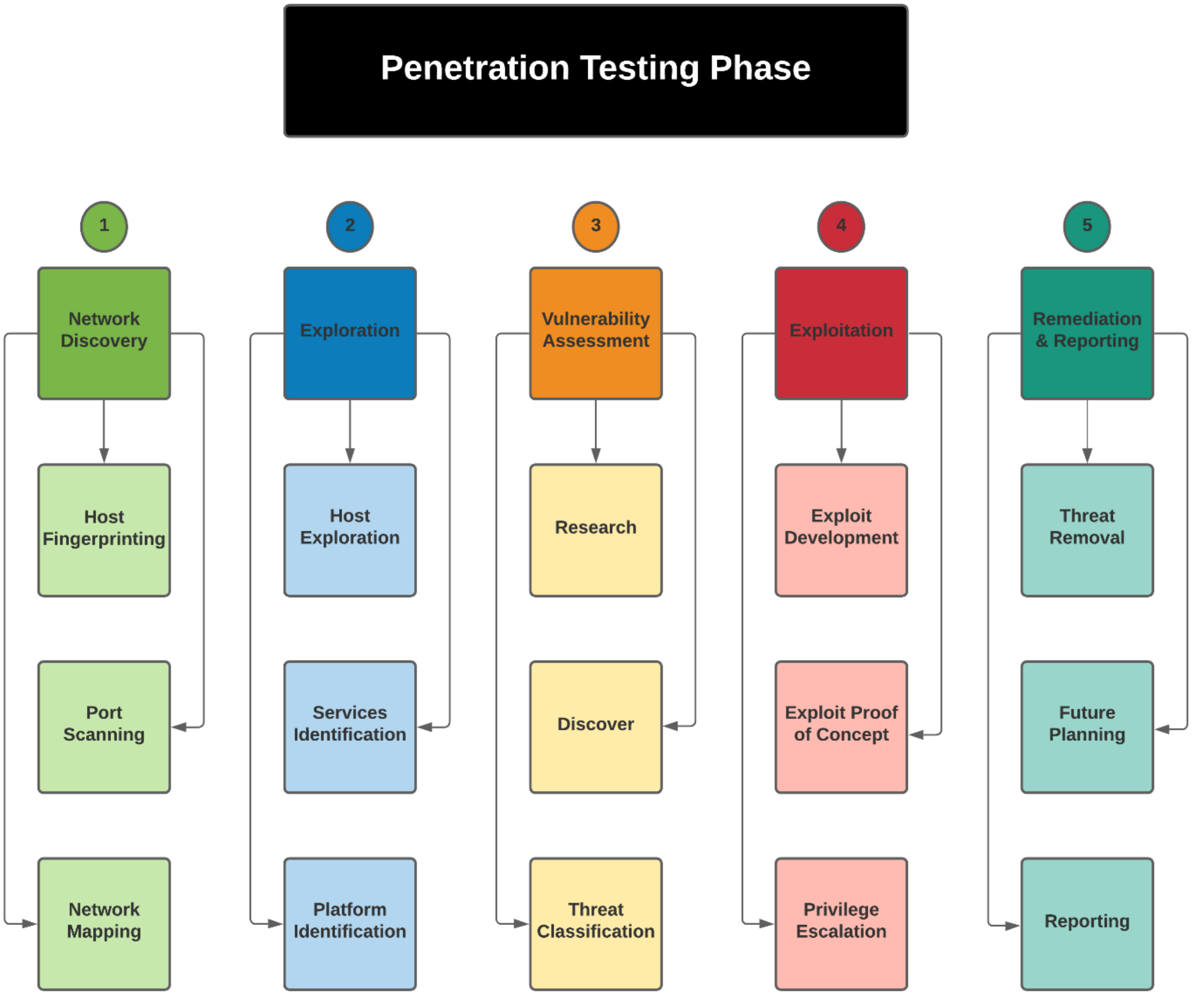
Network Infrastructure Security



Penetration Testing Phase

1 Network Discovery
- Host Fingerprinting
- Port Scanning
- Network Mapping

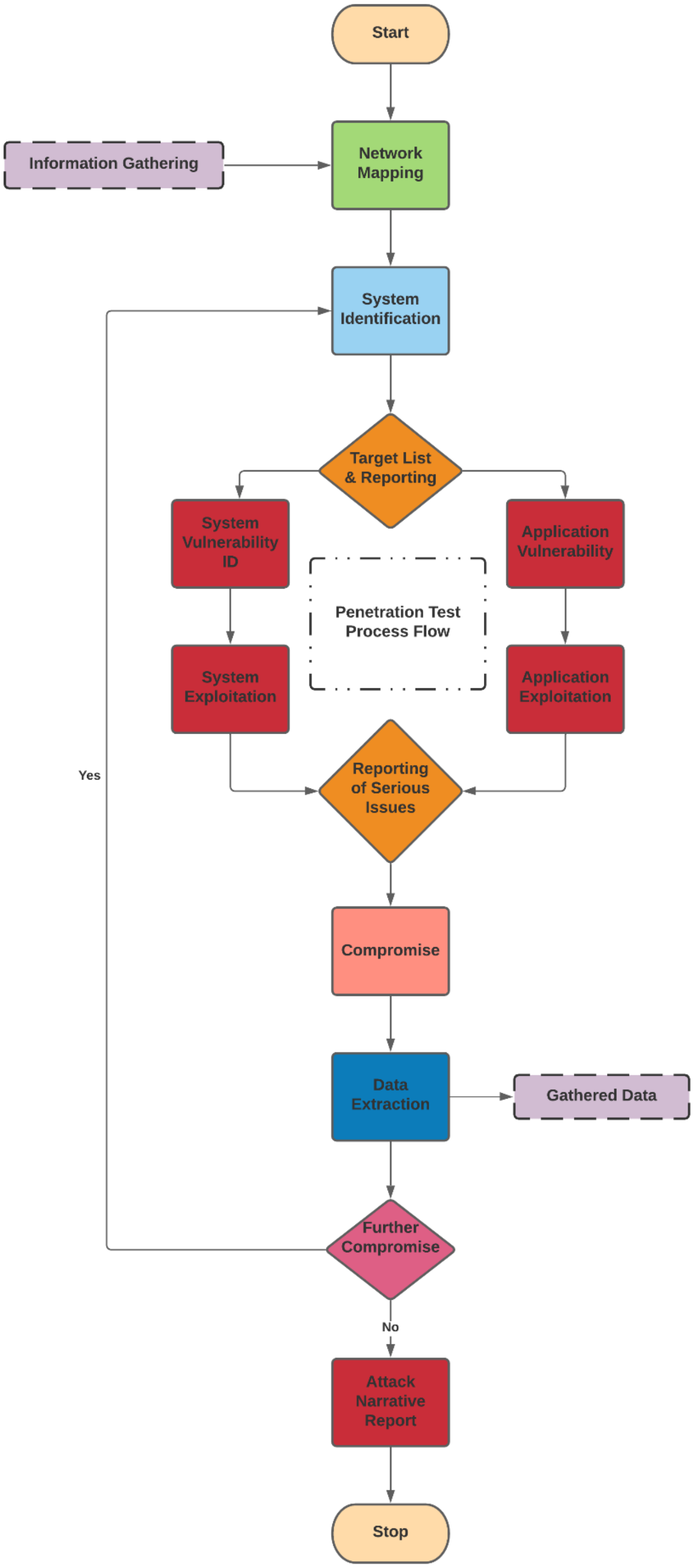
2 Exploration
- Host Exploration
- Services Identification
- Platform Identification

3 Vulnerability Assessment
- Research
- Discover
- Threat Classification

4 Exploitation
- Exploit Development
- Exploit Proof of Concept
- Privilege Escalation

5 Remediation & Reporting
- Threat Removal
- Future Planning
- Reporting

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***

1. 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

2. 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	Nmap	C/C++/Python
2	Telnet	C++
3	Nikto	Perl

3. Enumeration

The data collected in the intelligence gathering or scanning phase is then enumerated using tools like Excel or any other spreadsheet.

Using such tools mention:

- ***Open Ports.***
- ***Services.***
- ***Server Domain Names.***
- ***Server IP.***
- ***OS Information.***

4. Vulnerability Analysis

Vulnerability testing is the process of discovering flaws in systems and applications which can be leveraged by an attacker. These flaws can range anywhere from host and service misconfiguration, or insecure application design.

#	Tools	Platform
1	OpenVas	C
2	Nmap Vuln Scripts	C/C++/Python
3	CVE/ CERT/ NVD	Online Databases
4	Sfuzz	Python/ Shell

5. Exploitation

The vulnerabilities list obtained in the Vulnerability section is very useful in executing several attacks on the targeted machine. These attacks could alter the services or to maneuver or attain unwarranted access to the data stored on targeted machine.

#	Tools	Platform
1	Metasploit	Ruby
2	Dirbuster	Jar – Java
3	SQLMap	Python
4	Medusa	Shell
5	John The Ripper	Python/Shell
6	Hydra	C
7	LOIC	Shell
8	ArpSpoof	C++
9	TcpDump	C
10	Sfuzz	Python/ Shell
11	Wireshark	C
12	Aircrack-ng	Shell

6. Post Exploitation

The post exploitation is based on the report providing a detailed analysis of the penetration testing activities. It is explained that how the vulnerabilities are found and how they are exploited. The consequences of these vulnerabilities are also explained in the report. At the end, recommendations are provided for mitigating or removing the risk to make the system secure.