# Service Fingerprinting

We'll be covering service fingerprinting - the process of determining what services are running on open ports of a target system. Knowing what services are present is crucial for identifying potential vulnerabilities and planning further attacks.

Service fingerprinting involves sending probes to open ports and analyzing the responses to determine what application or service is listening. This can be done actively by directly connecting to the ports, or passively by monitoring network traffic.

To perform service fingerprinting in Nmap. We will use -sV flag.

```
sudo nmap -sS -sV IP
```

---