ETHICAL HACKING ACTIVE DIRECTORY OPERATIONS – EHADOP

DESCRIÇÃO

(Nível Intermediário)

Carga Horária: 40hrs

O curso Ethical Hacking Active Directory Operations (EHADOP) apresenta técnicas de enumeração, análise e exploração de ambientes Windows Domain e Active Directory (AD), abordando as táticas e procedimentos utilizados por adversários em ataques a redes corporativas.

Grande parte das empresas implementam ambientes de AD como modelo principal de gestão, controle e organização de ativos e usuários. Com o crescimento do trabalho em modalidade remota e com a modernização dos sistemas empresariais, cresce a superfície de ataque e a quantidade de vulnerabilidades que podem ser exploradas por adversários com fins maliciosos como: vazamentos de dados, campanhas de *ransomware*, entre outros, que podem causar grande impacto às organizações.

O curso traz a forma de pensar ofensiva, ou seja, na perspectiva de um adversário, para que os profissionais empregados em uma equipe de Red Team, ou até mesmo Blue Team, possam ter uma visão geral do leque de possibilidades e falhas que podem ser exploradas em ambientes empresariais complexos.

Todos os módulos abrangem, primeiramente, uma leve carga teórica conceitual para que os alunos possam entender os fundamentos que são empregados nos ataques. Após entender os conceitos, serão trabalhados exercícios e laboratórios onde os alunos terão a oportunidade de executar os ataques e compreender seus impactos.

Adicionalmente, serão apresentados aspectos e detalhes frutos de experiência em ambientes reais, onde houve sucessos e fracassos durante explorações, para que o aluno tenha uma ideia ampla das possibilidades e limitações das técnicas, táticas e procedimentos (TTPs), seja para simular ataques, seja para aprimorar os mecanismos de defesa e detecção.

Os assuntos seguirão uma ordem lógica das fases de exploração, contando com o uso de ferramentas atuais e que trazem resultados expressivos para atividades de Red Team, tratando alguns pontos como: conceitos de Active Directory, Powershell ofensivo, coleta de credenciais, escalação de privilégio, emprego do Mimikatz e Rubeus, uso do BloodHound, planejamento de *paths* de ataque, mapeamento e movimentação lateral, manipulação e persistência de tickets no domínio, entre outros.

MÓDULO 1: Conceitos de Active Directory

1. Conceitos básicos
   - Histórico
   - Visão Geral
2. Estrutura
   - Teoria de objetos
   - Características (SID, propriedades, correlações)
3. Forests
   - Visão Geral
   - Relação de confiança entre domínios e florestas
4. Protocolo Kerberos
   - Visão Geral
   - Processo de criação e implementação de Tickets

MÓDULO 2: Evasão Básica de Defesas

1. Powershell Operacional
   - Fundamentos, estrutura e principais comandos do PowerShell
   - Execução de scripts em PowerShell
   - Execução de scripts em memória (*fileless*)
   - Desenvolvimento e customização de ferramentas
2. AppLocker
   - Visão Geral
   - Enumeração e análise
   - Técnicas básicas de bypass
3. *Antimalware Scan Interface* – AMSI
   - Visão Geral
   - Técnicas básicas de bypass

MÓDULO 3: Escalação de Privilégio Local & Dump de Credenciais

1. Vulnerabilidades comuns em sistemas Windows
   - Enumeração manual e automatizada
   - Busca por arquivos com informações sensíveis
   - *Unquoted Path*
   - Exploração de serviços inseguros
   - Exploração de arquivos com permissões excessivas
   - Exploração de privilégios e permissões de usuários
   - Laboratório
2. Dump de Credenciais no processo LSASS
   - Visão Geral
   - Dump de credenciais usando Mimikatz
   - Dump de credenciais usando Rubeus

MÓDULO 4: Enumeração do Domínio

1. BloodHound
   - Instalação
   - Execução de collectors (SharpHound)
   - Análise de gráficos
   - Correlacionamento e descoberta de paths de exploração
   - Otimização de busca no Bloodhound
   - Laboratório
2. Emprego de ferramentas de enumeração
   - Utilização do utilitário ADModule para levantamento de informações
   - Utilização do utilitário Powerview para levantamento de informações
3. Hunting
   - Enumeração de Usuários
   - Enumeração de Grupos
   - Enumeração de ACE e ACLs
   - Enumeração de Trusts
   - Enumeração de Domínios e florestas
   - Enumeração de acessos
   - Laboratório

MÓDULO 5: Movimentação Lateral

1. Movimentação lateral com PSRemoting/Invoke-Command
   - Configurações
   - Parâmetros
   - PSRemoting via CrackMapExec (CME)
2. Movimentação lateral com PSExec
   - Configurações
   - Uso do PsExec da Microsoft Sysinternals
   - Uso do Impacket-PSExec
   - Laboratório
3. Técnicas de Pass-the-Hash / Over-Pass-The-Hash
   - Conceitos
   - Pass-the-Hash com Mimikatz
   - Pass-the-Hash com CrackMapExec (CME)
   - Laboratório
4. Kerberoasting
   - Conceitos
   - Aplicação com toolkits
   - Laboratório
5. MSSQL attack
   - Conceitos
   - Enumeração básica
   - Execução de queries e comandos
   - Habilitar execução de comandos com xp_cmdshell
   - Linked databases e stacked queries
   - Laboratório

