LA SEGURIDAD GESTIONADA POR EXPERTOS PROTEGE EL ACTIVO MÁS ESTRATÉGICO DE SU ORGANIZACIÓN: LA INFORMACIÓN

THE MAINFRAME & SECURITY COMPANY

Oferta curso VA 080

ACME

Válida hasta el 31 de MARZO de 2099

Bsecure – The Mainframe & Security Company

https://www.go2bsecure.com
https://www.go2bsecure.com/audihack/
hablamos@go2bsecure.com

OFERTA CORPORATIVA DEL CURSO ONLINE VA080_ONL_SP Seguridad, Hacking y Auditoría en entornos Mainframe z/OS

Dª John Doe
Director del Departamento de Auditoría
ACME Inc.

Madrid, 12 de febrero de 2022.

Estimados señores:

Tenemos el honor de hacerle llegar esta oferta para su corporación del curso VA080_ONL_SP.

Reciba un cordial saludo,

Ángel Gómez
CEO & CTO

INDICE

OFERTA CORPORATIVA DEL CURSO ONLINE VA080_ONL_SP Seguridad, Hacking y Auditoría en entornos Mainframe z/OS 2
II. CONTENIDO DEL CURSO. 4

II. CONTENIDO DEL CURSO.

Es un curso en el que personas con decenas de años de experiencia han invertido centenas de horas para crear algo único en el sector.

El curso VA-080 es un exclusivo sistema de auto estudio de Auditoría Técnica y Técnicas Hacking en español e inglés, desarrollado por el equipo técnico de Bsecure - The Mainframe and Security Company.

En él se explica como una persona prácticamente neófita en la plataforma Z/OS, pero que tiene acceso a ella, sería capaz de denegar el servicio en el peor de los casos relatados. Como ejemplo podemos pensar en un cliente tipo que use esta tecnología en una entidad Bancaria de las más grandes del mundo. Una semana sin procesamiento informático sería uno de los mayores problemas a la que se pudiera enfrentar esta entidad. Aparte de los problemas económicos directos, la falta de confianza en sus sistemas del resto de su industria y el desprestigio de la marca en sus clientes, podría hundirla en la bolsa de valores.

Este curso es vital por lo tanto para todas aquellas personas profesionales de la auditoría y la seguridad que deseen conocer las Técnicas Hacking y penetración de Sistemas Mainframe BASADOS EN CASOS REALES y qué tenemos que revisar para evitarlas, o al menos detectarlas.

La última parte del curso está orientado a aprender a realizar una excelente auditoría de estos sistemas de cara a comprobar la correcta implantación de controles tecnológicos de control y aminoración del riesgo.

Encontrarán dentro del curso no sólo información y formación, también encontrará documentación importante sobre muchos aspectos poco conocidos de las herramientas de seguridad que se utilizan de forma estándar en la protección de los sistemas.

La estructura del curso parte de la enunciación del problema principal que intenta resolver: "El mito de la inviolabilidad del Mainframe" hasta las configuraciones o procedimientos sugeridos en el sistema, con gran nivel de detalle.

Está diseñado para que tenga valor tanto para el profesional que está continuamente administrando el sistema como el que no ha usado nunca alguna aplicación del Mainframe.

ACME

Oferta curso VA_080_ONL_SP

Este curso está basado en la impartición durante más de diez años de un curso menos extenso en salas de formación. Hemos observado que las personas que eran administradores de seguridad, es posible que no aprendieran mucho de la parte del RACF básico, pero si que aprendían de la parte del Sistema Básico. Y, al contrario, los gestores de sistemas es posible que no aprendieran mucho de la parte del sistema básico, pero sí que aprendían de la parte del gestor de seguridad. Y todos ellos de la parte de hacking. Con todos los aspectos que se tocan en el curso orientados a la seguridad siempre hemos obtenido una gran puntuación sobre el interés y la adecuación del curso. Recuerden que no se trata de convertirlos en súper administradores de RACF o en súper administradores de z/OS, sino que focalicen todos sus conocimientos y los que están adquiriendo nuevos en un sólo punto: La securización del entorno.

En el caso de los auditores y los gestores de riesgos, el objetivo es comprender el porqué de los diferentes aspectos a auditar.

NO EXISTE EN EL MUNDO UN CURSO ONLINE O PRESENCIAL COMO ESTE.

Recuerden que el sentido es el mostrar técnicas muy básicas que se han encontrado en Internet y que han hecho mucho daño a clientes del constructor del sistema operativo, para que sus equipos de seguridad obren en consecuencia. En ningún momento este curso intenta hacer apología del hacking en estos sistemas.

Por último, hay que indicar que palabras como z/OS o MVS se utilizan de forma sinónima a lo largo del curso. Hay técnicos que se sentían más cómodos con una forma de denominarlo y otros con la otra forma.

El programa del curso se compone de más de 20 horas de training en vídeo online y material adicional en pdf, excel... así como una librería con todas las herramientas utilizadas en el mismo:

El curso está disponible 24 horas, 7 días a la semana durante un año. Es el tiempo que dispone para realizarlo. Nuestro cálculo es que se tarda un mes dedicando una hora diaria sólo para visualizar los vídeos. Además tendría que revisar el material escrito y probar en sus propios sistemas los ejercicios propuestos y las demostraciones realizadas.

