Port and Router Vulnerabilities

Dr Rosanne English

Port Scanning

Port scanning - a process which checks a hosts ports to see which are open, and listens to data arriving and leaving a port

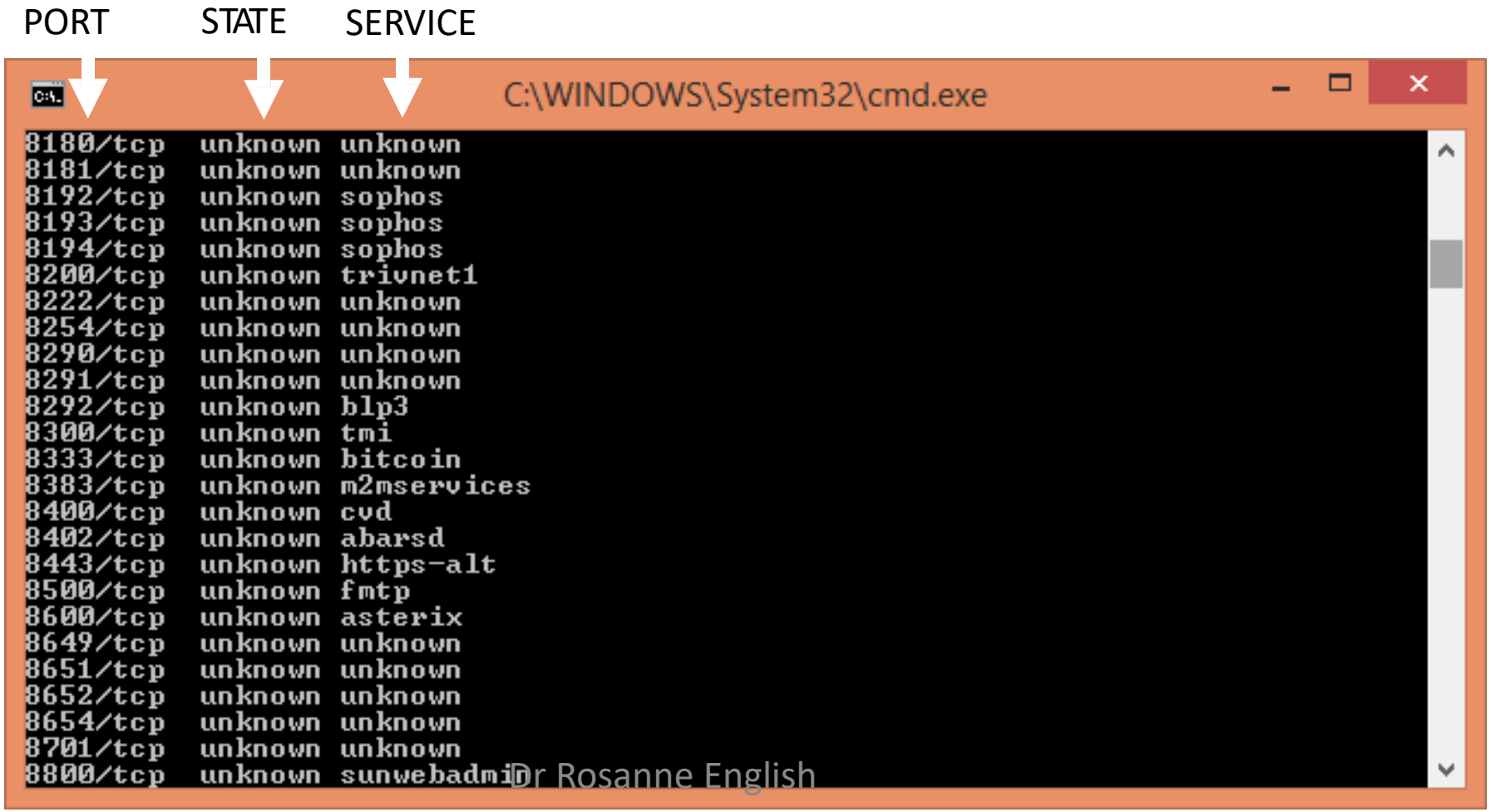
PORT 21: FTP

PORT 25: SMTP

PORT 80: HTTP

Nmap

```
nmap localhost
```



```
C:\Users\Rose>nmap localhost -sT
Starting Nmap 7.70 ( https://nmap.org ) at 2018-07-26 11:38 GMT Daylight Time
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 998 filtered ports
PORT    STATE SERVICE
135/tcp open  msrpc
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 51.03 seconds

C:\Users\Rose>
```

