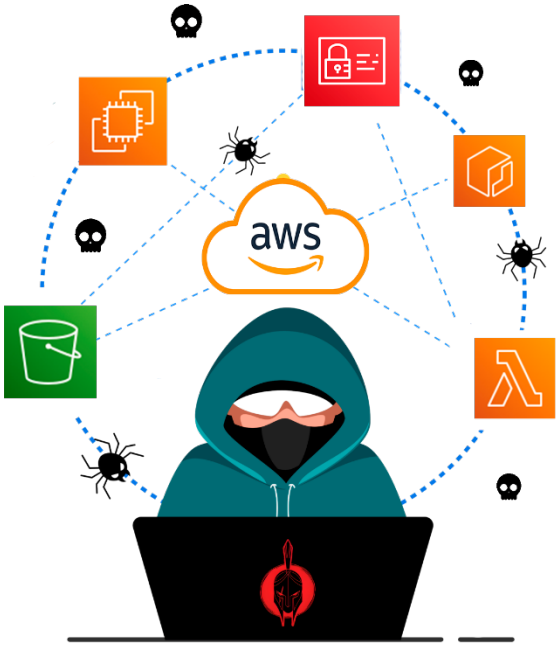
CURSO PROFESIONAL DE PENTESTING CONTRA AMAZON WEB SERVICES

Spartan-Cybersecurity



ADVERTENCIA

TODO nuestro contenido publicado se realiza con fines educativos, informativos y éticos.

TODAS las técnicas expuestas en este curso son desarrolladas y ejecutadas en entornos controlados.

¡NO SOMOS RESPONSABLES DEL MAL USO QUE LE PUEDAN DAR!

TABLA DE CONTENIDO

14. PENTESTING CONTRA IAM
    a. ENUMERACIÓN MANUAL DE IAM
        i. Enumerando usuarios
        ii. Enumerando grupos
        iii. Enumerando roles
        iv. Enumerando políticas
    b. ENUMERACIÓN AUTOMATIZADA POR MEDIO DE FUERZA BRUTA
15. ESCALACION DE PRIVILEGIOS EN IAM
    a. PERMISOS DE IAM EN OTROS USUARIOS
        i. Abusando del permiso IAM:CreateAccessKey
        ii. Abusando del permiso IAM:CreateLoginProfile
        iii. Abusando del permiso IAM:UpdateLoginProfile
        iv. Abusando del permiso IAM:AddUserToGroup
    b. PERMISOS SOBRE POLÍTICAS
        i. Abusando del permiso IAM:CreatePolicyVersion
        ii. Abusando del permiso IAM:SetDefaultPolicyVersion
        iii. Abusando del permiso IAM:AttachUserPolicy
        iv. Abusando del permiso IAM:AttachGroupPolicy
        v. Abusando del permiso IAM:AttachRolePolicy
        vi. Abusando del permiso IAM:PutUserPolicy
        vii. Abusando del permiso IAM:PutGroupPolicy
        viii. Abusando del permiso IAM:PutRolePolicy
    c. ACTUALIZACIÓN DE UNA ASSUMEROLEPOLICY
        i. Abusando del permiso IAM:UpdateAssumeRolePolicy
    d. PERMISOS IAM:PassRole:*
16. Introducción a S3 – (Simple Storage Service)
    a. ¿QUÉ ES UN BUCKET?
    b. ¿QUÉ ES UN OBJETO?
    c. ¿QUÉ ES UNA POLITICA DE BUCKET?

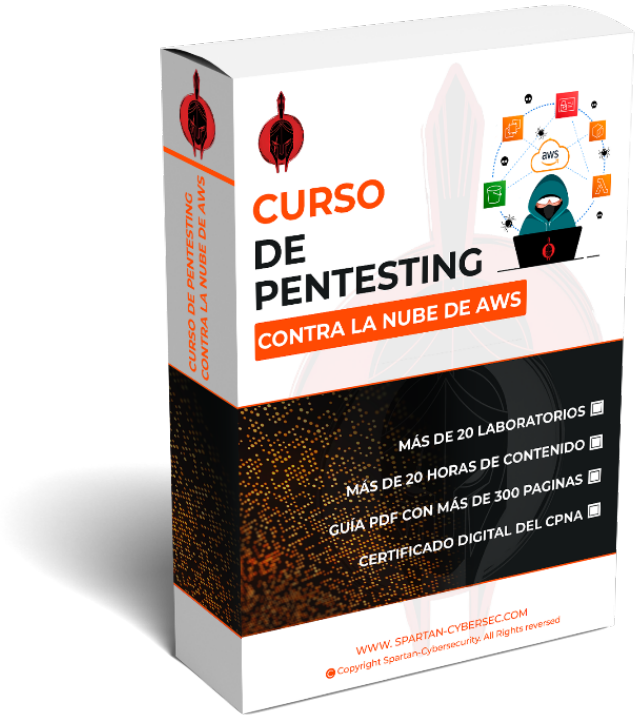
17. PENTESTING CONTRA S3
    a. ENUMERACIÓN MANUAL DE S3
        i. Enumerando buckets
    b. CASOS DE ESTUDIO
        i. Detectando malas configuraciones en un Bucket
18. Introducción a Lambda
    a. ¿Qué es una función de AWS Lambda?
    b. ¿Qué lenguajes admite AWS Lambda?
    c. ¿Qué tipo de código puede ejecutarse en AWS Lambda?
    d. ¿Qué es un API Gateway?
19. PENTESTING CONTRA LAMBDA
    a. ENUMERACIÓN MANUAL DE LAMBDA Y API GATEWAY
        i. Enumerando funciones Lambda
        ii. Enumerando API Gateway
    b. CASOS DE ESTUDIO
        i. Post-explotacion RCE Sobre Lambda
        ii. Escalación de privilegios IAM:PassRole con Lambda
        iii. Escalación de privilegios IAM:PassRole con Lambda y DynamoDB
        iv. Escalación de privilegios IAM:PassRole con Lambda #2
20. Introducción a EC2 – (Amazon Elastic Compute Cloud)
    a. ¿QUÉ ES UNA INSTANCIA EC2?
    b. ¿QUÉ ES UNA AMI?
    c. ¿QUÉ ES UN GRUPO DE SEGURIDAD DE EC2?
    d. ¿QUÉ SON LOS METADATOS DE INSTANCIA?

