Offensive Security

Penetration Test Report for Internal Lab and Exam

ΩCONSULTANT\_EMAILΩ

OSID: XXXX



# Table of Contents

[Table of Contents 2](#_Toc25273712)

[1.0 Offensive Security Lab and Exam Penetration Test Report 3](#_Toc25273713)

[1.1 Introduction 3](#_Toc25273714)

[1.2 Objective 3](#_Toc25273715)

[1.3 Requirements 3](#_Toc25273716)

[2.0 High-Level Summary 4](#_Toc25273717)

[2.1 Recommendations 4](#_Toc25273718)

[3.0 Methodologies 5](#_Toc25273719)

[3.1 Information Gathering 5](#_Toc25273720)

[3.2 Service Enumeration 6](#_Toc25273721)

[3.3 Penetration Testing Results 7](#_Toc25273722)

[3.4 Maintaining Access 12](#_Toc25273723)

[3.5 Sample Report – House Cleaning 12](#_Toc25273724)

[4.0 Additional Items 13](#_Toc25273725)

# Offensive Security Lab and Exam Penetration Test Report

**1.1 Introduction**

The Offensive Security Lab and Exam penetration test report contains all efforts that were conducted in order to pass the Offensive Security course. This report should contain all lab data in the report template format as well as all items that were used to pass the overall exam. This report will be graded from a standpoint of correctness and fullness to all aspects of the lab and exam. The purpose of this report is to ensure that the student has a full understanding of penetration testing methodologies as well as the technical knowledge to pass the qualifications for the Offensive Security Certified Professional.

**1.2 Objective**

The objective of this assessment is to perform an internal penetration test against the Offensive Security Lab and Exam network. The student is tasked with following methodical approach in obtaining access to the objective goals. This test should simulate an actual penetration test and how you would start from beginning to end, including the overall report. An example page has already been created for you at the latter portions of this document that should give you ample information on what is expected to pass this course. Use the sample report as a guideline to get you through the reporting.

**1.3 Requirements**

The student will be required to fill out this penetration testing report fully and to include the following sections:

* Overall High-Level Summary and Recommendations (non-technical)
* Methodology walkthrough and detailed outline of steps taken
* Each finding with included screenshots, walkthrough, sample code, and proof.txt if applicable.
* Any additional items that were not included

# High-Level Summary

ΩCONSULTANT\_NAMEΩ was tasked with performing an internal penetration test towards Offensive Security Labs. An internal penetration test is a dedicated attack against internally connected systems. The focus of this test is to perform attacks, similar to those of a hacker and attempt to infiltrate Offensive Security’s internal lab systems – the **THINC.local** domain. ΩCONSULTANT\_NAMEΩ’s overall objective was to evaluate the network, identify systems, and exploit flaws while reporting the findings back to Offensive Security.

When performing the internal penetration test, there were several alarming vulnerabilities that were identified on Offensive Security’s network. When performing the attacks, ΩCONSULTANT\_NAMEΩ was able to gain access to multiple machines, primarily due to outdated patches and poor security configurations. During the testing, ΩCONSULTANT\_NAMEΩ had administrative level access to multiple systems. All systems that were successfully exploited, as well as a brief description on how access was obtained are listed below:

* Lab Trophy 1 – Got in through X
* Lab Trophy 2 – Got in through X
* Lab Trophy 3 – Got in through X
* Exam Trophy 1 – Got in through X
* Exam Trophy 2 – Got in through X

**2.1 Recommendations**

ΩCONSULTANT\_NAMEΩ recommends patching the vulnerabilities identified during the testing 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 to protect additional vulnerabilities that are discovered at a later date.

Additional Recommendations

# Methodologies

ΩCONSULTANT\_NAMEΩ utilized a widely adopted approach to performing penetration testing that is effective in testing how well the Offensive Security Labs and Exam environments are secure. Below is a breakout of how ΩCONSULTANT\_NAMEΩ was able to identify and exploit the variety of systems and includes all individual vulnerabilities found.

**3.1 Information Gathering**

The information gathering portion of a penetration test focuses on identifying the scope of the penetration test. During this penetration test, ΩCONSULTANT\_NAMEΩ was tasked with exploiting the lab and exam network. The specific IP addresses were:

**Lab Network**

192.168.1.1, 192.168.1.2, 192.168.1.3

**Exam Network**

172.16.203.133, 172.16.203.134, 172.16.203.135, 172.16.203.136

**3.2 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 needed information before performing the actual penetration test. In some cases, some ports may not be listed.

|  |  |
| --- | --- |
| **Server IP Address** | **Ports Open** |
| 192.168.1.1 | **TCP:** 21,22,25,80,443 |
| 192.168.1.2 | **TCP:** 22,55,90,8080,80 |
| 192.168.1.3 | **TCP:** 1433,3389  **UDP:** 1434,161 |

**3.3** **Penetration Testing Results**

The penetration testing portions of the assessment focus heavily on gaining access to a variety of systems. During this penetration test, ΩCONSULTANT\_NAMEΩ was able to successfully gain access to 10 out of the 50 systems.

