Penetration Testing Methodology Project Template

ISTXXXX

Your Name

Table of Contents

Phase I: Planning and Preparation X

Phase II: Assessment X

Information Gathering X

Network Mapping X

Vulnerability Analysis X

Penetration Testing X

Phase III: Closing Activities X

Reporting X

Follow-on Actions X

Archiving X

Reference X

Appendix X

Example: Test Outputs X

Example: Vulnerability Scan Reports X

Example: Analysis Metrics from Tools X

Example: Presentations X

Example: Screenshots of Systems X

Example: Screenshots of Commands X

Example: Contractual Agreement X

Example: Service Level Agreement X

Example: Invoice X

Example: Non-disclosure Agreement X

List of Tables and Figures

Figure 1. Example: Scope X

Figure 2. Example: Deliverables X

Give a brief summary, one page or less, of what you believe the purpose of this penetration test to be, what methodologies are appropriate, provide a statement of purpose. A virtual scenario has been provided for completion of this project. That said, Wilmington University is an institute of higher learning. As such, research is highly encouraged and rewarded. You have the option, with prior approval, to conduct penetration tests on personally owned systems such as Boxee Boxes, internet connected televisions/refrigerators, MySQL, etc.

**Phase I: Planning and Preparation**

This is arguably the most important part of a penetration testing project. The logistical work done during this phase makes it possible to execute a successful penetration test. The origins of all problems experienced during the other two phases can usually be tracked back to a lack of planning during this phase. This phase concludes with an assessment agreement.

**Background**

Give the penetration test context. Provide answers to these questions such as: (a) What kind of company is this?, (b) What services are they requesting?, (c) Why is the company requesting the services?, and (d) Does the requestor have the authority to make the request?

**Assessment Agreement**

The assessment agreement will include:

1. Scope:
2. Rules of Engagement
	1. Internal, external, or both approach.
	2. White, gray, or black box approach.
	3. Announced, unannounced.
	4. Passive recon, active recon.
3. What will be tested? (Telephony, network, database, wireless (keyboard, mouse, Bluetooth, Zigbee), applications, web server, email servers, VPN, data leakage protection, VoIP, physical, DMZ, IDS, firewall, router, switch.)
4. What will it be tested with? (BackTrack, Metasploit, Canvas Immunity, personally developed code, low orbit internet cannon, etc.)
5. How? (Trojan, social engineering, denial-of-service, stealing/breaking and entering, viruses, wardialing.)

\*Use the Scope tables provided below as an example for logically organizing your information.

|  |
| --- |
| *Penetration Testing Scope* |
| In Scope | Out of Scope |
| 1. 2.3.4.5.  | 1.2.3.4.5. |

*Figure 1.* Penetration Tests Scope.

|  |
| --- |
| *Penetration Testing Tools Scope* |
| In Scope | Out of Scope |
| 1. 2.3.4.5.  | 1.2.3.4.5. |

*Figure 2.* Penetration Testing Tools Scope.

1. Deliverables:

|  |  |  |
| --- | --- | --- |
| Deliverable | Description | Acceptance Criteria |
| Presentation | Electronic Document  | As defined in scope, vetted by Team Lead, approved by Project Manager |
| Report | Electronic Document & Presentation | As defined in scope, vetted by Team Lead, approved by Project Manager |
| Etc. | Etc. | Etc. |

*Figure 3.* Deliverables.

1. Team Members:

|  |
| --- |
| Penetration Team Project Members |
| Role | Responsibility Description |
| Project Manager | Harcourt, Thomas – Manage team, ultimately responsible for success of project. |
| Project Sponsor | Valasquez, Juan – Handles escalated personnel issues, represents project and team to third parties. |
| Team Members | Last name, First, etc, - All act in penetration test engineer capacities. |
| Stakeholders | Company name, CIO, Department Heads, IT employees, etc. |
| Etc. | Etc. |

*Figure 4.* Team Members.

Penetration Testing Team Members

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Engineer** | **Specialty** | **Duty** | **Email** | **Phone Number** | **Alternate** |
| Harcourt, Thomas | Project Management, Wireless Penetration | Project Manager | thomas.harcourt@company.com | 1-800-943-2257 x142 | Rivera, Jorge |
| Smith, Andrew | Database, Email, Web Server Penetration | Engineer | andrew.smith@company.com | 1-800-943-2257 x138 | Mutton, Scott |
| Etc. | Etc. | Etc | Etc. | Etc. | Etc. |
| Etc. | Etc. | Etc | Etc. | Etc. | Etc. |
| Etc. | Etc. | Etc | Etc. | Etc. | Etc. |
| Etc. | Etc. | Etc | Etc. | Etc. | Etc. |
| Etc. | Etc. | Etc | Etc. | Etc. | Etc. |
| Etc. | Etc. | Etc | Etc. | Etc. | Etc. |
| Etc. | Etc. | Etc | Etc. | Etc. | Etc. |

*Figure 5.* Penetration Testing Team Members.

1. What is the escalation path for problems? (For example: What will you do if the owner asks you break into his wife’s personal email because he believes she is cheating on him, you discover child pornography, etc?)
2. Each department needs a point of contact. (For example, Network Administration, Server Administration, Client Administration, Help Desk, Network Security, Quality Assurance, Development, etc.)
3. Date/Time of Test. (Perhaps only weekends are acceptable or only early morning hours, etc.)
4. Miscellaneous Points of Contact:
	1. Law Enforcement (City, State, County)
	2. Internet Service Provider
	3. Consultants
	4. Subject Matter Experts
	5. Lawyers
5. Retest Policy.
6. Working conditions. (For example: (a) Where will you work from?, (b) What will you work with?, and (c) What do you require?
7. Non-disclosure Agreement.
8. Liability Insurance or Approval in Writing (For example: (a) Why do you need it? (b) Where do you find it?)
9. Contractual Constraints (For example: (a) Don’t denial of service servers because we have customers who will sue us., (b) Don’t transfer data., and (c) Don’t route attack traffic out of the country and back.)
10. Legal Issues – If illegal activity is found such as child porn then we will do what?
11. Quality Assurance – How? (For example: Is there a senior rater? Are double tests performed?)

