GOHACKING ACTIVE DIRECTORY DEFENSE FUNDAMENTALS (GHADD Fundamentals)

DESCRIÇÃO

(Nível Básico)

Carga Horária: 8 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 Fundamentals (GHADD Fundamentals) demonstra a construção de um ambiente corporativo simulado, a criação de políticas de segurança e apresenta técnicas básicas utilizadas por atacantes, bem como conceitos fundamentais na defesa do ambiente do AD.

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*) e efetuar configurações básicas que seguem as melhores práticas, tendo sempre em mente a defesa frente a essas ameaças, cada vez mais efetivas e silenciosas.

EMENTA DO CURSO

1. Apresentação inicial
2. Preparação do ambiente utilizando VMWare Workstation
    2.1. Fazendo download do VMWare Workstation
    2.2. Baixando as ISOs oficiais da Microsoft
    2.3. Alterando as configurações de rede do VMWare Workstation
    2.4. Criação do template Windows Server 2022
    2.5. Criação do template Windows 10
3. Conceitos básicos sobre *Active Directory* (AD)
    3.1. Parte 1 - Introdução
    3.2. Parte 2 - Componentes
        3.2.1. Criação e configuração do CORP-DC
        3.2.2. Criação e configuração do SRV-01 e SRV-02
        3.2.3. Criação e configuração do WKS-01 e WKS-02
        3.2.4. Estrutura básica de organização do domínio
4. Domínios, florestas e *trusts*
5. *Flexible Single Master Operations* (FSMO) *roles*
6. Usuários, grupos e computadores
7. *Group Policy Objects* (GPO)
    7.1. Introdução às GPOs
    7.2. GPOs - Configurando os arquivos de definição de Administrative Templates centralizados
    7.3. Implantando GPOs - proibição do Prompt de Comando
    7.4. Implantando GPOs - configuração de acesso aos servidores Tier 1
    7.5. Implantando GPOs - configuração de acesso aos servidores Tier 0
    7.6. Implantando GPOs - configuração de acesso as estações Tier 2
    7.7. Implantando GPOs - testando o resultado final da organização do domínio
8. *Domain Name System* (DNS)
    8.1. Visão geral do DNS integrado ao AD
9. Contas de serviço
10. *Fine-Grained Password Policy* (FGPP)
11. *Local Administrator Password Solution* (LAPS) e Movimentação lateral
12. Modelo em Camadas (*Tiering Model*)
13. Análise de *Access Control Lists* (ACLs) usando BloodHound
14. Análise de vulnerabilidades usando o PingCastle
15. Considerações finais

PRÉ-REQUISITOS

- Conhecimentos básicos do Sistema Operacional Windows.
- Familiaridade com ferramentas de Virtualização – VMWare.

PÚBLICO-ALVO

- Profissionais de TI
- Administradores de Redes de Computadores
- Analistas de Segurança da Informação
- Membros de SOC
- Membros de CSIRT
- Membros de Blue Team / Red Team
- 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 Pro* (para hosts Windows ou Linux) ou *Fusion Pro* (para host Mac OS). Depois da compra da VMWare pela Broadcom, os referidos *softwares* se tornaram gratuitos.
- https://softwareupdate.vmware.com/cds/vmw-desktop/

MATERIAL RECEBIDO

- Acesso ao Portal do Aluno – GoHacking Academy, que concentra o material do curso.
- Apostila do curso no formato PDF.
- Acesso às aulas gravadas.
- 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 básico de uma rede corporativa baseada no serviço de diretório Microsoft Active Directory (AD).
- Identificar e entender os principais componentes de um AD.
- Realizar as configurações básicas de um domínio em uma infraestrutura de AD.
- Entender os conceitos de domínio e floresta.
- Compreender e configurar *Group Policy Objects* (GPO).
- Entender a função de DNS em uma infra de AD.
- Configurar *Local Administrator Password Solution* (LAPS).
- Entender o Modelo em Camadas (*Tiering Model*).
- Entender o uso de *Access Control Lists* (ACLs).
- Realizar análise básica de vulnerabilidades em infra de AD.

ANDRÉ TORRES BREVES GONÇALVES