



Penetration Test Report of Findings

Academy VM Box.

November 20, 2024

Whisperer256

OFFENSESECURITY CONFIDENTIAL

No part of this document may be disclosed to outside sources without the explicit written authorization of OffenSecurity

Table of Contents

Statement of Confidentiality	3
Engagement Contacts.....	4
Executive Summary	5
Approach	5
Scope.....	5
Assessments Overview and Recommendations	5
Network Penetration Test Assessment Summary	7
Summary of Findings.....	7
Internal Network Compromise Walkthrough	8
Detailed Walkthrough	8
Detailed reproduction steps for this attack are as follow:	9
Remediation Summary.....	12
Short Term	12
Medium Term	12
Long Term	12

Statement of Confidentiality

The contents of this document have been developed by OffenSecurity. OffenSecurity and Academy considers the contents of this document to be proprietary and business confidential information. This information is to be used only as a practical, fictional and educational purpose. This document may be released to another vendor, business partner or contractor, with the GNU Open Source License. Additionally, any portion of this document could be communicated, reproduced, copied or distributed without the prior consent of OffenSecurity.

The contents of this document do not constitute legal advice. OffenSecurity's offer of services that relate to compliance, litigation or other legal interests are not intended as legal counsel and should not be taken as such. The assessment detailed herein ("Academy VM Box." from TCM Academy) against a fictional company for training and examination purposes, and the vulnerabilities in no way affect TCM Academy external or internal infrastructure.

Engagement Contacts

Academy VM Box Contacts		
Primary Contact	Title	Primary Contact Email
John Doe	Chief Executive Officer	john@academy.vmbox
Secondary Contact	Title	Secondary Contact Email
Bob Lee Swagger	Chief Technical Officer	bob@academy.vmbox

Assessor Contacts		
Assessor Name	Title	Assessor Contact Email
OffenSecurity	Security Consultant Company	notexistyet@offensecurity.local
Whisperer256	Junior Penetration Tester	whisperer256@protonmail.com

Executive Summary

Academy VM Box ("Academy" herein) contracted OffenSecurity to perform a Network Penetration Test of Academy's Internally facing network to identify security weaknesses, determine the impact to Academy, document all findings in a clear and repeatable manner, and provide remediation recommendations.

Approach

OffenSecurity performed testing under a "Black Box" approach November 11 2024, to November 15 2024 without credentials or any advance knowledge of Academy's internally facing environment with the goal to identify unknown weaknesses. Testing was performed from a non-evasive standpoint with the goal of uncovering as many misconfigurations and vulnerabilities as possible. Testing was performed locally specifically for this assessment. Each weakness identified was documented and manually investigated to determine exploitation possibilities and escalation potential. OffenSecurity sought to demonstrate the full impact of every vulnerability, up to and including privilege compromise. If OffenSecurity were able to gain a foothold in the internal network, any other human with the same knowledge can gain a foothold on the network too and that is the impact of an internal network compromise.

Scope

The scope of this assessment was one internal IP Address.

In-Scope Assets

Host/URL/IP Address	Description
172.16.76.128/24	Academy Internal IP Address

Table 1: Scope Details.

Assessments Overview and Recommendations

During the internal penetration test against Academy, OffenSecurity identified six (6) findings that threaten the confidentiality, integrity, and availability of Academy's information systems. The findings were categorized by severity level, with four (4) of the findings being assigned a high-risk rating, two (2) medium-risk. There was also one (1) informational finding related to enhancing security monitoring capabilities within the internal network.

The tester found Academy's patch and vulnerability management to be well-maintained. None of the findings in this report were related to missing operating system or third-party patches of known vulnerabilities in services and applications that could result in unauthorized access and system compromise. Each flaw discovered during testing was related to a misconfiguration or lack of hardening, with most falling under the categories of weak authentication and weak authorization.

