Apontamentos Slides 02

- **Vulnerabilidade**
  - Erro no software que pode ser usado diretamente por um atacante para ganhar acesso ao sistema ou à rede
  - Um erro só é uma vulnerabilidade se permitir que o atacante viole uma política de segurança
- **Uma vulnerabilidade é um estado de um sistema que permite:**
  - Que um atacante **execute comandos em nome de terceiros**
  - Que um atacante **aceda a dados** ultrapassando as restrições de acesso
  - Que o atacante se **apresente como outrem**
  - Que o atacante **negue a prestação de serviços**

- **Exposição**
  - Problema de configuração de um sistema ou em erro no software que permitem aceder a informação ou capacidades que podem auxiliar um atacante
  - **Não permite diretamente** comprometer um sistema/rede
- **Uma exposição é um estado de um sistema que:**
  - Permite que um atacante realize **recolhas de informação**
  - Permite a um atacante **esconder as suas atividades**
  - Inclui uma funcionalidade que funciona como esperado mas que pode ser facilmente comprometida
  - É um ponto de entrada comum para atacantes **obterem acesso**
  - É considerado problemático por uma política de segurança razoável

---

- **CVE (Common Vulnerabilities and Exposures)**
  - Dicionário público de vulnerabilidades e exposições
    - Gestão de vulnerabilidades
    - Gestão de patches
    - Alarmística de vulnerabilidades
    - Deteção de intrusões
  - **Detalhes podem ser privados**
- **Benefícios dos CVEs**
  - Fornece uma linguagem comum para referir problemas
  - Facilita a partilha de dados entre:
    - Sistema de deteção de intrusões
    - Ferramentas de aferição

        - Bases de dados de vulnerabilidades
        - Investigadores
        - Equipas de resposta a incidentes
    - Permite melhroar as ferramentas de segurança
    - Fomenta inovação

- **Deteção de Vulnerabilidades**
    - Ferramentas podem detetar vulnerabilidades
        - Exploram vulnerabilidades **conhecidas**
        - Testam **padrões de vulnerabilidades**
    - Ferramentas podem replicar ataques conhecidos
    - Vitais para aferir a robustez das aplicações e sistemas em operação
    - Podem ser aplicadas a:
        - **Código desenvolvido** (análise estática)
        - **Aplicação a executar** (análise dinâmica)
        - **Externamente como um sistema remoto**
    - **Não devem ser aplicadas cegamente a sistemas em produção!!!!!**
        - Potencial perda/corrupção de dados
        - Potencial negação de serviço
        - Potencial ato ilegal

- **CWE (Common Weakness Enumeration)**
    - Linguagem comum para discutir, encontrar e lidar com as causa das vulnerabilidades de segurança
    - Os CWEs são catalogados segundo uma estrutura hierárquica

---

- **Gestão de Vulnerabilidades**
    - Durante o ciclo de desenvolvimento, como bugs podem ser geridos por equipa de segurança ou de desenvolvimento
    - Quando o software é público, vulnerabilidades são geridas globalmente
    - **Gestão pública permite um maior foco**
        - Discussão centrada numa aplicação específica
        - Admins podem rapidamente testar os seus sistemas, melhroando a segurança
        - … Atacantes ficam também a saber melhor como atacar sistemas
    - Vulnerabilidades também são geridas de forma privada
    - Conhecimento sobre exploits é comercializado
    - E trocados em forma privada a preços desconhecidos

- **Ataque de dia Zero**
  - Ataque que usa vulnerabilidades que são desconhecidas de terceiros e não comunicadas ao fornecedor de software
  - Ocorre no dia zero de conhecimento dessas vulnerabilidades, para as quais não existe correção
- **Um ataque de dia zero pode existir por meses/anos**
  - Conhecido para atacantes mas não para utilizadores
  - Parte frequente de arsenais de ataques informáticos
  - Comercializados em mercados específicos

- **CERT (Computer Emergency Readiness Team)**
  - Organização para garantir que as práticas de gestão de tecnologias e sistemas são usadas para resistir a ataques em sistemas distribuídos em rede
    - Limitar o dano, garantir a continuidade de serviços críticos
- **• CERT/CC (Coordination Center) @ CMU**
  - Um hub para questões de segurança na Internet

- **CSIRT (Computer Security Incident Response Team)**
  - Organização responsável por receber, rever e responder a relatórios de incidentes e atividade
    - Serviço 24/7 para usuários, companhia, agências governamentais e organizações
    - Ponto único de contato fiável e confiável para reportar incidentes de segurança à escala global
    - Meios para reportar incidentes e disseminar informação relativa a incidentes

---

- **Ataques comuns**
  - **Phishing**
    - Criam réplicas de páginas/serviços
    - Link enviado para vítimas através de email/SMS
      - Por vezes de computadores de colegas (maior probabilidade de confiança)
    - Objetivo:
      - Obter dados das vítimas
      - Obter dinheiro
      - Levar vítima a instalar malware
  - **Malware**

        - Infetam sistemas com código malicioso
        - Operação:
            - Vítima executa ficheiro infetado
            - Vírus propaga-se por outros sistemas
            - Malware pode tornar-se persistente
            - Malware pode manter-se adormecido
    - **Ransomware**
        - Têm com objetivo obter um pagamento por parte da vítima
            - Operação:
                - Executam código malicioso num computador
                - Código compromete CIA
                    - C: Envia informação para um servidor remoto
                    - I: Apaga/corrompe/cifra informação
                    - A: Cifra Informação
                - Atacante exige pagamento
                - Ou atacante utiliza diretamente informação
    - **Spyware**
        - Program que regista eventos num sistema
            - Teclas pressionadas Capturas de ecrã
            - Webcam
        - Dados são enviados para sistema atacante
        - Objetivo:
            - Extorsão
            - Uso de informações obtidas