GOHACKING ACTIVE DIRECTORY CERTIFICATE SERVICES (GHADCS)

DESCRIÇÃO

(Nível Intermediário/Avançado)

Carga Horária: 28 hrs

Instrutor: André Torres

O Microsoft Active Directory Certificate Services (ADCS) é um serviço do Windows Server que funciona como uma Autoridade Certificadora (CA), permitindo que uma organização emita e gerencie certificados digitais dentro de sua rede. Esse serviço facilita a implementação e o gerenciamento de uma infraestrutura de chave pública (*Public Key Infraestructure* – PKI), que é fundamental para estabelecer a confiança em ambientes distribuídos e na Internet. O ADCS pode ser integrado ao Active Directory, o que simplifica o gerenciamento de certificados. Com esse recurso, uma organização pode:

- Emitir certificados digitais para autenticar usuários, dispositivos e serviços.
- Criar certificados para criptografar dados em trânsito e em repouso, protegendo a confidencialidade das informações.
- Verificar a integridade dos dados transmitidos, garantindo que não tenham sido alterados ou corrompidos.
- Implementar políticas de controle de acesso granular com base em certificados digitais.
- Proteger servidores e estabelecer comunicações seguras usando SSL/TLS.
- Facilitar a conformidade com regulamentos de segurança de dados.
- Realizar auditoria e rastreamento do uso de certificados digitais para fins de segurança e conformidade.

Em conjunto, esses elementos formam uma infraestrutura de segurança robusta que fornece autenticação, criptografia e integridade dos dados para proteger os ativos digitais e garantir a conformidade com os requisitos de segurança e regulamentações.

O curso **GoHacking Active Directory Certificate Services (GHADCS)** é um programa abrangente que explora as melhores práticas para implementação de uma PKI interna. Ao longo do treinamento, os alunos são guiados através das aplicações mais comuns dessa ferramenta vital dentro de uma organização.

Além de fornecer uma compreensão detalhada da PKI, o curso aborda técnicas avançadas de segurança cibernética, incluindo enumeração, escalonamento de privilégios, roubo de credenciais e estabelecimento de persistência. Estas são as mesmas técnicas empregadas por agentes de ameaça altamente sofisticados.

Por fim, o curso explora estratégias de prevenção e detecção que são essenciais para proteger as organizações contra ataques cibernéticos. Os alunos aprenderão a implantar medidas eficazes para mitigar riscos e garantir a segurança contínua dos sistemas de TI.

Com instrução especializada e exemplos práticos, o GHADCS capacita os alunos a entenderem e lidarem com os desafios de segurança cibernética mais complexos enfrentados pelas organizações modernas.

MÓDULO 1 – Introdução ao ADCS (*Active Directory Certificate Services*)

1. Conceitos
   - PKI, certificado digital, ADCS, hierarquias de CAs, enrollment, CRLs, certificate stores,
2. Implementação segura de PKI 2-Tier
   - Configuração da *Root CA* e *Subordinate CA*
3. Laboratórios e Exercícios

MÓDULO 2 – Exemplos de uso do ADCS

1. Certificados HTTPS
   - Configurando e implementando certificados HTTPS no ADCS
2. Criptografia de arquivos (EFS)
   - Configurando e implementando certificados para criptografia de arquivos no ADCS
3. Assinatura de arquivos (*Code Signing*)
   - Configurando e implementando certificados para assinatura de arquivos no ADCS
4. Autenticação utilizando token criptográfico USB, Smartcard e Security Keys
   - Configurando e implementando certificados para autenticação em um domínio (*Smartcard Logon*): token criptográfico USB, cartão inteligente e Security Keys (Yubikey e Lockeet)
5. Laboratórios e Exercícios

MÓDULO 3 – Técnicas de Ataque

1. Ferramentas de enumeração
   - Certify, Certipy, PSPKIAudit e Locksmith
2. Escalação de privilégios
   - Exploração de templates: ESC1, ESC2, ESC3, ESC9, ESC10
   - Exploração de configuração da CA: ESC6
   - Exploração de controles de acesso: ESC4, ESC5, ESC7
   - Exploração por NTLM Relay: ESC8, ESC11
   - Outros tipos de exploração: Certifried, BloodHound + Certipy
3. Roubo de credenciais
   - THEFT1, THEFT2, THEFT3, THEFT4, THEFT5
4. Persistência
   - Persistência em contas: PERSIST1, PERSIST2, PERSIST3
   - Persistência no domínio: DPERSIST1 (Golden Certificate), DPERSIST2 (Rogue CA), DPERSIST3
5. Laboratórios e Exercícios

MÓDULO 4 – Técnicas de defesa

1. Considerações gerais sobre segurança de PKI
2. Prevenção
   - PREVENT1 a PREVENT8.
3. Detecção
   - DETECT1 a DETECT7
4. Resposta a incidentes de segurança em PKI

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 os conceitos básicos relacionados a uma infraestrutura de chave pública (PKI)
- Entender os conceitos fundamentais do Active Directory Certificate Services (ADCS)
- Entender o funcionamento de uma PKI baseada no Microsoft ADCS
- Realizar a implementação segura de uma PKI em ADCS, baseado na arquitetura 2-Tier
- Entender a utilidade e exemplos de uso do ADCS em uma rede corporativa
- Analisar e entender a integração entre o ADCS e o AD
- Compreender as principais ameaças e vulnerabilidades do ADCS
- Entender as principais técnicas ofensivas utilizadas por atacantes no ADCS
- Realizar técnicas de enumeração no ADCS
- Realizar técnicas de escalação de privilégio no ADCS
- Realizar técnicas de roubo de credenciais no ADCS
- Realizar técnicas de persistência no ADCS
- Implementar as principais medidas de proteção e detecção em um ambiente de ADCS
- Avaliar um ambiente de ADCS, detectar suas principais vulnerabilidades e implementar as adequadas correções

INSTRUTOR: ANDRÉ TORRES