**Phase II: Assessment**

Provide a brief description of what will occur during this phase. For example: This is the phase where you will implement your plan. You will gather data about your intended target and infer enough information so you have the knowledge you need to pursue a penetration test. This phase has four sections: Information Gathering, Network Mapping, Vulnerability Analysis, Penetration Testing.

**1. Information Gathering**

There are many methods of gathering information on your company, as discussed during the planning phase. You should have already identified the information gathering techniques in scope of your work during the planning phase. Now it’s time to execute your information gathering techniques. Explain the difference between active and passive gathering. Categorize your work into two sections, active or passive gathering.

A block of words is provided below to jog your mind:

DNS/WHOIS, search engines, website (wget), Chamber of Commerce, company reviews, Google Maps, Facebook/MySpace/Twitter/YouTube, Internet Archive, job postings, key people, web addresses, servers OSs, locations of servers, web links, web server directory tree, enumerate services running on server and list, encryption standards (SSL, TLS, etc), form fields, web code/language, variables, meta tag info.

**2. Network Mapping**

This section is where we compile a list of devices and their locations on the network, also known as foot printing the network. It can be broken down into two sections, internal and external. A list of devices should be provided with as much information as possible. Rack and stack the devices for targeting. A block of words is provided below to jog your mind:

Live hosts, open/closed ports, services, perimeter devices, firewalls, routers, DMZs, operating systems, purpose of device, banner page, error pages, topological map, IP block, DNS registry information, ISP, tracert.

**3. Vulnerability Analysis**

Specific targets have been identified. You’ve racked and stacked. It’s time to focus on your targets. List them here and explain why you’ve chosen them.

Follow these steps below:

1. Identify vulnerable services/OSs/coding language(s)/form input(s):
2. Search for known vulnerabilities for each OS, service, etc, and list them: (CVE, CERT, NVD, etc.)
3. Reprioritize rack and stack list. Classify list by likelihood of success.
4. Create attack scenario. Tease out idea by drawing it on paper first. Provide a step-by-step with an accompanying descriptive paragraph detailing your thoughts. IMPORTANT: Verify your attack scenario is within scope. If it’s not, don’t do it. You could experience legal complications.

**4. Penetration Testing**

This is the actual test. You are executing your attack scenario.

Follow these steps:

1. Find/develop your exploits for the vulnerabilities you identified, give a brief description of each, describe the dangers of using a second party exploit: (M1lW0rm, Metasploit, etc.)

|  |
| --- |
| **Vulnerability/Exploit Rack and Stack** |
| **System** | **Vulnerabilities** | **Exploits** | **Exploit Description** | **Exploit Source** | **Ranking** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

1. Use tool/code, verify success or failure to access.
2. For each successful exploit list the system exploited, vulnerability, exploit used, paths, commands, impact on device. Provide screenshots, copies of file(s), intimate knowledge of system to prove claim.
3. Hot wash. For each failure make a speculation of what the issues could be. For example, is the exploit being used against a slightly newer version of the system and, therefore, no longer effective?

**Phase III: Closing Activities**

The previous two phases were for your benefit as a penetration tester. There was an initial interface with the business in order to agree on the terms and then you planned and conducted a penetration test. This is the phase where you communicate your findings to the business.

**1. Reporting**

It is extremely important you reiterate in a clear and concise way that you’ve done what you said you would do. Provide a brief PowerPoint slide for each audience listed below. Use your judgment in determining what to include. Special note, this is also a pitch for further business. Market future services.

1. Chief Information Officer/Director of Information Technology/Chief Security Officer/miscellaneous management: Example Management Summary: Scope, Tools, Exploits, Dates/Times, Verification, Residual Clean-up Actions Performed, Recommendations for Security Policy, Future Services (Post-Test Support, Countermeasures, Second Penetration Test, Training staff).
2. IT Department Heads. Example: List systems found with accompanying specs and configurations, Vulnerabilities, Exploits, Dates/Times, Verification, Output of Tests, Post Clean-up Actions Performed, Recommendations, Post-testing.
3. Technical Staff: server administrators, network administrators, client system administrators, etc. Example: Detail system exploited, date/time, output of tests, make specific recommendations that are actionable for the technicians such as fixing misconfigurations.

**2. Follow-on Actions**

Describe what you’ve done in regards to follow-on actions. Follow-on actions include a discussion of cleaning up code, patching, wiping systems, notifying law enforcement and the ISP and stakeholders the penetration test is concluded, destroy network information gathering data and list of vulnerabilities and exploits and construct a lessons learned. The lessons learned should answer these, and other, questions:

1. Were there any incidents, physical or cyber, with law enforcement, management, illegal activities found, pre-existing hacks already being exploited?
2. How were they managed?
3. Could they have been managed differently?

**3. Archiving**

List what information you will keep, why you will keep it, what the legal ramifications/risks of keeping it are, where you will keep it, and how long will you keep it?

How will you secure the data you do keep? (Encryption level, software, cloud-based and accessible from your smart phone, locally stored, backup, in your email, data integrity checks with hashes, data leakage protection measures, knowledge database)

**Reference**

**Appendix**