PENETRATION TESTING REPORT

Version 1.0

By *PAKIN PANAWATTANAKUL*

August 10, 2024

for Faculty of Engineering, Mahidol university, Thailand [3]

Engagement Details [1]
Contractor Company: Pentest Services, Inc.
Client Company: Faculty of Engineering, Mahidol University, Thailand
Contract Number: PSI20240801/001
Contract Date: Nov 15, 2023
Start Date: Dec 1, 2023
End Date: Dec 31, 2023

Document Details [1]
Document Title: Penetration Testing Report
Date: Jan 8, 2024
Ref No.: PSI20240801/001
Classification: {Public, **Internal**, Confidential, Highly Confidential}
Document Type: Report

Document History [1]
Date: Jan 8, 2024
Version: 1.0
Authors: Mr. PAKIN PANAWATTANAKUL
Comments: {**Initial Draft**, Review and Formatting, Final}

1. Executive Summary

Background

Pakin Panawattanakul was contracted by prof. Nopadol to perform a penetration testing on Mahidol university's network lab in order to determine the effectiveness of the implemented security measures. The test was agreed in the scope of the EGCI555 Penetration testing course. The fieldwork was completed between 30/6/2025, 8.00 AM. - 30/6/2025, 12.00AM.

Objectives

The objective of the penetration testing was to evaluate the current state of the target virtual machine in the scope from a security perspective and determine the risk of a successful attack by a hacker, malicious users on the internet, or bad students on Mahidol Salaya campus.

Scope

The following systems belonging to Mahidol university were in scope:

{Host/Network Address/URL}:	Devices in the network range of 172.28.128.0-172.28.128.255. Unknown VM host on the computer lab's computer
Start date/time:	June 30, 2025 / 10.00.00
Finish date/time:	June 30, 2025 / 12.00.00
Tests performed:	Host Discovery TCP Port Scanning Vulnerability Scanning HTTP Service Enumeration FTP Service Analysis Exploitation (ProFTPD 1.3.3c Backdoor) Post-Exploitation (Root Access & Hash Extraction)
Status:	Finished

Methodology

The penetration testing was performed in a "black box" manner, meaning that we did not have any prior information about the target systems. The only information given was the subnet of the target which is 172.28.128.0/24. Our tests simulated an external threat

(hacker, malicious user) located somewhere on the Internet who tried to find vulnerabilities in the target systems and exploit them in order to gain unauthorized access to sensitive information or affect the correct functionality of the systems.

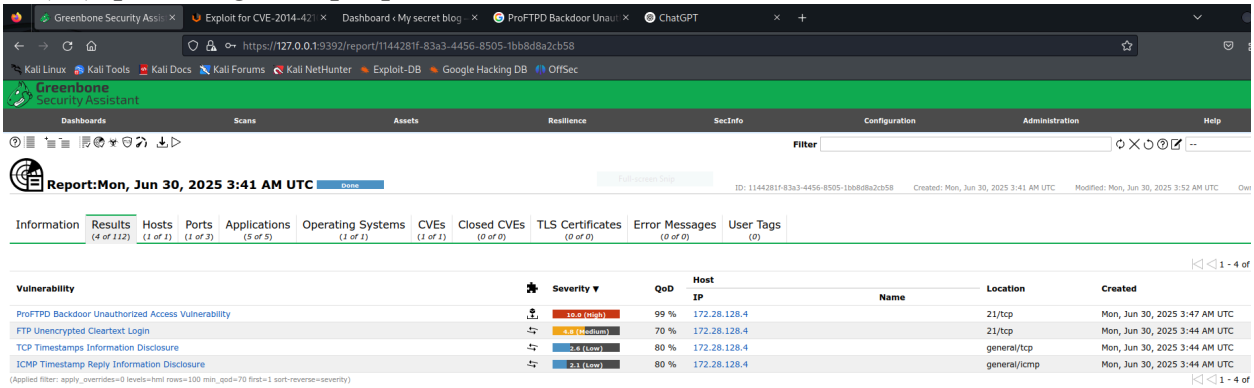
All of our tests were performed by combining our professional experience with well-known methodologies such as OWASP Top 10 and NIST 800-115.

