Cyber Security Workshop:
RED / BLUE Team Pentest Kungfu Series

Training Details:	Overview
Date: 9 - 12 March 2020 (Mon - Thu) **Time:** 09:30 - 17:00 **Venue:** 1/F, HKPC Building, 78 Tat Chee Avenue, Kowloon, Hong Kong **Medium:** Cantonese with English terminology **Organiser:** Hong Kong Productivity Council **Training Fee:** $17,600 (*Regular Price*) $16,800 (*Early Bird/ Supporting Organisation*) **Enquiry:** Ms CHOY +852 2788 5884 tracyc@hkpc.org	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! Register to save your seats now! Early bird or members of Supporting Organisations will enjoy up to **HK$800 discount (before 7 Feb 2020)**! **DON'T WAIT, ACT NOW!!!** **Application Procedure** Please complete enrolment via https://www.home.hkpcacademy.org/en/2019/12/02/10009357-cyber-security-workshop-red-blue-team-pentest-kungfu-series/ Inquiries: Ms CHOY tracyc@hkpc.org / Tel: +852 2788 5884 **Supporting Organisations**

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 (0.5 hours)**

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

✓ **Red Team Exercise (total 7-8 hours in two days)**

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

Day 2: Hands on Blue Team and Final Challenge

Blue Team Exercise (3 hours)

- ✓ 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 (2 hours)

- ✓ 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? (0.5 hours)
- ✓ What are their indicators? (0.5 hours)
- ✓ How can we simulate the attacks and what can the blue team see? (2 hours)

From indicators to deep analysis

- ✓ Malware analysis primitive: static and dynamic analysis with recent attack sample (1.5 hours)
- ✓ Yara rules primitives (1 hour)
- ✓ IOC primitives (0.5 hours)

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

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.