Port States

- Open
- Closed
- Filtered
- Unfiltered
- Open|Filtered
- Closed|Filtered

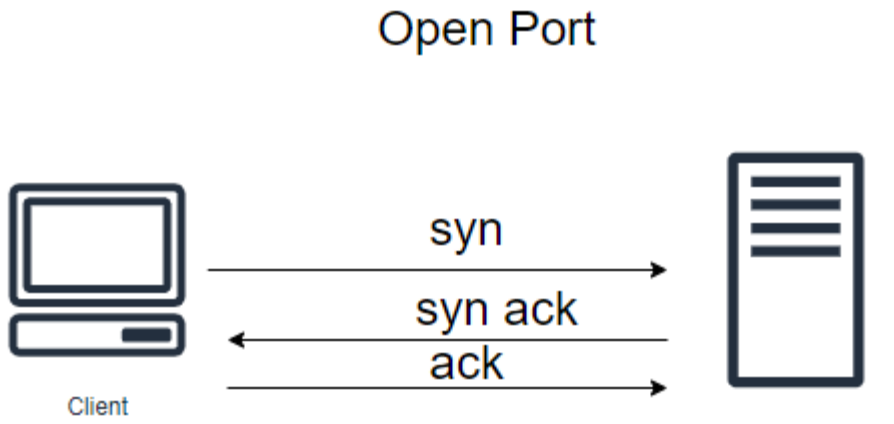
Basic Types of Scan

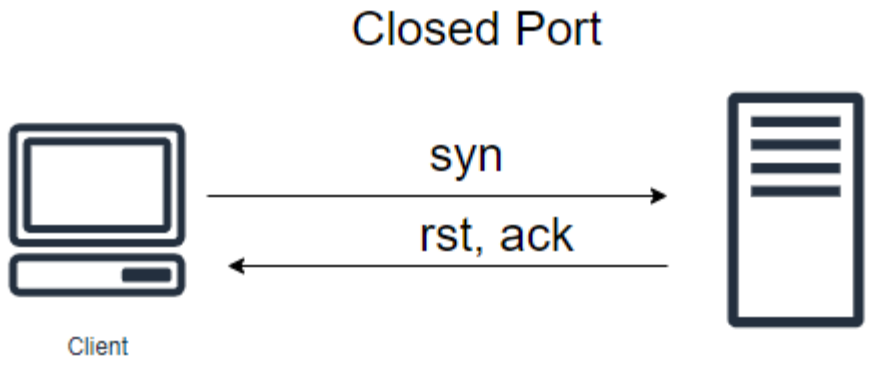
Vanilla:
Scanner attempts to connect to all I/O ports

Strobe:
A specialised scan looking for specific services

TCP Vanilla Scan

Vanilla TCP sends TCP SYN messages to multiple ports, normally in sequence

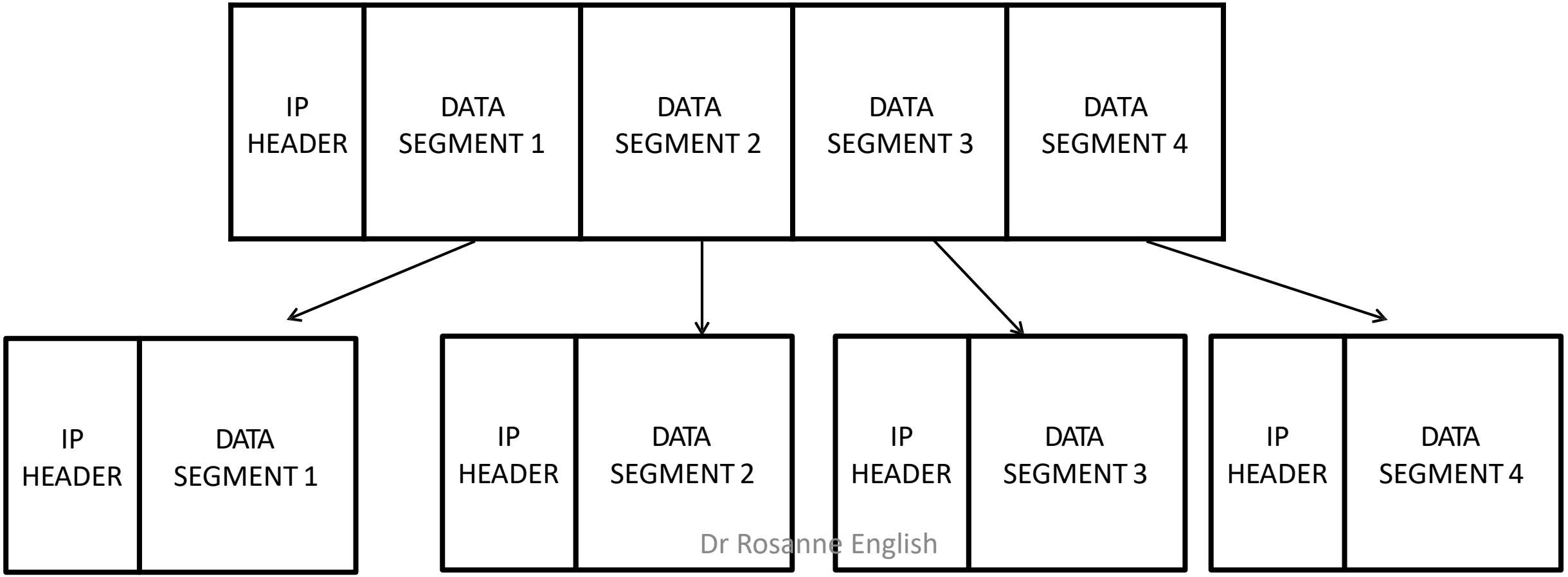




Stealth Scan

Fragments of packets are sent and can sometimes get through filters in the firewall

The diagram below shows how the IP header followed by the data segments can be split into multiple fragments by sending segments along with the IP header



Router

- Devices physically close to a router can potentially gain access to the network
- Wardriving