The tester also found file sharing service with excessive permissions, meaning that any user in the internal network can access a considerable amount of data. While sharing files internally between departments and users is important to day-to-day business operations, wide open permissions on file shares may result in unintentional disclosure of confidential information. Even if a file share does not contain any sensitive information today, someone may unwittingly put such data there thinking it is

protected when it isn't. This configuration should be changed to ensure that only certain authorized users can access what is necessary to perform their day-to-day duties.

The next issue is an Unprotected web directory that discloses database information, including the CMS admin credential. Allowing possibility to gain administrative privilege inside the CMS. Academy should begin formulating a plan to properly configure the service.

The next issue is an Unrestricted file upload involving possibility to authenticated user to upload any type of file on the server. Malicious user could use a well-crafted file to take over the system. Academy should remediate this by restricting the type of file being uploaded using a whitelist to control the uploading file format.

Academy should create a remediation plan based on the Remediation Summary section of this report, addressing all high findings as soon as possible according to the needs of the business. Academy should also consider performing periodic vulnerability assessments, if they are not already being performed. Once the issues identified in this report have been addressed, a more collaborative, in-depth security assessment may help identify additional vulnerabilities, making it more difficult for attackers to move around the network and increasing the likelihood that Academy will be able to detect and respond to suspicious activity.

Network Penetration Test Assessment Summary

OffenSecurity began all testing activities from the perspective of an unauthenticated user on the internal network. Academy provided the tester an IP Address but did not provide additional information such as operating system or configuration information.

Summary of Findings

During the course of testing, OffenSecurity uncovered a total of five (6) findings that pose a material risk to Academy's information systems. OffenSecurity also identified one informational finding that, if addressed, could further strengthen Academy's overall security posture. Informational findings are observations for areas of improvement by the organization and do not represent security vulnerabilities on their own. The below table provides a summary of the findings by severity level.

Finding Severity		
High	Medium	Total
4	2	6

Table 2: Severity Summary.

Below is a high-level overview of each finding identified during testing.

Finding #	Severity Level	Finding Name
1.	High	Weak Password Policy
2.	High	Unrestricted File Upload
3.	High	Password Re-used
4.	High	SQL Injection
5.	Medium	FTP Anonymous Login
6.	Medium	Unprotected Web Directories
7.	Info	Enhance Security Monitoring Capabilities

Table 3: List of Finding.

Internal Network Compromise Walkthrough

During the course of the assessment, OffenSecurity was able to gain a foothold and compromise the Academy host. The steps below demonstrate steps taken from initial access, to full-compromise and does not include all vulnerabilities and misconfigurations discovered during the course of testing. The intent of this attack is to demonstrate to Academy the impact of each vulnerability shown in this report and how they fit together to demonstrate the overall risk of the client environment and help to prioritize remediation efforts (i.e., patching two flaws quickly could break up the attack chain while the company walk to remediate all issues reported). While other findings shown in this report could be leverage to gain a similar level of access, this attack chain shows the initial path taken by the tester to achieve the compromise.

Detailed Walkthrough

OffenSecurity performed the following to fully compromise the Academy host.

1. The tester uses a network mapper tool ([Nmap](#)) to identify useful information of opened ports. Revealing 21,22,80 ports in the process and some juicy information.
2. Using the FTP tool, the tester obtains a text file message of two users **Heath**, **Grimmie**, and **Jdelta**. Including a credential to log into the Academy CMS.
3. Using the web fuzzing tool ([dirbuster](#)) the tester found a database file containing admin credential of the Academy CMS.
4. The tester uses the previously gained credentials (i.e. user and admin credential of the CMS) to successfully log into the Academy CMS, using both credentials.
5. After a successful login and exploring the CMS, the tester finds a potential unrestricted file upload mechanism, where he could upload any file format to set a profile picture.
6. The tester gains a reverse shell to the system, by uploading and executed a well-crafted malicious file.
7. The tester then ran the [Linpeas.sh](#), a bash version of the popular privilege escalation collection script to enumerate the host and create a visual representation of the system to identify all of the possible privilege escalation paths. Upon review, the tester found that the **Grimmie** user uses a password to access the PHPMyAdmin panel.
8. After accessing the PHPMyAdmin panel using the previously found password, the tester gains access via SSH to **Grimmie** account by re-using the password.
9. Inside **Grimmie** account, the tester found an automatic process running every minute by the user root related to a file that **Grimmie** has file permission on.
10. Knowing that this file is executed by root, every minute, and **Grimmie** has full permission to, and that the tester gains access to **Grimmie** account. The tester uses the file to implement a command giving the tester higher privilege i.e. root.

