ETHICAL HACKING CLOUD PENTESTING (EHCP)

DESCRIÇÃO

(Nível Intermediário/Avançado)

Carga Horária: 40hrs

Instrutores: Rodrigo "Sp0oKeR" Montoro e Felipe "Prot0eus"

Os ecossistemas dos provedores de nuvem/cloud ampliaram as superfícies de ataque, promovendo novos métodos e caminhos de exploração. Especificamente, na Amazon Web Services (AWS), estamos falando de mais de trezentos e oitenta (380+) serviços que um atacante pode utilizar para atingir seu objetivo e comprometer redes, sistemas e aplicações.

Esse grande cenário, complexo e intrigante, trouxe consigo inúmeras técnicas ofensivas (novas e antigas), métodos diferentes de movimentação lateral, novas ferramentas, modos de reconhecimento e muitos aspectos ainda por serem desvendados, o que torna a Segurança em Nuvem em um trabalho desafiador e bem interessante.

O objetivo principal do curso é apresentar parte desses novos vetores e técnicas de ataque, entendendo como os ambientes se conectam, como utilizar esse novo arsenal de ferramentas e aprender, de forma prática, os detalhes da exploração dos serviços de nuvem em ambientes AWS.

MÓDULO 0x00 – Preparação (2h)

1. Introdução ao ecossistema AWS
2. O que é Cloud Security ?
3. MITRE ATT&CK Cloud

MÓDULO 0x01 – Identificando e ganhando acesso a AWS (2h)

1. OSINT
2. Finding Exposed Resources
3. Dumping Creds

MÓDULO 0x02 – Escalação de Privilégios (2h)

1. Visão geral do Identity and Access Management (IAM)
2. Escalando Privilégios
3. AWS Identity Center
4. Roubando Segredos

MÓDULO 0x03 – Movimentação Lateral (2h)

1. Data Plane
2. Control Plane
3. AWS Identity Center

MÓDULO 0x04 – Evading Security Controls (2h)

1. Evitando CloudtTrail
2. Bypassando GuardDuty
3. Bypassando o Macie

MÓDULO 0x05 – Persistência (2h)

1. Backdooring user accounts
2. Backdooring services
3. Backdooring CI/CD

MÓDULO 0x06 – Exfiltração de Dados (2h)

1. Exfiltração de dados entre contas
2. Exfiltração de dados de contas avançadas

MÓDULO 0x07 – CTF (2h)

1. Exercício Hands-on
2. Recomendações Finais

PRÉ-REQUISITOS

- Conhecimentos sólidos em Sistema Operacional Windows
- Conhecimentos sólidos em Sistema Operacional Linux
- Conhecimentos sólidos de Rede de Computadores e Serviços de Rede
- Experiência de programação em linguagens de alto nível (Python, Java, Go, correlatos)
- Noções de programação em linguagens de baixo nível (Assembly, C, C++)
- Conhecimentos básicos de Cloud (preferencialmente AWS)
- Conhecimentos básicos de Cloud Security
- Familiaridade com Ferramentas de Virtualização (VMWare, Virtual Box)

PÚBLICO ALVO

- Especialistas em Segurança da Informação
- Analista de Segurança da Informação
- Pentesters
- Membros de Red Team
- Membros de Blue Team
- Membros de CSIRT
- Membros de SOC
- Profissionais de TI com interesse e afinidade na área de Segurança da Informação

MATERIAL NECESSÁRIO

- Os alunos precisam de um computador (Windows, Linux ou Mac OS), com acesso de administrador e capacidade de instalar *softwares*/programas (Terraform, Git)
- Configuração mínima de 8GB de RAM, 40 GB de espaço livre em disco
- Sistema Operacional MacOS ou Linux (*host* ou máquina virtual) com Python3
- Ter ou criar uma conta na AWS específica para o treinamento

MATERIAL RECEBIDO

- Acesso ao portal do aluno, o GoHacking Academy
- Acesso às ferramentas priv8
- Apostila do Curso no formato PDF
- Certificado de Conclusão do Curso no formato PDF (com a carga horária e ementa)

CAPACIDADES ALCANÇADAS

No final do curso, espera-se que o aluno estará apto a:

- Compreender os Fundamentos da Segurança na Nuvem: Entender os conceitos básicos e os novos paradigmas da segurança em ambientes de nuvem, focando especialmente na infraestrutura da AWS.
- Desenvolver Habilidades de Inteligência de Fonte Aberta (OSINT): Aprender a utilizar técnicas de OSINT para identificar e acessar recursos expostos na AWS, promovendo uma abordagem proativa à segurança.
- Entender e Aplicar Técnicas de Escalação de Privilégios: Ganhar proficiência no entendimento e aplicação de técnicas para escalar privilégios em ambientes AWS, incluindo o uso eficaz do IAM e técnicas para roubar segredos.
- Aprimorar Habilidades de Movimentação Lateral: Desenvolver habilidades para realizar movimentações laterais seguras e eficazes em ambientes AWS, compreendendo profundamente os planos de dados e controle.
- Compreender e Evadir Controles de Segurança AWS: Aprender técnicas avançadas para evitar controles de segurança estabelecidos na AWS, incluindo a evasão de ferramentas como CloudTrail e GuardDuty.
- Desenvolver Técnicas de Persistência: Adquirir habilidades para criar backdoors em contas de usuários e serviços AWS, permitindo operações de persistência em ambientes de nuvem.
- Dominar Técnicas de Exfiltração de Dados: Aprender a executar técnicas avançadas de exfiltração de dados, focando na transferência segura e eficaz de dados entre contas AWS e fora delas.