**SEGURANÇA AVANÇADA LINUX.**

Criptografia : Processo de converter um texto simples em um texto criptografado usando algoritmos matemáticos (hashing).

Hashing : Uma forma de criptografia. MD5, SHA2 e SHA3 são algoritmos de hash mais conhecidos.

* MD5 - Este é suficiente para garantir a integridades de downloads, embora não seja livre de colisão, o que significa que neste algoritmo não há garantias de que o mesmo hash não será usado para duas palavras totalmente diferentes.
* SHA2 e SHA3 - Este são livres de colisão, o que significa que para cada palavra haverá um hash diferente.

Para os tipos de situações abaixo são utilizados cifras criptográficas especiais, dentre os mais comuns desta cifras estão o DES(não considerado seguro mais), 3DES e RSA. E são usadas para criptografar :

* Arquivos individuais
* Partições ou volumes
* Conexões de página web
* Conexões de rede
* Backup
* Arquivos Zip

**Criptografia Simétrica** : Utiliza a mesma chave privada para criptografia e decriptografia

**Criptografia Assimétrica** : Utiliza uma chave pública e uma privada, onde a púbica deve ser compartilhada com quem deverá ter permissão de decriptografar.

**Assinatura eletrônica** : É um token, um método de garantir que a mensagem veio do remetente correto, ou seja, que não foi alterada no meio do caminho antes de chegar no destinatário.

**PAM (pluggable authentication modules)** : É um processo de autenticação de usuário e processos dentro do sistema linux. O processo de autenticação usando PAM é centralizado e com o gerenciamento mais fácil. Os módulos funcionam como pilhas, e cada programa que possui compatibilidade com o PAM vai ler o arquivo de configuração do PAM, logo esse arquivo apontará os módulos que ele deverá chamar, em seguida os módulos se formarão como pilhas, e as autenticações deverão ocorrer um a um até completar em todos os módulos, a partir daí o acesso é negado o concebido.

**SELINUX**

O SELINUX é uma política de controle de acesso baseada em papéis, a segurança tradicional do linux (DAC). O SELINUX (RBAC) é uma segurança adicional e não substitui a segurança básica do linux (DAC), O linux verifica o acesso via DAC, e caso haja autorização o SELINUX é lido para prover uma segurança adicional. Mas caso o DAC não autorize o sujeito o SELINUX no é lido.

getenforce = Avalia o estado do selinux

setenforce = 0 (permissive) 1(enforced)

**FERRAMENTAS DE SEGURANÇA**

**nmap**: Um utilitário para realizar scan nas portas dos servidores linux. Ele retorna o estado da porta, que podem ser :

* **open**: A porta está aberta
* **closed**: A porta está fechada
* **Filtered**: Não é possível determinar se a porta está aberta ou se um servidor linux está na varredura (este é o melhor estado para uma porta).
* **unfiltered**: A varredura vê a porta , mas não pode determinar se ela está aberta oou fechada.
* **open| filtered**: A varredura vê a porta, mas não pode determinar se ela está open ou filtered
* **closed| filtered**: A varredura vê a porta, mas não pode determinar se ela está close ou filtered

nmap 127.0.0.1 -sT //escaneia as portas que usam protocolo TCP

*PORT STATE SERVICE*

*631/tcp open ipp*

*Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds*