Identificando Serviços

+ Agora que identificamos as portas abertas, podemos identificar
também os serviços que estão ativos

+ Quando fazemos um SYN Scan normal e são identificadas portas abertas,
o nmap responde quais eram os serviços baseado na lista de
porta-serviço padrão

```
nmap -v -sS -Pn 172.16.1.2
```

```
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
53/tcp  open  domain
80/tcp  open  http
111/tcp open  rpcbind
```

+ Para ter maior certeza dessas informações, é necessário que haja interação
com o serviço para que se possa capturar sua resposta.

```
nmap -v -sV -Pn 172.16.1.2
```

```
PORT    STATE SERVICE VERSION
21/tcp  open  ftp     ProFTPD 1.3.4a
22/tcp  open  ssh     OpenSSH 6.0p1 Debian 4+deb7u2 (protocol 2.0)
53/tcp  open  domain  ISC BIND 9.8.4-rpz2+rl005.12-P1
80/tcp  open  http    Apache httpd 2.2.22 ((Debian))
111/tcp open  rpcbind 2-4 (RPC #100000)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

+ Basicamente, ele envia requisição no mesmo padrão da requerida pelo serviço
Podemos fazer também manualmente.

+ Exemplo, pro http, ele envia uma requisição do tipo HEAD:
HEAD / HTTP/1.0
(enviando via nc)