

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 autenticação de usuário, teremos uma vulnerabilidade 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:

```
root@pentest:~/Desktop# nc -v 172.30.0.128 25
172.30.0.128: inverse host lookup failed: Unknown host
(UNKNOWN) [172.30.0.128] 25 (smtp) open
mail from: pentest
220 ubuntu.bloi.com.br ESMTP Postfix (Ubuntu)
250 2.1.0 Ok
rcpt to: root
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
Ola root
.
250 2.0.0 Ok: queued as 5277FC009B
mail from: pentest
250 2.1.0 Ok
rcpt to: ricardo
550 5.1.1 <ricardo>: Recipient address rejected: User unknown in local recipient table
```