Advanced+ Penetration Test Report

VirtualHackingLab Advanced+ Report

email address, Student id, Name

2020-04-09

Contents

1 VirtualHackingLab Certificate of Completetion Penetration Test Report

1.1 Introduction

The VirtualHackingLab Advanced+ Certificate of Completetion penetration test report contains all efforts that were conducted in order to obtain the VirtualHackingLab Advanced+ Certificate of Completetion. This report will be graded from a standpoint of correctness and fullness to all aspects of the Certificate of Completion Guidelines. 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 VirtualHackingLab Advanced+ Certificate of Completetion.

1.2 Objective

The objective of this assessment is to perform an internal penetration test against the VirtualHackingLab Advanced+ network machines. 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.

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 key.txt
- Any additional items that were not included

2 High-Level Summary

I was tasked with performing an internal penetration test towards VirtualHackingLabs Advanced+ Network. 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 Of VirtualHackingLab's internal systems. My overall objective was to evaluate the network, identify systems, and exploit flaws while reporting the findings back to VirtualHackingLabs.

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 When performing the attacks, I was able to gain access to multiple machines, primarily due to outdated patches and poor security configurations.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

- 10.1x.1.xx (hostname) - Name of initial exploit - (Manual Exploitation)
- 10.1x.1.xx (hostname) - Name of initial exploit - (Manual Exploitation)
- 10.1x.1.xx (hostname) - Name of initial exploit
- 10.1x.1.xx (hostname) - Name of initial exploit
- 10.1x.1.xx (hostname) - Name of initial exploit
- 10.1x.1.xx (hostname) - Name of initial exploit
- 10.1x.1.xx (hostname) - Name of initial exploit
- 10.1x.1.xx (hostname) - Name of initial exploit
- 10.1x.1.xx (hostname) - Name of initial exploit
- 10.1x.1.xx (hostname) - Name of initial exploit

2.1 Recommendations

I recommend 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.

3 Methodologies

I utilized a widely adopted approach to performing penetration testing that is effective in testing how well the Virtual Hacking Labs environments is secured. Below is a breakout of how I 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, I was tasked with exploiting the exam network. The specific IP addresses were:

VirtualHackingLab's Advanced+ Network

- 10.1x.1.xx
- 10.1x.1.xx
- 10.1x.1.xx
- 10.1x.1.xx
- 10.1x.1.xx
- 10.1x.1.xx
- 10.1x.1.xx
- 10.1x.1.xx
- 10.1x.1.xx
- 10.1x.1.xx

3.2 Penetration

The penetration testing portions of the assessment focus heavily on gaining access to a variety of systems. During this penetration test, I was able to successfully gain access to **10** out of the **40** systems.

3.2.1 System IP: 10.1x.1.x (hostname) - Manual Exploitation

3.2.1.1 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
10.1x.1.x	**TCP**: 21,80,5466
	UDP: 53,161

Nmap Scan Results:

Initial Shell Vulnerability Exploited

Additional info about where the initial shell was acquired from

Vulnerability Explanation:

Vulnerability Fix:

Severity:

Proof of Concept Code Here:

3.2.1.2 Privilege Escalation

Additional Priv Esc info

Vulnerability Exploited:

Vulnerability Explanation:

Vulnerability Fix:

Severity:

Proof of Concept Code Here:

Key Screenshot Here:

Key.txt Contents:

3.2.2 System IP: 10.1x.1.x (hostname) - Manual Exploitation

3.2.2.1 Service Enumeration

Server IP Address	Ports Open
10.1x.1.x	**TCP**: 1433,3389 **UDP**: 1434,161

Nmap Scan Results:

Initial Shell Vulnerability Exploited

Additional info about where the initial shell was acquired from

Vulnerability Explanation:

Vulnerability Fix:

Severity:

Proof of Concept Code Here:

Local.txt Proof Screenshot

Local.txt Contents

3.2.2.2 Privilege Escalation

Additional Priv Esc info

Vulnerability Exploited:

Vulnerability Explanation:

Vulnerability Fix:

Severity:

Exploit Code:

Key Screenshot Here:

Key.txt Contents:

3.2.3 System IP: 10.1x.1.x (hostname)

3.2.3.1 Service Enumeration

Server IP Address	Ports Open
10.1x.1.x	**TCP**: 1433,3389 **UDP**: 1434,161

Nmap Scan Results:

Initial Shell Vulnerability Exploited

Additional info about where the initial shell was acquired from

Vulnerability Explanation:

Vulnerability Fix:

Severity:

Proof of Concept Code Here:

3.2.3.2 Privilege Escalation

Additional Priv Esc info

Vulnerability Exploited:

Vulnerability Explanation:

Vulnerability Fix:

Severity:

Exploit Code:

Key Screenshot Here:

Key.txt Contents:

3.2.4 System IP: 10.1x.1.x (hostname)

3.2.4.1 Service Enumeration

Server IP Address	Ports Open
1x.1x.1.x	**TCP**: 1433,3389
	UDP: 1434,161

Nmap Scan Results:

Initial Shell Vulnerability Exploited

Additional info about where the initial shell was acquired from

Vulnerability Explanation:

Vulnerability Fix:

Severity:

Proof of Concept Code Here:

