AICC101

Sumativa 6: Análisis de caso

Sumativa 6: Análisis de caso

Aprendizaje esperado:

3. Ejecutar pruebas básicas de ethical hacking.

Indicadores de logro:

3.3. Codifican los componentes de software que permitan el desarrollo de los casos de prueba de acuerdo con criterios de pentesting.

3.4. Ejecutan los distintos hallazgos de los casos de prueba utilizando herramientas de scripting de acuerdo con criterios de pentesting, interpretando sus resultados.

Instrucciones generales

1. **Lean con atención la experiencia de aprendizaje situada y la rúbrica correspondiente.**
2. Revisen los recursos de la semana y guíate en ellos para desarrollar la actividad.
3. De manera grupal, deberán analizar el caso presentado aplicando los conceptos web asociados con pentesting y con herramientas de gestión de permisos y búsquedas.

Les recordamos que contarán con la posibilidad de plantear sus consultas respecto de los contenidos tratados, en el foro “Consultas al docente” que estará abierto durante toda la semana.

Esta es una instancia de evaluación **sumativa, con calificación, ponderando un 5% de tu nota de presentación al Examen.**

Instrucciones específicas

De acuerdo con el pentesting tenemos muchas fases para poder realizar esto de manera efectiva:

Fase 1 - Reconocimiento: Es una fase de preparación, en donde se recolecta la información para realizar el ataque. En esta fase no hay intervención.

Fase 2 - Escaneo: En esta fase se explotan las vulnerabilidades, por lo que se busca la forma de agregar más métodos de explotación.

Fase 3 - Obtener accesos: Se ejecuta el plan de explotación de las vulnerabilidades y se logra el acceso.

Fase 4 - Mantener el acceso: Se busca obtener a partir del acceso ciertos accesos privilegiados para poder perdurar el acceso.

Fase 5 - Eliminar huellas: Se buscan todos los medios de correlación, log y registros en donde se realicen los historiales de accesos, con esto se mantiene el anonimato del *hacker*.

En esta actividad se solicita a la empresa de seguridad externa que realice un reconocimiento utilizando nmap:

1. Recopilar la información de red de los *host* Windows o Linux, con ipconfig y ifconfig, dependiendo del sistema operativo. Con esto determinamos el rango de la ip (generalmente 192.168.1 o 192.168.0 dependiendo del *router*).
2. Realizar un barrido de la red con nmap (ejemplo con 192.168.1 es: nmap -sP 192.168.1.0/24). Recopilar todos los hosts, si tienes un Windows, es muy bueno.
3. Realizar un barrido de la red sin hacer ping (ejemplo: nmap -sn 192.168.1.0/24).
4. Realizar un barrido de los puertos vulnerables (ejemplo: nmap -Pn 192.168.1.X en donde el X es el *host,* en lo posible que sea Windows).
5. Realizar un barrido de los puertos vulnerables solo TCP (ejemplo: nmap -sT 192.168.1.X), estos puertos son apreciados porque se saben a dónde están dirigidos.

6. Realizar un barrido de los puertos vulnerables solo UDP (ejemplo: nmap -sU 192.168.1.X).
7. Realizar un barrido de puertos específicos de bases de datos (ejemplo: nmap -p3306,1433,5432 192.168.1.X).
8. Realizar un barrido en profundidad de los puertos del *host* (ejemplo: namo -p- 192.168.1.X), esto tarda mucho tiempo por lo que se tiene que utilizar con cuidado.
9. Cuidar ortografía y redacción.
10. Respetar los aspectos formales solicitados.

Aspectos formales

- El nombre del archivo se debe ajustar al siguiente ejemplo: **aicc101_s10_grupo1**
- Si se detecta plagio en el trabajo, será calificado automáticamente con nota mínima.

Esta evaluación es grupal. Complétenla y luego envíenla en formato Word en el buzón de entrega correspondiente. Para esto:

a) Un (1) integrante del grupo deberá enviar el archivo final.
b) Ir a la sección “Entrega de actividad”.
c) Hacer clic en “Examinar mi equipo”.
d) Adjuntar el archivo con la tarea.

