FICHA DE ASIGNATURA

Título: Auditoría de sistemas-Hacking ético

Descripción: Una de las estrategias que a menudo se utilizan para analizar la seguridad de sistemas de información consiste en analizar la seguridad de los sistemas siguiendo los pasos que llevaría a cabo un posible atacante. Como ethical hacking se entiende el conjunto de técnicas y prácticas que se utilizan a nivel profesional para auditar la seguridad simulando ataques informáticos a partir de metodologías de trabajo debidamente definidas a tales efectos. El objetivo del curso consiste en el análisis y la revisión de las técnicas y metodologías más actuales que se utilizan para el análisis de vulnerabilidades y la realización de pruebas de penetración en sistemas informáticos. El equipo docente que imparte el curso es uno de los mejores equipos en auditorías de hacking ético a nivel internacional y a nivel de formación dispone de una amplia experiencia en la realización de cursos de hacking..

Carácter: *Obligatoria*

Créditos ECTS: 6

Contextualización: Conocer los principios y las bases principales de la realización de auditorías de hacking ético. Aprender los objetivos, las actividades y los resultados esperados en las diferentes fases de una auditoría. Profundizar en el conocimiento de las diferentes metodologías existentes para la realización de auditorías de seguridad.

Modalidad: Online

Temario:

Semana 1. Introducción y Planificación

- Temario:
  - o Introducción a la seguridad informática.
  - o Planificación. Tipos de auditoría, objetivos y variable a tener en cuenta.

Semana 2. Information Gathering y vulnerabilidades comunes

- Temario:
  - o DNS
  - o Google hacking
  - o Metadatos
  - o Otras técnicas
  - o Escaneo de red y enumeración: Nmap
  - o Vulnerabilidades: Descripción, estándares y tipos
- Ejercicios:
  - o Descubriendo metadatos con FOCA

- Uso de scripts Nmap

Semana 3: Análisis

- Temario:
  - Análisis manual
    - OWASP
    - Badstore
  - Análisis automatizado
    - WFUZZ
    - Nikto
    - w3af
    - OpenVas
    - Ejercicios:
  - OWASP sobre Metasploitable
  - Auditoría sobre Badstore (puntuable)

Semana 4: Exploiting

- Temario:
  - Introducción
  - Búsqueda de exploits
  - Buffer Overflow
  - Metasploit Framework
  - Explotación de SEH
- Ejercicios:
  - Exploit de Windows para Buffer Overflow (Seattle Lab Mail (SLMail) 5.5)
  - Exploit Buffer Overflow (Ultra Mini HTTPD 1.21) (Puntuable)
  - Uso de Metasploit

Semana 5: Elevación de privilegios

- Temario
  - Introducción
  - Obtención de información
  - Elevación de privilegios mediante exploits
  - Elevación de privilegios mediante deficiencias en al configuración
  - Ejemplos de técnicas habituales en Windows y Linux

- o Pivotación

- Ejercicios:

  - o Postexplotación de DVD con varias técnicas

Competencias:

Generales

- CG8 – Capacidad para la aplicación de los conocimientos adquiridos y de resolver problemas en entornos nuevos o poco conocidos dentro de contextos más amplios y multidisciplinares, siendo capaces de integrar estos conocimientos.

Básicas

- CB6 – Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolver problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio.
- CB7 – Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de estos.
- CB8 – Que los estudiantes sepan comunicar sus conclusiones y conocimientos, así como las razones que las sustentan, a públicos especializados y no especializados de una forma clara y sin ambigüedades.
- CB9 – Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de una manera auto-dirigida o autónoma en gran medida.

Transversales

- CT4 – Gestionar la adquisición, estructuración, análisis y visualización de datos e información (en el ámbito informático y de seguridad), y valorar de forma crítica los resultados de esta gestión.
- CT12 – Que los estudiantes tengan la capacidad de reunir e interpretar datos relevantes (en el ámbito informático y de seguridad) para emitir juicios que incluyan una reflexión sobre temas relevantes de índole social, científica o ética.