¬report/findings\_list/findings:::risk>3¬

**πtitleπ**

Systems Vulnerable:

π affected\_hosts π

Vulnerability Explanation:

¬overview/paragraph¬ µzzzzµ π.π

ƒcodeƒ π.π

ƒitalicsƒ *π.π*

* ƒbulletƒ π.π

ƒh4ƒ **π.π**

÷ π.π ≠

Vulnerability Fix:

¬remediation/paragraph¬ µzzzzµ π.π

ƒcodeƒ π.π

ƒitalicsƒ *π.π*

* ƒbulletƒ π.π

ƒh4ƒ **π.π**

÷ π.π ≠

Severity: **CRITICAL**

Proof of Concept and Screenshots:

¬poc/paragraph¬ µzzzzµ π.π

ƒcodeƒ π.π

ƒitalicsƒ *π.π*

* ƒbulletƒ π.π

ƒh4ƒ **π.π**

÷ π.π ≠

∆

¬report/findings\_list/findings:::risk<4:::risk>2¬

**πtitleπ**

Systems Vulnerable:

π affected\_hosts π

Vulnerability Explanation:

¬overview/paragraph¬ µzzzzµ π.π

ƒcodeƒ π.π

ƒitalicsƒ *π.π*

* ƒbulletƒ π.π

ƒh4ƒ **π.π**

÷ π.π ≠

Vulnerability Fix:

¬remediation/paragraph¬ µzzzzµ π.π

ƒcodeƒ π.π

ƒitalicsƒ *π.π*

* ƒbulletƒ π.π

ƒh4ƒ **π.π**

÷ π.π ≠

Risk: **HIGH**

Proof of Concept and Screenshots:

¬poc/paragraph¬ µzzzzµ π.π

ƒcodeƒ π.π

ƒitalicsƒ *π.π*

* ƒbulletƒ π.π

ƒh4ƒ **π.π**

÷ π.π ≠

∆

¬report/findings\_list/findings:::risk<3:::risk>1¬

**πtitleπ**

Systems Vulnerable:

π affected\_hosts π

Vulnerability Explanation:

¬overview/paragraph¬ µzzzzµ π.π

ƒcodeƒ π.π

ƒitalicsƒ *π.π*

* ƒbulletƒ π.π

ƒh4ƒ **π.π**

÷ π.π ≠

Vulnerability Fix:

¬remediation/paragraph¬ µzzzzµ π.π

ƒcodeƒ π.π

ƒitalicsƒ *π.π*

* ƒbulletƒ π.π

ƒh4ƒ **π.π**

÷ π.π ≠

Risk: **MEDIUM**

Proof of Concept and Screenshots:

¬poc/paragraph¬ µzzzzµ π.π

ƒcodeƒ π.π

ƒitalicsƒ *π.π*

* ƒbulletƒ π.π

ƒh4ƒ **π.π**

÷ π.π ≠

∆

¬report/findings\_list/findings:::risk<2:::risk>0¬

**πtitleπ**

Systems Vulnerable:

π affected\_hosts π

Vulnerability Explanation:

¬overview/paragraph¬ µzzzzµ π.π

ƒcodeƒ π.π

ƒitalicsƒ *π.π*

* ƒbulletƒ π.π

ƒh4ƒ **π.π**

÷ π.π ≠

Vulnerability Fix:

¬remediation/paragraph¬ µzzzzµ π.π

ƒcodeƒ π.π

ƒitalicsƒ *π.π*

* ƒbulletƒ π.π

ƒh4ƒ **π.π**

÷ π.π ≠

Risk: **LOW**

Proof of Concept and Screenshots:

¬poc/paragraph¬ µzzzzµ π.π

ƒcodeƒ π.π

ƒitalicsƒ *π.π*

* ƒbulletƒ π.π

ƒh4ƒ **π.π**

÷ π.π ≠

∆

## 3.4 Maintaining Access

Maintaining access to a system is important to us as attackers, ensuring that we can get back into a system after it has been exploited is invaluable. The maintaining access phase of the penetration test focuses on ensuring that once the focused attack has occurred (i.e. a buffer overflow), we have administrative access over the system again. Many exploits may only be exploitable once and we may never be able to get back into a system after we have already performed the exploit.

ΩCONSULTANT\_NAMEΩ added administrator and root level accounts on all systems compromised. In addition to the administrative/root access, a Metasploit meterpreter service was installed on the machine to ensure that additional access could be established.

**3.5 Sample Report – House Cleaning**

The house cleaning portions of the assessment ensures that remnants of the penetration test are removed. Often fragments of tools or user accounts are left on an organizations computer which can cause security issues down the road. Ensuring that we are meticulous, and no remnants of our penetration test are left over is important.

After the trophies on both the lab network and exam network were completed, ΩCONSULTANT\_NAMEΩ removed all user accounts and passwords as well as the Meterpreter services installed on the system. Offensive Security should not have to remove any user accounts or services from the system.

# Additional Items

This section is placed for any additional items that were not mentioned in the overall report.