Security Assessment

Rules of Engagement

Objective:

You have been tasked to perform a penetration test against The Pasta Mentors ("TPM"), by your employer, TCM Security, Inc. ("TCMS"). The intent of this document is to clearly define the roles and responsibilities and the details of the test agreement.

Roles and Responsibilities:

Penetration Testing Team
The penetration team is made up of TCMS and TPM team members.

TPM
The penetration test needs to be unannounced to provide maximum benefit to TPM. However, there is a need for TPM interaction at some level. The following describes the general guidelines, roles and responsibilities for TPM.

The TPM team is responsible to observe and document responses to intrusion attempts by the TCMS team. They will serve as the last escalation point for TCMS intrusion 'incidents', preventing law-enforcement involvement. In addition to these general guidelines, the following roles are assigned:

Client Point of Contact (CPOC)/Exam Point of Contact (EPOC)
The CPOC will be primarily responsible for coordination with the penetration team. This person will have the ability to verify suspicious activities with the TCMS team to differentiate between testing and coincidental real-world hacking attempts.

CPOC Name:	Alessandra Fettuccini
CPOC Position:	Owner & Executive Trainer

Should you encounter any issues during your exam, please reach out to support@tcm-sec.com.

TCMS
The TCMS team will be responsible for the actual testing activities. Each member will be covered by the non-disclosure agreement between TCMS and TPM. The team will document all assessment activities, successes, and failures.

Rules of Engagement:

Test Dates

You will have **five** (5) days (120 hours) from the exam start time to complete your testing.

You will have an additional **two** (2) days (48 hours) beyond the testing period to provide a written report.

Penetration Test in Scope

The following IPs and scope will be assessed during testing:

- OSINT on TPM, including https://thepastamentors.com
- External Pentest: 10.10.155.0/24
- Internal Pentest: 10.10.10.0/24
- Changing account passwords, as needed.

Out of Scope

The following items are not in scope for this assessment

- Denial of Service (DoS) attacks against production infrastructure
- Phishing / Social Engineering attacks
- Attacks against the https://thepastamentors.com website or any other ***public*** facing infrastructure. Active and passive reconnaissance is permitted.

Note: Going out of scope will result in the immediate termination of your exam environment and disqualification from your exam attempt. Please stay in scope.

Environment Resets & Assistance

You will be permitted up to **two** (2) exam resets during your testing window. Resets due to environment errors on the behalf of TCMS will not be counted against this total. Reset requests are performed in the order that they are received. Please do not submit multiple requests to reset an environment. To request a reset, please email support@tcm-sec.com.

The TCMS Staff will **not** provide any hints during the exam window.

Stop Point

The penetration team will stop testing at the end of business on the last day of authorized testing or as soon as all testing has been completed. Should you complete your exam early and no longer need the environment, please notify us at support@tcm-sec.com.

Exam Deliverables:
The following items **must** be completed to earn a passing grade on the exam:

1) Penetration test leading to the full compromise of the TPM domain controller.

2) Professionally written report outlining your findings. Your findings **MUST** include screenshots and remediations for **ALL** steps to compromise and/or additional findings as well a method of maintaining access after domain compromise. Failure to include these items can lead to a failure of your exam.

3) A sample report can be found here and a video on report writing can be found here and here. A report template can be found here, however you are welcome to use your own template as long as it is professionally written. The exam report must be delivered to support@tcm-sec.com and **MUST** be in PDF format. Any other format types, such as *docx* and *zip*, will not be opened.

4) Complete a 15 minute debrief to the TPM security team with the results of your findings. A debrief will only be scheduled if you pass the written portion of your exam.

Academic Honesty Policy:
As a reiteration of the Terms and Conditions agreed to upon the purchase of your exam voucher, you agree that:

1) You will not disclose, publish, reproduce, transmit, or make available, in part or in full, any portion of the examination environment or course materials by any means, to include, but not limited to, voice, electronic, cryptological, mechanical, etc., without the expressed written consent of TCM Security Academy.

2) You are the person who is taking the PNPT exam and agrees that at no time will you solicit assistance from others during your exam attempt.

Failure to adhere to the agreed Terms and Conditions may result in, at a minimum, the termination of your exam environment. Please carefully review the full Terms and Conditions and contact help@tcm-sec.com if you have any questions.

Exam Tips:
- Any brute force attempts can be done with the Fast Track wordlist.
- Any password cracking attempts can be done with rockyou.txt.
- Keep it simple. Treat your environment as a practical engagement and not a CTF.
- Have fun and do not stress. Ensure you take breaks, eat, sleep, and stay hydrated!