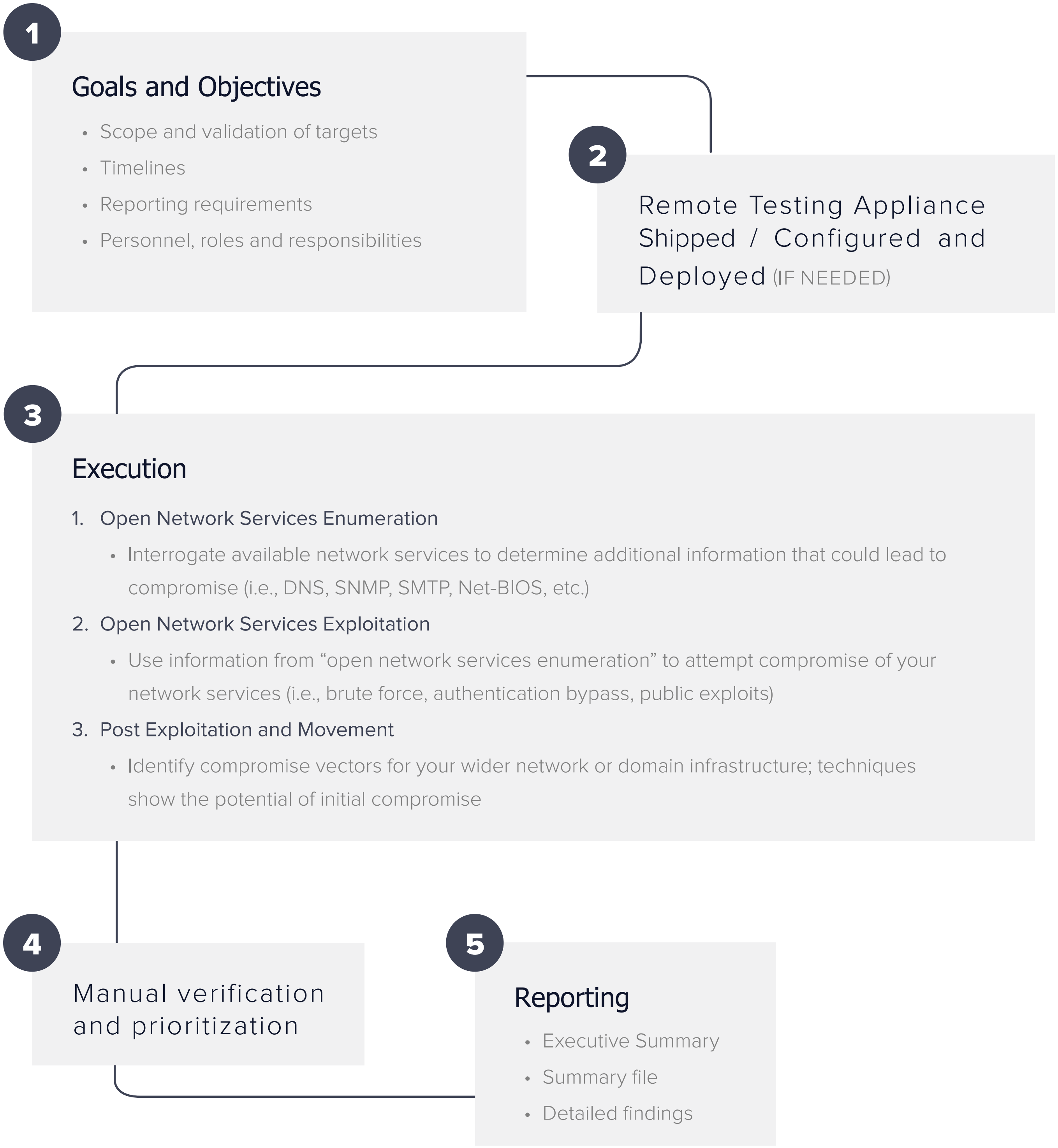
PENETRATION TESTING METHODOLOGY



1

Goals and Objectives

- Scope and validation of targets
- Timelines
- Reporting requirements
- Personnel, roles and responsibilities

2

Remote Testing Appliance Shipped / Configured and Deployed (IF NEEDED)

3

Execution

1. Open Network Services Enumeration
   - Interrogate available network services to determine additional information that could lead to compromise (i.e., DNS, SNMP, SMTP, Net-BIOS, etc.)
2. Open Network Services Exploitation
   - Use information from “open network services enumeration” to attempt compromise of your network services (i.e., brute force, authentication bypass, public exploits)
3. Post Exploitation and Movement
   - Identify compromise vectors for your wider network or domain infrastructure; techniques show the potential of initial compromise

4

Manual verification and prioritization

5

Reporting

- Executive Summary
- Summary file
- Detailed findings