Detailed reproduction steps for this attack are as follow:

Upon connecting to the network and after revealing the opened port, the tester starts the FTP tool and was able to anonymously log into the file transfer.

```
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 1000    1000          776 May 30   2021 note.txt
226 Directory send OK.
ftp> █
```

Figure 1: Anonymously log into the file sharing.

And the tester gets the file inside the file transfer, containing credential to log into the Academy CMS.

```
I couldn't create a user via the admin panel, so instead I inserted directly
into the database with the following command:

INSERT INTO `students` (`StudentRegno`, `studentPhoto`, `password`,
`studentName`, `pincode`, `session`, `department`, `semester`, `cgpa`,
`creationdate`, `updationDate`) VALUES
('10201321', '', 'cd73502828457d15655bbd7a63fb0bc8', 'Rum Ham', '777777', ''
, '', '7.60', '2021-05-29 14:36:56', '');

The StudentRegno number is what you use for login.
```

Figure 2: Getting the file note.txt into the Anonymous file transfer.

The tester proceeds to crack the hash value of the password, to reveal its value, which is “student”.

Using the web fuzzing tool (dirbuster) the tester found a database file containing admin credential of the Academy CMS.

department.php	302
session.php	302
includes	200
db	200
onlinecourse.sql	200
logout.php	200
phpmyadmin	200

Figure 3: Getting the file note.txt into the Anonymous file transfer.

Inside the *onlinecourse.sql* database file, contains admin credential of the Academy CMS. The tester proceeds to crack the hash value of the password, to reveal its value, which is “admin”.

```
INSERT INTO `admin` (`id`, `username`, `password`, `creationDate`,  
(1, 'admin', '21232f297a57a5a743894a0e4a801fc3', '2020-01-24 16:21:
```

Figure 4: Academy CMS credential.

Once inside the Academy CMS, the tester finds a vulnerable file upload mechanism, that can lead the tester to fully take over the system.

