INSTITUCIÓN UNIVERSITARIA
SNIES 4709

DIPLOMADO EN SEGURIDAD CIBERNÉTICA:

ÉNFASIS EN HACKING ÉTICO VERSIÓN 2019

FECHA DE INICIO 17 DE SEPTIEMBRE

JORNADA DE ESTUDIO: Martes, jueves y viernes de 6 p.m. a 10 p.m.

CERTIFICACIÓN: La IU EAM expedirá el certificado correspondiente.

VALOR INVERSIÓN

Matricula público en general: 1.44 SMMLV
Comunidad EAM 1.15 SMMLV

Financiación: Bancolombia - Cooservunal - Fondo Nacional del Ahorro - Avanza

Bancolombia · cooservunal · fna · Avanza · Crédito directo EAM

DESCRIPCIÓN:

Este es un curso de seguridad cibernética cuyo nivel de dificultad es intermedio. Los contenidos y la metodología de estudio esta orientada a la práctica. Abarca de una manera muy completa todo el ciclo técnico de auditorías de seguridad conocido como “Pentesting y/o Pruebas de Intrusión”.

Los módulos de estudio se centran en técnicas y pruebas de auditorías relacionados con hacking a infraestructuras, pero con un contexto totalmente ético, controlado y legal, para aprender a realizar auditorias de seguridad corporativas.

Los dispositivos de red usados en la temática son: Firewalls, Routers, UTMs, NAS. Además de servidores Linux, Windows y FreeBSB.

METODOLOGÍA DE ESTUDIO Y ENSEÑANZA:

La metodología práctica busca implementar de forma previa un laboratorio controlado LEGAL usando máquinas virtuales en el sistema de virtualización VMware, donde se simulan los escenarios de las infraestructuras tecnológicas corporativas, en los cuales se aplican de forma práctica cada técnica de auditoría y/o prueba de intrusión.

UNIDADES DE ESTUDIO:

DÍA 1:

Introducción al curso: Laboratorio Seguridad Cibernética: Énfasis Hacking Ético y/o Pentesting
- Pruebas de funcionamiento de las máquinas virtuales y laboratorios en VMware.
- Arquitectura de red para el auditor pentester: posicionamiento y visibilidad.
- Pruebas de intrusión (PenTesting) terminología básica y esencial.

Fase 1 Ciclo Pentesting: Recolección de Información
- Técnicas aplicadas de OSINT.
- Uso de herramientas OSINT: Maltego, Recon-NG, Theharvester, CEWL, DNSRECON.
- Construcción de diccionarios para futuras pruebas de password cracking.
- Hacking con buscadores (Google Hacking).
- Uso de Shodan pare recolectar Información.
- Uso de los Módulos de Metasploit Framework para recolección de información.

-Lab 1: Técnicas de recolección de Información Aplicadas.

DÍA 2:

Fase 2 Ciclo Pentesting: Scanning y Enumeración
- Uso básico de NMAP.
- Scanning de puertos (TCP-UDP), servicios, versiones y sistemas operativos.
- ZENMAP.
- Técnicas de scanning con NMAP.
- Scanning con los módulos auxiliares de Metasploit Framework.
- Técnicas de evasión de scanning.
- Top 20 comandos NMAP aplicados de forma practica.

-Lab 2: Técnicas de Scanning de Puertos Aplicadas

EAM
INSTITUCIÓN UNIVERSITARIA
SNIES 4709

DÍA 3:

Fase 3 Ciclo Pentesting: Análisis de Vulnerabilidades Infraestructura

- Pruebas automatizadas de análisis de vulnerabilidades con **Tennable NESSUS** Home Edition.
- Pruebas automatizadas de análisis de vulnerabilidades con **RAPID7-NEXPOSE.**
- Analizando y clasificando los resultados análisis de vulnerabilidades.
- Buscando los códigos de explotación recomendados por NESSUS y NEXPOSE.

-Lab 3: Lanzando análisis de vulnerabilidades: Linux-Windows-Dispositivos de red.

DÍA 4:

Fase 4 Ciclo Pentesting: Explotación de Vulnerabilidades Infraestructura

- Conceptos esenciales explotación: Exploit, Payloads (Reversas-Directas).
- Uso de Netcat para labores de explotación y post explotación.
- Explotación remota y local.
- Explotación del tipo Server Side.
- Explotando sistemas Windows.
- Explotando sistemas Linux.

DÍA 5:

- Explotando dispositivos de red.
- Ataques del lado cliente (Client Side Attacks).
- Técnicas de ingeniería social aplicada con script SET (Social Engineering Toolkit).
- Línea de comandos para auditores y labores de explotación.
- Evasión de antivirus con: MSFVENOM y Veil Framework.

-Lab 4: Explotación de vulnerabilidades: Linux-Windows-Dispositivos de red.