The following tools were used in the penetration testing:

- Nmap Version 7.95
- Greenbone OpenVAS
- Metasploit Framework

Key Findings

- **Critical ProFTPD Vulnerabilities:** The target system, 172.28.128.4, is running an outdated and highly vulnerable version of ProFTPD (1.3.3c). This includes a critical backdoor (CVE-2010-4221) and a high-severity use-after-free vulnerability (CVE-2011-4130), both allowing remote code execution.
- **Cleartext FTP Credentials:** The FTP service on the target system transmits login credentials in cleartext, even for failed attempts. This allows for easy interception and compromise of user accounts through network sniffing.
- **Root-Level Compromise:** The identified ProFTPD backdoor was successfully exploited to gain a reverse shell, achieving root-level access on the target system.
- **Password Hash Exposure:** Following root access, password hashes were extracted from /etc/shadow, indicating a severe compromise of user authentication data.
- **Open Ports:** The target system has open ports for FTP (21), SSH (22), and HTTP (80), providing multiple potential attack vectors.



Recommendations

This penetration testing revealed several high risk vulnerabilities together with multiple medium and low risk issues. We recommend implementing the measures suggested for each finding in order to improve the security posture of the affected systems.

- Patch/Upgrade ProFTPD: Immediately upgrade the ProFTPD server to a version that is not vulnerable to the backdoor (e.g., 1.3.5rc1 or later). Alternatively, replace it with a secure, supported FTP solution.
- Enforce Secure FTP Protocols: Configure the FTP service to enforce the use of secure protocols such as FTPS (FTP over SSL/TLS) or SFTP (SSH File Transfer Protocol) to prevent cleartext transmission of credentials.
- Implement Strong Password Policies: Ensure all user accounts have strong, unique passwords and consider multi-factor authentication where possible.

2. List of tests performed

2.1 Host Discovery: Used Nmap (nmap -sn 172.28.128.0/24) to identify active hosts within the target network range, leading to the discovery of 172.28.128.4.
2.2 TCP Port Scanning: Performed a TCP port scan (nmap -p 1-65535 172.28.128.4) to identify open ports, revealing FTP (21), SSH (22), and HTTP (80).
2.3 Vulnerability Scanning: Utilized Greenbone OpenVAS to conduct automated vulnerability scans, which identified several severe vulnerabilities, including the ProFTPD 1.3.3c backdoor and FTP unencrypted cleartext login.
2.4 HTTP Enumerations to find command path of the website and found the /secret that contain the secret blog, and with a weak password policy allow people to login by just guessing.

2.5 FTP Service Analysis: Attempted direct connections to the FTP service on port 21 using the command-line ftp client. This confirmed the presence of ProFTPD 1.3.3c and the cleartext transmission of credentials during login attempts (even failed ones).
2.6 Exploitation (ProFTPD 1.3.3c Backdoor): Employed Metasploit Framework's exploit/unix/ftp/proftpd_133c_backdoor module with a reverse shell payload (cmd/unix/reverse_netcat) to gain a command shell on the target system.
2.7 Post-Exploitation (Root Access & Hash Extraction): Successfully confirmed root privileges on the compromised host and extracted password hashes from /etc/shadow for further analysis.

