**Focal X Company**

**Start Date:** 29/12/2026 – 01:00 PM

**End Date:** 01/08/2026 – 06:00 PM

# CyberX Penetration Testing Report

**By** : Judy Muhammad Darwish

## Table of Contents

## Introduction

This project aims to conduct a structured penetration test on the CyberX training system, following a methodology similar to real-world penetration testing. The objective is to analyze the system, identify open ports and services, determine the attack surface, and then proceed to exploitation and privilege escalation phases.

## Executive Summary

The goal of this assessment is to evaluate the security posture of the CyberX environment by analyzing its core services and reviewing the system configurations it relies on. The test revealed several critical vulnerabilities in FTP, SSH, and HTTP services, which allowed unauthorized access to the server and full system compromise.

A severe vulnerability in the ProFTPD service enabled remote command execution without authentication. Additionally, weak SSH credentials allowed administrative access. The WordPress installation was also insecure, exposing sensitive files and using simple passwords, which resulted in full control over the admin dashboard.

These findings indicate a lack of essential security updates, strong password policies, and proper access controls. If left unaddressed, these vulnerabilities could lead to full server compromise, data leakage, or the server being used as a pivot point for further attacks.

Immediate remediation, periodic updates, and improved access management are required to protect the environment from future risks.

## Scope

### In Scope

- CyberX virtual machine
- Open services on the target
- Port analysis (FTP, SSH, HTTP)
- Vulnerability testing
- Exploitation
- Post-exploitation

### Out of Scope

- Internal network outside VMware
- Denial of Service (DoS)
- Source code analysis
- External web applications

## Testing Environment

### Systems Used

- Kali Linux (Attacker)
- CyberX VM (Target)

### Network Setup

- Both systems running inside VMware
- NAT mode used to:
    - Ensure internal connectivity
    - Assign CyberX an IP via DHCP
    - Allow Kali to scan the target

### Target IP

Extracted from GUI:

- Interface: ens33
- IP Address: **192.168.159.135**

## Methodology

The penetration test followed industry standards, primarily:

- **PTES (Penetration Testing Execution Standard)**
- **OWASP WSTG (Web Security Testing Guide)** for web components, especially WordPress.

The methodology included:

1. Reconnaissance
2. Scanning
3. Enumeration
4. Vulnerability Analysis
5. Exploitation
6. Post-Exploitation
7. Reporting & Recommendations

## Scanning Phase

A full scan was performed on **192.168.159.135** using Nmap with version detection.

### Open Ports Identified

| Port | Service | Version |
|---|---|---|

| port | service | version |
|---|---|---|
| 21 | FTP | ProFTPD 1.3.3c |
| 22 | SSH | OpenSSH 7.2p2 |
| 80 | HTTP | Apache 2.4.18 |

Additional findings:

- SSH keys detected
- OS: Linux kernel 3.2–4.14
- MAC address indicates VMware
- Device type: General Purpose

## FTP Enumeration – Port 21

Anonymous login was tested but not allowed. The service version **ProFTPD 1.3.3c** is known to contain a **backdoor RCE vulnerability** due to a compromised source repository.

Using Metasploit, the module:

`exploit/unix/ftp/proftpd_133c_backdoor`

was identified and used to gain a **root shell** without authentication.

## Exploitation – ProFTPD Backdoor

A reverse shell was successfully obtained, granting:

- Remote command execution
- Full system control

- Root privileges

## Post-Exploitation – FTP

Actions performed:

- Identified current user
- Navigated directories
- Listed users
- Searched for flags
- No privilege escalation needed (already root)

## Risk – ProFTPD Backdoor

- Full remote code execution
- Complete system takeover
- Ability to install malware
- Data theft
- Service disruption
- Pivoting to internal network
- Hard to detect due to embedded backdoor

## Recommendations – ProFTPD

1. Disable the service immediately
2. Update to **ProFTPD 1.3.8+** or migrate to a secure FTP server (vsftpd, Pure-FTPd)

## SSH Enumeration – Port 22

OpenSSH 7.2p2 was identified. Weak password authentication was enabled.

## Exploitation

Two approaches were used:

### 1. Manual Guessing

Based on common training environments, the credentials:

- **username:** marlinspike
- **password:** marlinspike

were successful.

### 2. Hydra Brute Force

Hydra confirmed:

- Weak credentials
- No brute-force protection
- Unlimited login attempts

Privilege escalation to **root** was achieved using built-in commands.

## Post-Exploitation – SSH

Performed:

- System info collection
- User enumeration
- File system exploration
- Password hash extraction

- Network connection analysis

## Risk – Weak SSH Credentials

- Full system compromise
- Data theft
- Malware installation
- Internal attacks
- Service disruption
- Compliance violations
- Financial and reputational damage

## Recommendations – SSH

- Change all default passwords
- Disable root login
- Enforce strong password policies
- Regular account audits
- Monitor authentication logs
- User awareness training

## Apache/HTTP Enumeration – Port 80

Apache 2.4.41 detected. WordPress installation discovered.

## Weaknesses Identified

- Valid admin username
- No brute-force protection
- No CAPTCHA
- Password = **admin**

## Exploitation – WordPress

Using **admin/admin**, full dashboard access was obtained.

Capabilities:

- Manage users
- Modify themes/plugins
- Upload files
- Edit content
- Access system settings

SQL injection testing was attempted via custom code in `functions.php`.

## Risk – WordPress Weak Authentication

- Full website compromise
- Database theft
- Malware distribution
- Phishing attacks
- Privilege escalation to server
- Pivoting to other systems
- Ransomware potential

## Recommendations – WordPress

- Update WordPress immediately
- Change admin username
- Enforce strong passwords
- Monitor login attempts
- Regular backups

- Periodic security audits

## Vulnerabilities Identified

| # | Vulnerability | Service | Severity | OWASP |
|---|---|---|---|---|
| 1 | ProFTPD 1.3.3c Backdoor RCE | FTP | Critical | A03: Injection |
| 2 | Weak SSH Credentials | SSH | Critical | A07: Identification & Authentication |
| 3 | Weak WordPress Admin Authentication | HTTP | Critical | A07: Identification & Authentication |

## Security Risk Assessment

| # | Vulnerability | Severity | Ease of Exploitation | Impact | Login Required | User Interaction |
|---|---|---|---|---|---|---|
| 1 | ProFTPD Backdoor | Critical | Very Easy | Very High | No | No |
| 2 | Weak SSH Credentials | Critical | Very Easy | Very High | Yes | No |
| 3 | Weak WordPress Authentication | Critical | Very Easy | Very High | Yes (but trivial) | No |

## Tools Used

- Nmap
- Metasploit (ProFTPD Backdoor)
- Hydra (SSH brute force)
- FTP Client
- SSH Client
- Linux Commands
- WPScan
- curl
- Gobuster

## Conclusion

The CyberX environment contains multiple critical vulnerabilities that directly impact its overall security. Outdated services, weak credentials, and insecure configurations allowed full system compromise through multiple attack vectors.

Addressing these issues through updates, strong password policies, and improved service hardening is essential to enhance the security posture and reduce future risks.

**References:**


1. Penetration Testing Execution Standard (PTES)
2. OWASP Web Security Testing Guide (WSTG)
3. CVE Details Database (Common Vulnerabilities and Exposures)
4. Nmap Documentation
5. Metasploit Framework Documentation
6. Hydra Tool
7. WPScan Official Documentation