3.2.4.2 Privilege Escalation

Additional Priv Esc info

Vulnerability Exploited:

Vulnerability Explanation:

Vulnerability Fix:

Severity:

Exploit Code:

Key Screenshot Here:

Key.txt Contents:

3.2.5 System IP: 10.1x.1.x (hostname)

3.2.5.1 Service Enumeration

Server IP Address	Ports Open
10.1x.1.x	**TCP**: 1433,3389
	UDP: 1434,161

Nmap Scan Results:

Initial Shell Vulnerability Exploited

Additional info about where the initial shell was acquired from

Vulnerability Explanation:

Vulnerability Fix:

Severity:

Proof of Concept Code Here:

3.2.5.2 Privilege Escalation

Additional Priv Esc info

Vulnerability Exploited:

Vulnerability Explanation:

Vulnerability Fix:

Severity:

Exploit Code:

Key Screenshot Here:

Key.txt Contents:

3.2.6 System IP: 10.1x.1.x (hostname)

3.2.6.1 Service Enumeration

Server IP Address	Ports Open
10.1x.1.x	**TCP**: 21,80,443,8080
	UDP: 53,161

Nmap Scan Results:

Initial Shell Vulnerability Exploited

Additional info about where the initial shell was acquired from

Vulnerability Explanation:

Vulnerability Fix:

Severity:

Proof of Concept Code Here:

3.2.6.2 Privilege Escalation

Additional Priv Esc info

Vulnerability Exploited:

Vulnerability Explanation:

Vulnerability Fix:

Severity:

Proof of Concept Code Here:

key Screenshot Here:

Key.txt Contents:

3.2.7 System IP: 10.1x.1.x (hostname)

3.2.7.1 Service Enumeration

Server IP Address	Ports Open
10.1x.1.x	**TCP**: 1433,3389
	UDP: 1434,161

Nmap Scan Results:

Initial Shell Vulnerability Exploited

Additional info about where the initial shell was acquired from

Vulnerability Explanation:

Vulnerability Fix:

Severity:

Proof of Concept Code Here:

Local.txt Proof Screenshot

Local.txt Contents

3.2.7.2 Privilege Escalation

Additional Priv Esc info

Vulnerability Exploited:

Vulnerability Explanation:

Vulnerability Fix:

Severity:

Exploit Code:

Key Screenshot Here:

Key.txt Contents:

3.2.8 System IP: 10.1x.1.x (hostname)

3.2.8.1 Service Enumeration

Server IP Address	Ports Open
10.1x.1.x	**TCP**: 1433,3389
	UDP: 1434,161

Nmap Scan Results:

Initial Shell Vulnerability Exploited

Additional info about where the initial shell was acquired from

Vulnerability Explanation:

Vulnerability Fix:

Severity:

Proof of Concept Code Here:

3.2.8.2 Privilege Escalation

Additional Priv Esc info

Vulnerability Exploited:

Vulnerability Explanation:

Vulnerability Fix:

Severity:

Exploit Code:

Key Screenshot Here:

Key.txt Contents:

3.2.9 System IP: 10.1x.1.x (hostname)

3.2.9.1 Service Enumeration

Server IP Address	Ports Open
1x.1x.1.x	**TCP**: 1433,3389
	UDP: 1434,161

Nmap Scan Results:

Initial Shell Vulnerability Exploited

Additional info about where the initial shell was acquired from

Vulnerability Explanation:

Vulnerability Fix:

Severity:

Proof of Concept Code Here:

3.2.9.2 Privilege Escalation

Additional Priv Esc info

Vulnerability Exploited:

Vulnerability Explanation:

Vulnerability Fix:

Severity:

Exploit Code:

Key Screenshot Here:

Key.txt Contents:

3.2.10 System IP: 10.1x.1.x (hostname)

3.2.10.1 Service Enumeration

Server IP Address	Ports Open
10.1x.1.x	**TCP**: 1433,3389
	UDP: 1434,161

Nmap Scan Results:

Initial Shell Vulnerability Exploited

Additional info about where the initial shell was acquired from

Vulnerability Explanation:

Vulnerability Fix:

Severity:

Proof of Concept Code Here:

3.2.10.2 Privilege Escalation

Additional Priv Esc info

Vulnerability Exploited:

Vulnerability Explanation:

Vulnerability Fix:

Severity:

Exploit Code:

Key Screenshot Here:

Key.txt Contents:

3.3 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.

3.4 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 organization's 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 collecting trophies from the exam network was completed, (user account if made) 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.

4 Additional Items

4.1 Appendix - Key.txt Contents:

IP (Hostname)	Key.txt Contents
10.1x.1.x	hash_here
10.1x.1.x	hash_here
10.1x.1.x	hash_here
10.1x.1.x	hash_here
10.1x.1.x	hash_here
10.1x.1.x	hash_here
10.1x.1.x	hash_here
10.1x.1.x	hash_here
10.1x.1.x	hash_here
10.1x.1.x	hash_here

4.2 Appendix - Manual Machines

Below is a list of the two machines I preformed manual exploition on. Following the Advanced+ guideline criteria outlined by VirtualHackingLabs.

- 10.1x.1.x - (What was exploited manually)
- 10.1x.1.x - (What was exploited manually)