Objetivos da Atividade:

1. Identificar o host vulnerável na rede.
2. Reconhecer e compreender os tipos de vulnerabilidades presentes.
3. Explorar métodos para invadir a máquina vulnerável.
4. Elaborar um relatório detalhado sobre as descobertas e processos utilizados.

Cronograma e Fases da Atividade:

Observação: Cada fase corresponde a uma semana de aula.

Fase 1: Introdução ao Teste de Penetração e Reconhecimento

- **Semana 1 (Início):** Apresentação dos conceitos fundamentais de teste de penetração, incluindo suas fases: planejamento, reconhecimento, varredura, exploração, manutenção de acesso e análise.
- **Semana 2:** Utilização de ferramentas de reconhecimento para coletar informações sobre a rede e identificar possíveis hosts ativos.

Fase 2: Varredura e Identificação de Vulnerabilidades – Iniciando (02/04/2025.1)

- **Semana 3:** Emprego de ferramentas como Nmap para realizar varreduras nos hosts identificados, determinando portas abertas e serviços em execução.
- **Semana 4:** Análise das informações coletadas para identificar possíveis vulnerabilidades nos serviços detectados.

Fase 3: Exploração de Vulnerabilidades

- **Semana 5:** Introdução ao Metasploit Framework e sua utilização para explorar vulnerabilidades conhecidas nos serviços identificados.
- **Semana 6:** Execução de exploits específicos para obter acesso não autorizado ao sistema alvo, documentando cada passo realizado.

Fase 4: Pós-Exploração e Manutenção de Acesso

- **Semana 7:** Após obter acesso, análise das possibilidades de escalonamento de privilégios e manutenção do acesso ao sistema comprometido.
- **Semana 8:** Discussão sobre as implicações éticas e legais da manutenção de acesso e técnicas para cobrir rastros.

Fase 5: Elaboração e Apresentação do Relatório Final

- **Semana 9:** Compilação de todas as informações coletadas, técnicas utilizadas, vulnerabilidades exploradas e recomendações de mitigação em um relatório estruturado.

- **Semana 10 (Finalização em 10 de junho):** Apresentação dos relatórios pelos grupos, seguida de discussão e feedback coletivo sobre os achados e processos empregados.

Observações Importantes:

- O ambiente vulnerável será fornecido pelo professor, não sendo necessário que os alunos configurem a máquina vítima.
- Os alunos são encorajados a explorar ao máximo as possibilidades durante as atividades, utilizando diversas ferramentas e técnicas de teste de penetração.
- É fundamental que os alunos sigam práticas éticas e legais durante todo o processo, respeitando as diretrizes estabelecidas pelo professor e pela instituição.
- A atividade visa proporcionar uma experiência completa em um ambiente controlado, preparando os alunos para desafios reais na área de Segurança Cibernética.

1. Vulnerabilidades Conhecidas no Metasploitable 2

O Metasploitable 2 possui uma variedade de serviços e aplicações com vulnerabilidades conhecidas. Abaixo estão algumas das principais:

1. **Vsftpd v2.3.4 (FTP - Porta 21):**
    a. **Descrição:** Esta versão do vsftpd contém uma backdoor que permite a execução remota de comandos.
    b. **Exploração:** Utilizando o Metasploit, é possível explorar essa vulnerabilidade para obter acesso ao sistema.
    c. **Referência:** Exploit vsftpd 2.3.4 no Metasploit
2. **Apache Tomcat (HTTP - Porta 8180):**
    a. **Descrição:** Credenciais padrão são frequentemente não alteradas, permitindo acesso ao gerenciador do Tomcat.
    b. **Exploração:** Acesso ao gerenciador com credenciais padrão pode levar à implantação de war files maliciosos.
3. **Distccd (Porta 3632):**
    a. **Descrição:** Serviço de compilação distribuída vulnerável à execução remota de comandos.

    b. **Exploração:** Pode ser explorado para obter acesso shell ao sistema.
4. **Samba smbd v3.0.20 (Porta 139):**
    a. **Descrição:** Vulnerável à execução remota de código conhecida como "Username Map Script".
    b. **Exploração:** Permite execução de comandos arbitrários no sistema.
5. **MySQL (Porta 3306):**
    a. **Descrição:** Credenciais padrão permitem acesso ao banco de dados.
    b. **Exploração:** Acesso não autorizado ao banco pode levar à exposição de dados sensíveis.
6. **PostgreSQL (Porta 5432):**
    a. **Descrição:** Configuração padrão permite autenticação trust, possibilitando acesso sem senha.
    b. **Exploração:** Acesso não autorizado ao banco de dados.
7. **PHP-CGI (HTTP - Porta 80):**
    a. **Descrição:** Vulnerável a ataques que permitem a execução remota de código.
    b. **Exploração:** Pode ser explorado para obter acesso shell ao sistema.
8. **Webmin (Porta 10000):**
    a. **Descrição:** Versão desatualizada com vulnerabilidades conhecidas que permitem execução remota de comandos.
    b. **Exploração:** Acesso não autorizado ao painel de administração.
9. **VNC (Porta 5900):**
    a. **Descrição:** Senha fraca ou inexistente permite acesso remoto à interface gráfica.
    b. **Exploração:** Acesso completo ao ambiente de desktop do sistema.
10. **NFS (Porta 2049):**
    a. **Descrição:** Exportações NFS sem restrições permitem montagem remota de sistemas de arquivos.
    b. **Exploração:** Acesso não autorizado a arquivos e diretórios.

Para uma lista mais completa e detalhada das vulnerabilidades, consulte o Metasploitable 2 Exploitability Guide.

2. Possibilidades de Exploração

As vulnerabilidades acima permitem diversas formas de exploração, incluindo:

- **Execução Remota de Código (RCE):** Através de serviços como o vsftpd e o distccd, é possível executar comandos arbitrários remotamente.
- **Escalonamento de Privilégios:** Após obter acesso inicial, técnicas podem ser aplicadas para elevar privilégios e obter controle total do sistema.
- **Exfiltração de Dados:** Acesso não autorizado a bancos de dados MySQL e PostgreSQL pode levar à extração de informações sensíveis.
- **Acesso Persistente:** Configurações inadequadas em serviços como NFS e VNC permitem que atacantes mantenham acesso contínuo ao sistema.

3. Ferramentas Recomendadas para Testes de Penetração

Durante as diferentes fases de um teste de penetração, as seguintes ferramentas são amplamente utilizadas:

- **Nmap:** Utilizado para descoberta de hosts e varredura de portas, identificando serviços ativos e suas versões.
- **Metasploit Framework:** Plataforma que fornece exploits, payloads e auxilia na automação de ataques.
- **Armitage:** Interface gráfica para o Metasploit que facilita a gestão de exploits e sessões.
- **Wireshark:** Analisador de tráfego de rede que permite a inspeção de pacotes em tempo real.
- **Burp Suite:** Ferramenta para testes de segurança em aplicações web, incluindo interceptação de requisições e análise de vulnerabilidades.
- **Hydra:** Utilizada para ataques de força bruta em serviços como FTP, SSH, HTTP, entre outros.
- **Nikto:** Scanner de vulnerabilidades em servidores web, identificando configurações inadequadas e falhas conhecidas.