Modelo de Plano de Invasão para Alunos de T.I. na Disciplina de Segurança Cibernética

Introdução

Este modelo de plano de invasão é destinado a estudantes de T.I. para fins educacionais, com o objetivo de entender as etapas de um teste de invasão (pentest) e aplicar práticas seguras e éticas. O plano segue padrões e normas de segurança da informação, como ISO/IEC 27001, OWASP, e NIST.

1. Objetivos do Plano de Invasão

- **Identificar Vulnerabilidades:** Descobrir fraquezas em sistemas, redes e aplicações.
- **Avaliar Impacto:** Avaliar as consequências potenciais de uma exploração bem-sucedida.
- **Recomendar Medidas de Mitigação:** Propor ações para corrigir as vulnerabilidades identificadas.
- **Promover a Conscientização:** Aumentar a conscientização sobre a importância da segurança cibernética.

2. Escopo do Teste de Invasão

- **Sistemas Incluídos:** Listar todos os sistemas, redes, aplicações e dispositivos que serão testados.
- **Limitações e Restrições:** Definir claramente o que não será testado para evitar interrupções ou danos não intencionais.
- **Metodologia:** Utilizar frameworks e metodologias reconhecidas, como OWASP Testing Guide e NIST SP 800-115.

3. Normas e Padrões

- **ISO/IEC 27001:** Prover diretrizes para o estabelecimento, implementação, manutenção e melhoria contínua de um Sistema de Gestão de Segurança da Informação (SGSI).
- **OWASP:** Seguir as diretrizes do Open Web Application Security Project para testes de segurança em aplicações web.
- **NIST SP 800-115:** Utilizar o guia técnico do National Institute of Standards and Technology para testes de segurança e avaliações técnicas.

4. Etapas do Plano de Invasão

4.1. Planejamento e Preparação

- **Definição de Objetivos:** Estabelecer metas específicas para o teste de invasão.
- **Autorização:** Obter permissão por escrito dos proprietários dos sistemas a serem testados.

- **Equipe:** Designar papéis e responsabilidades, incluindo um gerente de projeto e testadores.
- **Ferramentas:** Selecionar ferramentas apropriadas, como Nmap, Metasploit, Burp Suite, etc.

4.2. Coleta de Informações (Reconhecimento)

- **Reconhecimento Passivo:** Coleta de informações sem interagir diretamente com o alvo, como pesquisa de DNS, whois, e uso de motores de busca.
- **Reconhecimento Ativo:** Varreduras de rede e serviços para mapear a topologia e identificar alvos específicos.

4.3. Enumeração e Varredura

- **Varredura de Portas:** Identificação de portas abertas e serviços em execução usando ferramentas como Nmap.
- **Enumeração de Serviços:** Coleta de informações detalhadas sobre os serviços identificados, incluindo banners de versão, configuração, e vulnerabilidades conhecidas.

4.4. Exploração

- **Exploração de Vulnerabilidades:** Uso de exploits conhecidos para comprometer sistemas e serviços vulneráveis.
- **Engenharia Social:** Realização de ataques de engenharia social, como phishing, para obter credenciais ou acesso adicional.

4.5. Pós-Explotação

- **Escalação de Privilégios:** Tentar obter níveis mais altos de acesso no sistema comprometido.
- **Manutenção de Acesso:** Instalação de backdoors ou outros métodos para manter acesso persistente ao sistema.
- **Extração de Dados:** Coleta de informações sensíveis para avaliar o impacto potencial.

4.6. Relatório e Análise

- **Documentação:** Criar um relatório detalhado com todas as descobertas, incluindo vulnerabilidades identificadas, métodos de exploração, e impacto potencial.
- **Recomendações:** Propor medidas corretivas para mitigar as vulnerabilidades encontradas.
- **Revisão com Stakeholders:** Apresentar os resultados aos proprietários dos sistemas e discutir as recomendações.

5. Ferramentas Utilizadas

- **Nmap:** Para varredura de portas e mapeamento de rede.
- **Metasploit:** Para exploração de vulnerabilidades.
- **Burp Suite:** Para testes de segurança em aplicações web.
- **Wireshark:** Para análise de tráfego de rede.

6. Conclusão

O plano de invasão descrito aqui oferece uma estrutura clara e organizada para realizar testes de invasão em um ambiente controlado e educacional. Ao seguir este plano, os alunos podem aprender as técnicas e práticas de pentest, ao mesmo tempo em que respeitam as normas e padrões de segurança da informação.

Anexos

- **Formulário de Autorização:** Documento a ser assinado pelos proprietários dos sistemas autorizando o teste de invasão.
- **Lista de Verificação de Ferramentas:** Checklist das ferramentas a serem utilizadas.
- **Modelo de Relatório de Vulnerabilidade:** Template para documentação das descobertas.