Princípios de segurança da informação

domingo, 25 de junho de 2023

10:22

* **Autenticidade** - é quando a informação é direta, sem clonagem - feita diretamente do remetente

Ex: Geronimo envia uma mensagem até Eunice - se foi geronimo realmente que enviou a mensagem então a mensagem é autentica

* **Confidencialidade** - Privacidade dos dados - uma pessoa envia uma mensagem a outra essa mensagem é privada, ou seja uma informação de uma empresa apenas uma empresa tem acesso - as informações são restritas apenas pessoas autorizadas tem acesso a essas informações.

* **Disponibilidade** - É o quão as informações estão disponíveis para quando necessárias ter acesso a elas, ou seja, quando um processo depende de uma informação porém perdemos o acesso a ela, isso será crítico, pois a empresa pode parar.

* **Integridade** - Garantir a informação integra até o destino, exemplo, uma mensagem enviada para outra pessoa, a integridade é garantir que a mensagem seja a mesma que foi enviada, sem alterações.

Análises de vulnerabilidade e tipos

domingo, 25 de junho de 2023

15:36

* As análises de vulnerabilidades são feitas para ser auditadas a corrigidas

**Tipos de análises Vulnerabilidade**

* **Black box** - Análise de quando não conhecemos nada da estrutura - descobrir vulnerabilidades em acessos, arquivos não permitidos, permissões

* **White box** - Análise quando temos um conhecimento da estrutura como OS, servidores, IP - Descobrir versão de software, sistema operacional

* **Gray Box** - Análise quando temos conhecimento parcial - uma mistura dos dois tanto mais vulnerabilidades mais profundas quando outras mais básicas

**Planejamento de análises de vulnerabilidade**

domingo, 25 de junho de 2023

15:52

* **Informações gerais** - Informações da empresa
* **Contrato de acordo** - Um contrato onde iremos informar a análise feita
  + **Objetivo do acordo**
  + **Limitações da análise** - O que vamos testar e como vamos testar
  + **Relatórios** - Com as vulnerabilidades

* **Fases da análise**

* **Reconhecimento ( Footprint )** - Conhecimento do ambiente, coletar informações
* **Varredura ( Scanning )** - Escanear vulnerabilidades pode ser feitas manualmente ou automaticamente com ferramentas
* **Exploração (Gaining Acess )** - Tentar ganhar acesso, explorando as vulnerabilidades
* **Escalação de privilégios ( Maintaining Acess )** - Quando conseguimos acesso ao sistema, conseguimos subir nosso nível de privilégios

**Para fazer essas análises existem alguns métodos usados**

OSSTMM

ISSAF

WASC-TC

OWASP