Segurança

Os computadores podem fazer muito estrago em pouco tempo pois geram muita informação e processam/comunicam rapidamente. Existem cada vez mais prontos fracos devido aos sistemas serem cada vez mais complexos e porque o time-to-market é cada vez mais reduzido.

O facto de estar tudo interligado em rede, permite ataques “anônimos” a partir de qualquer lado, a propagação automática de ciber pragas e a existência e uso de máquinas hostis,.

Os utilizadores por norma não estão cientes dos problemas e soluções. Não se preocupam ou arriscam.

Pragmatismo da segurança

- Protecção a 100% é impossível
- A segurança é dispendiosa
    - Em material/pessoas
    - Dispor apenas do mínimo necessário

A proteção tem que ser suficiente boa para impedir ataques frequentes. Deve interferir menos com o trabalho diário do que os possíveis danos causados por atacantes e existir mecanismos de punição para os ataques. Não se deve dar a sensação que a impunidade é total.

Vulnerabilidade - Característica de um sistema que o torna sensível a ataques

Ataque - Conjunto de passos que levam execução de atividades ilícitas, normalmente explorando vulnerabilidades.

Risco/ameaça - Dano resultante de um ataque

Defesa - Conjunto de políticas e mecanismos de segurança que visam diminuir as vulnerabilidades de um sistema, detetar o mais rápido possível ataques passados ou atuais e diminuir os riscos de um sistema.

Principais fontes de vulnerabilidades

- Aplicações com bugs ou hostis
- Utilizadores desconhecedores/descuidados e hostis
- Má administração
    - Sistemas cada vez mais complexos

    - Configuração por omissão nem sempre as melhores
    - Medidas restritivas de bases vs flexibilidade de operação
- Comunicações sobre redes não controladas

Políticas de segurança

- Definem o poder/privilégio dos sujeitos
- Definem procedimentos de segurança
- Definem requisitos de segurança de um domínio
    - Níveis de segurança, autorização
- Estratégias de defesa e táticas de contra-ataque
- Definem o universo de atividades ilícitas ou licitas
    - Tudo o que não é negado, é permitido
    - Tudo o que não é permitido e negado

Mecanismos de segurança

- Implantam as políticas. As políticas definem o que é para ser feito e os mecanismos fazem-no
- Autenticação, filtragem, registo, auditoria, etc…

O nível de segurança oferecido por um computador depende das políticas de segurança e da correção e eficácia da sua especificação / implantação.

Políticas em sistemas distribuídos

- Precisa de abranger várias máquinas e redes
    - Domínios de segurança
        - Definição do conjunto de máquinas e redes do domínio
        - Definição do universo de utentes válidos
        - Definição do universo de atividades lícitas
    - Security gateways
        - Conjunto de interações permitidas com o exterior

Ataques específicos

- Feitos especificamente para uma máquina ou redes
- Feitos e conduzidos em tempo real por especialistas

Ataques automatizados

- Feitos para explorar vulnerabilidades bem conhecidas e comuns
- Pré-codificados e lançados sobre alvos aleatórios
- Tempo médio de sobrevivência
    - Tempo entre dois ataques automatizados consecutivos
    - Existem sensores de rede que permitem calcular esse tempo

Vulnerabilidades

A aplicação de medidas requer conhecimento sobre:

- Vulnerabilidades conhecidas
  - Problema, forma de exploração impacto, etc..
- Padrões dos ataques
  - Modus operandi
  - Assinaturas de ataques
- Padrões anormais de atividade
  - Difícil de definir em ambientes heterogéneos

As ameaças em redes de computadores são diferentes são diferentes de outros tipos de ameaças

- Os ataques podem ser lançados em qualquer hora, de qualquer local
- Podem ser facilmente coordenados
- São baratos
- Podem ser automatizados
- São rápidos
-

Isto faz com que necessitem de uma capacidade permanente (24x7) de reação a ataques

- Equipas de especialistas em segurança
- Alertas de ataque na hora
- Teste e avaliação dos níveis de segurança existentes
- Procedimentos de reação expeditos

Detecção de vulnerabilidades

Existem ferramentas específicas que podem detectar vulnerabilidades. Exploram vulnerabilidades conhecidas e testam padrões de vulnerabilidades - buffer overflow, SQLi, XSS, etc…

Este tipo de ferramentas é vital para aferir a robustez das aplicações e sistemas e operação. É um serviço frequentemente contratado.

Podem ser aplicadas a:

- Código desenvolvido (análise estática)
- Aplicação a executar (análise dinâmica)
- Externamente como um sistema remoto
-

Não devem ser aplicadas de forma cega a sistemas em produção.

- Potencial perda/corrupção de dados
- Potencial negação de serviço

CVE

Vulnerabilidade

É um 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. Exclui políticas de segurança abertas onde todos os utentes são de confiança ou onde não se considera a existência de riscos para o sistema.

Exposição

É um problema de configuração de um sistema ou erro no software que permite aceder a informação ou capacidades que podem auxiliar um atacante

O CVE considera um problema de configuração ou um erro como uma exposição se não permitir comprometer diretamente um sistema ou rede. No entanto pode ser uma componente importante para o sucesso de um ataque.

- Permite que um atacante realize recolhas de informação
- Que esconda as suas atividades
- Comporta-se como esperado mas pode facilmente ser comprometida
- Ponto de entrada frequente para atacantes que tentam obter acesso ao sistema ou a dados
- È considerado problemático por uma política de segurança razoável

O CVE fomenta a inovação. Não ajuda no entanto à defesa contra ataques do dia zero!

CVE tem um identificador único: CVE names, CVE numbers, CVE-IDs ou CVEs. Identificam vulnerabilidades conhecidas e públicas da CVE List.
O estado de um CVE pode ser “candidate” ou “entry”.
Candidate: sob revisão **para ser incluído na CVE List**
Entry: aceite na CVE List.

CVE-Ano-índice
Estado
Descrição da vulnerabilidade ou exposição
Referências para informação adicional