Específicas

- CE9 – Capacidad para aplicar métodos matemáticos, estadísticos y de inteligencia artificial para modelar, diseñar y desarrollar aplicaciones, servicios, sistemas inteligentes y sistemas basados en el conocimiento.

Actividades Formativas:

Actividad Formativa	Horas	Presencialidad
Clases Magistrales (Video-Sesiones)	6	100
Clases de Tutoría	6	100
Ejercicios prácticos Individuales	20	0
Estudio autónomo	30	0

Metodologías docentes:

- Clase magistral / método expositivo
- Plataforma virtual de aprendizaje
- Aprendizaje Cooperativo (realización de trabajos)
- Aprendizaje Basado en Problemas (ABP)
- Entornos de simulación (recreación de problemas reales)

Sistema de Evaluación:

Sistemas de evaluación	Ponderación mínima	Ponderación máxima
Presentación de trabajos y/o proyectos	25.0	50.0
Examen escrito/oral (prueba objetiva, prueba de respuesta corta y/o prueba de desarrollo).	50.0	65.0

Normativa específica *(en el caso de que haya prerrequisitos):*

Bibliografía:

Introducción y Planificación

[1] Manel Medina, Mercè Molist. (2015). Cibercrimen. Barcelona: Tibidabo.

[2] jon Erickson. (2008). Hacking, the art of exploitation. San Francisco:No starch press

[3] OWASP. (2016). OWASP Testing Guide. Septiembre 2016, Sitio web:

https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents

Análisis

[1] OpenVas [2016]. Technical documentation. Noviembre 2016, Sitio Web:

http://docs.greenbone.net/index.html#user_documentation

[2] Wfuzz [2016]. Edge Security. Noviembre 2016, Sitio Web:

http://www.edge-security.com/wfuzz.php

[3] Kali Linux Downloads [2016]. Noviembre 2016, Sitio Web:

https://www.kali.org/downloads/

Information gathering:

[1] OWASP [2016]. Testing: Information Gathering. Octubre 2016, Sitio web:

https://www.owasp.org/index.php/Testing:_Information_Gathering

[2] Borja Merino, Jose Miguel Olguín. [2011] Pentest: Recolección de información (Information Gathering). INCIBE

https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_seguridad_information_gathering.pdf

[3] FOCA [2016]. Eleven paths. Octubre 2016, Sitio Web:

https://www.elevenpaths.com/es/labstools/foca-2/index.html

Explotación:

[1] HD Moore & Valsmith. [2007] Tactical Explotation: “the other way to pentest”. Black Hat USA. https://www.blackhat.com/presentations/bh-usa-07/Moore_and_Valsmith/Presentation/bh-usa-07-moore_and_valsmith.pdf

[2] Anley, Chris, and Jack Koziol. [2007] The shellcoder's handbook: discovering and exploiting security holes. ISBN 978-0470080238.

[3] Erickson, Jon. [2008] Hacking: the art of exploitation.ISBN 978-1593271442.

[4] Kennedy, David. Metasploit: the penetration tester's guide. ISBN 978-1593272883.

[5] Offensive Security. Metasploit Unleashed: The ultimate guide to the Metasploit Framework.https://www.offensive-security.com/metasploit-unleashed/

[6] Corelan Team. https://www.corelan.be/

Post Explotación:

[1] g0tmi1k. [2011] Basic Linux Privilege Escalation. https://blog.g0tmi1k.com/2011/08/basiclinux-privilege-escalation/

[2] Jonathan Renard [2015] To Shell And Back: Adventures In Pentesting.

http://toshellandback.com/2015/11/24/ms-priv-esc/

[3] FuzzySecurity Team. [2014] Windows Privilege Escalation Fundamentals.

http://www.fuzzysecurity.com/tutorials/16.html

[4] Ignacio Sorribas. [2014] Post-Exploitation with “Incognito”. http://hardsec.net/postexploitation-with-incognito