GOHACKING ACTIVE DIRECTORY DEFENSE (GHADD)

DESCRIÇÃO

(Nível Básico/Intermediário)

Carga Horária: 40 hrs

O ambiente Active Directory (AD) é uma plataforma de gestão de identidade e acesso fundamental para a infraestrutura de muitas empresas e organizações. Ele permite o controle centralizado do acesso aos recursos de rede, além de fornecer recursos de segurança, como autenticação e autorização, que ajudam a proteger as informações confidenciais e evitar ataques cibernéticos.

Ataques cibernéticos em ambientes corporativos possuem como um dos alvos principais a infraestrutura de AD da empresa, pois é onde estão armazenadas informações relevantes sobre os usuários e ativos da rede. Se esses dados forem comprometidos, os invasores podem acessar recursos confidenciais da organização e causar danos significativos. Adicionalmente, qualquer interrupção do AD pode resultar em problemas de acesso aos recursos da rede, afetando diretamente a produtividade dos funcionários e prejudicando a reputação da organização.

Em resumo, defender o ambiente de AD é crucial para garantir a segurança e a integridade das operações e do negócio de uma organização. É importante implementar medidas de segurança adequadas e manter o ambiente atualizado para se proteger contra diversos ataques cibernéticos e garantir que os recursos de rede estejam acessíveis apenas para usuários autorizados.

O curso GoHacking Active Directory Defense (GHADD) apresenta o ciclo de vida de ataques em AD e, a partir disso, trabalha as melhores práticas na detecção e mitigação das táticas, técnicas e procedimentos (TTPs) ofensivas utilizadas pelos atacantes. Além disso, demonstra, de uma forma prática, quais medidas devemos adotar para defender nossas organizações de ataques cada vez mais avançados.

O aluno terá a oportunidade de aprender a construir um ambiente de laboratório de AD desde a instalação do primeiro Controlador de Domínio (*Domain Controller*), até efetuar configurações que seguem as melhores práticas e conhecer as vulnerabilidades mais comuns e seus ataques relacionados, tendo sempre em mente a defesa frente a essas ameaças, cada vez mais efetivas e silenciosas.

MÓDULO 1 – Introdução ao AD DS (*Active Directory Domain Services*)

1. Introdução ao AD DS (Active Directory Domain Services)
2. Conceitos básicos (*Domain Controller, Primary Domain Controller, Domain, Roles*)
3. Domínios (*Domain*), Florestas (*Forest*) e Trusts
4. *Flexible Single Master Operation* (FSMO) *roles* 
5. Usuários, grupos e computadores 
   - *Group Managed Service Accounts*
6. *Group Policy Objects* (GPOs) 

MÓDULO 2 – Centralização de logs

1. Introdução
2. Implementação 
3. Referências

MÓDULO 3 – Ciclo de vida em ataques ao AD

1. Modelo Unified Killchain
2. Modelo AD Killchain (infosecn1nja)
3. Modelo AD Killchain (Altered Security)

MÓDULO 4 – Reconhecimento, enumeração e escalação local de privilégios

1. Reconhecimento e Enumeração do AD 
   - Ferramentas nativas, Microsoft Sysinternals, PowerSploit, BloodHound, PingCastle, PurpleKnight
2. Técnicas de escalação local de privilégios

MÓDULO 5 – Movimentação lateral

1. Introdução ao modelo em camadas (*tiering*)
2. Movimentação lateral via administrador local 
3. Microsoft LAPS (*Local Administrator Password Solution*) e o novo Windows LAPS 
4. Implementação de 2FA com *Lithnet Access Manager* (Community Version) 
5. Acesso JIT (*Just-In-Time*) e grupos temporários 
6. O desafio do administrador local para usuários 
7. Identificando Kerberoasting
8. Garantindo o uso de senhas seguras para contas 
   - No momento da criação/alteração da senha
   - Em contas com senha já setada
   - *Fine-Grained Password Policy* (FGPP)
9. Análise de ACLs
10. Credenciais em computadores
11. Grupo “Protected Users” 
12. Microsoft Windows Defender Credential Guard 
13. Implementação do modelo em camadas (*tiering*) 
14. Monitoramento de ações no AD
15. Falhas comuns em ambientes AD

MÓDULO 6 – Obtendo privilégios administrativos no domínio

1. AD CS e suas vulnerabilidades (*Active Directory Certificate Services*) 🧪
   - Técnicas de roubo de credenciais (THEFT)
   - Técnicas de persistência (PERSIST)
   - Técnicas de escalação de privilégios (ESC)
   - Técnicas de prevenção (PREVENT)
   - Técnicas de detecção (DETECT)
2. Delegações 🧪
3. Grupos privilegiados 🧪
4. Integração AD on-premises e Azure AD e seus principais riscos
5. PAW (*Privilege Access Workstation*)
6. Jump Server (Apache Guacamole) 🧪
7. PAM (*Privileged Access Management*)

MÓDULO 7 – Movimentação entre domínios, persistência e exfiltração

1. Domínios e florestas: limites de segurança
2. Escalação de privilégios entre domínios de uma mesma floresta 🧪
3. Técnicas de persistência e mecanismos de detecção 🧪
   - Credenciais
   - ACLs: DCSync clássico, DCSync via AD CS, AdminSDHolder
   - Tickets Kerberos: Golden, Silver e Diamond
   - Certificados (AD CS)
   - SIDHistory
   - GPOs
   - Skeleton Key
   - Custom SSP
   - Golden gMSA

MÓDULO 8 – Resumo final

1. Resumo final dos processos e controles sugeridos para proteção do AD
2. Fontes relevantes

PRÉ-REQUISITOS

- Conhecimentos básicos em Sistema Operacional Windows
  - Estrutura de diretórios, comandos básicos do prompt (cmd.exe), configuração de rede, verificação de serviços e processos, gerenciamento de usuários locais
- Conhecimentos básicos de Microsoft *Active Directory*
- Conhecimentos básicos de Rede de Computadores e Serviços de Rede
- Familiaridade com Powershell
- Familiaridade com ferramentas de Virtualização – VMWare

PÚBLICO ALVO

- Especialistas em Segurança da Informação
- Analista de Segurança da Informação
- Membros de CSIRT
- Analista de SOC
- Membros de Red Team / Blue Team
- Pentesters
- 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 3 a 4 Máquinas Virtuais (VM) simultaneamente.
- Desejável 02 (dois) monitores para incremento na produtividade do curso
- Configuração mínima de 16GB de RAM, 80 GB de espaço livre em disco, porta USB e placa de rede (RJ45 ou *wireless*) para acesso à Internet.
- 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 o funcionamento de uma rede corporativa baseada no serviço de diretório Microsoft Active Directory (AD)
- Realizar as configurações básicas de um domínio em uma infraestrutura de AD
- Analisar e implementar os mecanismos de gerenciamento de segurança do AD
- Gerenciar os registros e logs de um ambiente de AD
- Compreender as principais técnicas e vetores de ataque ao AD em ambiente corporativo
- Implementar as principais medidas de proteção em um ambiente de AD
- Configurar mecanismos de detecção e defesa dos principais ataques a infraestrutura de AD
- Entender as diferenças, vantagens e desvantagens entre ambientes de AD *on-premise* e de nuvem/*cloud* (Azure)
- Avaliar um ambiente de AD, detectar suas principais vulnerabilidades e implementar as adequadas correções

ANDRÉ TORRES BREVES GONÇALVES