# Penetration Test Report

PENETRATION TESTER

Dec 12, 2019

# CONTENTS:

CHAPTER

ONE

# EXECUTIVE SUMMARY - INCOMPLETE

[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 the company. Efforts were placed on the identification and exploitation of security weaknesses that could allow an 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 the recommendations outlined in [SET OF PENTEST GUIDELINES][1], with all tests and actions being conducted under controlled conditions.

## 1.1 Summary of Results - INCOMPLETE

While conducting the internal penetration test, there were several alarming vulnerabilities that were identified within [COMPANY NAME]'s network. As a result, the pentester was able to exploit multiple systems to gain total access and control, primarily due to outdated patches, weak password policies, and poor security configurations. The affected systems, as well as a summary of their attack methodologies, are listed below:

| Target | Exploitation Methodology |
|---|---|
| `IPADDRESS` | How the system was exploited and rooted. |

## 1.2 Recommendations

The pentester recommends patching the vulnerabilities identified during the penetration test to ensure that an attacker cannot exploit these systems in the future. One thing to remember is that these systems require frequent patching, and once patched, should remain on a regular patch program in order to mitigate additional vulnerabilities that may be discovered at a later date.

The pentester also advises stricter password guidelines and requirements, as suggested by NIST in publication 800-171r1[1], section 3.5.

[1] LINK TO THE GUIDELINES FOLLOWED

[1] https://doi.org/10.6028/NIST.SP.800-171r1

CHAPTER

TWO

# ATTACK METHODOLOGIES - INCOMPLETE

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 - INCOMPLETE

The information gathering portion of a penetration test focuses on identifying the scope of the test. During this test, the pentester was tasked with exploiting [COMPANY NAME]'s systems. The following sections outline each of the subnets and systems within the scope of this test.

### 2.1.1 SUBNET

This was the pentester's first point of contact with the network. The specific IP addresses were:

| IP | Domain |
|---|---|
| IPADDRESS | DOMAIN |

## 2.2 Service Enumeration - INCOMPLETE

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 systems and ports were identified. In some cases, some ports may not be listed.

### 2.2.1 SUBNET

| System IP Address | Ports Open |
|---|---|
| IPADDRESS | TCP: None |
|  | UDP: None |

## 2.3 Penetration - INCOMPLETE

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 and control on [NUMBER OF SYSTEMS] systems.

The following sections outline the vulnerable systems, as well as the methods used to compromise those systems.

## 2.4 Maintaining Access - INCOMPLETE

Maintaining access to a system is important to attackers. Ensuring that they can get back into a system after it has been exploited is invaluable. Many exploits may only be exploitable once, preventing further attempts to gain access to the system. The maintaining access phase of the penetration test focuses on ensuring that once the pentester has access to the system, they can keep that access in the future.

[BRIEFLY DESCRIBE STEPS TAKEN FOR MAINTAINING ACCESS]

e.g. The pentester added administrator- and root-level accounts on all systems compromised.

## 2.5 House Cleaning - INCOMPLETE

The house cleaning portion of the assessment ensures that all remnants of the penetration test are removed. Often fragments of tools or user accounts are left on an organization's computer which can cause security issues down the road. It is important to ensure that the pentester is meticulous and that no remnants of the test remain upon completion.

[BRIEFLY DESCRIBE STEPS TAKEN TO CLEAN HOUSE.]

e.g. After the penetration test was completed, the pentester removed all user accounts and *meterpreter* services that had been installed during the pentest. [COMPANY NAME] should not have to remove any user accounts or services from their systems.

CHAPTER

THREE

# APPENDICES - INCOMPLETE

## 3.1 About the Penetration Tester - INCOMPLETE

[TODO: Write about the penetration tester.]