DÍA 6:

Fase 5 Ciclo Pentesting: POST Explotación de Vulnerabilidades Infraestructura

- Línea de comandos para auditores y labores de explotación.
- Uso de Netcat para labores de explotación y post explotación .
- Payload Meterpreter.
- Uso de los módulos post de Metasploit.
- Escalando privilegios.
- Manteniendo la persistencia en los sistemas explotados.
- Infección de puertas traseras (Backdoors).
- Labores de espionaje: Keylogegrs, Ataques de Hombre en el Medio, Snapshot.
- Técnicas de post explotación: Pivoting, PortFW y Tunneling.
- Modulos extras meterpreter: MIMIKATZ, Sniffing, espia.
- Recolección de información interna desde labores de post explotación.

-Lab 4-5: Post Explotación de Vulnerabilidades: Linux-Windows-Dispositivos de red

DÍA 7 :

Fase 6 Ciclo Pentesting: Password Cracking

- Password Attack (conceptos y terminología esencial).
- Tipos de hashes; MD5, MD4, SHA, NT-LM HASH.
- Técnicas de extracción de Hashes (Hashdumping).
- Extracción de hashes: Linux, Windows, Red, Aplicaciones web, Archivos de configuración.
- Ataques por fuerza bruta.
- Password Cracking & Rainbow Tables.
- Password Guessing.
- Ataques por diccionario.
- Hashcat Password Cracking.
- Ataques con reglas.
- Ataques con mascaras.
- Pass the hash-PTH.

-Lab 6: Password Cracking aplicado

DÍA 8:

Pruebas de Intrusiones Corporativas con METASPLOIT PRO

- Introducción y visión general de la poderosa herramienta Metasploit Pro.
- Versiones comerciales y gratuitas de Metasploit.
- Integración de NEXPOSE con Metasploit Pro.
- Las interfaces de Metasploit Pro (GUI y Consola - Shell).
- El ciclo del pentesting con Metasploit Pro.
- Explotación y post explotación con Metasploit Pro.
- Ataques y explotación del lado cliente y server con Metasploit Pro.

DÍA 9:

- Ataques por fuerza bruta con Metasploit Pro.
- Campañas de phising e ingeniería social.
- Creando payloads, evasión de antivirus y ataques de lado cliente.
- Pruebas de intrusión web con Metasloit Pro.
- Los metamódulos en Metasploit Pro.
- Metasploit Pro Quick Pentest.

-Lab 7: Pruebas de Intrusión con METASPLOIT PRO

DÍA 10:

Pruebas de Intrusiones y Seguridad en Aplicaciones Web

- Vecores de ataques a aplicaciones web.
- SQLI-XSS, ejecución de comandos remotos.
- Uso de SQLMAP y Burpsuite.

-Lab 8: Pruebas de Intrusión en Aplicaciones web

Presentación de Reportes:

- Reporte técnico.
- Reporte ejecutivo.
- Plan de acción y pruebas complementarias para la eficacia y eficiencia en acciones y/o correcciones de auditoria.

Al finalizar:

- Examen Final: Reto Informático Capture The Flag.
- Solución Examen Final: Reto Informático Capture The Flag.

Herramientas tecnologías que se aprenderán a manejar en el curso:

-Kali Linux 2019-1
-Metasploit Framework
-Nmap
-Nessus
-Caine & Abel
-John The Ripper
-Metasploit Pro
-Hashcat
-Ophcrack
-Suite Sysinternals
-PowerExploit
-MSFVENOM
-Veil framework
-Burpsuite PRO-FREE

PRE-REQUISITOS:

Ser profesional graduado o de últimos semestres en carreras de tecnología (sistemas, informática, telecomunicaciones, electrónica, entre otros). Importante tener conocimientos en infraestructura tecnológica, manejo básico de Linux, redes informáticos, protocolos de red TCP-IP, sistemas operativos, shell cmd y bash. Ideal MÁS NO MANDATORIO, el manejo de herramientas de auditoria como Kali Linux, Metasploit y Wireshark.

RECURSOS NECESARIOS:

Cada estudiante debe de tener: una maquina PC o portátil, con mínimo 8 GB en memoria RAM y 100 GB libres en disco duro, tarjeta de red y procesador que soporte virtualización en VMware.

SABEMOS QUE TIENES MUCHAS ACTIVIDADES,

POR ESO ESTE DIPLOMADO ES COMPLETAMENTE

VIRTUAL

COMUNÍCATE E INSCRÍBETE CON NOSOTROS

WWW.EAM.EDU.CO

(036) 741 11 01 EXT. 105

(+57) 318 851 6428

INSTITUCIONUNIVERSITARIAEAM

EAMDELQUINDIO

EDUCACIÓN CONTINUADA
INSTITUCIÓN UNIVERSITARIA
SNIES 4709
48 AÑOS
NEGOCIOS TECNOLOGÍA E INNOVACIÓN