21. PENTESTING CONTRA EC2
    a. ENUMERACIÓN MANUAL DE EC2
        i. Enumerando instancias
    b. Despliegue de laboratorios con Cloudgoat
    c. CASOS DE ESTUDIO
        i. EC2_SSRF – Abusando del servicio de metadatos
        ii. Escalación de privilegios IAM:PassRole con EC2
        iii. Escalación de privilegios IAM:PassRole con GlueDevEndpoint
22. Introducción a VPC – (Virtual Private Cloud)
    a. ¿Cuáles son los componentes de Amazon VPC?
    b. ¿Cómo puedo proteger las instancias de Amazon EC2 que se ejecutan en mi VPC?
    c. ¿Qué diferencias existen entre los grupos de seguridad que están en una VPC y las ACL de red de una VPC?
23. PENTESTING CONTRA VPC
    a. ENUMERACIÓN MANUAL DE VPC
        i. Enumerando VPC
    b. CASOS DE ESTUDIO
        i. Pivoting en la nube
24. Introducción a RDS (Relational Database Service)
    a. ¿Qué es una instancia de base de datos?
    b. ENUMERACIÓN MANUAL DE RDS
        i. Enumerando RDS
25. Introducción a ECS (Elastic Container Service)
    a. ¿Qué es Elastic Container Registry (ECR)?
    b. ¿Qué es un cluster de ECS?

26. PENTESTING CONTRA ECS
    a. ENUMERACIÓN MANUAL DE ECS
        i. Enumerando ECR
        ii. Enumerando ECS
        iii. Enumerando EKS
    b. CASOS DE ESTUDIO
        i. Post-explotacion RCE sobre EC2 con clusters de dockers
27. Introducción a AWS Secrets Manager
    a. ¿Qué datos confidenciales puede administrar AWS Secrets Manager?
28. PENTESTING CONTRA AWS SECRETS MANAGER
    a. ENUMERACIÓN MANUAL DE AWS SECRETS MANAGER
        i. Enumerando AWS SECRETS MANAGER
29. Introducción CloudFormation y Datapipeline
    a. ¿Qué es Cloudformation?
    b. ¿Qué es Datapipeline?
    c. CASOS DE ESTUDIO
        i. Escalacion de privilegios IAM:PassRole con CloudFormation
        ii. Escalacion de privilegios IAM:PassRole con DataPipeline
30. Pentesting contra arquitectos de AWS
    a. Exfiltración de credenciales dentro de un repositorio de GitHub

31. Análisis de vulnerabilidades con herramientas automatizadas
    a. Utilizando Prowler
    b. Utilizando Cloudsplaining
    c. Utilizando Pacu
32. Introducción a Blue Team en AWS
    a. ¿Qué es AWS CloudTrail?
        i. Evasión de CloudTrail
    b. ¿Qué es AWS CloudWatch?
    c. ¿Qué es AWS GuardDuty?
        i. Evasión de GuardDuty
    d. ¿Qué es AWS Inspector?
    e. ¿Qué es AWS Shield?
    f. ¿Qué es AWS Web Application Firewall (WAF)?

DETALLES DEL CURSO



Material entregable:

- ✓ Acceso a más de 20 horas de contenido en MATERIAL GRABADO.
- ✓ E-Book de +300 páginas.
- ✓ Acceso a laboratorio vulnerable para hackear una infraestructura alojada en AWS durante 1 mes.
- ✓ Acceso a un grupo exclusivo del curso para interactuar con los demás estudiantes y el profesor.
- ✓ Certificado del CPNA por parte de Spartan-Cybersecurity.

Costo del curso: $200 USD

Comunícate con el área de ventas para conocer nuestros descuentos:

WhatsApp: https://wa.link/j265a0

Telegram: https://t.me/Spartan_Cybersecurity

Te esperamos 😎