**Atividade em Sala: Exploração Prática de Testes de Intrusão com Nmap, Nikto e Wireshark**

**Objetivo da Atividade:** Proporcionar aos alunos uma experiência prática nos diferentes tipos de testes de intrusão — caixa branca, caixa preta e caixa cinza — utilizando as ferramentas Nmap, Nikto e Wireshark. A atividade visa aprofundar a compreensão dos alunos sobre as metodologias de teste de segurança e o uso eficaz dessas ferramentas em cenários reais.

**Descrição dos Tipos de Teste:**

- **Teste de Caixa Branca:** O testador possui total conhecimento da infraestrutura e do código-fonte do sistema alvo. Este tipo de teste permite uma análise detalhada da lógica interna e das possíveis vulnerabilidades do sistema.
- **Teste de Caixa Preta:** O testador não tem conhecimento prévio sobre a infraestrutura ou o código-fonte do sistema alvo. O foco está em avaliar a funcionalidade e identificar vulnerabilidades explorando o sistema como um usuário externo.
- **Teste de Caixa Cinza:** Combina elementos dos testes de caixa branca e preta, onde o testador tem conhecimento parcial da infraestrutura ou do código-fonte, permitindo uma avaliação equilibrada entre a perspectiva interna e externa do sistema.

**Ferramentas Utilizadas:**

- **Nmap:** Utilizado para varredura de redes, identificação de hosts ativos e serviços em execução, além de detecção de sistemas operacionais e possíveis vulnerabilidades.
- **Nikto:** Ferramenta de código aberto para análise de servidores web, capaz de identificar vulnerabilidades conhecidas, configurações inadequadas e outros problemas de segurança em aplicações web.
- **Wireshark:** Analisador de protocolos de rede que permite a captura e inspeção detalhada do tráfego de rede em tempo real, auxiliando na identificação de atividades suspeitas e na análise de comunicações entre sistemas.

**Desenvolvimento da Atividade:**

1. **Divisão em Grupos:** Os alunos serão organizados em grupos de três, com cada membro assumindo um dos seguintes papéis: testador de caixa branca, testador de caixa preta e testador de caixa cinza.
2. **Configuração do Ambiente:**
    a. Cada grupo configurará um ambiente de teste utilizando máquinas virtuais ou sistemas dedicados que simulem servidores e redes vulneráveis.

b. As ferramentas Nmap, Nikto e Wireshark deverão ser instaladas e configuradas adequadamente em cada estação de trabalho.

3. **Execução dos Testes:**
    a. **Caixa Branca:** O testador analisará o código-fonte e a configuração do sistema alvo para identificar vulnerabilidades internas, utilizando o Nmap para mapear a rede e identificar portas abertas, o Nikto para analisar possíveis falhas em servidores web e o Wireshark para monitorar o tráfego de rede em busca de comunicações inseguras.
    b. **Caixa Preta:** Sem informações prévias sobre o sistema, o testador realizará uma varredura externa utilizando o Nmap para descobrir hosts e serviços ativos, aplicará o Nikto para detectar vulnerabilidades em aplicações web e usará o Wireshark para capturar e analisar pacotes de dados que possam revelar informações sensíveis ou falhas de segurança.
    c. **Caixa Cinza:** Com conhecimento parcial do sistema, o testador combinará abordagens internas e externas, utilizando as três ferramentas para validar a segurança do sistema, identificar vulnerabilidades conhecidas e desconhecidas, e avaliar a eficácia das medidas de proteção implementadas.
4. **Documentação dos Resultados:**
    a. Cada grupo deverá registrar detalhadamente as metodologias aplicadas, os resultados obtidos, as vulnerabilidades identificadas e as recomendações para mitigação dos riscos encontrados.
    b. Os relatórios devem incluir capturas de tela, logs das ferramentas utilizadas e uma análise crítica das descobertas.
5. **Apresentação dos Resultados:**
    a. Os grupos apresentarão suas descobertas para a turma, discutindo as técnicas empregadas, os desafios enfrentados e as lições aprendidas durante a atividade.
    b. As apresentações servirão como base para uma discussão coletiva sobre as melhores práticas em testes de intrusão e o uso eficaz das ferramentas Nmap, Nikto e Wireshark.