Enumerando SMTP

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
SMTP - Single Message Transfer Protocol - PORTA 25
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
+ Buscando os hosts com essa porta aberta:

```
nmap --open -sS -p 25 -Pn 172.30.0.1/24
```

+ Podemos fazer a resposta via nc:

```
nc -v 172.30.0.125 25
```

+ Comandos mais comuns são o HELO, EHLO, VFRY (para verificar usuario)
+ Forma de uso:
HELO desec
EHLO desec
VFRY root

+ Toda vez que temos uma tecnologia que responde a não autentificação de usuário, teremos uma vulneerabilidade pois estaremos diante de um padrão que pode ser identificado e usado para realizar a enumeração de usuários

+ Faremos a interação de modo a enviar um email, da seguinte forma: