## Practical 1

### Title: Network scanning and reconnaissance using Nmap and other tools to identify open ports, operating systems, and potential vulnerabilities

## Objective:

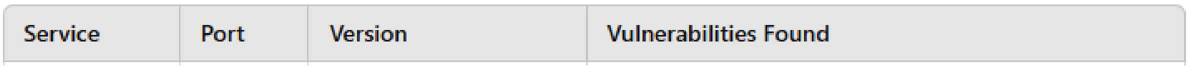
The objective of this practical exercise is to use tools like Nmap and other reconnaissance tools to:

- Identify open ports on a target machine.
- Determine the operating system running on a target machine.
- Detects potential vulnerabilities that may exist based on open ports and services running.

### Tools Required:

1. **Nmap** – A network exploration tool and security scanner.
2. **Netcat** – A networking utility used for reading from and writing to network connections.
3. **Nikto** – A web server scanner to find vulnerabilities in web servers.
4. **OS-Fingerprint Database** (for OS fingerprinting with Nmap).
5. **Shodan** – A search engine for internet-connected devices (useful for reconnaissance).
6. **OpenVAS** (Optional) – A vulnerability scanner for detecting security issues.

### Example Report:



| Service | Port | Version | Vulnerabilities Found |
|---|---|---|---|

### Conclusion: