



## Syllabus

### ***Heorot Intermediate Penetration Testing course***

Welcome to the Heorot Intermediate Penetration Testing (HIPT) course, presented by Heorot.net. This course is designed to teach you advanced techniques within Penetration Testing, and how to conduct your own penetration test using the Open Source Security Testing Methodology Manual (OSSTMM). This course is a mixture of online lecture, and hands-on use of the tools and methods detailed in the lecture. Since this is an online class, there will undoubtedly be questions not answered in the material. Access to the instructor is available throughout your access to this course, so please don't hesitate to use the contact information available on this site.

The first few days involve setting up your lab, obtaining the required course material, watching the online material, and performing hands-on exercises to familiarize you with the various steps involved in the OSSTMM and the tools used throughout this course. The last two days are intended for you to concentrate on conducting your own Penetration Test Effort (PTE). However, you will have access to this lab for 60 days, starting the day of enrollment. You have 90 days to submit your final PTE documentation for course completion.

Because this course is geared towards those already familiar with many of the tools used within a penetration test, this course does not provide detailed instruction into use of tools. However, we do mention tools that are useful in each step of the methodology, so that students have some frame of reference to use when conducting their own pentest. For those students who are unfamiliar with the use and selection of tools to use, it is suggested they enroll in the Heorot.net Penetration Testing Fundamentals course. Remember - the purpose of this course is to teach you the methodology behind penetration testing so you may conduct your own PenTest efforts.

## Table of Contents

Course Structure.....	2
Course Schedule.....	2
Day One.....	2
Day Two.....	3
Day Three.....	3
Day Four.....	4
Day Five.....	4
Required Material .....	5
Online Course.....	5
Course Certificate of Completion.....	5
About the Online Material .....	5
Video Presentations.....	5
Hands-On Exercises.....	5
Certificate of Completion.....	6
Formal Penetration Test Document .....	6
Completed Templates .....	6
Contact Information.....	7

## Course Structure

This course is self-guided, meaning that you can take the course at your own personal pace. We present a suggested time frame in which to cover all the material within a one-week period, but you can extend this to within the limits of the course access of 60 days.

The course has been designed to break activities into 8-hour blocks, which includes lecture, demonstrations, hands-on exercises, and reading assignments. The hands-on exercises and reading assignments build on previous modules, which are then used in later modules. Therefore, it is ***strongly*** suggested that all exercises and assignments be completed before moving on to the next module.

Links to the steps, lectures, and exercises listed in this syllabus can be found within the wiki, located at the training site provided to you upon enrollment. Once you have obtained access to the course, you will find this syllabus with links and detailed instructions to proceed through the class.

# Course Schedule

## Day One

- Create your Penetration Test Lab
  - Choose either a physical lab setup or virtual lab
  - Obtain necessary LiveCDs
- Obtain OSSTMM methodology
- Module 1 - Introduction
  - Video Presentation
  - Powerpoint Slide
- Module 2A - Penetration Testing Methodologies
  - Video Presentation
  - Powerpoint Slide
- Module 2B - Penetration Testing Methodologies Continued
  - Video Presentation
  - Powerpoint Slide
- **Required Reading:**
  - OSSTMM Methodology
    - pages 1-43
    - pages 87 - 129 (just familiarize yourself with them)

## Day Two

- Module 3 - Network Packet Crafting
  - Video Presentation
  - Powerpoint Slide
- Module 4 - Password Cracking
  - Video Presentation
  - Powerpoint Slide
- Module 5 - Reviewing Code for Exploits
  - Video Presentation
  - Powerpoint Slide
- **Required Reading:**
- Methodology
  - OSSTMM Methodology - pages 65-68
    - Packet Crafting:
      - "Packet Crafting for Firewall & IDS Audits (Part 1 of 2)"
      - "Packet Crafting for Firewall & IDS Audits (Part 2 of 2)"
    - Password Cracking
      - Documentation for "John the Ripper". Sections that are "must reads":
        - CONFIG - especially useful to change wordlists
        - MODES - learn why to stay away from "INCREMENTAL" (evil)
        - OPTIONS
    - Cryptographic Hashes
      - SHA hash functions
      - MD5 hash
      - Rainbow Tables
    - Reviewing Code for Exploits
      - "A Process for Performing Security Code Reviews" - Michael Howard
- Optional Work:
  - Hands On Exercises

## **Day Three**

- Module 6 - Documenting your Penetration Test
  - Video Presentation
  - Powerpoint Slide
- OSSTMM Internet Technology Modules (Video Presentations)
  - Network Surveying
  - Port Scanning
  - Services Identification
  - System Identification
  - Vulnerability Research and Verification
  - Internet Application Testing
  - Trusted System Testing
- Required Reading:
  - OSSTMM Methodology - pages 49-65
- Optional Work:
  - Hands On Exercises

## **Day Four**

- Create Outline of your own Penetration Test Effort document to submit for course completion
  - Understand the format requirements for your PTE final document
  - Download the Penetration Test Effort templates
  - Integrate provided Scope Statement
  - Integrate provided Gathered Information
- Perform attacks against disk 2.101
- Perform attacks against disk 2.102 (This disk will not be visible to you initially - to attack it, you will need to use disk 2.101 as a pivot)
  - NOTE: It will be tempting to modify your BackTrack IP address to attack Disk 2.102, but this should be avoided at all costs, so you can demonstrate your understanding of "Trusted System Testing"

## ***Day Five***

- Exploit disk 2.101 using discovered vulnerabilities and/or misconfigurations
- Perform attacks from disk 2.102 using system 2.101 as a pivot
- Exploit disk 2.102 using discovered vulnerabilities and/or misconfigurations
- Integrate findings into your PTE documentation
- Submit your final PTE for course completion

## **Required Material**

### ***Online Course***

In order to perform the Hands-On Exercises, you need to download the following:

- De-ICE.net Disk 2.100
- BackTrack LiveCD
- OSSTMM Methodology

### ***Course Certificate of Completion***

If you intended to obtain a certificate of completion for this course, you need to download the following:

- HIPT LiveCD Disk 1
- HIPT LiveCD Disk 2
- BackTrack LiveCD
- OSSTMM Methodology

## **About the Online Material**

### ***Video Presentations***

The video presentations are intended to provide a foundation to understanding how to formally conduct a penetration test. The topics of discussion are focused heavily on the methodology behind PenTesting, and touch briefly on suggested tools to use during each phase of a penetration test.

### ***Hands-On Exercises***

The Hands-On portion of the course is primarily self-guided study, and should take a minimum of two hours each (any amount less than this will undoubtedly hamper your efforts during the PTE). The purpose behind this section of the course is to provide you with a chance to learn how to use the suggested tools and understand the specific tasks discussed in each module. The Hands-On exercises within the class aren't intended to make you learn one particular tool (or all of them, for that matter) - it is intended to provide you with enough exposure to tools so you can discover which ones work best for your personal style, so you can complete your own individual Penetration Test Effort (PTE).

Remember, the objective of this course is to provide an advanced understanding on how to conduct a penetration test, not to learn all the tools presented here. Knowledge of the tools is required to successfully complete your individual PTE, but is a sub-set of information you should have when done with this class.

# Certificate of Completion

## ***Formal Penetration Test Document***

Once a penetration tester has completed their examination of a target, a formal document discussing the overall effort and findings is required. In order to evaluate a student's performance and adherence to the OSSTMM methodology, a student must submit their own formal penetration test document, along with supporting evidence.

In order to complete the course, you need to conduct your own penetration test against disk 2.101 and 2.102. These disks are intended to test your new knowledge and ability to perform a pentest according to the OSSTMM methodology. In order to evaluate your performance, each student is required to submit the following supporting document as proof of effort:

- Formal Penetration Test Document
- Completed Templates
- Screenshots of important findings (included in the formal penetration test document)
- "script" file, which records a student's keystrokes during their effort

IMPORTANT: you MUST include all four items when submitting your PTE - we have been getting submissions without the script file, and are rejecting them as incomplete. All four components are absolutely required

Once a student has successfully produced these documents, they must be e-mailed to the course instructor. All documents are evaluated by a panel and a certificate of completion will be awarded based on the criteria listed below. If the material provided by the student is insufficient to obtain a certificate of completion, the student will be informed as to the deficiencies, so they may amend their material. The student can then re-submit their documents for evaluation. Students may re-submit as many times as they desire during the 90-day submission window. The objective behind this is for the student to have the experience in completing a real-world example of a penetration test, along with documenting this effort.

## ***Completed Templates***

The OSSTMM has included some templates to help manage your penetration test. To complete this course, copies of completed templates are required. However, there is no expectation that the penetration tester will need to use all the templates presented in the OSSTMM. Only submit those templates that you use.

## ***Screenshots of Important Findings***

During your penetration test, you will make discoveries that need to be documented. In some cases, your client might contest these discoveries. This is why evidence is required. Any compromise you achieve must have evidence, and this can be accomplished through use of screenshots. Any time you obtain access to something you should not have, a screenshot is required, and must be submitted as part of your final PTE within the Appendix.

### ***"script" file***

All keystrokes performed by a student during their individual Penetration Test Effort must be recorded and submitted, in order to complete this course. There are a variety of different programs that can be used to do this, but the "script" command is by far the easiest. Just be sure that when you use this (or any) command, you save each session in such a way as to not overwrite your earlier capture.

NOTE: We will not accept incomplete documents. If by some unfortunate incident, you have lost some of the recorded keystrokes, you must reconstruct your efforts to show continuity in your effort.

## **Contact Information**

While participating in this course, if you should have any problems or questions, please don't hesitate to contact us. Contact information can be found on the course wiki.