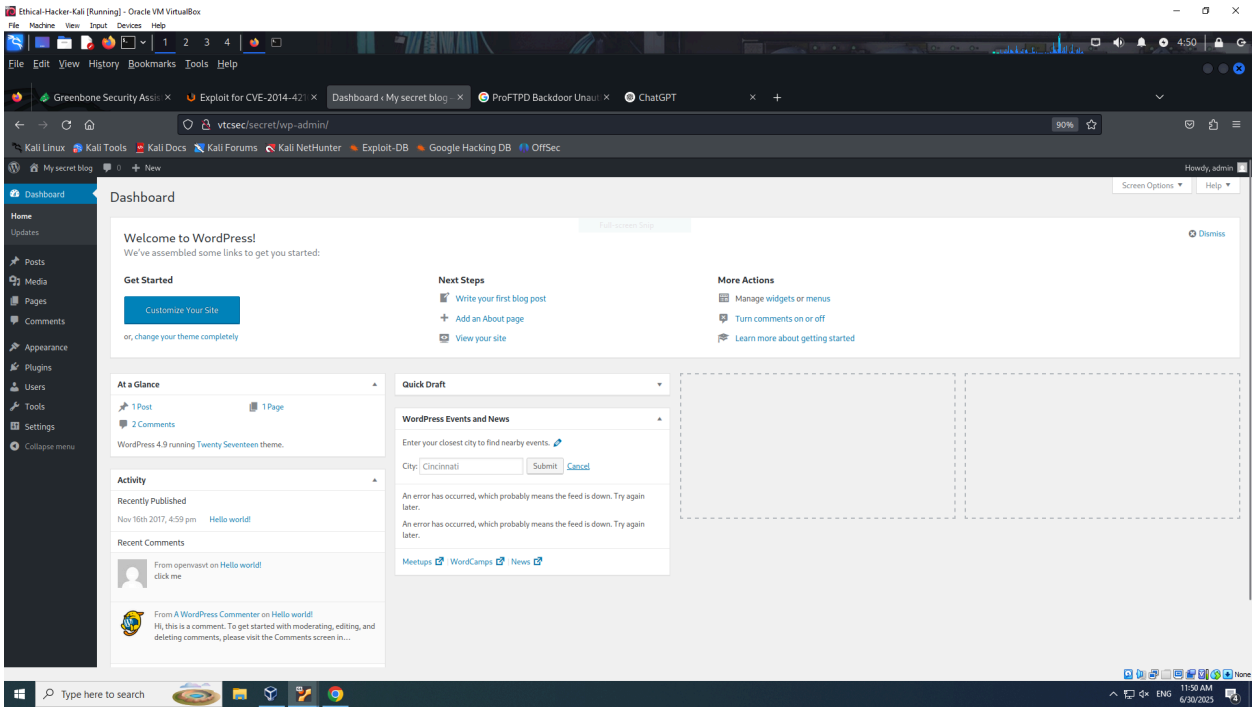
3. TECHNICAL FINDINGS

3.1 Server software and technology found

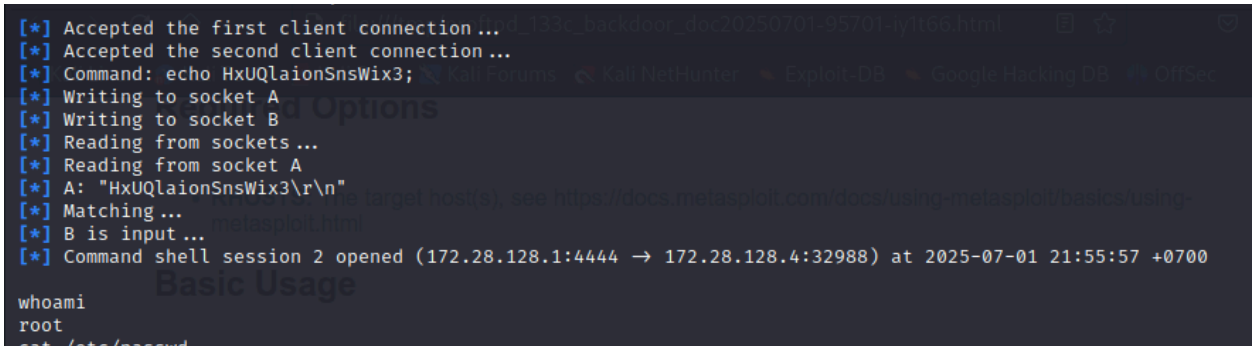
Software/Version	Category
ProFTPD 1.3.3c	Remote : Backdoor command execution
Canonical Ubuntu Linux 16.04	Operating Systems
OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)	Remote : Username Enumeration
Apache http 2.4.18 ((Ubuntu))	Web apps

3.2 Vulnerabilities found

A weak password policy on the /secret blog allowed for easy password guessing, potentially compromising administrative access to sensitive web content.



