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.