



## Syllabus

### **Heorot Penetration Testing Fundamentals course**

Welcome to the Heorot Penetration Testing Fundamentals (HPTF) course, presented by Heorot.net. This course is designed to teach you the fundamentals of Penetration Testing, and how to conduct your own penetration test using the Information Systems Security Assessment Framework (ISSAF). 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 ISSAF 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 30 days, starting the day of enrollment. You have 60 days to submit your final PTE documentation for course completion.

While this course provides an opportunity to learn tools associated with pentesting, 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 30 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 ISSAF methodology
- Module 1 - Introduction
  - Video Presentation
  - Powerpoint Slide
- Module 2 - Penetration Test Overview
  - Video Presentation
  - Powerpoint Slide
- Module 3 - Information Gathering
  - Video Presentation
  - Powerpoint Slide
- Required Reading:
  - ISSAF Manual 0.2.1B - Section A, pages 13 - 24
  - ISSAF Manual 0.2.1B - Section B, pages 25 - 29
  - ISSAF Manual 0.2.1.A - Section 3, pages 18 - 30
  - ISSAF Manual 0.2.1B - Familiarize yourself with "Passive Information Gathering" within Section B (pages 30 - 61)

## **Day Two**

- Module 4 - Network Mapping
  - Video Presentation - Part 1
  - Video Presentation - Part 2
  - Powerpoint Slide
- Module 5 - Vulnerability Identification
  - Video Presentation
  - Powerpoint Slide
- Required Reading:
  - ISSAF Manual 0.2.1B - Familiarize yourself with "Network Mapping" within Section B, pages 87 - 126
  - ISSAF Manual 0.2.1B - Familiarize yourself with "Vulnerability Identification" within Section B, pages 127 - 133

## **Day Three**

- Module 6 - Penetration
  - Video Presentation
  - Powerpoint Slide
- Module 7 - Gaining Access & Privilege Escalation / Enumerating Further
  - Video Presentation
  - Powerpoint Slide
- Module 8 - What's Next?
  - Video Presentation
  - Powerpoint Slide
- Required Reading:
  - ISSAF Manual 0.2.1B - Section B4 to B6, pages 134 - 136
  - ISSAF Manual 0.2.1B - Familiarize yourself with "Covering the Tracks" within Section B9, pages 127 - 169

## **Day Four**

- Create Outline of your own Penetration Test Effort document to submit for course completion
  - Decide on format for your PTE final document
  - Download the Penetration Test Effort templates
  - Integrate provided Scope Statement
  - Integrate provided Gathered Information
- Perform Network Mapping against disk 1.101
- Perform Vulnerability Identification against disk 1.101
- Perform Penetration against Disk 1.101
- Required Reading:
  - ISSAF Manual 0.2.1B - Familiarize yourself with "Unix/Linux System Security Assessment" within Section P, pages 483 - 522

## **Day Five**

- Perform Gaining Access & Privilege Escalation against disk 1.101
- Perform Enumerating Further against disk 1.101
- 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 and follow along with the video instruction, you need to download the following:

- Disk 1.100 (LiveCD)
- BackTrack LiveCD
- ISSAF Methodology

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

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

- Disk 1.101 (LiveCD)
- BackTrack LiveCD
- ISSAF 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 discussed in each module. This course provides video captures of students conducting their own Hands-On exercises, which can be used as a basis for your own discovery. 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 a foundation to use a penetration test methodology to conduct your own PenTest effort, 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 ISSAF methodology, a student must submit their own formal penetration test document, along with supporting evidence. The following areas are required and graded:

- General Documentation – 250
  - Management Summary
  - Scope of the project (and Out of Scope parts)
  - Tools that have been used (including exploits)
  - Dates & times of the actual tests on the systems
- Identification of Weakness & Vulnerabilities – 650
  - A list of all identified vulnerabilities
  - Output of tests performed (screenshots or “script” text file)
- Action Points – 100
  - Recommendation of what to mitigate first
  - Recommended solution

An example of the final document is provided in this course for comparison, but a student is permitted to use any format they wish (we are not grading on format, just content). Understand, however, that this document is intended to be presented to your "client" who has paid you for your time. There is an expectation that any documents you provide will be professional.

Since some information required is impossible for you to complete, due to the limitations of this course, the following is provided to you for inclusion in your final document:

- Scope Statement
- Information Gathering Phase results

Everything else within the document must be supplied by the student, to successfully complete this course.

## ***Completed Templates***

The ISSAF has included some templates to help manage your penetration test. To complete this course, copies of completed templates are required. It is important to include all related documents, as any omission will be viewed as incomplete work. For example, there should be one Service Enumeration Template for each application found on your target system. Example: if your target has http, ssh, and pop3, your final submission should include three Service Enumeration Templates.

## ***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.

### ***"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.

Retrieved from "<http://heorot.net/instruction/PTF/index.php/PTE>"

## **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.