

Hunting Web Attackers

URL	http://www.tehtri-security.com/en/trainings.php
Trainer	Oudot Laurent (Founder, TEHTRI-Security)
Duration	2 days

Overview

The goal of this innovative training is to **prepare white-hats** and to **improve their skills** in this already running cyber war against web attackers. Thanks to this course, attendees will learn **how to detect web intruders**, and then sometimes **how to strike-back** so that they can better identify the assailants or neutralize their actions.

This technical hunt will be based on **hands-on exercises** launched with the help of the instructor on a dedicated LAN, so that the students will have the opportunity to apply those special techniques for real, in case they would have to do it **by themselves in their own environment**.

The trainer has been involved in the IT Security field for the last 15 years. His international experience about **offensive and defensive technologies** will allow the students to get a cutting-edge training and to be prepared to hunt down web attackers once they are back on their own networks...

Target Audience

- System & Network administrators, who want to improve their protection against web attackers
- Pen-testers, Security analysts & auditors, who want to get new solutions against web attackers
- IT Security & Computer Emergency Responses Team, who want to get prepared for this cyberwar
- Authorities & Law enforcement teams, who want to know how to take a step further with new technical opportunities to handle cyber crimes

Course Agenda

1) Web threats & Advanced intrusions

The first part will explain and remind to the students, every needed concepts about **intrusions through the web vector**, and the resulting fingerprints left during such steps.

1. Pre-intrusion: how attackers prepare their future evil actions
2. Intrusion: how attackers get an access on a remote box through the web
3. Post-intrusion: what kind of actions are launched by the attackers, like:
 - a. Keeping control: how they try to backdoor and control your boxes
 - b. Cleaning fingerprints: how they try to hide and cover their tracks
 - c. Privilege escalation: how they try to improve their rights on the systems
 - d. Local exploration: how they try to explore your computer and your local network
 - e. Remote bounce: how they try to bounce from your servers to remote networks
 - f. Abuse incoming clients: how they try to compromise incoming clients

Thanks to this part, each attendee will know the real current threats for their web servers.

2) Detect Attackers

This second part will talk about **how to detect web intrusions**. The goal will be to get through any technical possibilities that might help white-hats at detecting standard & stealth attackers through different layers.

1. **Application** Layers: how to detect attacks and intrusions (successful attacks) through the applications layers (web server logs, data on the hard drive...)
2. **System** layers: how to look at the OS to find the attackers (processes, system logs...)
3. **Network** layers: how to use network in order to improve detection (routers, firewalls, NIDS...)

3) React!

Once we find that something get wrong on our web server, the question is how to handle those events properly. The classical behavior looks like: shutting down services or infected computers, deleting the tools of the attackers or reinstalling the computer, and then hardening the computer just before going online again. Sometimes, the logs are used for legal purposes, etc.

But here, in this training, this third big part will propose innovative ways to behave. We will show **how to react against the attackers with a live offensive behavior**. This will help at fighting back web intruders so that we can get more info about their identity or sometimes to neutralize their forces.

Those innovative actions will be used to strike back remote attackers for different kind of purposes:

1. About **striking-back attackers**
 - a. Legal issues
 - b. Timeline issues
 - c. Technical issues
 - d. Attacking the tools of the attackers
2. **Identify** attackers
 - a. Get more information on remote attackers (identity, information, tools, data...)
3. **Compromise** the attackers
 - a. Get a remote control of the IT resources of the intruders
 - b. Neutralization of the attackers

4) Final hands-on

Though the training is already full of hands-on exercises, we will finish with a final advanced session, with a **live hacking simulation**, so that any concepts seen during the two days might be applied successfully on a kind of real case.

Prerequisites

- Basic experience with ASP or JSP or PHP, SQL and HTTP. No stress: minimum needed knowledge will be reminded and explained at the beginning of the training
- TCP/IP (IPv4) to connect your laptop to the hands-on lab
- Experience of Windows or Unix-like operating systems and shell scripting

Prerequisite material

- Students need a laptop (any OS welcome) with:
 - Clients: SSH, FTP, and web browser (Latest Firefox suggested with those plug-ins: Live HTTP Header, Cookie Monster, Header Spy, Modify Headers, Tamper Data...)
 - Services: a local web server (like a recent Apache/PHP/MySQL enabled (LAMP/WAMP architecture)...))
 - Shell tools and scripting languages (Instructor will use python, bash, curl, netcat, wget, etc). Windows end-users should install Cygwin.

About the trainer

Laurent is a French senior IT Security consultant, who founded TEHTRI-Security (link: <http://www.tehtri-security.com>) in 2010. Last 15 years, he has been hired as a security expert to protect and pentest networks and systems of highly sensitive places like the French Nuclear Warhead Program, the French Ministry of Defense, the United Nations, etc.

He has been doing research on defensive technologies and underground activities with numerous security projects handled, and he was a member of team RstAck and of the Steering Committee of the HoneyNet Research Alliance. Laurent has been a frequent presenter or instructor at computer security and academic conferences like Cansecwest, Pacsec, Black Hat USA-Asia-Europe, Hack-In-The-Box Dubai, Defcon, US DoD/DoE, Hope, HoneyNet, PH-Neutral, Hack.LU, as well as a contributor to several research papers for SecurityFocus, MISC Magazine, IEEE, etc.