ISACA
Costa Rica Chapter

Active Directory a prueba de hackers: Taller de seguridad y auditoría

Objetivo:

Taller práctico donde se aprenderá a fortalecer tu Active Directory contra hackers y a realizar auditorías de seguridad efectivas para mantener tu red empresarial segura. Se evidenciarán los principales vectores de ataque utilizados por hackers y como protegerse ante dichos ataques.

Objetivo1: Lograr un aprendizaje práctico y efectivo a través de la combinación de teoría y ejercicios prácticos sobre ataques reales sobre el Active Directory.

Objetivo2: Lograr un aprendizaje práctico sobre los controles de seguridad que deben ser implementados para minimizar e identificar ataques informáticos sobre el Active Directory.

Dirigida a:

- Auditores de Sistemas
- Oficiales de Seguridad de Información
- Apoderado de Sistemas
- Analistas / administradores de seguridad de informática
- Personal de Tecnología encargado de la administración de servidores

Modalidad: Virtual (ZOOM)

Fecha: 5,6,7,8,y 9 de agosto,2024

Sesiones: 5 Sesiones

Hora: 6:00 p.m. a 9:00 p.m.

Horas CPE´s:16 horas

ISACA
Costa Rica Chapter

Prerrequisitos para el participante:

- Manejo del sistema operativo Windows a nivel básico
- Conocimiento básico del funcionamiento del directorio activo.

Requerimientos para desarrollar el curso:

- Un computador/laptop cori5 o superior
- 12GB de RAM o superior
- Sistema operativo Windows 10 o superior

Curso Incluye:

- Material que brinde el expositor.
- Certificado de participación

Contenido:

1. Introducción a la arquitectura de evaluación del AD
2. Cracking Online de usuarios con CRACKMAPEXEC
3. Cracking Online de usuarios locales con CRACKMAPEXEC
4. Extracción de política del AD y enumeración de usuarios
5. Extracción de NTDS
6. Cracking Offline a través de tablas pre-computadas
7. Impacket para extraer historial de contraseñas
8. Kerberoasting Attack
9. AS -REP Roasting Attack
10. Identificación de MSSQL (Microsoft SQL Server)
11. Ataques de cracking ONLINE sobre MSSQL con CRACKMAPEXEC
12. Enumerando información a través de MSSQL
13. Cracking OFFLINE de password MSSQL
14. Store Procedure XP_CMDSHELL
15. Reverse shell a través de XP_CMDSHELL
16. Delegación de permisos: Constrained / Unconstrained
17. Ataque de Persistencia: Golden Ticket
18. Controles de seguridad para identificar y prevenir ataques
19. Conclusiones y recomendaciones

ISACA
Costa Rica Chapter

Instructor:

Mi nombre es Omar Palomino, soy Ingeniero de Sistemas y consultor senior en ciberseguridad para KUNAK Consulting, una firma especializada en ciberseguridad presente en varios países de Latinoamérica: Perú, Chile, México, Honduras y Brasil. Me dedico a desarrollar proyectos de Gestión de Riesgos en Seguridad de la Información, Ciberseguridad, Red Team, entre otros. A lo largo de mi carrera he tenido la oportunidad de presentar ponencias en distintos congresos internacionales como: OWASP Perú 2012, NoConName Barcelona 2013,ISACA LatinCACS 2018,ISACA LatinCACS Chile 2019,OWASP Perú 2019,OWASP Latam 2020, ISACA LATINCACS 2023 Costa Rica, entre otros. Actualmente lidero el equipo de ciberseguridad de KUNAK Consulting y dedico parte de mi tiempo a compartir mis conocimientos en español a través de EcCouncil, donde imparto cursos de Ethical Hacking y Pentesting, y a través de mis redes sociales, donde publico mis conferencias y capacitaciones con el fin de mejorar el nivel de seg. de las organizaciones. Además, cuento con una amplia gama de certificaciones internacionales como:

Certificado	Organización Emisora
ISO 27001 Lead Auditor	PECB
ISO 27001 Lead Implementer	PECB
ISO 27032 CyberSecurity	PECB
ISO 31000 Lead Risk Manager	PECB
CISM (Certified Information Security Manager)	ISACA
CSX (Cybersecurity Fundamental Certificate)	ISACA
ECSA (Ec-council Certified Security Analyst)	ECCOUNCIL
CEI (Certified Ethical Hacker Instructor)	ECCOUNCIL
CEH (Certified EcCouncil Instructor)	ECCOUNCIL
CNDA (Certified Network Defense Architect)	ECCOUNCIL
CPENT (EC-Council Certified Penetration Testing)	ECCOUNCIL
CEH PRACTICAL	ECCOUNCIL
ECPPT (eLearnSecurity Certified Professional Penetration Tester)	ELEARNSECURITY
EWPTX (Web application Penetration Tester eXtreme)	ELEARNSECURITY
EWPT (Web Application Penetration testers)	ELEARNSECURITY
EJPT (eLearnSecurity Junior Penetration Tester)	ELEARNSECURITY
CEH MASTER	ECCOUNCIL
CPTC (Certified Penetration Testing Consultant)	MILE2
CPTE (Certified Penetration Testing Engineer)	MILE2
CSWAE (Certified Security Web Application Engineer)	MILE2
CPEH (Certified Professional Ethical Hacker)	MILE2
CISSO (Certified Information Systems Security Officer)	MILE2
ISO 27002 Fundamentals	EXIN
ITIL v3	EXIN

ISACA
Costa Rica Chapter

Inversión:

Miembros ISACA: ₡ 99.000 colones
Convenios CPIC: ₡ 108.000 colones
Público General: ₡ 120.000 colones
***Precios Incluyen IVA.**

Formas de pago:

- ✓ Transferencia
- ✓ Depósito a la cuenta de Asociación Costarricense de Auditores en Informática

- **A Nombre de la Asociación Costarricense de Auditores en Informática.**
- **Cédula Jurídica:** 3-002-045936

Cta. IBAN Colones -BCR CR69015201001013860853
Cta. IBAN Dólares - BCR CR96015201001022338943

Nota:

Enviar copia del depósito / comprobante de transferencia a la cuenta electrónica capacitacion@isacacr.org