Using **Metasploit**, root access was gained on the server, enabling the extraction of user password hashes.



3.3 The table below summarizes the findings identified in this penetration testing:

Risk Level	CVSS	CVE/CWE	Summary	Exploit	Affected Software
	10.0	***CVE-2010-4221***	*Multiple buffer overflows in ProFTPD (versions before 1.3.3c) allow remote code execution via a crafted TELNET IAC escape character to FTP/FTPS.*	https://www.exploit-db.com/exploits/16851	*ProFTPD 1.3.3c*
	9.0	*Multiple buffer overflows in ProFTPD (versions before 1.3.3c) allow remote code execution via a crafted TELNET IAC escape character to FTP/FTPS.*	*Multiple buffer overflows in ProFTPD (versions before 1.3.3c) allow remote code execution via a crafted TELNET IAC escape character to FTP/FTPS.*	N/A	*ProFTPD 1.3.3c*
	6.8	*CVE-2010-4652*	Heap-based buffer overflow in ProFTPD (versions before 1.3.3d) when mod_sql is enabled allows remote attackers to cause denial of service or execute code via a crafted username.	*N/A*	*ProFTPD 1.3.3c*

	5.0	*CVE-2011-1137*	*Integer overflow in the mod_sftp (aka SFTP) module in ProFTPD 1.3.3d and earlier allows remote attackers to cause a denial of service (memory consumption leading to OOM kill) via a malformed SSH message.*	*https://www.exploit-db.com/exploits/16921*	*ProFTPD 1.3.3c*
	4.8	*FTP Unencrypted Cleartext login*	*The remote host is running a FTP service that allows cleartext logins over unencrypted connections.*	*Can be exploited using network sniffing tools (e.g. Wireshark, tcpdump) to capture FTP credentials sent in plaintext https://wiki.wireshark.org/FTP*	*FTP*
	2.1	*CVE-1999-0524*	*ICMP information such as (1) netmask and (2) timestamp is allowed from arbitrary hosts.*	*N/A*	*ICMP*
	1.2	*CVE-2012-6095*	*ProFTPD before 1.3.5rc1, when using the UserOwner directive, allows local users to modify the ownership of arbitrary files via a race condition and a symlink attack on the (1) MKD or (2) XMKD commands.*	*N/A*	*ProFTPD 1.3.3c*

3.4 Graphical Summary

This is a visual representation of overall risk level:

Overall risk level: ($Overall\ Risk = \frac{\sum_{i=0}^{n}(CVSS)}{n}$)

High Medium Low

Risk ratings: (Risk = CVSS)

