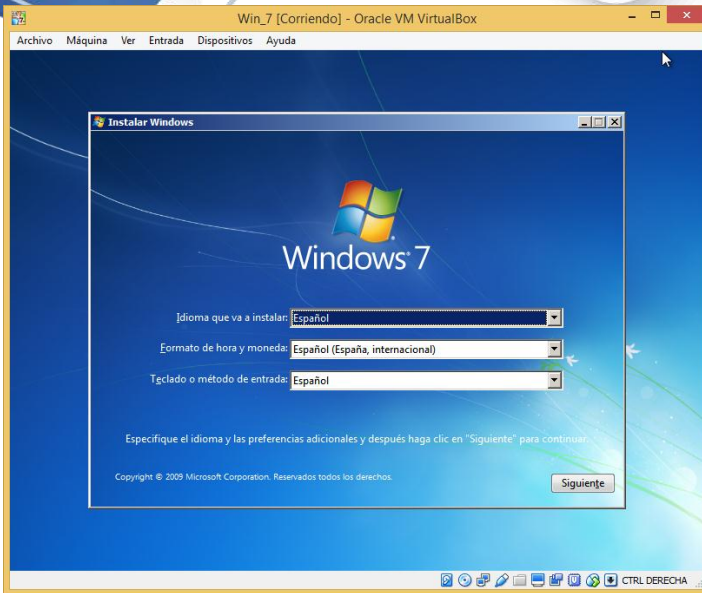


Inician la instalación del sistema operativo de forma normal.

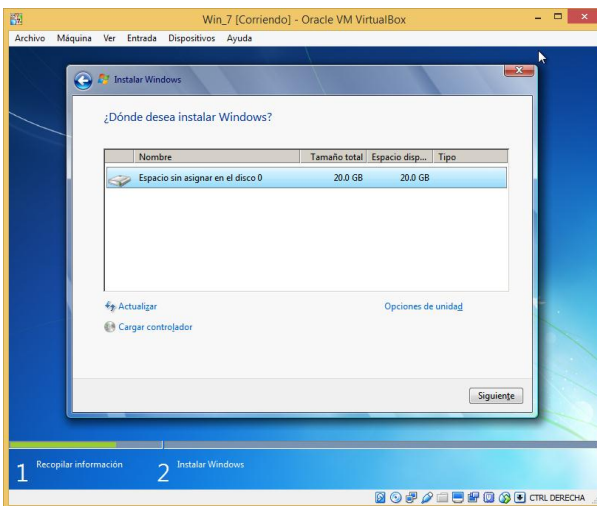


Inicia la instalación de Windows 7 pro

Selecciona el lenguaje



Elige el espacio del disco asignado para la instalación del sistema operativo.



Teniendo instalado el sistema operativo se debe configurar el controlador de la tarjeta de red de forma que ambos equipos estén bajo el mismo segmento de red.



Maquina base, por medio del prom se aplica el comando ipconfig para averiguar cuál es la dirección ip que tiene asignado, para así poder configurar el de la máquina virtual.

Ejemplo:

El equipo base tiene la dirección ip 192.168.0.10 con mascara de red de 24 bits.

192.168.0.10

255.255.255.0

182.168.0.5 es el Gateway

A la máquina virtual le asigna 192.168.0.50 con mascara de red 24 bits también. El Gateway seria el mismo del equipo base es decir 192.168.0.5.

Tener en cuenta lo anterior para aplicarlo de acuerdo a las direcciones IP del segmento de red en que realizaran la práctica.

Maquina virtual

