PENETRATION TEST - PENTEST

Carga horária: 20 horas

Objetivos: Disponibilizar ao aluno o conhecimento da táticas de invasão e técnicas de defesa.

Descrição: Teste de Invasão(ou PenTest - Penetration Test) é o processo de busca e identificação de vulnerabilidades de segurança em uma rede, sistema ou ferramenta, bem como a extensão em que as mesmas podem ser exploradas por indivíduos maliciosos. Ideais para determinar a postura atual de segurança de empresas e identificar problemas potenciais em processos e ativos críticos de negócios, os Testes de Invasão funcionam como ataques reais, que se utilizam das últimas técnicas e ferramentas adotadas por invasores, incluindo Engenharia Social. As técnicas ensinadas durante o curso seguem padrões utilizados internacionalmente como ISSAF, NIST SP800.42, OSSTMM e OWASP.

Conteúdo:

1. Planejamento e preparação

1.1. Escopo do Teste
- 1.1.1. Objetivo/Propósito
- 1.1.2. Alvos
- 1.1.3. Profundidade
- 1.1.4. Exclusões

1.2. Perfil do atacante
- 1.2.1. Tipos de testes
- 1.2.2. Caixa preta, branca ou cinza?

1.3. Limitações de Tempo
- 1.3.1. Restrições de Horário
- 1.3.2. Duração do teste

1.4. Tratamento de questões especiais
- 1.4.1. Sistema alvo caiu
- 1.4.2. Dados sensíveis encontrados - Quem contactar?

1.5. Permissão
- 1.5.1. Por escrito
- 1.5.2. Assinada pelo responsável

1.6. Detalhes da Infraestrutura
1.7. Acordo de confidencialidade (NDA)
1.8. Equipamento e recursos necessários
1.9. Relatório de linha do tempo
1.10. Acesso a testes anteriores
1.11. Inspeção física

2. Obtenção de Informações

2.1. Whois
- 2.1.1. Buscas na Internet
- 2.1.2. Entradas DNS
- 2.1.3. Engenharia Social
- 2.1.4. Trashing (Dumpster Diving)
- 2.1.5. Cópia de Website

2.2. Sondagem e mapeamento
- 2.2.1. Busca por hosts vivos
- 2.2.2. Varredura por portas e serviços
- 2.2.3. Mapeamento de perímetro
- 2.2.4. Identificando serviços críticos
- 2.2.5. Fingerprinting de SO's e serviços
- 2.2.6. Identificando rotas

2.3. Identificação de Vulnerabilidades
- 2.3.1. Identificação de Serviços Vulneráveis
- 2.3.2. Varredura por vulnerabilidades
- 2.3.3. Senhas padrão
- 2.3.4. Correlacionamento de vulnerabilidades
- 2.3.5. Enumeração de vulnerabilidades encontradas

2.4. Classificação de vulnerabilidades (estimativa de impacto provável)
- 2.4.1. Identificação de circuitos de ataques e cenários para exploração

2.4.2. Caminho de menor resistência
2.4.3. Árvores de ataque

3. Invasão

3.1. Quebrando senhas
3.2. Ataques a aplicações Web
3.2.1. Injeção de SQL
3.2.2. Buffer Overflow
3.2.3. Cross-site Scripting (XSS)
3.2.4. Execução Remota de Código
3.2.5. Vulnerabilidades de Strings de Formatação
3.2.6. Autenticação e Autorização Fracas (enumeração,senhas,SIDs)
3.3. Ataques de negação de serviço
3.4. Testar em ambiente controlado
3.5. Usar contra o(s) alvo(s)
3.6. Confirmar/refutar vulnerabilidade em questão
3.7. Documentar resultados
3.8. Escalada de Privilégios
3.8.1. Repetir passos anteriores em ambiente local
3.9. Enumeração posterior
3.9.1. Quebra offline de senhas
3.9.2. Sniffing e análise de tráfego
3.9.3. Exploração de sessões e senhas através de cookies
3.9.4. Obtenção de endereços de email
3.9.5. Identificação de rotas e redes
3.9.6. Mapeamento de redes internas
3.9.7. Repetição das etapas anteriores a partir deste ponto
3.10. Mantendo Acesso