TROOPERS TRAININGS Make the world a safer place.

HMTS HM Training Solutions

Training:
Reverse Engineering a (M)MORPG

Date of the training: **March 12-13 ,2018** in Heidelberg, Germany

Book Now using the voucher code: **TR18HMTSEB** and save an additional 5% of the current valid rate of any package!

YOUR TRAINER: ANTONIN BEAUJEANT

WHO SHOULD ATTEND THIS TRAINING?

- Beginner RE. People who want to learn how to reverse engineer a binary protocol.
- People who wants improve their reverse engineering skills with a fun target.

REQUIREMENTS:

- Basics of networking (OSI model)
- Basics of assembly (64bit)
- Laptop with Linux (ideally Ubuntu) that can run Pwn Adventure 3 (available for free so they can test prior to the workshop)

Don't hesitate to call us. We're fluent in English and German..

http://troopers.de

info@troopers.de

+49 (0) 6221-480390

Description

This workshop will cover the basics of reverse engineering a (M)MORPG:

- Reverse engineer the network protocol
- Build a Wireshark disector
- Build an asynchronous proxy (python)
- Reverse engineer the binary to unveil secret
- Reverse engineer the binary to find vulnerabilities
- Patch the binary for hacks
- Hook the library (Linux) for hacks

Finally, we will also take a look into the future, because a lot of important things will change shortly, so everyone should be well prepared to avoid any major disruption of important services. And don't forget to bring a laptop with administrative privileges, this is a hands-on training and you have to install tools, if you would like to participate in the exercises.

INTRODUCTION

Introduction about the video game: Pwn Advenrure 3: Pwnie Island. The game was developed by Vector35 for the Ghost in the Shellcode 2015 CTF. The purpose of the game is to reverse engineer the GameLogic as well as the network in order to finish quests that would be impossible otherwise. I explain the game itself, show its interface, a bit of gameplay.

REVERSE ENGINEERING NETWORK PROTOCOL

Here I explain the methodology used to reverse engineering unknown binary protocol. Like most of RE task, it is based on the ability of the analyst to raise accurate assumption. Once the assumptions raised, we need to find a way to isolate the data and analyze the changes in the network traffic to identify where it is located. Once identified, we need to understand how the data is represented (integer, string, little-endian, etc). In this part we will first walk the audience through the full process of parsing the location of the player (X, Y, Z; direction; state; etc). Then I will let the audience reverse two packets as an exercise.

BUILDING WIRESHARK PARSER

Now that we have reversed most of the network protocol, we will build a Wireshark dissector plugin in Lua. I will walk the audience through the process and, in the end, we will have a complete parser to analyze the protocol deeper.

ASYNCHRONOUS PROXY IN PYTHON

We will build an asynchronous proxy in python in order to intercept the network traffic. We will be able to get any weapon, but we won't be able to use them since the damages are not taken into considering due to checks on the server side. We will use this example to clearly explain that local hack are not that interesting and we need to focus on packet sent to the server. We will also manipulate the spawn point so we can spawn wherever we want on the map. We will fake our position to the server in order to activate actions impossible otherwise. We will solve 2 challenges from the GhostInTheShellcode 2015.

REVERSE ENGINEERING BINARY & BINARY PATCHING

In the next part of the workshop, we will reverse engineering the client/server logic in order to highlight "secret" to finish the quest and identify vulnerabilities in the game. We will also patch the binary to become a Superman (running faster, jumping higher). I will show how to create a patcher in python with Capstone and Keystone.

LIBRARY HOOKING

Finally, we will hook the DLL in order to hack the game "on the fly", followed by game hacking!

ABOUT YOUR TRAINER: ANTONIN BEAUJEANT

Antonin Beaujeant is a professional penetration tester and researcher. His primary focus is web app and network penetration test but he also enjoy spending time on hardware, reverse and CTF in general.

TROOPERS TRAININGS Make the world a safer place.

HMTS HM Training Solutions

Booking

Recommended Online Booking of Trainings Through:

Sign-Up Form https://www.troopers.de
Voucher code: **TR18HMTSEB**

Using this voucher code automatically gives you an additional 5% off the current valid price! You can register with this code up until March 11th, 2018 or until seats have run out.

Contact

Troopers Organization Team

Need assistance? +49 6221 480390

info@troopers.de

Don't hesitate to call us. We are fluent in English and German.

Zögern Sie nicht uns zu kontaktieren. Wir sprechen fließend Englisch und Deutsch.

Booking is also possible offline through your trusted partner from:

HMTS HM Training Solutions

HM Training Solutions, Falkenstrasse 6 , 63820 Elsenfeld, Germany

+49 6022 508200 info@hmtrainingsolutions.com

+49 6022 5089999 www.hmtrainingsolutions.com

Don't hesitate to call us. We're fluent in English and German..