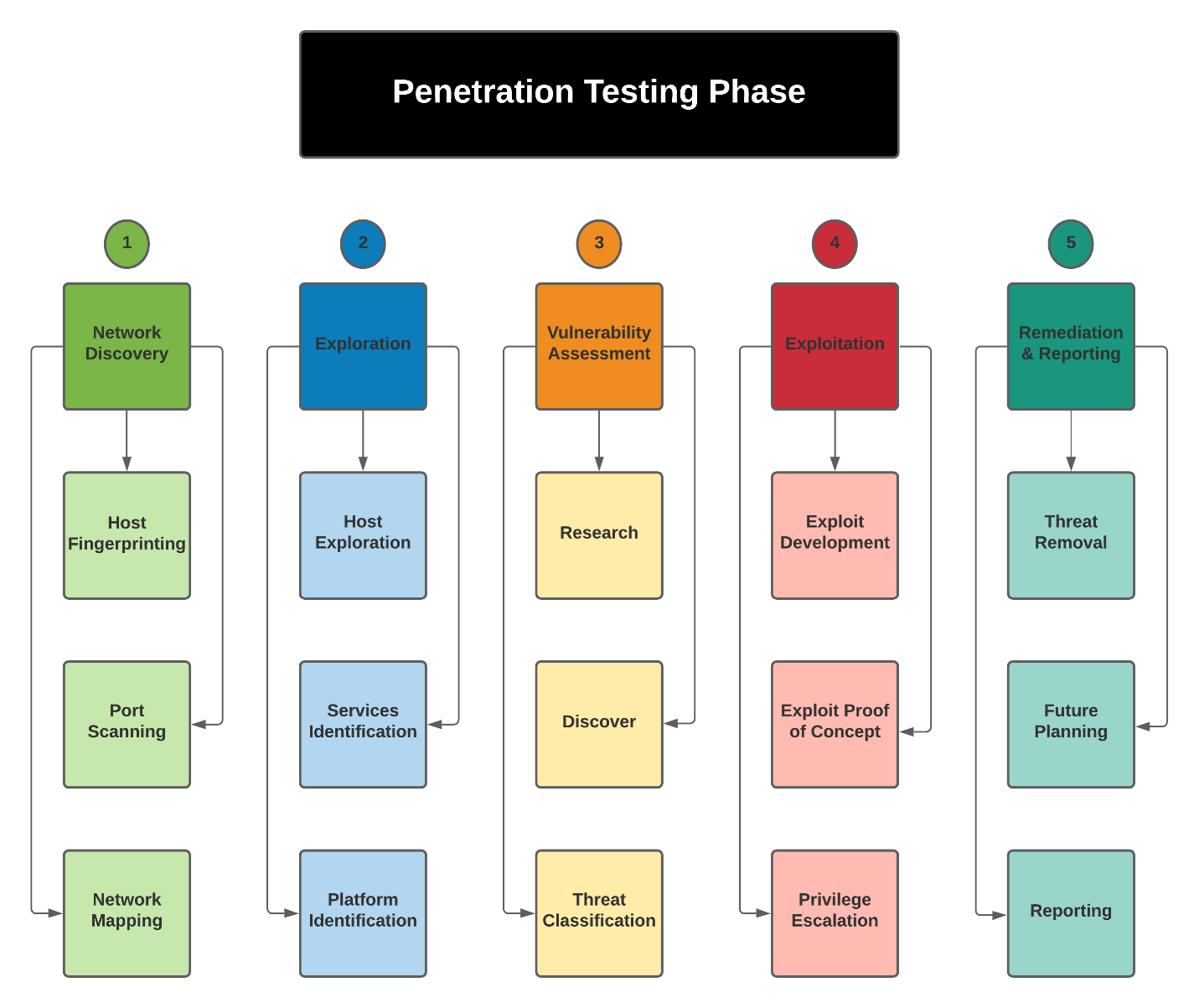
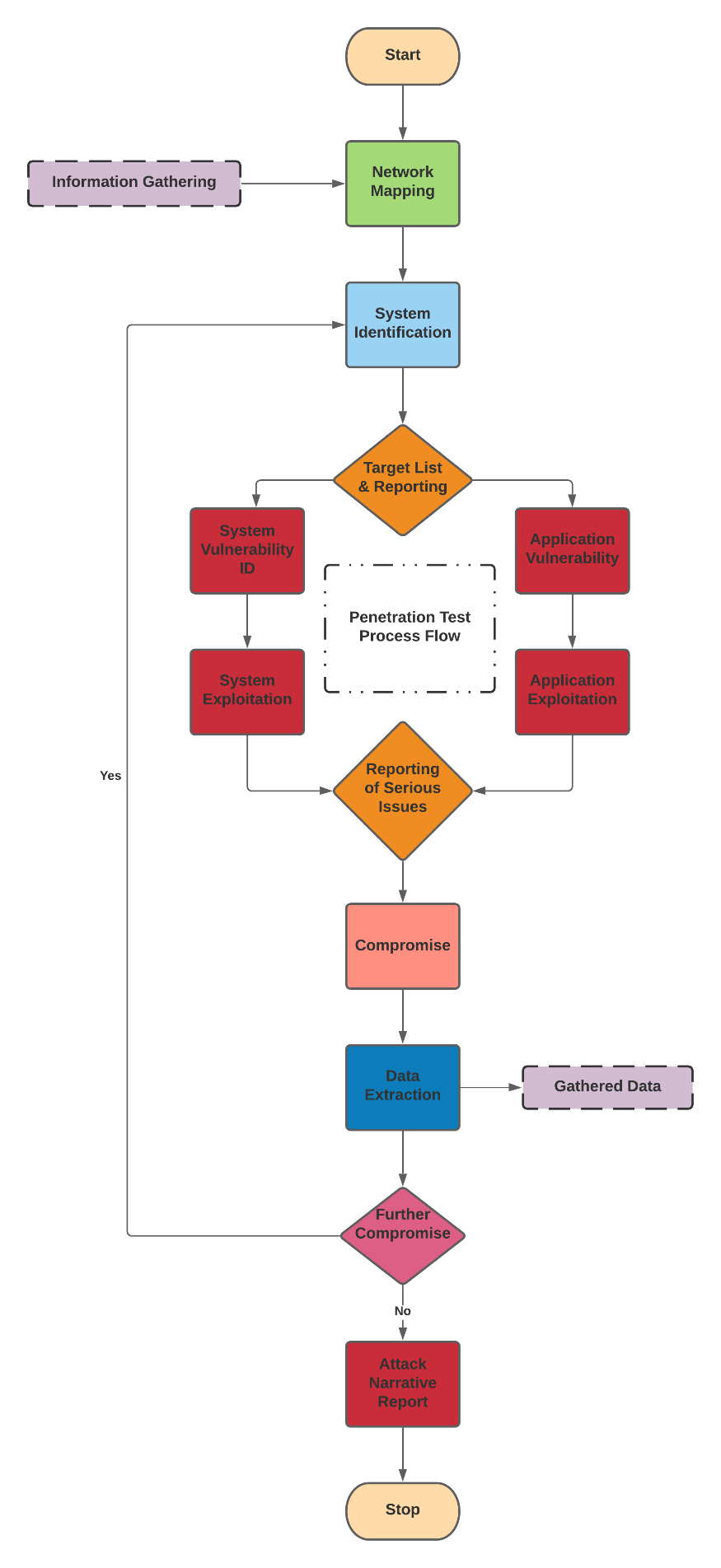
**Network Infrastructure Security**



# **Penetration Testing Flow of Process**



# **Methodology**

* The PTES (Penetration Testing Execution Standard).

There are seven stages involved in this methodology. Following are seven stages:

1. ***Pre-engagement Interactions***
2. ***Intelligence Gathering***
3. ***Threat Modeling***
4. ***Vulnerability Analysis***
5. ***Exploitation***
6. ***Post Exploitation***
7. ***Reporting***

# **Pre-Engagement Interactions**

The pre-engagement interactions involve:

* Introduction to Scope
* Metrics for Time Estimation
* Scoping Meeting
* Questionnaires
* Specify Start and End Dates
* Specifying Ip Ranges and Domains
* Dealing with Third Parties
* Cloud Services
* ISP
* Payment Terms
* Goals
* Establish Lines of Communication
* Emergency Contact Information
* Incident Reporting Process
* Rules of Engagement
* Legal Considerations

# **Intelligence Gathering**

This step involves intelligence gathering activities for penetration testing. The purpose of this document is to provide reconnaissance against a target. Following are list of tools:

|  |  |  |
| --- | --- | --- |
| # | Tools | Platform |
| 1 |  |  |