Segue uma proposta de projeto em grupo para ser desenvolvido ao longo do semestre na disciplina de Segurança Cibernética, conforme o cronograma previamente estabelecido. O projeto iniciará no dia 12/03/2025 e envolverá etapas de planejamento, execução e apresentação final.

Tema do Projeto: Simulação de Cenários de Ataque e Defesa em Ambiente Controlado.

Objetivo Geral: Proporcionar aos alunos a experiência prática de planejar, executar e mitigar ataques cibernéticos em um ambiente controlado, utilizando ferramentas de código aberto disponíveis nas distribuições Debian e Kali Linux.

Cenários Envolvidos:

- **Atacante:** Equipe responsável por identificar e explorar vulnerabilidades em sistemas e redes simuladas.
- **Defesa:** Equipe encarregada de proteger os sistemas contra possíveis ataques, implementando medidas de segurança e monitoramento.
- **Cliente:** Representa a entidade que possui os sistemas e dados a serem protegidos, fornecendo requisitos e expectativas de segurança.

Ferramentas Sugeridas:

- **Pentest e Invasão:**
  - ✓ **Metasploit Framework:** Plataforma para desenvolvimento e execução de exploits contra máquinas remotas.
  - ✓ **Nmap:** Ferramenta para varredura de redes e descoberta de hosts e serviços.
  - ✓ **Aircrack-ng:** Conjunto de ferramentas para avaliar a segurança de redes sem fio.
- **Proteção:**
  - ✓ **Snort:** Sistema de detecção e prevenção de intrusões em rede.
  - ✓ **iptables:** Ferramenta de filtragem de pacotes e firewall para Linux.
  - ✓ **Fail2ban:** Programa que analisa logs e impede tentativas de intrusão bloqueando endereços IP suspeitos.
- **Documentação:**
  - ✓ **Dradis:** Plataforma de colaboração para relatórios de segurança.
  - ✓ **CherryTree:** Aplicativo de anotações hierárquicas para organização de informações.
  - ✓ **LaTeX:** Sistema de preparação de documentos para criação de relatórios técnicos e científicos.

Cronograma de Entregas:

1. **12/03/2025:** Formação das equipes e definição dos papéis (Atacante, Defesa, Cliente).
2. **19/03/2025:** Entrega do plano de projeto, incluindo objetivos específicos, metodologia e cronograma detalhado.
3. **26/03/2025:** Apresentação do ambiente de teste configurado e das ferramentas selecionadas.
4. **02/04/2025:** Entrega do relatório de análise de vulnerabilidades identificadas pela equipe Atacante.
5. **09/04/2025:** Entrega do plano de mitigação e defesa elaborado pela equipe Defesa.
6. **16/04/2025:** Execução dos testes de invasão e defesa no ambiente controlado.
7. **23/04/2025:** Entrega do relatório de incidentes e respostas aplicadas durante os testes.
8. **30/04/2025:** Revisão e aprimoramento das estratégias de ataque e defesa com base nos resultados obtidos.
9. **07/05/2025:** Simulação final integrando todos os componentes do projeto.
10. **14/05/2025:** Preparação da apresentação final e do relatório conclusivo.
11. **21/05/2025:** Apresentação dos resultados e discussão das lições aprendidas.

Desenvolvimento do Trabalho:

- **Preparação do Ambiente:** Cada equipe deverá configurar máquinas virtuais utilizando Debian ou Kali Linux, conforme seu papel no projeto. As configurações devem incluir a instalação das ferramentas selecionadas e a aplicação de configurações de rede que simulem um ambiente realista.
- **Execução das Atividades:**
  - ✓ **Equipe Atacante:** Realizará varreduras de rede, identificação de vulnerabilidades e tentativas de exploração utilizando as ferramentas de pentest.
  - ✓ **Equipe Defesa:** Implementará medidas de segurança, monitoramento contínuo e respostas a incidentes para proteger os sistemas simulados.
  - ✓ **Equipe Cliente:** Fornecerá requisitos de segurança, avaliará os relatórios de vulnerabilidades e validará as medidas de mitigação aplicadas.
- **Documentação:** Todas as etapas do projeto devem ser devidamente documentadas, incluindo planos, configurações, procedimentos executados, resultados obtidos e análises realizadas. As ferramentas de documentação sugeridas auxiliarão na organização e apresentação das informações.
- **Apresentação Final:** Cada equipe apresentará seus resultados, desafios enfrentados, soluções implementadas e lições aprendidas. A apresentação deve ser acompanhada de um relatório conclusivo detalhando todo o processo.