Máster Ciberseguridad y Privacidad

Seguridad y pentesting de servidores de datos

Prueba de Evaluación Continua, PEC 2

1. Para dudas y aclaraciones sobre el enunciado, debéis dirigiros al consultor responsable de vuestra aula.
2. La actividad es completamente individual y se podrá calificar con suspenso todas aquellas entregas que sean susceptibles de haber realizado una copia.
3. Hay que entregar la solución en un fichero .docx o PDF y enviarlo al área **Entrega y registro de EC**.

IMPORTANTE:

El objetivo de esta actividad no consiste en llevar a cabo ninguna intrusión o romper ningún sistema de seguridad, si no ser capaz de extraer la máxima información posible del propio portal de la UOC. Se trata únicamente de encontrar la información pública del portal web mediante técnicas de reconocimiento pasivo.

Por lo tanto, queda completamente prohibido hacer uso de herramientas intrusivas o de detección de vulnerabilidades como *Nessus*, *Metasploit* y similares, ya que podríamos afectar al rendimiento del portal y perjudicar a otros estudiantes. En caso de dudas sobre si una herramienta pudiera causar algún problema en el Campus, evitad usarla.

El uso de este tipo de herramientas intrusivas hará suspender directamente la asignatura.

Enunciado

Arquitectura Aplicaciones Web

En cualquier auditoría o test de intrusión a una aplicación web, una de las fases iniciales es la identificación de tecnologías utilizadas, análisis del código fuente de la aplicación o el descubrimiento de carpetas o archivos mediante herramientas no intrusivas que no alerten al objetivo de las actividades del auditor o el atacante.

Os proponemos que apliquéis diferentes técnicas **pasivas y no intrusivas** sobre el portal del campus de la UOC con el objetivo de descubrir lo máximo posible sobre la arquitectura de la aplicación web, su infraestructura, los lenguajes de programación utilizados o las medidas de seguridad aplicadas. Es aceptable el uso de escáner de puertos, *fingerprinting* de sistemas operativos, uso de técnicas OSINT, análisis de metadatos, etc. Pero **queda completamente prohibido hacer uso de herramientas intrusivas o de detección de vulnerabilidades como Nessus, Metasploit y similares, ya que podríamos afectar al rendimiento del portal y perjudicar a otros estudiantes.**

El análisis lo debéis realizar desde una perspectiva de caja negra, es decir, **sin utilizar vuestro usuario y contraseña para autenticaros en la aplicación**.

Debéis presentar un documento con la información que hayáis podido obtener incluyendo los siguientes apartados:

1. **Resumen Ejecutivo:** En este apartado se debe explicar de manera clara y precisa todos los aspectos relevantes hallados sobre la arquitectura del Portal de la UOC y las medidas de seguridad presentes. Se recomienda también seguir una cierta organización lógica al presentar los resultados (capa de red, capa de aplicación, etc...).

2. **Metodología utilizada:** En este apartado se debe explicar la metodología y herramientas utilizadas para la elaboración de la PEC. A la vez que se explica cómo se han realizado las pruebas.

3. **Evidencias:** A modo de anexo, en este último apartado se deberán exponer las capturas de pantalla u otras evidencias halladas mediante a la aplicación de la metodología expuesta en el apartado 2 que soporten las conclusiones establecidas en el apartado 1. Importante: Se deben añadir únicamente evidencias relevantes evitando añadir capturas u otra información que no sea útil.

Os damos unas primeras ideas para que sepáis por dónde empezar:

- Datos a nivel de red - rangos de IPs, puertos abiertos, qué aplicativos/CMSs existen…

- Datos a nivel de dominio - discovery, whois, passive dns
- Datos a nivel de aplicativo - tecnologías usadas, comentarios, googleDorks
- Datos a nivel de cifrado - certificados usados
- Otros.

Podéis encontrar información adicional en el siguiente enlace a OWASP: https://www.owasp.org/index.php/Testing_Information_Gathering