Disponibilidad: Hasta las 23:59 horas del último día de la semana en impartición. Puedes revisar la fecha y hora límite de tus evaluaciones en el **Programa del Curso**. ¡Planifica tu semana!

¿Cómo citar en APA?

Para artículo de revista:

MARENGO, C. y ELORZA, A. L. (2010). “Calidad de vida y políticas de hábitat. Programa de Mejoramiento Barrial en Córdoba, Argentina. Caso de estudio: barrio Malvinas Argentinas”. En: *Bitácora Urbano\Territorial*, 2(17), 79-94.

Para cita de libro:

CASTELBLANCO Caicedo, D. Z. (2010*). Los relatos del objeto urbano. Una reflexión sobre las formas de habitar el espacio público*. Bogotá: Universidad Nacional de Colombia.

Para cita de *World Wide Web* (www) y textos electrónicos:

BORRERO, O. y DURÁN, E. (2010). *Efectos de las políticas de suelo en los precios de terrenos urbanos sin desarrollar en Colombia. Los casos de Bogotá, Medellín y Pereira*. Consultado en: http://www.lincolninst.edu/pubs/dl/1784_1004_2009 Borrero Spanish Final.pdf

A continuación, revisa la tabla de especificaciones y la rúbrica asociada a la evaluación.

Tabla de especificaciones

Aprendizaje esperado	Indicador de logro	R Reconocer	E Entender	A Aplicar	AN Analizar	E Evaluar	C Crear
3. Ejecutar pruebas básicas de ethical hacking.	3.3. Codifican los componentes de *software* que permitan el desarrollo de los casos de prueba de acuerdo con criterios de *pentesting*.	–	–	X	–	–	–
	3.4. Ejecutan los distintos hallazgos de los casos de prueba utilizando herramientas de *scripting* de acuerdo con criterios de *pentesting*, interpretando sus resultados.	–	–	X	–	–	–
TOTAL EQUILIBRIO		**–**	**–**	**2**	**–**	**–**	**–**

Rúbrica de evaluación

CRITERIOS DE CALIDAD	NIVELES DE LOGRO				
	EXCELENTE 100%	BUENO 75%	ACEPTABLE 50%	INSUFICIENTE 25%	NO CUMPLE 0%
Recopilación de red **20%**	Recopila los datos de red identificando todos los datos y metadatos.	Recopila los datos de red identificando todos los datos y metadatos de la mayoría de los hosts.	Recopila los datos de red identificando solo los datos principales de las redes.	Recopila datos de host irrelevantes para el reconocimiento.	No hay recopilación.
Recopilación de red asociada **20%**	Recopila los datos de red identificando todos los datos y metadatos de la red asociada.	Recopila los datos de red identificando todos los datos y metadatos de la mayoría de los hosts asociados.	Recopila los datos de red identificando solo los datos principales de las redes asociadas.	Recopila datos de host asociados irrelevantes para el reconocimiento.	No posee ilación.
Recopilación de puertos **20%**	Los puertos recopilados son suficientes para poder realizar la fase siguiente, encontrando buenos candidatos a análisis.	Los puertos recopilados son variados, aunque no se tiene una total certeza de candidatos a análisis para la posterior fase.	Los puertos recopilados son muchos, pero con poca certeza de análisis posterior.	Los puertos recopilados en su mayoría no sirven para poder realizar un análisis posterior.	No encuentra puertos.
Recopilación de puertos de bases de datos **20%**	Los puertos recopilados son suficientes para poder realizar la fase siguiente, encontrando buenos candidatos a análisis.	Los puertos recopilados son variados, aunque no se tiene una total certeza de candidatos a análisis para la posterior fase.	Los puertos recopilados son muchos, pero con poca certeza de análisis posterior.	Los puertos recopilados en su mayoría no sirven para poder realizar un análisis posterior.	No encuentra puertos.
Recopilación profunda de puertos **20%**	Los puertos recopilados son suficientes para poder realizar la fase siguiente, encontrando buenos candidatos a análisis.	Los puertos recopilados son variados, aunque no se tiene una total certeza de candidatos a análisis para la posterior fase.	Los puertos recopilados son muchos, pero con poca certeza de análisis posterior.	Los puertos recopilados en su mayoría no sirven para poder realizar un análisis posterior.	No encuentra puertos.