Cyber Security Expert Training

Training

> **Art of Hacking**

October 2nd (Tue) – 3rd (Wed), 2018
Penetration testing for Basic Infrastructure

October 4th (Thu) – 5th (Fri), 2018
Basic Web Hacking

JP Tower Hall & Conference (KITTE 5F)

Term 1 > Penetration testing for Basic Infrastructure

Up to 30

October 2nd (Tue) – 3rd (Wed), 2018 9:00-17:00
JP Tower Hall & Conference (KITTE 5F)

This courses familiarizes the attendees with a wealth of hacking tools and techniques.

The course starts from the very basic and gradually build up to the level where attendees can not only use the tools and techniques to hack various components involved in infrastructure hacking, but also walk away with a solid understanding of the concepts on which these tools work.

WHO SHOULD TAKE THIS COURSE

・System Administrators
・SOC analysts
・Entry level/intermediate level penetration testers
・Network engineers
・Security enthusiasts
・Anyone who wants to take their skills to next level.

Benefits

・Access to a hacking lab not just during the course but for 30 days after the class too. This gives them plenty of time to practice the concepts taught in the class.
・Numerous scripts and tools will also be provided during the training, along with student hand-outs.
・A certificate of attendance

PROGRAM

Day1

- Module 1: The Art of Port Scanning
- Module 2: The Art of Online Password Attacks
- Module 3: The Art of Hacking Databases
- Module 4: Metasploit Basics
- Module 5: Password Cracking
- Module 6: Hacking Unix

Day2

- Module 7: Hacking Application Servers on Unix
- Module 8: Hacking Third Party CMS Software
- Module 9: Windows Enumeration
- Module 10: Client Side Attacks
- Module 11: Hacking Application Servers on Windows
- Module 12: Post Exploitation
- Module 13: Hacking Windows Domains

Trainer   ※Common to 2 courses

Sam Sanoop
Security Consultant

Sam is an information security enthusiast with interest in web application security. Sam holds a Bachelor of Science (BSc) degree in Computer Security with Forensics from Sheffield Hallam University, and international certifications such as Offensive Security Certified Professional (OSCP) and CREST Registered Penetration Tester (CRT).
Sam works as a Security Consultant and delivers a multitude of security assessments covering web application security, code reviews and network security. Within NotSoSecure's team of Information Security specialists, he works primarily on web application security projects and is one of the trainer for NotSoSecure's Basic Web Hacking training course. Sam undertakes a variety of security-consulting services including penetration testing applications and infrastructure to clients within a variety of industries while working closely with them, establishing fruitful professional relationships.

Up to 30

October 4th (Thu) – 5th (Fri), 2018 9:00-17:00
JP Tower Hall & Conference (KITTE 5F)

This is an entry-level web Application Security-testing class.

This class familiarizes the attendees with the basics of Web and Application hacking. A number of tools and techniques will be taught during the 2 day class. If you would like to step into the world of ethical hacking / pen testing with a focus on web applications, then this is the right class for you

-Class Details

This class familiarizes the attendees with a wealth of tools and techniques needed to breach the security of web applications and also covers the industry standards such as OWASP Top 10, PCI DSS and contains numerous real life examples to help the attendees understand the true impact of these vulnerabilities.

WHO SHOULD TAKE THIS COURSE

- ・System Administrators ・Web Developers
- ・SOC analysts ・Penetration Testers
- ・Network engineers ・Security enthusiasts
- ・anyone who wants to take their skills to the next level.

Benefits

- ・Access to a hacking lab not just during the course but for 30 days after the class too. This gives them plenty of time to practice the concepts taught in the class.
- ・Numerous scripts and tools will also be provided during the training, along with student hand-outs.
- ・A certificate of attendance

PROGRAM

Day1

Information Gathering, Profiling and Cross-Site Scripting

- Understanding HTTP Protocol
- Identifying the Attack Surface
- Username Enumeration
- Information Disclosure
- Issues with SSL/TLS
- Cross-Site Scripting
- Cross-Site Request Forgery

Day2

Injection, Flaws, Files and Hacks

- SQL Injection
- XXE Attacks
- OS Code Injection
- Local/Remote File Include
- Cryptographic Weakness
- Business Logic Flaws
- Insecure File Uploads

WHAT STUDENTS SHOULD BRING ※Common to 2 courses

The only requirement for this class is that you must bring your own laptop and have admin/root access on it.

During the class, we will give you VPN access to our state-of-art hacklab which is hosted in our datacenter in UK. Once you are connected to the lab, you will find all the relevant tools/VMs there.

We also provide a dedicated Kali VM to each attendee on the hacklab. So, you don't need to bring any VMs with you. All you need is admin access to install the VPN client and once connected, you are good to go!

STUDENT REQUIREMENTS

Bring your own laptop and have admin/root access on it.

Also, note that we will use an wireless network for this class.

Training > Art of Hacking

The Voice of the attendees

・I had never had the opportunity to learn the attacking method, so I was happy to be able to take this time. I knew the existence of metasploit and thought that I would like to fiddle with it, but since I had no opportunity, I was glad that I could experience this time.

・This experience will be helpful for me in the future because there were lots of useful information, practical contents, materials were also detailed.

・I learned a lot. I will review it in order to acquire what I have studied today. I would like to take class again.

・It was more difficult than I expected. I realize that I have to learn more. It definitely was a learning experience.

・Thank you for teach me practical technique.

・Thanks to the interpreter I was able to study without stress.
This course was high level for me and I learned a lot.

Art of Hacking Training fee ※Including lunch for 4 days

Early bird 1 ~August 22nd (Wed)	Early bird 2 ~September 12th (Wed)	Usual price
¥365,000 (w/o tax)	¥385,000 (w/o tax)	¥500,000 (w/o tax)

Venue

2-7-2 Marunouchi, Chiyoda-ku, Tokyo
100-0005 JAPAN
JP Tower Hall & Conference (KITTE 5F)

Contact us

CSET Show Management Office

Email : contact@f2ff.jp
Tel : +81-3-6258-0590