hkpc Academy 生產力學院

Cyber Security Workshop : RED / BLUE Team Pentest Kungfu Series

In the ever-changing cyber world today, a better way to protect your network and defence-in-depth of your assets is to understand your adversary tactics and techniques.

The primary aim of this workshop is to equip the participants with the necessary cyber security skill sets from both sides of the world: the **RED** Team and the **BLUE** Team. The **RED** Team focuses on penetration testing of different systems and the levels of security programmes, to detect, prevent and eliminate vulnerabilities, while the **BLUE** Team finds ways to defend, change and regroup defence mechanisms making incident response much stronger!

Programme code	10010252
Date and time	22-25 September 2020 09:30 – 17:00
Venue	1/F, HKPC Building, 78 Tat Chee Avenue, Kowloon, Hong Kong
Medium	Cantonese with English terminology
Fee	Early bird price on or before 25 Aug 2020 - Non-member: HK$17,200 per person - Member of Supporting Organisation: HK$16,800 per person Regular Price - Non-member: HK$17,600 per person - Member of Supporting Organisation: HK$17,200 per person
Remarks	The application deadline is **15 September 2020**. Late submission will NOT be considered.

Supporting Organisations

ACFE Association of Certified Fraud Examiners Hong Kong Chapter 特許詐騙審查師學會 香港分會

CSA cloud security alliance

CAHK 香港通訊業聯會 Communications Association of Hong Kong

HKCERT

Hong Kong Computer Society

IPSA

澳門電腦學會 Macao Computer Society

Inquiry Ms Judy LIU | +852 2788 5704 | judysmliu@hkpc.org

Course Highlights

Day 1: Hands on Red Team and Metasploit KungFu

A lab with different types of clients and servers (e.g. web servers, mail servers, DNS servers, log servers, Windows client, etc.) is built to simulate real-life environment for Red Team and Blue Team to experience how attacks are launched and logs server / alert system will react.

Lab Infrastructure and Environment Setup

1) Introduction of the lab infrastructure
2) Install Kali Linux on laptops
3) Set up of environment (connect to lab server)

Red Team Exercise

1) Methodology of Red Team testing
2) Reconnaissance of the targets in the lab
3) Identifying the targets, e.g. ports, services, application version
4) Exploitation
5) SQL map attack
6) Metasploit payload generation
7) Deploying payload to different targets
8) Writing payload to the target
9) Maintaining access of the targets
10) Reporting guidelines

Course Highlights

Day 2: Hands on Blue Team and Final Challenge

Blue Team Exercise

- ✓ Familiarising with log servers and agents in the Lab
- ✓ Analysing the logs
- ✓ Differentiating attack logs from normal logs
- ✓ Setting up alerts of abnormal behaviour
- ✓ Setting up rules for actions on different type of attacks
- ✓ Generating charts for analysis

Final Challenge

- ✓ Given vulnerable servers, participants are required to attack the target and get the secret from it. At the same time, participants are required to analyse the logs to determine what sort of attacks are launched and set up alerts.

Day 3: Malware and Targeted Attack Analysis & Simulation

Introduction and Simulation

- ✓ What is targeted attack?
- ✓ What are their indicators?
- ✓ How can we simulate the attacks and what can the blue team see?

From indicators to deep analysis

- ✓ Malware analysis primitive: static and dynamic analysis with recent attack sample
- ✓ Yara rules primitives
- ✓ IOC primitives

Day 4: Advanced Blue Team Techniques: Attack

Malware Detection with Machine Learning

- ✓ What is machine learning?
- ✓ What kind of indicators do we have in malware and attack server logs? (Ken/Byron)
- ✓ How to train the machine learning model?
- ✓ Discussion and hands-on with machine learning for attack logs (Ken/Byron)
- ✓ Discussion and hands-on with machine learning framework for malware analysis

hkpc Academy 生產力學院

Cyber Security Workshop : RED / BLUE Team Pentest Kungfu Series

Trainers

Mr Anthony LAI

Founder & Security Researcher, VX Research Limited

Anthony LAI is the holder of SANS GREM (Gold Paper) since 2010 (Level 3 in Incident Response Management) and SANS GXPN (Level 3 of Penetration Test). He has over 15 years of experience in information security and quality assurance, including penetration test, exploitation research, malware analysis, threat analysis, reverse engineering, and incident response and management.

Mr Alan HO

Red Team Engineer, VX Research Limited

Alan HO is the holder of OSCP and SANS GWAPT certified security professional. He has over 10 years of experience in the information security industry, including penetration testing, security assessment, incident response, security operation planning, and investigation.

Certificate of Training

Participants who have attained 75% or more attendance of lecture will be awarded an Attendance Certificate.

Enrolment method

1. Scan the QR code to complete the enrolment and payment online.
2. Mail the crossed cheque with payee name "Hong Kong Productivity Council" (in HK dollar) and the application form should be mailed to HKPC Academy, Hong Kong Productivity Council, 2/F, HKPC Building, 78 Tat Chee Avenue, Kowloon (attention to Ms Judy LIU). Please indicate the course name and course code on the envelope.

https://www.home.hkpcacademy.org/en/10010252

(Only receipt printed with receipt printers at HKPC is valid. Receipt of cheque payment is subject to bank clearance.)

Inquiry Ms Judy LIU | +852 2788 5704 | judysmliu@hkpc.org