Segurança Informática

Aula 6

Programa

1. Conceitos introdutórios
2. Criptografia básica
3. Autenticação e Controlo de Acessos
4. Ameaças à segurança
5. Penetração em redes e sistemas
6. Políticas de segurança
7. Mecanismos de proteção e técnicas de defesa
8. Entidades de Segurança

5. Penetração em Redes e Sistemas (Parte 2)

Objetivos:

* Analisar criticamente os riscos de segurança associados à utilização de sistemas e redes.

* Reconhecer falhas e indicar técnicas de ataque à segurança informática.

Teste de Penetração/Intrusão

- O teste de intrusão (do inglês "Penetration Test" ou pentest"), também traduzido como "teste de penetração", é um método que avalia a segurança de um sistema ou de uma rede, simulando um ataque de uma fonte maliciosa.

- O processo envolve uma análise das atividades do sistema:
  - Que envolvem a procura de alguma vulnerabilidade em potencial
    - Que possa ser resultado de uma má configuração do sistema
    - Falhas em hardwares/softwares desconhecidas
    - Falhas no sistema operativo
    - Técnicas de defesa

Teste de Penetração/Intrusão

- Todas as análises submetidas pelos testes escolhidos são apresentadas no sistema:
  - Junto com uma **avaliação do seu impacto**
  - E muitas vezes com uma **proposta de resolução**
  - Ou de uma **solução técnica**

PCI Security Standards Council®

pcisecuritystandards.org

Teste de Penetração vs Exploração de Vulnerabilidades

- As diferenças entre testes de penetração e exploração de vulnerabilidades, (conforme exigido pelo PCI DSS) podem ser resumidas da seguinte forma:

	Exploração de Vulnerabilidades	Teste de Penetração
Finalidade	Identificar, classificar e relatar vulnerabilidades que, se exploradas, podem resultar em falha intencional ou não intencional de um sistema.	Identificar modos de explorar as vulnerabilidades a fim de enganar ou anular os recursos de segurança dos componentes do sistema.
Quando	Pelo menos trimestralmente, e após mudanças significativas.	Pelo menos uma vez por ano, e mediante mudanças significativas.
Como	Normalmente, uma variedade de ferramentas automatizadas combinadas com verificação manual dos problemas identificados.	Um processo manual que pode incluir o uso de exploração de vulnerabilidades ou outras ferramentas automatizadas, resultando em relatório abrangente.

Considerações / Defesa Básica de Ataques

- As passwords por defeito e frágeis.
- A monitorização eficaz dos sistemas.
- Quando as configurações de origem são um problema.
- Serviços e passwords ativos por defeito.
- A cultura do "facilitismo" tem um preço elevado.

Teste de Penetração – Ferramentas (Exemplos)

- SearchSploit - https://www.exploit-db.com/searchsploit/
  - Ferramenta de pesquisa de linha de comando para o Exploit-DB.
  - O SearchSploit oferece a capacidade de realizar pesquisas offline detalhadas em repositórios guardados localmente. Esse recurso é particularmente útil para avaliação de segurança da rede sem acesso à Internet.
  - Muitas vulnerabilidades têm links para ficheiros binários que não estão incluídos no repositório padrão, mas podem ser encontrados em binários Exploit-DB.
  - Vídeo Exemplo
    - https://www.youtube.com/watch?v=29GlfaH5qCM

Teste de Penetração – Ferramentas (Exemplos)

- Nikto - https://cirt.net/Nikto2
  - Scanner de servidor web de código aberto (GPL) que executa testes abrangentes em servidores da Web para vários itens, incluindo mais de 6700 ficheiros/programas potencialmente perigosos.
  - Nikto não foi desenvolvido como uma ferramenta furtiva. Testa um servidor da Web no menor tempo possível e é óbvio em ficheiros de log ou em um IPS / IDS.
  - Existem alguns itens que são verificações de tipo "apenas informações" que procuram itens que podem não ter uma falha de segurança, mas o webmaster ou o administrador de segurança pode não saber que estão presentes no servidor.
  - Vídeo Exemplo
    - https://www.youtube.com/watch?v=K78YOmbuT48

Teste de Penetração – Ferramentas (Exemplos)

- Google Dorks
  - O Google Hacking, também chamado de Google Dorking é uma técnica de hacking de computador que usa a Pesquisa do Google e outras aplicações da Google para encontrar falhas de segurança na configuração e no código do computador usado pelos sites.
  - Vídeo Exemplo
    - https://www.youtube.com/watch?v=u_gOnwWEXiA

Teste de Penetração – Ataques (Exemplos)

- SQL Injection
  - Técnica de injeção de código, usada para atacar aplicações controladas por dados, nas quais instruções SQL maliciosas são inseridas no campo de entrada para execução.
  - A injeção de SQL é conhecida principalmente como ataque para sites, mas pode ser usada para atacar qualquer tipo de base de dados SQL.
  - Este tipo de ataque permite falsificar a identidade, alterar dados existentes, causar problemas de repúdio, como anular transações, permitir a divulgação completa dos dados no sistema, destruir os dados ou torná-los indisponíveis.
  - Vídeo Exemplo
    - https://www.youtube.com/watch?v=WFFQw01EYHM

Teste de Penetração – Ataques (Exemplos)

- Remote Code Execution (RCE)
  - Um dos tipos mais perigosos de vulnerabilidades do computador. Permite que um atacante execute remotamente código malicioso dentro do sistema de destino, na rede local ou pela Internet.
  - O acesso físico ao dispositivo não é necessário.
  - Vídeo Exemplo
    - https://www.youtube.com/watch?v=9wbbKNURx54

Teste de Penetração – Ataques (Exemplos)

- Brute Force em páginas de login
  - Ataque destina a páginas web com login.
  - Obter acesso ilícito.
  - Intercetar a requisição de login e senha de acesso à página de login.
  - O acesso físico ao dispositivo não é necessário.

Teste de Penetração – Etapas

- Fase Pré-Ataque / Planeamento
  - Definir o modelo de intrusão (interno ou externo, direitos e privilégios)
  - Definição de metas, dados de origem, plano de trabalho e objetivos de teste
  - Determinar o ambiente alvo
  - Desenvolver a metodologia de teste
  - Definição da interação e procedimentos de comunicação
  - Teste de Penetração.

Teste de Penetração – Etapas

- Fase de Ataque / Teste
  - Trabalho de campo, identificação do serviço
  - As ferramentas personalizadas de intrusão são desenvolvidas se necessário
  - Deteção de vulnerabilidades, eliminação de falsos positivos
  - Utilização de sistemas comprometidos como meio para novas intrusões

Teste de Penetração – Etapas

- Fase Pós-ataque / Relatórios
  - Análise de resultados e relatórios com recomendações para redução de riscos
  - Demonstração visual dos danos que podem ser causados ao sistema por um ataque

QUESTÕES

?