Penetration Test Report

PENETRATION TESTER

Jun 05, 2019

CONTENTS:

CHAPTER

ONE

EXECUTIVE SUMMARY

PENTESTER NAME ("the pentester" henceforth) was contracted by COMPANY NAME to conduct a penetration test in order to determine its exposure to a targeted attack. All activities were conducted in a manner that simulated a malicious attacker engaged in a targeted attack against COMPANY NAME with the goals of:

- Identifying if a remote attacker could penetrate COMPANY NAME's defenses
- **Determining the impact of a security breach on:**
  - Confidentiality of the company's private data
  - Internal infrastructure and availability of COMPANY NAME's information systems

Efforts were placed on the identification and exploitation of security weaknesses that could allow a remote attacker to gain unauthorized access to organizational data. The attacks were conducted with the level of access that a general Internet user would have. The assessment was conducted in accordance with WHATEVER SET OF GUIDELINES[1], with all tests and actions being conducted under controlled conditions.

1.1 Summary of Results

[TODO: Include a summary of discoveries.]

1.2 Recommendations

[TODO: Include recommendations to the executives.]

[1] WHERE TO FIND THE GUIDELINES

CHAPTER

TWO

ATTACK METHODOLOGIES

The pentester utilized a widely-adopted approach to performing penetration testing that is effective in testing how well COMPANY NAME's systems have been secured. Below is a breakdown of how he was able to identify and exploit the variety of systems, including all individual vulnerabilities found.

2.1 Information Gathering

The information gathering portion of a penetration test focuses on identifying the scope of the penetration test. During this penetration test, the pentester was tasked with exploiting COMPANY NAME's systems.

2.1.1 Subnet EXAMPLE

The EXAMPLE NETWORK subnet was the pentester's original point of entry for the penetration test. The following live hosts were identified within the subnet:

[TODO: Include table of discovered hosts.]

2.1.2 Methodology

[TODO: Explain the information gathering methodology.]

2.2 Service Enumeration

The service enumeration portion of a penetration test focuses on gathering information about what services are alive on a system or systems. This is valuable for an attacker as it provides detailed information on potential attack vectors into a system. Understanding what applications are running on the system gives an attacker vital information before performing the actual penetration test.

The following sections detail the open ports discovered on the various systems discovered in the information gathering phase. In some cases, some ports may not be listed.

2.2.1 Methodology

In order to discover the services running on the various target systems, the pentester employed the following methods.

2.2.1.1 Overview Scan

[TODO: Include methodology for overview scan.]

2.3 Penetration

The penetration portion of a test focuses heavily on gaining access to the various systems within a target's networks. During the penetration test, the pentester was able to successfully gain access to a number of systems, including INSERT SIGNIFICANT INFORMATION HERE.

The following sections outline the vulnerabilities exploited, the vulnerable systems, and a breakdown of the steps to exploit those vulnerabilities.

2.3.1 Vulnerabilities

2.3.2 Methodology

DESCRIBE METHODS USED TO GAIN ACCESS TO TARGET SYSTEMS.

CHAPTER

THREE

APPENDICES

3.1 About the Penetration Tester

[TODO: Write about the penetration tester.]