Creando una Trayectoria Profesional en Seguridad Digital: Resumen Final y el Panorama Inteligente de la Seguridad

Agosto, 2021

OEA Más derechos para más gente

Citi Foundation citi

Tabla de contenidos

Resumen final

- **¡Un pentester NO es un transcriptor de herramientas!**
- ¿Cómo hacer un reporte de una prueba de penetración?
- ¿Cómo hacer un reporte de un análisis forense?

Consideraciones acerca del Pentesting

- Las herramientas permiten automatizar tareas, resumir información, simplificar pruebas, pero no reemplazan la capacidad intelectual de un consultor
- *Antes de reportar/explotar un hallazgo/vulnerabilidad se debe validar que dicho hallazgo no es un* **falso positivo**:
  - *¿Puedo validar manualmente dicho hallazgo?*
  - ¿ Conozco a fondo el protocolo sobre el cual opera el servicio/sistema vulnerable?
  - *¿Existe documentación al respecto?*
  - *¿El hallazgo que voy a reportar es realmente explotable?*

Aspectos para escribir un reporte de **Penetration Testing** (1/3)

- Alcance y fecha de ejecución de las pruebas
- Topología y tipo de prueba realizada. ¿Desde dónde se hizo la prueba?
- **RESUMEN EJECUTIVO**: presentar resultados en lenguaje relacionado al negocio
- Descripción de metodologías, procedimientos y actividades ejecutadas
- Hallazgos técnicos, con evidencia, recomendaciones y referencias
  - CVSS de los hallazgos
  - Consideraciones del entorno
  - Validación manual de hallazgos
  - ¿Impactó al negocio?

Aspectos para escribir un reporte de **Penetration Testing** (2/3)

- Referencias del fabricante, proveedores de servicio, academia, etc.
- No divulgar información sensible
- **CONCLUSIONES Y RECOMENDACIONES GENERALES**

Aspectos para escribir un reporte de **Penetration Testing** (3/3)

2.5.1.6. Fallo Heartbleed permite obtener acceso a información protegida

Fallo Heartbleed permite obtener acceso a información protegida	
El componente de código abierto OpenSSL en su versión 1.0.1 a 1.01f es vulnerable a la exposición de información protegida almacenada en la memoria del sistema debido a un incorrecto manejo de los paquetes de la extensión Heartbeat. Un atacante podría obtener acceso a información privilegiada, e incluso a las llaves privadas o cookies que mantienen abierta una sesión protegida por el canal SSL, de forma remota y sin presentar credenciales de autenticación.	
Puerto(s) asociado(s):	TCP 443
Impacto:	Confidencialidad
Criticidad:	Alta
Facilidad de exploración:	Baja
Acción recomendada:	Actualizar la versión de ePolicy Orchestrator, siguiendo las instrucciones del link a continuación. Actualizar OpenSSL en el sistema Ubuntu afectado.
Referencias:	https://kc.mcafee.com/corporate/index?page=content&id=KB81674 http://askubuntu.com/questions/444702/how-to-patch-the-heartbleed-bug-cve-2014-0160-in-openssl CVE-2014-0160

Esta vulnerabilidad fue encontrada en la siguiente dirección IP:

- 192.168.200.4:443
- 192.168.200.32:443

Figura 1: Elementos de un reporte de Pentest.

Aspectos para escribir un reporte de **Análisis Forense** (1/2)

- Alcance y fecha de la investigación
- Listado de evidencia analizada, descripción (*plataforma, rol, etc.*), *hash* de verificación de integridad, fecha de adquisición, etc.
- **RESUMEN EJECUTIVO**: presentar resultados en lenguaje relacionado al negocio:

  Responder la pregunta que motiva la investigación
  Evidencia ¿CONCLUYENTE? ¿NO CONCLUYENTE?
- Descripción de metodologías, procedimientos y actividades ejecutadas
- Hallazgos técnicos, con **evidencia** e interpretación de los hallazgos:
  - Análisis de información volátil

Aspectos para escribir un reporte de **Análisis Forense** (2/2)

- Análisis del registro de Windows y artefactos forenses
- Análisis de bitácoras. Los datos deben contar la historia
- LÍNEA DE TIEMPO DE EVENTOS

- **CONCLUSIONES Y RECOMENDACIONES GENERALES**

Sistemas defensivos de Inteligencia Artificial

Detección de malware:
Multicapa, multidefensa

SOC, IDS/IPS y Honey Pots:
Auto aprendizaje y Deep Learning

Anti-SPAM

Gestión de vulnerabilidades:
Identificar y priorizar remedación

Clasificación de datos:
Rastrear datos para identificar, clasificar y protreger

Inteligencia de amenazas:
Categorizar el comportamiento
Analizar tráfico (¿Deep web?)

OEA Más derechos para más gente

Citi Foundation citi

Sistemas ofensivos con Inteligencia Artifical

Creación de malware:
Creación en masa, fortaleza a capacidades de evasión

Botnets inteligentes:
Botnets con aprendizaje automático
Zombies inteligentes

Spear phishing:
Ingeniería social inteligente

IA de adversarios:
Redes generativas antagónicas: envenenar procedimientos de IA, producir resultados controlados o falsos

Ataques condicionales:
Ataques inteligentes a blockchain y contratos

Clasificación de víctimas:
Optimizar ataques dirigidos a organizaciones

OEA Más derechos para más gente

Citi Foundation citi

Sistemas adversarios con Inteligencia Artificial

Entradas de adversarios:
Artefactos diseñados para enñagar sistema de IA

Envenenamiento de datos:
Entrenar datos envenenados en las herramientas de IA

Robo de modelos:
Para aumentar las capacidades de entradas adversarias

Ataques de feedback:
Envenenar los modelos de IA para generar DoS