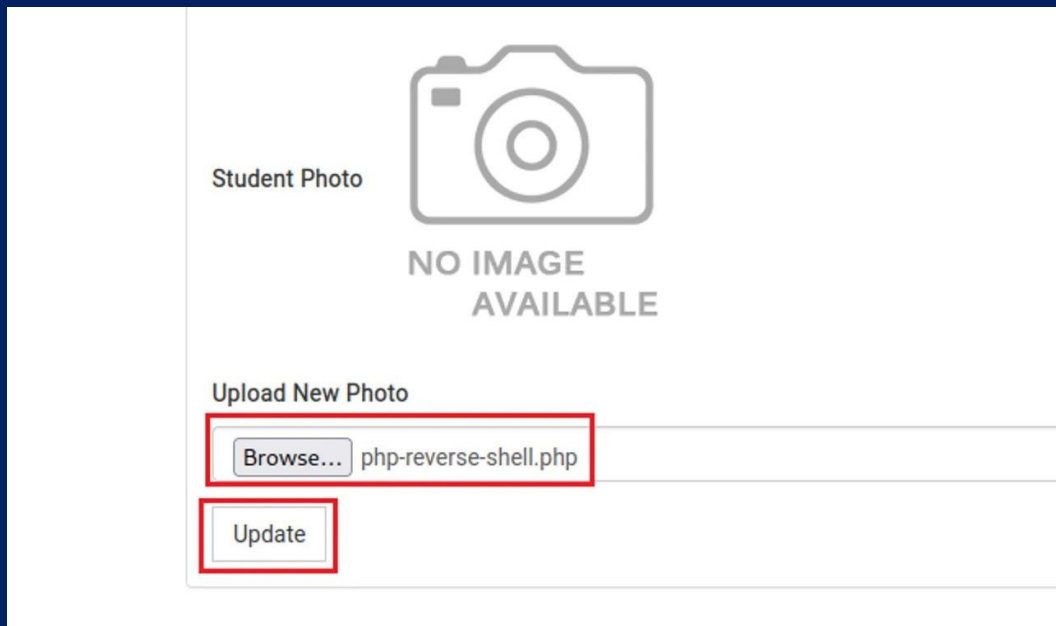


Figure 5: The tester proceeds to exploit the unrestricted file upload.

```
www-data@academy:/$ id  
uid=33(www-data) gid=33(www-data) groups=33(www-data)  
www-data@academy:/$ hostname  
academy  
www-data@academy:/$
```

Figure 6: Reverse shell of the system.

By running a Linpeas.sh on the system (a bash version of the popular privilege escalation collection script) to enumerate the system, the tester found that the user Gimmie re-use a password.

```
[+] Searching passwords in config PHP files
$mysql_password = 'My_V3ryS3cur3_P4ss';
$mysql_password = "My_V3ryS3cur3_P4ss";
```

Figure 7: Re-use password for Gimmie account and PHPMYAdmin.

```
grimmie@academy:~$ id
uid=1000(grimmie) gid=1000(administrator) groups=1000(administrator),24(cdrom)
grimmie@academy:~$ hostname
academy
grimmie@academy:~$
```

Figure 8: First privilege escalation of the tester.

The tester identified that the root user executing a process of a file every minute that grimmie have write permission on.

2022/08/13	23:07:35	CMD: UID=0	PID=1	/sbin/init
2022/08/13	23:08:01	CMD: UID=0	PID=13442	/usr/sbin/CRON -f
2022/08/13	23:08:01	CMD: UID=0	PID=13443	/usr/sbin/CRON -f
2022/08/13	23:08:01	CMD: UID=0	PID=13444	/bin/sh -c /home/grimmie/backup.sh
2022/08/13	23:08:01	CMD: UID=0	PID=13445	/bin/bash /home/grimmie/backup.sh
2022/08/13	23:08:01	CMD: UID=0	PID=13446	/bin/bash /home/grimmie/backup.sh
2022/08/13	23:08:01	CMD: UID=0	PID=13449	/bin/bash /home/grimmie/backup.sh
2022/08/13	23:08:01	CMD: UID=0	PID=13448	/bin/bash /home/grimmie/backup.sh
2022/08/13	23:08:01	CMD: UID=0	PID=13447	/bin/bash /home/grimmie/backup.sh

Figure 9: Identification of process runs by root.

The tester finally has access to the highest privilege on the system, by exploiting the execution of the automated process.

```
root@academy:~# id
uid=0(root) gid=0(root) groups=0(root)
root@academy:~# hostname
academy
root@academy:~#
```

Figure 10: The tester fully escalates his privilege by having root shell.

Remediation Summary

As a result of this assessment there are several opportunities for Academy to strengthen its internal network security. Remediation efforts are prioritized below starting with those that will likely take the least amount of time and effort to complete. Academy should ensure that all remediation steps and mitigating controls are carefully planned and tested to prevent any service disruptions or loss of data.

Short Term

- **[Finding 1]** – Set strong (24+ character) passwords on all accounts.
- **[Finding 6]** – Disable Directory Listing on the affected web server.
- **[Finding 1]** – Enforce a password change for all users because of the compromise.

Medium Term

- **[Finding 1]** – Enhance the host password policy.
- **[Finding 5]** – Perform a network file transfer audit.
- **[Finding 7]** – Enhance network logging and monitoring.
- **[Finding 7]** – Implement an enterprise endpoint detection & response solution.

Long Term

- **[Finding 2]** – Educate systems and network administrators and developers on security hardening best practice.
- Perform ongoing internal network vulnerability assessments and password audits.
- Perform periodic security assessments.
- Enhance network segmentation to isolate critical hosts and limit the effects of an internal compromise.