ACME

Oferta curso VA_080_ONL_SP

Unidad	Nombre
1	Presentación del Curso 2020
	Metas a Conseguir Realizando el Curso
	Información sobre el copyright
	La situación de la seguridad en el entorno (el mito del Mainframe)
	Vulnerabilidades básicas conocidas
2	El entorno z/OS conocimientos básicos de arquitectura y programas de uso
	Su historia y los retos de los profesionales de Seguridad y Auditoría.
	Conocimientos básicos de la Arquitectura del Sistema I
	Conocimientos básicos de la Arquitectura del Sistema II
	Ejercicios de Funcionamiento y Auditoría
	Conocimientos básicos de la Arquitectura del Sistema III
	Conocimientos básicos de la Arquitectura del Sistema IV
3	Introducción al entorno z/OS desde el punto de vista de la seguridad
	Conocimiento básico del JCL y del uso de procedimientos.
	Uso del ISPF I
	Uso del ISPF II.- Gestión de la ejecución de trabajos y procedimientos
	Tratamiento de ficheros en ISPF
	RACF básico I (Gestor de Seguridad)
	RACF básico II (Gestor de Seguridad)
4	Construye tu entorno de laboratorio
	Fuentes de Información Oficial
	Fuentes NO Oficiales
	Breve historia de los emuladores de Hardware,
	Descripción de un entorno “Hércules” necesario para el Laboratorio de pruebas
	IPL en un Hércules
	Sistemas ADCD y “cortados” para instalación en emuladores de Hardware
5	FOOTPRINTING

Oferta curso VA_080_ONL_SP

	Subiendo herramientas con el emulador de terminal
	Subiendo herramientas con el FTP
	Curiosidades de la implementación del FTP en z/OS
	Utilidad DDLIST o como localizar cualquier elemento en memoria
	Diferenciación entre PROCLIBS, STC´S y JOB´s
	Uso del ShowMVS
	Uso del Tasid
	Footprinting (Donde estamos y que somos capaces de ver y hacer)
	Resultado del Footprinting
6	HACKING & DOS
	Disclaimer sobre el tipo de entorno y el objetivo principal
	Ejemplo / Reto sobre la posibilidad de hackear un z/OS
	Descripción de "nuestro" entorno de pruebas para el curso
	Chequeo del Internal Reader
	Robo y abuso del RACF
	Infecciones I y Puertas Traseras
	Crackeo de Password
	Resultado Cracking Total
	Robo de Información no Autorizada I
	Escalada de privilegios desde un usuario normal a usuario “maestro”
	Robo de Información no autorizada (II).-Salto al RACF con la PPT
	Infecciones II- ahora automáticas (Rasomware)
	STC´s trabajando para mi
	DOS en el centro primario y alternativo a la vez
	El problema del SNA aumentado por el TCP/IP
7	Metodología Básica Auditoría y Seguridad

Oferta curso VA_080_ONL_SP

La checklist del Auditor I

1 Audit Administration
1.1 Audit Project Documentation
1.2 Audit Program
1.3 Audit Findings/Client's Response
1.4 Pre-audit Procedures (organization audit standards)
1.5 First Day Activities Checklist
1.6 Last Day Activities Checklist (company audit standards)
2 z/OS System Environment
2.1 System Environment Analysis
3 System Data Set Integrity
3.1 System Datasets: GENERAL
3.2 System Datasets: CATALOGS
4 PARMLIB Members
4.1 PARMLIB Concatenation
5 Authorized Program Facility
5.1 Other APF-related Security Controls
5.2 APF Libraries
5.3 LINKLIST Libraries
5.4 SMF Activity

La checklist del Auditor II

6 Program Properties Table (PPT)
6.1 PPT Entry Properties
7 Supervisor Calls (SVC)
7.1 IBM Supplied SVCs
7.2 Installation SVCs
8 Appendages
8.1 Determine Use of Appendages
9 Link Pack Areas
9.1 Program Authorization
10 System Management Facility (SMF)

Oferta curso VA_080_ONL_SP

10.1 SMF Overview
11 z/OS Subsystems
11.1 z/OS Subsystem Overview
12 Job Entry Subsystem
12.1 JES2 Overview
12.2 JES2 Datasets
12.3 JES2 Exits
13 Time Sharing Option (TSO)
13.1 TSO Logon
13.2 TSO Commands
13.3 TSO User IDs
13.4 TSO Exits
14 System Log (SYSLOG)
14.1 z/OS Commands Issued at IPL
15 z/OS System Exits
15.1 Overview z/OS System Exits

La checklist del Auditor III

16 RACF AUDIT
16.1 RACF SETROPS AUDIT
16.2 USERS: GENERAL
16.3 USERS: CONNECT
16.4 USERS: OMVS SEGMENT
16.5 GROUPS: GENERAL CHECKING
16.6 GROUPS: OMVS
16.7 DATASETS: GENERAL CHECKING
16.8 DATASETS: STANDARD PERMITS
16.9 DATASETS: CONDITIONAL PERMITS
16.10 DATASETS: ACCESS INTEGRITY

La checklist del Auditor IV

17 RACF CLEANING
17.1 DATASETS
17.2 GROUPS
18 z/OS Unix System Services
18.1 General
19 z/OS Change Control
19.1 Overview z/OS Change Control and FIM

Aspectos Normativos a considerar
Otros Documentos para apoyar buenas auditorías básicas

8 RESUMEN DEL CURSO Y NUESTRA OPINIÓN PARA EVITAR ESTAS TÉCNICAS
Resumen del curso