Resumo 1º Prova - EH

Segurança da Informação

Disponibilidade, Integridade, Confidencialidade.

- Serviços de Segurança
  - **Autenticação** → garantia
  - **Autorização** → limita o acesso
  - **Confidencialidade** → guardar info
  - **Integridade** → info enviada = info recebida
  - **Irretratabilidade** → permite negar uma transmissão

Definições

Ethical Hacking → Protege, indentifica vulnerabilidades, fornece medidas preventivas, aumenta segurança

Ethical Hacker → executa invasões de maneira ética, pentester

Pentest → Penetration Test

Tipos de Hackers

White Hats → Ethical Hackers

Black Hats → Hackers mal intecionados

Gray Hats → Hacker que utiliza meios ilegais, mas para boa ação

Suicide Hackers → Hacker que não ligam para consequências

Script Kiddies → Hackers Iniciantes

Cyber Terrorist → São motivados por religião/política

APT → atacantes topzera, financiados pelo governo
Hacktivist → Hackers mal intecionados protestantes

Pentest (Penetration Test)

Tipos de Pentest

Black Box → pouca / nenhuma informação (Ameaça Externa)

Gray Box → endereços IP e links (Ameaça Interna / Clientes / Fornecedores)

White Box → maior número de informação (Simula empresa de Segurança / Consultoria)

Etapas do Pentest

Planejamento → expectativas e objetivos

Reconhecimento → coleta de informação, análise de tecnologias e vulnerabilidades

Ataque → Obtenção de acesso, navegação e instalação de ferramentas

Relatório → Vulnerabilidades conhecidas, classificações de riscos, orientações para correção

Metodologias

- **OSSTMM → Open Source Security Testin Methodology**
  - Desenvolvida pelo **ISECOM**.
  - Documento completo com dicas.
  - Abrange todas as áreas de segurança da informação.
  - Pode ser aplicada a **qualquer** tipo de organiza
  - Como testar a Segurança Operacional de Cinco Canais
    - Segurança Humana
    - Segurança Física

        - Comunicações sem Fio
        - Telecomunicações
        - Redes de Dados

- **OWASP → Open Web Application Security Project**
    - Desenvolvida por profissionais da área da tecnologia.
    - Sem fins lucrativos, prover melhorias no desenvolvimento de sistemas.
    - Produz e disponibiliza documentos, ferramentas e tecnologias no campo de segurança de aplicação WEB
    - OWASP Top 10
        - Relatório atualizado que descreve questões de segurança, foco nos 10 riscos mais críticos

        ▼ **Documento de Conscientização → Top 10 (2021)**

        - **A01** → Broken Access Control
        - **A02** → Cryptographic Failures
        - **A03** → Injection
        - **A04** → Insecure Design
        - **A05** → Security Misconfiguration
        - **A06** → Vulnerable and Outdated Components
        - **A07** → Identification and Authentication Failures
        - **A08** → Software and Data Integrity Failures
        - **A09** → Security Logging and Monitoring Failures
        - **A10** → Server-Side Request Forgery (SSRF)

- **NIST Cybersecurity Framework**
    - Desenvolvida pelo **Intituto Nacional de Padrões e Tecnologia**

    - Conjunto de diretrizes
    - 5 Funções:
        - **Identificar** → gerenciar risco de segurança cibernética
        - **Proteger** → desenvolver e implementar salvaguardas
        - **Detectar** → identificar ocorrência de um evento
        - **Responder** → tomar medidas em relação a um incidente
        - **Recuperar** → manter planos de resiliência e restaurar recursos/serviços

- **PTES → Penetration Testin Execution Standard**
    - Norma padrão para Pentests
    - Divide os testes em:
        - Predefinição
        - Coleta de Inteligência
        - Modelagem de Ameaças
        - Análise de Vulnerabilidade
        - Exploração
        - Publicar Exploração
        - Relatório

Vulnerabilidades

SQL Injection

- **Union-Based** → concatenar resultados de uma consulta original com resultados de um consulta maliciosa. Extrair nomes de tabelas, colunas, senhas, etc.

- **Boolean-Based** → tabela verdade, sentença verdadeira (‘ or V)

- **Time-Based** → identif. vulnerabilidade (1’ and sleep(5)) e aplicar os códigos.

— 1' AND IF(**substring(VERSION(),1,1)** = '5', SLEEP(10), 0)# —

- Comando que identifica a **versão** → alterar o número colorido para pegar a segunda, terceira, quarta letra…
- IF → comparar, depois da virgula colocar o que a função deverá fazer caso o IF retorne True

- **Error-Based** → mensagens de erro exibidas na tela.
  - **extractvalue(x, y)**: Extraí conteúdo XML, usando notação XPath. Quando essa função dá erro, ela exibe o que foi digitado na tela.
  - **x**: Origem de onde vamos extrair a informação
  - **y**: Aqui coloca o comando/consulta que será executada.

  - **concat(x, y)**: Faz a união de X e Y na mesma String
  - **0x0a**: Comando de nova linha

' and EXTRACTVALUE("teste",concat(0x0a,(select database()))); -- -

' and EXTRACTVALUE("teste",concat(0x0a,(select user()))); - -

' and EXTRACTVALUE("teste",concat(0x0a,(select table_name from information_schema.tables))); -- -

' and EXTRACTVALUE("teste",concat(0x0a,(select table_name from information_schema.tables limit 1))); -- -retorna uma row

' and EXTRACTVALUE("teste",concat(0x0a,(select table_name from information_schema.tables limit 1 offset X))); -- -começa a contar a partir do X registro

' and EXTRACTVALUE("teste",concat(0x0a,(select(table_name from information_schema.tables limit 1 offset 2))); -- -

XSS Injection

- **Reflected** → o código malicioso é refletido diretamente de uma entrada do usuário na resposta HTML do servidor.

- **Stored** → o código malicioso é armazenado no servidor e posteriormente exibido para a vítima quando ela acessa uma página específica ou visualiza conteúdo.
- **DOM-based** → o código malicioso é injetado e manipulado diretamente no Document Object Model (DOM) do lado do cliente (navegador).

- Com <SCRIPT>
  - Inclusão de códigos de JavaScript diretamente na página WEB, que serão executados na pagina de outros usuários.

- Sem <SCRIPT>
  - Utilização de alguns códigos HTML, como onload, onclick, onerror, onmouseover… Esses códigos executam os comandos de JavaScript correspondentes sem utilizar o uso da tag <script>

MITM - Man In The Middle

- É um tipo de ataque cibernético em que um terceiro mal-intencionado se insere na comunicação entre duas partes sem o conhecimento ou consentimento delas. O atacante age como um intermediário não autorizado, interceptando e possivelmente alterando as mensagens ou dados transmitidos entre as duas partes.
