GUIA INTRODUTÓRIO DE CONSCIENTIZAÇÃO EM CIBERSEGURANÇA

Kerberoasting, AS-REP Roasting, Silver Ticket, Golden Ticket, Phishing, Ransomware e Prevenção

UNIESP Centro Universitário
Especialização em Ethical Hacking e Cybersecurity
Módulo : Hardening em Ambientes Windows

Aluno : Vianney R. F. da Costa
Professor : Jessé da Costa Cabral Neto

INTRODUÇÃO

- Os ataques cibernéticos estão cada vez mais sofisticados, explorando vulnerabilidades técnicas e falhas humanas. Conhecer as ameaças é essencial para proteger dados e a reputação da empresa.
- No cenário atual, ataques cibernéticos tornaram-se cada vez mais sofisticados, explorando vulnerabilidades técnicas e falhas humanas.
- O conhecimento sobre ameaças específicas é fundamental para proteger ativos digitais, dados sensíveis e a reputação de organizações.

Em um segundo foi detectado 4.698 ataques apenas no Brasil

Ataques Baseados em Autenticação do Active Directory

KERBEROASTING

- Técnica que captura tickets de serviço Kerberos (TGS) para quebrar senhas offline. Impacto: Comprometimento de contas de serviço e movimentação lateral.
- **Definição:** Técnica em que um invasor solicita tickets de serviço Kerberos (TGS) para contas de serviço no Active Directory. Esses tickets são criptografados com a senha da conta de serviço.
- **Objetivo:** Capturar o ticket, exportá-lo e tentar quebrar offline a senha usando força bruta ou dicionário.
- **Impacto:** Comprometimento de contas de serviço com privilégios elevados, permitindo movimentação lateral e acesso a dados críticos.
- **Exemplo real:** Ataques internos onde um colaborador mal-intencionado usa credenciais legítimas para extrair TGS e comprometer outros sistemas.

AS-REP ROASTING

- Explora contas sem pré-autenticação Kerberos para obter hashes de senha. Impacto: Rápida quebra de senhas fracas e elevação de privilégios.
- **Definição:** Exploração de contas no AD configuradas com "Não requer pré-autenticação Kerberos".
- **Objetivo:** Obter respostas AS-REP criptografadas diretamente com o hash da senha, facilitando ataques offline.
- **Impacto:** Rápida quebra de senhas fracas, levando ao acesso inicial ou elevação de privilégios.
- **Exemplo real:** Ambientes legados com más configurações de segurança, onde usuários antigos mantêm essa flag ativa.

SILVER TICKET

- Criação de tickets Kerberos falsificados para serviços específicos. Impacto: Acesso persistente e invisível a recursos sem passar pelo controlador de domínio.

- **Definição:** Criação de tickets Kerberos falsificados (TGS) para serviços específicos sem precisar do KDC.
- **Objetivo:** Usar a chave secreta do serviço comprometido para gerar tickets e acessar diretamente recursos.
- **Impacto:** O invasor pode permanecer invisível no ambiente, explorando serviços específicos como SQL Server ou SharePoint.
- **Exemplo real:** Atacante com hash NTLM da conta de serviço consegue acesso persistente sem passar pelo controlador de domínio.

GOLDEN TICKET

- Uso da chave KRBTGT para gerar TGTs falsos e obter acesso total ao domínio. Impacto: Controle completo e persistente da infraestrutura.

- **Definição:** Geração de um ticket Kerberos TGT falsificado usando a chave secreta da conta **KRBTGT** do AD.
- **Objetivo:** Obter acesso total e ilimitado a todos os serviços do domínio.
- **Impacto:** Controle completo e persistente da infraestrutura, podendo criar, modificar ou excluir qualquer conta e dado.
- **Exemplo real:** Uso em ataques avançados persistentes (APT), permitindo que grupos de cibercriminosos permaneçam por meses sem detecção.

PHISHING

- E-mails ou mensagens falsas induzem usuários a fornecer credenciais ou clicar em links maliciosos. Consequências: Roubo de senhas, malware, perda de dados.

- **Descrição:** E-mails ou mensagens falsas induzem usuários a fornecer credenciais ou clicar em links maliciosos.

- **Consequência:** Roubo de senhas, instalação de malware, perda de dados.

- **Exemplo:** Funcionário clica em link de e-mail que simula aviso bancário e instala keylogger.

RANSOMWARE

- Malware que criptografa arquivos e exige pagamento para liberação. Consequências: Interrupção de operações, perda de dados, custos de recuperação.

- **Descrição:** Malware que criptografa arquivos e exige pagamento para liberação.

- **Consequência:** Interrupção total das operações, perda de dados e custos de recuperação.

- **Exemplo:** Empresa de logística tem servidores bloqueados, causando paralisação de entregas por dias.

CONSEQUÊNCIAS PARA EMPRESAS

- - Perdas financeiras diretas
- - Interrupção de serviços
- - Danos à reputação
- - Vazamento de dados

- Perda financeira direta (resgate, multas, processos).
- Interrupção de serviços e perda de produtividade.
- Danos à reputação e perda de confiança de clientes.
- Vazamento de dados estratégicos e informações pessoais.

ESTRATÉGIAS PREVENTIVAS

5.1 Treinamento de Funcionários

- Simulações periódicas de phishing.
- Capacitação sobre engenharia social e boas práticas.
- Política de senhas fortes e únicas.

5.2 Backups Regulares

- Backups offline e criptografados.
- Teste periódico da restauração.
- Política de retenção de longo prazo.

5.3 Atualizações e Patches

- Correção rápida de vulnerabilidades.
- Remoção de sistemas e protocolos legados.
- Uso de ferramentas de gerenciamento centralizado.

5.4 Políticas de senhas fortes

- Tamanho Mínimo e Complexidade. **Senhas** devem ter pelo menos 12 caracteres.
- Proibição de **Senhas** Reutilizadas. ...
- Troca Periódica Inteligente. ...
- Bloqueio Após Tentativas Inválidas. ...
- Uso Obrigatório de Autenticação Multifatorial (MFA) ...
- Treinamento e Cultura de Segurança.

CONCLUSÃO

- A segurança da informação é responsabilidade coletiva.
- A combinação de tecnologia, processos e pessoas bem treinadas reduz riscos e perdas.

Relevância no Contexto Atual

Vivemos numa era em que **dados são ativos estratégicos**. Ataques como Kerberoasting e Golden Ticket exploram vulnerabilidades em ambientes corporativos amplamente utilizados, enquanto phishing e ransomware atacam diretamente a superfície humana e operacional.
Com a transformação digital acelerada, proteger sistemas e treinar equipes deixou de ser opcional — é **sobrevivência corporativa**.

A segurança da informação é responsabilidade coletiva.

Combinar **tecnologia, processos e pessoas bem treinadas** é a chave para resistir a ameaças cada vez mais avançadas.
Empresas que investem em **prevenção e conscientização** reduzem drasticamente riscos e perdas.