Autenticação no SSH com Chave Pública

+ É um processo longo, mas de bom uso quando temos acesso a um diretório com poucos comandos habilitados e queremos elevar nosso nível de acesso ao ssh

+ As configurações do ssh estão registradas em /etc/ssh/sshd_config

+ Para modificar as configurações, usamos o editor padrão do nano:

```
nano /etc/ssh/sshd_config
```

+ Para permitir a autenticação do root no sistema (o que n é recomendado)

```
PermitRootLogin yes
```

→ service ssh restart

+ Para n permitir a publickey autentication:

```
PublickeyAuthentication no
```

+ O ideal é remover a parte de autenticação por senhas e deixar apenas as chaves públicas registradas

+ Ao método

1. Dentro do diretório root, temos um diretório oculto chamado .ssh
2. ao acessá-lo com cd /root/.ssh/, veremos alguns arquivos importantes
- authorized_keys
- known_hosts
3. Para que o acesso funcione, precisamos gerar a chave pública no host 2 computador e então registrar nesse arquivo do authorized_keys
4. No host 2:

```
ssh-keygen
```

→ insiro o local onde salvar: /home/kali/idt_rs
→ passamos uma senha
→ São geradas então duas chaves: idt_rs e a idt_rs.pub (pub de public)
5. A chave pública é que vamos copiar e colar dentro do arquivo authorized_keys do host 1
6. Para cadastrar nossa chave privada (host 2), usaremos

```
ssh-add idt_rsa
```

→ Antes de fazer isso, é necessário iniciar o ssh-agent com o comando

```
eval 'ssh-agent -s'
```

→ colocamos a senha definida antes no passo 4
7. Para logar, só precisamos usar o

```
ssh -v <endereço de ip do host2>
```

AddKeysToAgent
CASO O ROOT ESTEJA DESABILITADO:
+ Criamos um usuario novo

```
add user Catulo
```

+ Criamos o diretorio .ssh

```
mkdir .ssh
```

+ Dentro do diretório .ssh, criamos o arquivo authorized_keys
+ E então fazemos todo o procedimento acima descrito