Penetration Testing Plan Template

Instructions: Replace the information in brackets [ ] with information relevant to your penetration testing project. Fill out each of the sections below with information relevant to your project.

A Penetration Tester evaluates the security of an information infrastructure by intentionally, and safely, exploiting vulnerabilities. Take on the role of Penetration Tester for the approved organization you chose in Week 1. Research the following information about the organization you chose. Use this template to create a Penetration Testing Plan.

# [Organization Name]

| Criteria | Response |
| --- | --- |
| Project Title: | [Response] |
| Project Sponsor(s): | [Response] |
| Business Context for the Penetration Test: | [Response] |
| Project Scope Description: | [Response] |
| Date Prepared: | [Response] |
| Prepared By: | [Response] |

## Penetration Testing Scope Statement

## Penetration Test Pre-Planning

| Team Location(s) | Organization Location(s) | Client Personnel Aware of Testing | Resources Provided to Pentest Team | Pentest Technologies Used |
| --- | --- | --- | --- | --- |
| [Response] | [Response] | [Response] | [Response] | [Response] |
| [Response] | [Response] | [Response] | [Response] | [Response] |
| [Response] | [Response] | [Response] | [Response] | [Response] |
| [Response] | [Response] | [Response] | [Response] | [Response] |

## High-Level Work Schedule: Project Scope

| Description of Work/Pentest Boundaries | Assumptions and Constraints |
| --- | --- |
| What is tested? Social engineering test boundaries? What is acceptable? What are the boundaries of physical security tests? What are the restriction on invasive pentest attacks? What type of corporate policy affect your test?  [Response] | [Response] |
| Milestones | Due Dates |
| [Response] | [Response] |

| ID | Activity | Resource | Labor | | | Material | | | Total Cost |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Hours | Rate | Total | Units | Cost | Total |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |

## Appropriate Authorization (Including Third-Party Authorization)

| Name | Title/Organization | Description of Authorization and Consent (Identify reference documents) |
| --- | --- | --- |
| [Response] | [Response] | [Response] |
| [Response] | [Response] | [Response] |
| [Response] | [Response] | [Response] |
| [Response] | [Response] | [Response] |
| [Response] | [Response] | [Response] |
| [Response] | [Response] | [Response] |

| Reconnaissance Deliverable Name | Reconnaissance Deliverable Description |
| --- | --- |
| [Response] | [Response] |
| [Response] | [Response] |
| [Response] | [Response] |
| [Response] | [Response] |
| [Response] | [Response] |
| [Response] | [Response] |

## Reconnaissance Pentest Activities

## Scanning Pentest Activities

| Scanning Test Deliverable Name | Scanning Test Deliverable Description |
| --- | --- |
| [Response] | [Response] |
| [Response] | [Response] |
| [Response] | [Response] |
| [Response] | [Response] |
| [Response] | [Response] |
| [Response] | [Response] |

## Gaining Access Activities

| Gaining Access Activity Name | Gaining Access Activity Description |
| --- | --- |
| [Response] | [Response] |
| [Response] | [Response] |
| [Response] | [Response] |
| [Response] | [Response] |
| [Response] | [Response] |
| [Response] | [Response] |

## Maintaining Access Activities

| Maintaining Access Activity Name | Maintaining access Activity Description |
| --- | --- |
| [Response] | [Response] |
| [Response] | [Response] |
| [Response] | [Response] |
| [Response] | [Response] |
| [Response] | [Response] |
| [Response] | [Response] |

## Covering Tracks Activities

| Covering Tracks Activity Name | Covering Tracks Activity Description |
| --- | --- |
| [Response] | [Response] |
| [Response] | [Response] |
| [Response] | [Response] |
| [Response] | [Response] |
| [Response] | [Response] |
| [Response] | [Response] |

## Pentest Analysis and Report Planning

| Describe plan for analyzing and reporting pentest results. |
| --- |
| [Response] |