MÓDULO 6: Domain Privilege Escalation

1. Delegation
   - Conceitos
   - Exploração de *Constrained Delegation*
   - Exploração *Unconstrained Delegation*
   - Exploração de *Resource Based Delegation*
2. Exploração de contas privilegiadas
   - DNSAdmins
   - Planejamento de attack path com Bloodhound
   - Red Team insights
   - Laboratório

MÓDULO 7: Técnicas de persistência no domínio

1. Persistência por Tickets forjados
   - Conceitos
   - Persistência com Silver Tickets
   - Persistência com Golden Tickets
2. Persistência por abuso de funcionalidades
   - Skeleton key
   - DCShadow

MÓDULO 8: Movimentação Lateral entre Domínios e Florestas

1. Movimentação lateral por Trusts
   - Conceitos
   - Parent-child Trust
   - Cross-Forest Trust
2. Movimentação lateral por abuso de permissões
   - Foreign members
   - Análise e determinação de *paths* de ataque
   - Red Team *insights*
   - Laboratório

PRÉ-REQUISITOS

- Conhecimentos básicos em Sistema Operacional Windows
  - Estrutura de diretórios, comandos básicos do prompt (cmd.exe e powershell), configuração de rede, verificação de serviços e processos, gerenciamento de usuários locais
- Conhecimentos básicos em Sistema Operacional Linux
  - Estrutura de diretórios, comandos básicos do shell (bash), configuração de rede, verificação de serviços e processos, gerenciamento de usuários locais, permissão de arquivos
- Conhecimentos básicos de Rede de Computadores e Serviços de Rede
  - Protocolo TCP/IP, FTP, HTTP, HTTPS, SMB, SSH, DNS, ICMP
- Conhecimentos básicos de Penetration Testing – Metodologia e Procedimentos
- Familiaridade com a distribuição Kali Linux
- Familiaridade com ferramentas de Pentesting – Metasploit, Meterpreter
- Familiaridade com ferramentas de Virtualização – VMWare

PÚBLICO ALVO

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

MATERIAL NECESSÁRIO

- Os alunos devem utilizar suas próprias estações de trabalho (Windows, Linux ou Mac OS), com a capacidade de executar de 02 a 03 Máquinas Virtuais (VM) simultaneamente.
- Configuração mínima de 8GB de RAM, 60 GB de espaço livre em disco, porta USB e placa de rede (RJ45 ou *wireless*) para acesso à Internet.
- Desejável 02 (dois) monitores para incremento na produtividade do curso.
- Software de Virtualização: VMWare, versão mais atualizada, de preferência *Workstation* (para hosts Windows ou Linux) ou *Fusion* (para host Mac OS). É possível utilizar a versão de avaliação (*trial*). O VMWare *Player* também é capaz de executar as VMs do curso (não possui a capacidade de realizar *snapshots*, importante mas não imprescindível para o curso).

MATERIAL RECEBIDO

- Acesso ao Portal do Aluno – GoHacking Academy, que concentra o material do curso
- Apostila do Curso no formato PDF
- Gravações das sessões ao vivo
- Certificado de Conclusão do Curso no formato PDF (com a carga horária e ementa)

CAPACIDADES ALCANÇADAS

No final do curso, o aluno estará apto a:

- Entender aspectos fundamentais da Segurança Ofensiva
- Entender a arquitetura e características principais existentes num ambiente de *Windows Domain* e *Active Directory* (AD)
- Entender a metodologia de um ataque cibernético em um ambiente de AD
- Mapear a estrutura de ambientes de AD e identificar fraquezas
- Escalar privilégios em ativos Windows
- Extrair credencias de acesso em memória
- Empregar o PowerShell para atividades de enumeração, evasão de defesas e ações ofensivas
- Empregar ferramentas nativas da Microsoft na enumeração do ambiente
- Utilizar de ferramentas atualizadas para executar atividades ofensivas e entender seu funcionamento para monitoramento e detecção
- Entender e realizar ataques ao protocolo de autenticação Kerberos
- Identificar falhas de configuração de ativos de um AD
- Planejar caminhos de ataque ou pontos críticos por meio da ferramenta BloodHound
- Planejar caminhos de ataque para se alcançar um objetivo dentro de uma rede corporativa
- Realizar atividades de movimento lateral e pivoteamento em uma infraestrutura de uma organização
- Realizar enumeração e exploração de servidores MSSQL para expansão no ambiente
- Extrair (exfiltrar) dados e informações de um sistema ou infraestrutura comprometida
- Realizar ataques a ambientes de AD
- Forjar tickets de persistência e acesso a recursos
- Estabelecer mecanismos de persistência em um ambiente de AD
- Detectar e responder a atividades ofensivas em um ambiente de AD

JORGE JARDIM