High : 2

Medium : 3

Low : 2

3.5 Details of each vulnerability

1. **CVE-2010-4221 (CVSS 10.0 - Critical)**: This critical vulnerability in ProFTPD (versions before 1.3.3c) involves multiple stack-based buffer overflows within the pr_netio_telnet_gets function. A remote attacker can exploit this by sending a specially crafted TELNET IAC escape character, leading directly to arbitrary code execution on the server. This allows for complete system compromise and control.
2. **Unspecified CVE (CVSS 9.0 - High):** Likely referring to CVE-2011-4130, a high-severity use-after-free vulnerability affecting ProFTPD versions before 1.3.3g. This flaw allows remote authenticated users to execute arbitrary code. The exploitation typically occurs via specific errors that arise after an FTP data transfer, making it a post-authentication attack vector.
3. **CVE-2010-4652 (CVSS 6.8 - Medium):** A heap-based buffer overflow exists in ProFTPD (versions before 1.3.3d) when the mod_sql module is enabled. Remote attackers can trigger this by providing a crafted username containing unhandled substitution tags, which are then processed incorrectly during SQL query construction. This can lead to a denial of service (server crash) and potentially arbitrary code execution.
4. **CVE-2011-1137 (CVSS 5.0 - Medium):** An integer overflow vulnerability is present in the mod_sftp module of ProFTPD 1.3.3d and earlier. By sending a malformed SSH message, a remote attacker can cause this overflow. The result is excessive memory consumption, which often leads to the operating system's Out-Of-Memory (OOM) killer terminating the ProFTPD process, effectively causing a denial of service.
5. **FTP Unencrypted Cleartext Login (CVSS 4.8 - Medium):** The remote FTP service transmits user credentials (username and password) in plaintext over unencrypted connections. This fundamental security weakness means that any attacker with network access can easily capture these sensitive credentials using readily available network sniffing tools like Wireshark or tcpdump, leading to unauthorized access to FTP accounts.
6. **CVE-1999-0524 (CVSS 2.1 - Low):** This ICMP information disclosure vulnerability allows any arbitrary host to request and receive specific network details, including netmask and timestamp information. While not a direct exploit for system access, this leakage provides valuable data for attackers during their reconnaissance phase, helping them map the network topology and ascertain system uptime for more targeted attacks.
7. **CVE-2012-6095 (CVSS 1.2 - Low):** ProFTPD versions before 1.3.5rc1, when configured with the UserOwner directive, are vulnerable to a local privilege escalation. This involves a race condition and symbolic link (symlink) attack

during MKD or XMKD commands. A local attacker can exploit this timing window to modify the ownership of arbitrary files on the system, potentially gaining control over critical files.

4. CONCLUSION

This penetration test successfully identified critical security deficiencies within the Mahidol University network lab's target system (172.28.128.4). The exploitation of outdated **ProFTPD vulnerabilities** led to a complete **root-level compromise** of the Linux host, allowing for the **extraction of user password hashes** from /etc/shadow. Furthermore, the presence of an **unencrypted FTP service** poses an immediate risk of cleartext credential interception, and a **weak password policy** on the /secret web blog presented another easy access point via guessing. These findings collectively highlight a significant and immediate security risk, demonstrating that the system is vulnerable to unauthorized access, data compromise, and potential service disruption. Prompt and comprehensive remediation, as outlined in the recommendations, is crucial to address these high-impact vulnerabilities and enhance the overall security posture of the network lab.

5. APPENDICES

5.1 Appendix A – Finding Risk Level

Each finding has been assigned a risk level of high, medium, and low. The level is based on an assessment of the priority with which each finding should be viewed and the potential impact each has on the confidentiality, integrity, and availability of client's data (Impact).

Risk Level	Definition
High	Exploitation of the technical or procedural vulnerability will cause substantial harm. Significant political, financial, and/or legal damage is likely to result. The threat exposure is high, thereby increasing the likelihood of occurrence. Security controls are not effectively implemented to reduce the severity of impact if the vulnerability were exploited.
Medium	Exploitation of the technical or procedural vulnerability will significantly impact the confidentiality, integrity, and/or availability of the system, application, or data. Exploitation of the vulnerability may cause moderate financial loss or public embarrassment. The threat exposure is moderate-to-high, thereby increasing the likelihood of occurrence. Security controls are in place to contain the severity of impact if the vulnerability were exploited, such that further political, financial, or legal damage will not

	occur. The vulnerability is such that it would otherwise be considered High Risk, but the threat exposure is so limited that the likelihood of occurrence is minimal.
Low	Exploitation of the technical or procedural vulnerability will cause minimal impact to operations. The Confidentiality, Integrity and Availability (CIA) of sensitive information are not at risk of compromise. Exploitation of the vulnerability may cause slight financial loss or public embarrassment. The threat exposure is moderate-to-low. Security controls are in place to contain the severity of impact if the vulnerability were exploited, such that further political, financial, or legal damage will not occur. The vulnerability is such that it would otherwise be considered Medium Risk, but the threat exposure is so limited that the likelihood of occurrence is minimal.