CURSO PROFESIONAL DE PENTESTING CONTRA AMAZON WEB SERVICES

Spartan-Cybersecurity

[CPNA-v2]

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
        i. Utilizando Enumerate-IAM.py
        ii. Utilizando CLIAM
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 y sts:AssumeRole
    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?
    d. CASOS DE ESTUDIO
        i. Enumerando buckets
        ii. Utilizando S3Scanner
        iii. Detectando malas configuraciones en un Bucket
17. 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?
18. PENTESTING CONTRA LAMBDA
    a. ENUMERACIÓN MANUAL DE LAMBDA Y API GATEWAY
        i. Enumerando funciones Lambda
        ii. Enumerando API Gateway
    b. CASOS DE ESTUDIO
        i. Identificando malas prácticas en variables de entorno de un Lambda
        ii. XSS en API Gateway
        iii. Análisis de un API Gateway con Lambda Authorizer
        iv. Escalación de privilegios utilizando iam:PassRole, lambda:CreateFunction y lambda:InvokeFunction
        v. Escalación de privilegios utilizando iam:PassRole, lambda:CreateFunction, lambda:CreateEventSourceMapping, dynamodb:PutItem, dynamodb:CreateTable y lambda:InvokeFunction
        vi. Escalación de privilegios utilizando iam:PassRole y lambda:UpdateFunctionCode

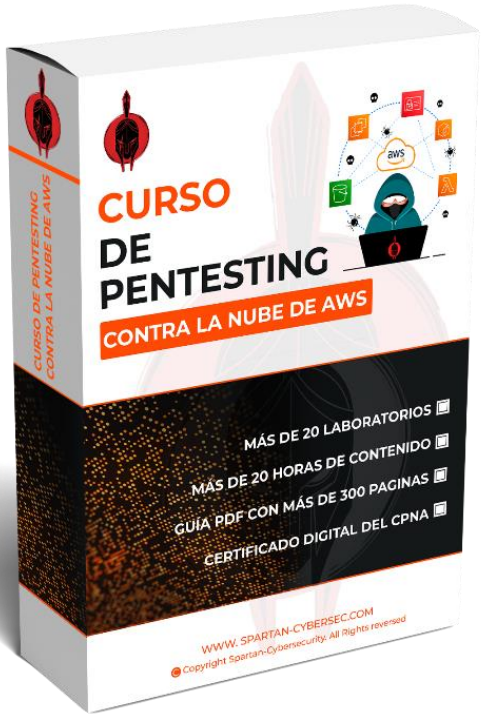
19. Introducción a EC2 – (Amazon Elastic Compute Cloud)
    a. ¿QUÉ ES UNA INSTANCIA EC2?
    b. ¿QUÉ ES UNA AMI?
    c. ¿QUÉ ES UN GRUPO DE SEGURIDAD DE EC2?
    d. ¿QUÉ SON LOS METADATOS DE INSTANCIA?
20. PENTESTING CONTRA EC2
    a. ENUMERACIÓN MANUAL DE EC2
        i. Enumerando instancias
    b. CASOS DE ESTUDIO
        i. Abusando del servicio de metadatos IMDSv1 por medio de un SSRF
        ii. Escalación de privilegios utilizando IAM:PassRole y ec2:RunInstances
        iii. Escalación de privilegios utilizando IAM:PassRole y glue:CreateDevEndpoint
21. 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?
    d. CASOS DE ESTUDIO
        i. Enumerando VPC
        ii. Movimientos laterales en red o Pivoting en la nube
22. Introducción a RDS (Relational Database Service)
    a. ¿Qué es una instancia de base de datos?
    b. ENUMERACIÓN MANUAL DE RDS
        i. Enumerando RDS
23. Introducción a ECS (Elastic Container Service)
    a. ¿Qué es Elastic Container Registry (ECR)?
    b. ¿Qué es un cluster de ECS?

24. 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
        ii. Utilizando Cloud Container Attack – (CCAT)
25. Introducción a AWS Secrets Manager
    a. ¿Qué datos confidenciales puede administrar AWS Secrets Manager?
    b. CASOS DE ESTUDIO
        i. Enumerando AWS SECRETS MANAGER
26. Introducción a AWS KMS
    a. ¿Qué datos confidenciales puede administrar AWS KMS?
    b. CASOS DE ESTUDIO
        i. Enumerando AWS KMS
27. Introducción a AWS LightSail
    a. ¿Qué es AWS LightSail?
    b. CASOS DE ESTUDIO
        i. Enumeración de AWS LightSail
        ii. Explotación de CVE-2018-20463 para obtener acceso a un WordPress alojado en AWS LightSail
28. Introducción a AWS SES y AWS SNS
    a. ¿Qué es Amazon Simple Email Service (SES)?
    b. ¿Qué es Amazon Simple Notification Service (SNS)?
    c. CASOS DE ESTUDIO
        i. EMAIL BOMB o Spam indiscriminado de OTPs

29. Introducción a AWS Cognito
    a. ¿Qué es AWS Cognito?
    b. ¿Qué es User Pool?
    c. ¿Qué es Identity Pool?
    d. CASOS DE ESTUDIO
        i. Enumeración de AWS Cognito
        ii. Utilizando un JWT de Cognito para tener acceso a recursos de AWS con un STS
        iii. Escalación de privilegios por medio de atributos del usuario
30. Introducción CloudFormation y Datapipeline
    a. ¿Qué es Cloudformation?
    b. ¿Qué es Datapipeline?
    c. CASOS DE ESTUDIO
        i. Escalación de privilegios utilizando iam:PassRole y cloudformation:CreateStack
        ii. Escalación de privilegios utilizando iam:PassRole , datapipeline:CreatePipeline y datapipeline:PutPipelineDefinition
31. Pentesting contra arquitectos de AWS
    a. Exfiltración de credenciales dentro de un repositorio de GitHub
    b. Phishing utilizando el Login de AWS SSO
    c. Utilizando Flipper como BadUSB para la ejecución de un Malware Moderno que exfiltra credenciales de AWS
32. Análisis de vulnerabilidades con herramientas automatizadas
    a. Utilizando Prowler
    b. Utilizando ScoutSuite
    c. Utilizando Cloudsplaining
    d. Utilizando Pacu

33. Analizando un aplicativo web con PasswordLess Authentication
    a. ¿Autenticación personalizada con Cognito?
    b. ¿Qué es WebAuthn?
    c. ¿Qué es FIDO2?
    d. ¿Qué es Magic Link Sign In?
    e. ¿Qué es SMS Auth?
34. Introducción a Blue Team en AWS
    a. ¿Qué es AWS CloudTrail y como deshabilitarlo?
    b. ¿Qué es AWS CloudWatch?
    c. ¿Qué es AWS GuardDuty y como deshabilitarlo?
    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 25 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.
- ✓ Un Intento para resolver examen práctico.
- ✓ Certificado del CPNA-v2 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 😎