# Phase 1: Planning

### 1.1 Scope

Since we are working on **Metasploitable 2**, our focus is strictly on **network vulnerabilities**:

| Service | Port |
|---|---|
| **FTP** | **21** |
| **Rsh** | **512** |
| **NFS** | **23** |
| **Java RMI** | **1009** |
| **SMB** | **139, 445** |
| **IRC** | **6697** |
| **PostgreSQL** | **5432** |
| **HTTP** | **8180** |

⛔ **Out of Scope:**

- Physical security attacks
- Denial-of-Service (DoS)
- Social engineering

### 1.2 Methodology (Testing Approach)

We will follow the **PTES (Penetration Testing Execution Standard)** framework:

1. **Scanning & Enumeration** – Gather system information.
2. **Exploitation** – Attempt to gain unauthorized access.
3. **Post-Exploitation & Reporting** – Document findings and recommend fixes.

### 1.3 Tools Selection

| Phase | Tool(s) Used |
| --- | --- |
| 🔍 Scanning & Enumeration | Nmap, OpenVAS, Enum4Linux |
| 🎯 Exploitation | Metasploit, Hydra, SQLmap |
| 📄 Reporting | PDF && Markdown Reports |

### 1.4 Setting Up the Testing Environment

✅ **Download & Install Metasploitable 2** → SourceForge
✅ **Use VirtualBox or VMware** → Import Metasploitable 2
✅ **Network Configuration** → Set to **NAT or Host-Only**