Port Scanning

Port Scanning

Purpose

Process

Tools

Purpose

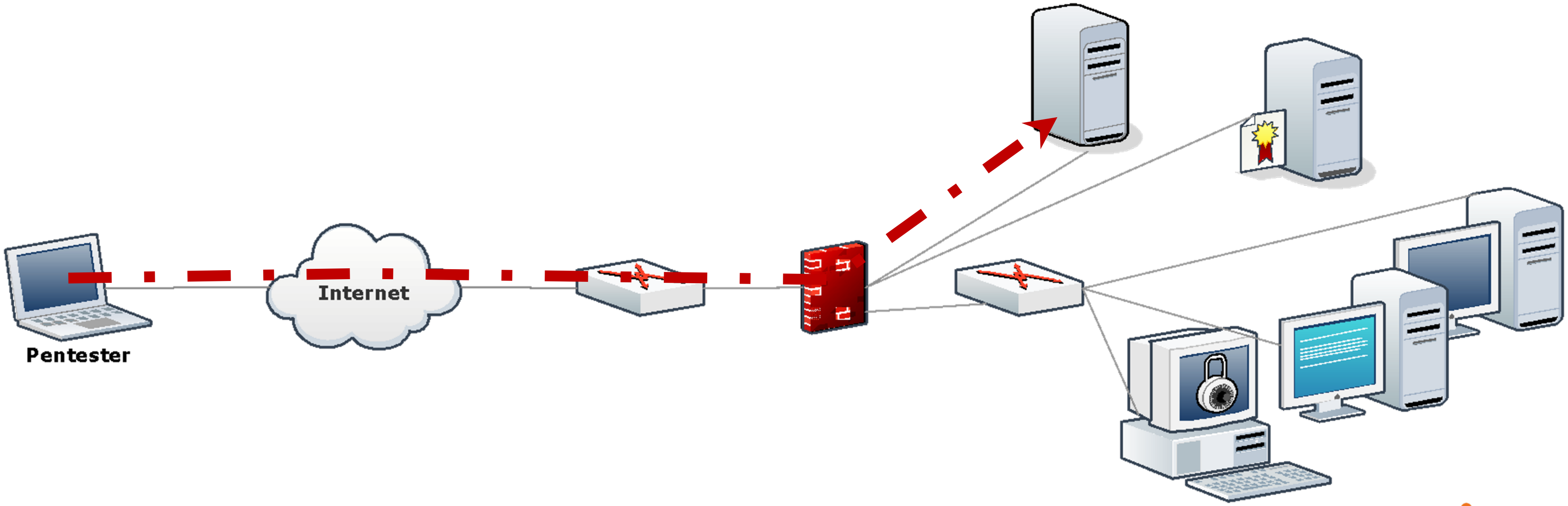
- Identify Operating System
- Identify Services

Identify Operating System

- Revealed by Signatures
- Revealed by Services

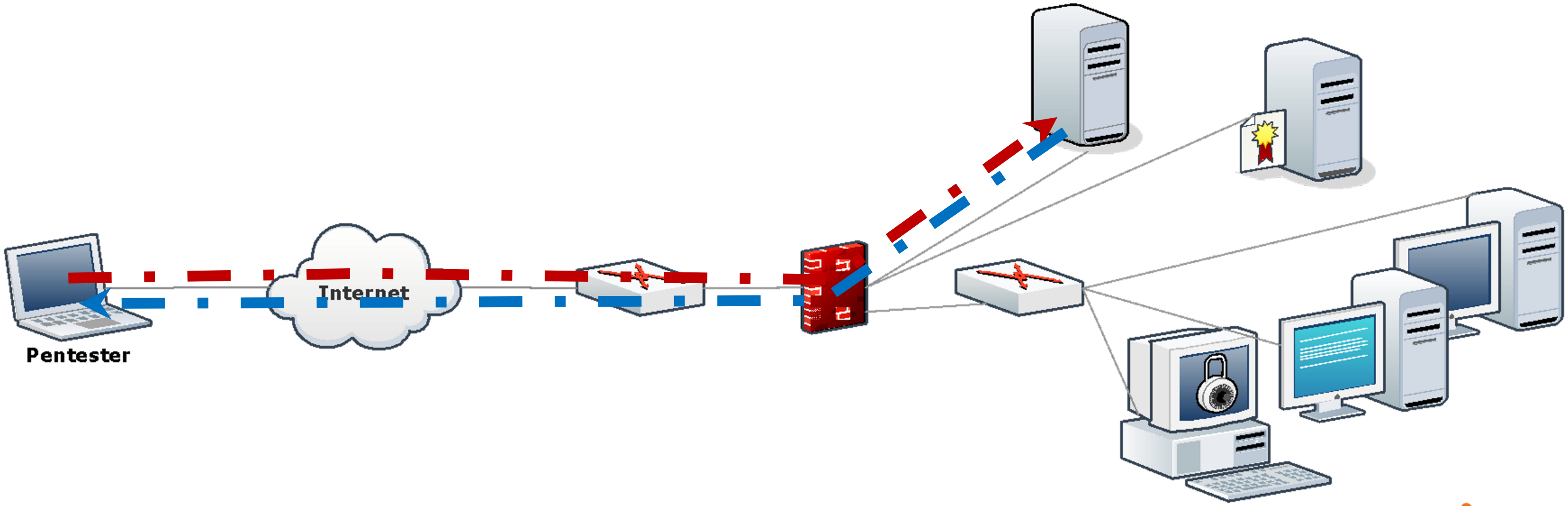
Identify Operating System

- Send **requests**



Identify Operating System

- Examine response
- Compare to **signature** database



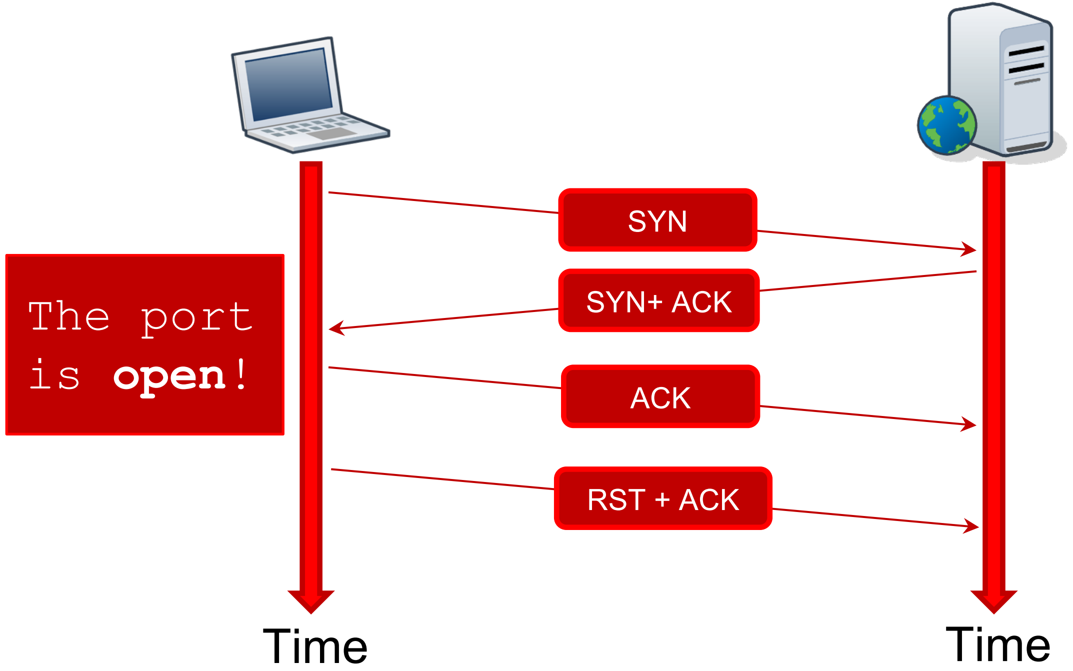
Identify Operating System

IP Address	OS	Confidence
200.200.3.1	PAN-OS	85%
200.200.3.10	Linux 3.7	100%
200.200.3.78	Linux 2.6.19 – 2.6.36	90%
200.200.4.12	Windows 7 SP1	100%
200.200.4.16	Windows 7 SP1	75%
200.200.4.18	FreeBSD	85%
200.200.4.19	HP-OS	78%

