Team X Penetration Testing Report

[List team member names here]

Executive Summary (5%)

One-page executive summary that highlights the most important findings of your report. Must be no more than one page. This should be written so that non-technical executives can understand.

Describe the number of serious successful exploits and the amount of sensitive data you were able to obtain.

Give a high-level summary of your recommendations to fix the problem.

Don’t describe specifics or use technical terms that may be unfamiliar to a non-technical person in this section.

# Project Scope Description (5%)

Description of the scope of the project (including the IP of the computer you are attacking, and dates and times that you are given permission to attempt to access it), objectives, and your authorization to perform the assessment (i.e., my instructions to you).

This should be written so that non-technical executives can understand.

## Objectives

1. Document vulnerabilities that you are able to successfully exploit on the server. Describe in detail what you did and what level of access you were able to obtain. If you obtain a user account with limited privileges, document whether you were able to escalate the privileges to root. Document each exploit that you are able to successfully launch.
2. Document potentially sensitive information that you are able to obtain from the server. These could include user files or web, database, or other server files.
3. For both 1 and 2 above, suggest ways that vulnerabilities exploited or sensitive information obtained could be protected.

## Authorization

* A copy of your authorization to perform the threat assessment

# Target of Assessment (5%)

Information about the server examined (IP address, MAC address, OS version, user accounts). Give a brief description of major applications installed, web sites hosted, services running, and databases that exist (both database applications, such as Oracle, and information stored within those database applications).

# Relevant Findings (25%)

High-level description of vulnerabilities successfully exploited and sensitive data obtained.

Organize for impact. This means you should discuss the most serious vulnerabilities first.

This should be written so that non-technical executives can understand. Define technical terms and concepts described in the glossary section.

List sensitive data obtained in the final subsection of section 3. Clearly state the names and paths of files accessed, and if secured, how you were able to access them. If files are too numerous to include in the main body of the report, list them in an appendix. If you obtain passwords, list what those passwords are.

Use style “Heading 2” to number each exploit and sensitive data obtained. Give a brief 1–4 sentence overview of what you were able to accomplish. Then include a cross-reference to a subsection in section 4 with supporting details on how you performed the attack. Give a high-level recommendation on what to do to fix the problem, cross-referencing a subsection in section 5.

See below for an example.

## SSH Backdoor (example)

*The version of SSH installed on the server, WeakSSH, contained a backdoor… Because of this exploit, we were able to obtain… Please refer to section 4.1 for further details. This problem can be remediated by uninstalling WeakSSH and installing the latest version of OpenSSH. See section 5.1 for specific remediation steps. See Appendix A for a listing of affected users. (end example)*

# Supporting Details (30%)

This section provides supporting details for each of the relevant details listed in the previous section. The detail should be sufficient for another person to replicate the results of your main findings using your report.

This section should be written so that a technical person can exactly replicate the steps that you performed. List every command/step used to perform the attack. This should follow the methodology discussed in class for the steps of vulnerability scanning, moving through to the exploitation lab material.

Cross reference sections 3 and 5.

See below for an example.

## SSH Backdoor (example)

*We discovered this vulnerability by… We performed this exploit by (list all steps) by:*

*1.*

*2.*

*3.*

*Because of this exploit we were able to obtain… See section 3.1. See section 5.1 for recommended steps to fix this vulnerability, see section …* (end example)

# Vulnerability Remediation (25%)

Explanation for how to protect against vulnerabilities successfully exploited and sensitive data obtained. Provide specific steps.

This section should be written so that a technical person can know what she/he can do to fix the problem.

Cross reference sections 3 and 4.

See below for an example.

## SSH Backdoor (example)

*Uninstall WeakSSH and install the latest version of OpenSSH. See sections 3.1 and 4.1. (end example)*

# Glossary

Define technical terms used in the report here.

# Appendix A

Optional. Include here technical detail that is useful to include for replication or documentation purposes, but would disrupt the flow of the report because of its length. Number appendices to make them easy to reference from the “Supporting Details” section.

Do *not* give me a Nessus report.