Sistemas de información fiables y valiosos

Valencia Chapter

AUDITORÍA DE HACKING ÉTICO

Proceso y resultados esperados

Florencio Cano Gabarda

Director de Seguridad Servicios On-Line ISACA Valencia

seguridad@isacavalencia.org - @florenciocano

#isacahack

Fecha: 8 de marzo de 2012

¿Qué es el hacking ético?

Es un procedimiento mediante el cual se analiza la seguridad de un sistema informático, se identifican vulnerabilidades de seguridad y se explotan para alcanzar información sensible y evidenciar que la amenaza es factible y real y poder evaluar su impacto.

Objetivo

Mejorar la seguridad de nuestra empresa o de nuestro cliente

Metodología

1. Alcance del proyecto
2. Recopilación de información
3. Mapeo de la red
4. Enumeración
5. Análisis de vulnerabilidades
6. Acceso
7. Escalada de privilegios
8. Informes
9. Presentación de resultados

1. Alcance del proyecto

Determinar, junto a una persona responsable de la organización, que sistemas se analizarán.

URL, rango de direcciones IP, organización.

2. Recopilación de información

2.1 Buscadores

2.2 Servidores WHOIS

2.3 Servidores DNS

2.4 Metadatos (FOCA)

2.5 Maltego

2.1 Buscadores

Google

Dogpile

Altavista

Yahoo

Sabi

Google Dorks

2.2 Servidores WHOIS

Herramienta whois (Linux)

2.3 Servidores DNS

Herramienta dig (Linux)

NSLookup

Fierce (Perl)

Otras herramientas

FOCA

Maltego

3. Mapeo de la red

3.1 Rango de direcciones IP

3.2 Puertos

3.3 Servicios

3.4 Versiones

3.5 Sistemas operativos

3.6 Tipo de dispositivo

3. Mapeo de la red

Herramientas:

Nmap

Traceroute

Amap

4. Enumeración

Aprovechar las características y configuración de cada servicio para extraer información adicional como recursos accesibles, usuarios válidos, etc.

5. Análisis de vulnerabilidades

5.1 Escáners de vulnerabilidades

5.2 Vulnerabilidades conocidas

5.3 Fuzzing

5.4 Análisis estático

5.5 Revisión de código

5.1 Escáners de vulnerabilidades

OpenVAS

Nessus

Nikto

W3af

5.2 Vulnerabilidades conocidas

Bugtraq

Exploit-db

5.3 Fuzzing

Peach Fuzzer

5.4 Análisis estático

Procesadores de lenguajes

Interpretación abstracta

5.5 Revisión de código

Manual + Herramientas de apoyo.

6. Acceso

- Acceso a información sensible
- Ejecución de comandos remota
- Metasploit: Shellcoding & Exploiting

7. Escalada de privilegios

Acceder a permisos distintos de los que deberíamos tener según nuestro usuario.

8. Informes

8.1 Informe ejecutivo

8.2 Informe técnico

9. Presentación de resultados

Las personas

ISACA®
Trust in, and value from, information systems

ISACA®
Sistemas de información fiables y valiosos
Valencia Chapter

IT GOVERNANCE INSTITUTE®

GRACIAS POR VUESTRA ATENCIÓN

CISA® Certified Information Systems Auditor®
An ISACA® Certification

CISM® Certified Information Security Manager®
An ISACA® Certification

CGEIT® Certified in the Governance of Enterprise IT®
An ISACA® Certification

CRISC™ Certified in Risk and Information Systems Control™
An ISACA® Certification