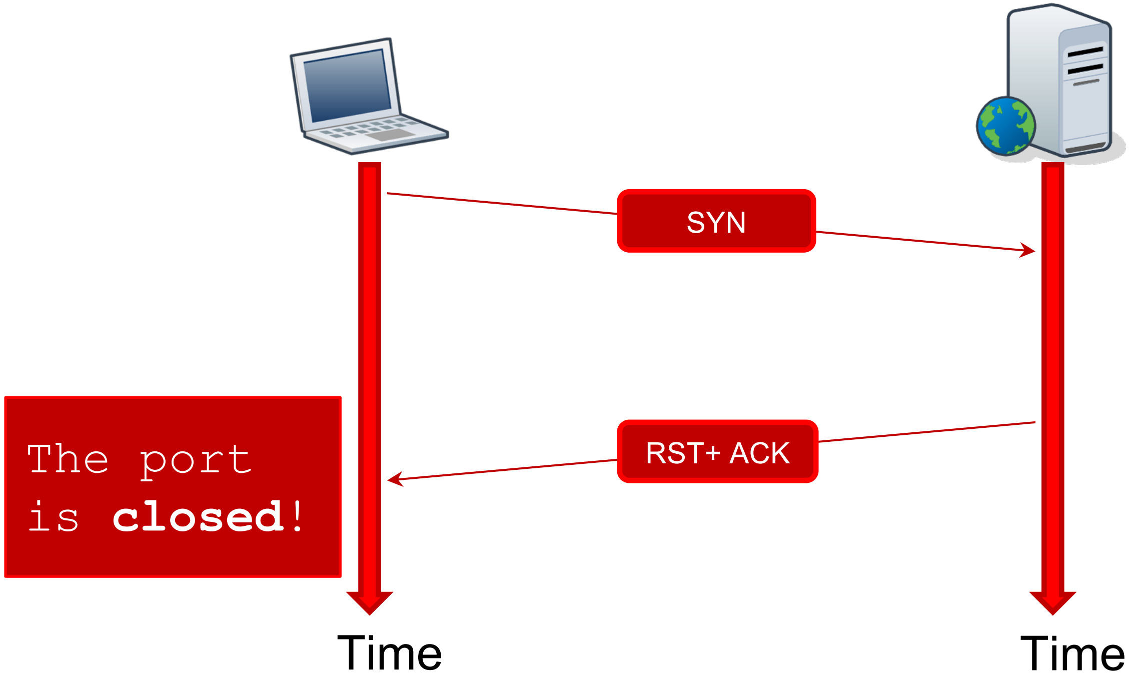
Scanning for Services

- Try to connect to ports
- Check for responses

Connect to TCP

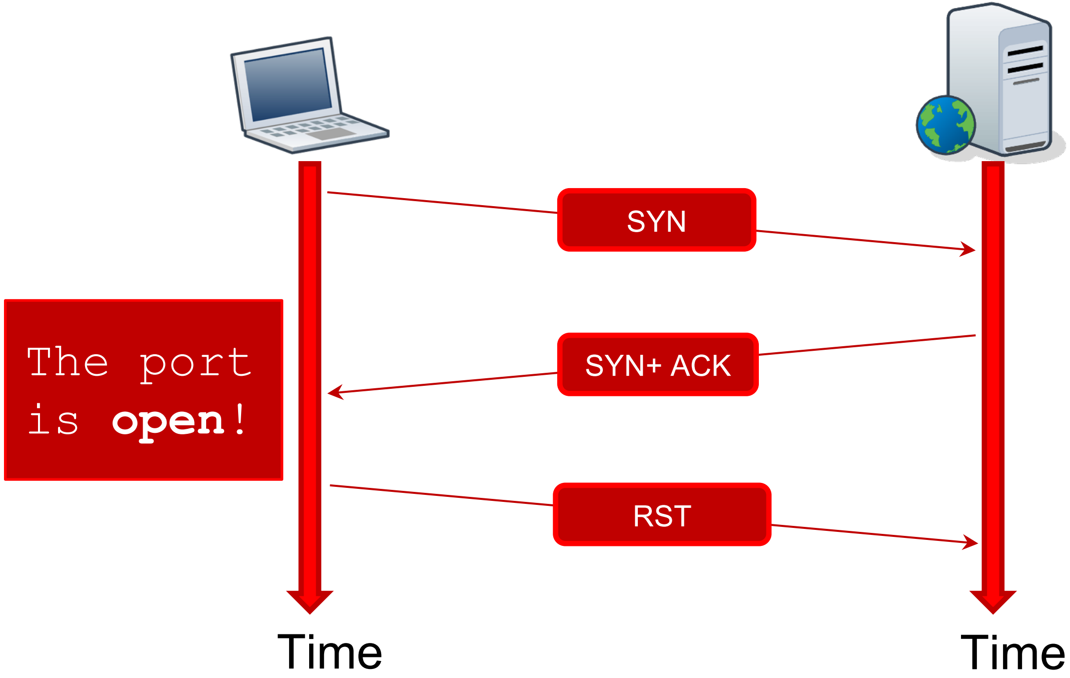


Connect to TCP



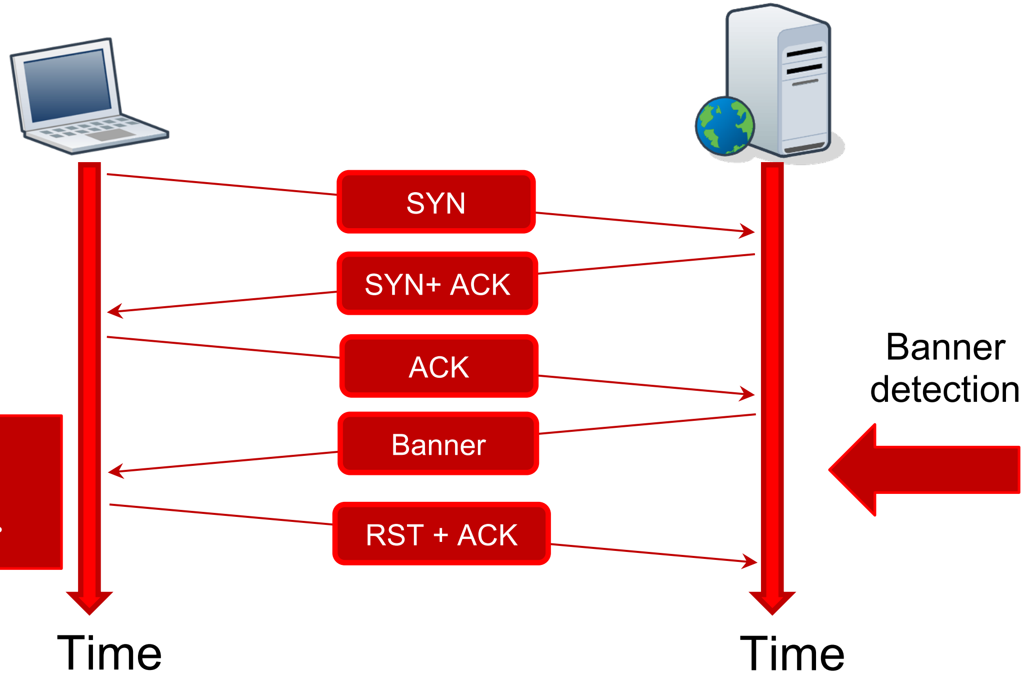
The port is **closed**!

Connect to TCP - “Stealthy”



The port is **open**!

Connect to TCP - Service Version



```
The application
listening is ...
```

Connect to UDP

- Slower
- Open|filtered
- Can be sped up

NMAP

Other tools

- Zenmap - GUI NMAP
- NMAP Automator
- Masscan
- Rustscan
- Autorecon