Advanced Infrastructure Hacking

Date	June 25th (Mon) – June 29th (Fri) 9:00-17:00
Venue	NANO OPT Media Inc. Conference Room (12F/ Shinjuku L-Tower)
Organizer	NANO OPT Media Inc.

Advanced Infrastructure Hacking

OVERVIEW

An Advanced Infrastructure Hacking class designed for those who wish to push their knowledge … The fast-paced class teaches the audience a wealth of hacking techniques to compromise various operating systems and networking devices. The class will cover advanced penetration techniques to achieve exploitation and will familiarise you with hacking of common operating systems, networking devices and much more. From hacking Domain Controllers to local root, VLAN Hopping to VoIP Hacking, we have got everything covered.

Whether you are Penetration Testing, Red Teaming, or hoping to gain a better understanding of managing vulnerabilities in your environment, understanding advanced hacking techniques for infrastructure devices and systems is critical.

The Advanced Infrastructure class will get the attendees familiarised with a wealth of hacking techniques for common Operating Systems and networking devices. While prior Pen Testing experience is not a strict requirement, a prior use of common hacking tools such as Metasploit is recommended for this class.

WHO SHOULD TAKE THIS CLASS?

The course is ideal for those preparing for CREST CCT (ICE), CHECK (CTL), TIGER SST and other similar industry certifications, as well as those who perform Penetration Testing on infrastructure as a day job and wish to add to their existing skill set.

Day1

- **IPv4 and IPv6 Refresher**

Advanced topics in network Scanning
Understanding and exploiting IPv6 Targets

- **OSINT, DVCS Exploitation**

Advanced OSINT Data gathering
Exploiting git and Continuous Integration (CI) servers.

- **Database Servers**

Mysql
Postgres
Oracle

- **Recent Vulnerabilities**

Heart-Bleed and Shell-Shock
PHP Serialization Exploit
Web-sphere Java Exploits

Day2

- **Windows Exploitation**

Domain and User Enumeration

AppLocker / GPO Restriction Bypass

Local Privilege Escalation
Post Exploitation #1 (AMSI Bypass & Mimikatz)

Post Exploitation #2 (LSASecrets)

Day3

- **AD Exploitation**

Active Directory Delegation issues

WOW64

Pivoting and WinRM

Persistence (Golden Ticket and DCSync)

Lateral Movement Using WMIC

Day4

- **Linux Exploitation**

Port scanning and Enumeration

FS + SSH

Privilege Escalation

rservices

Apache

X11 Services

Day5

- **Container Breakout**

Docker breakout

- **VPN Exploitation**

VPN

- **VoIP Exploitation**

VoIP enumeration
VoIP exploitation

- **VLAN Exploitation**

VLAN concepts
VLAN hopping attacks.

WHAT STUDENTS WILL BE PROVIDED WITH

・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

TRAINER

Anant Shrivastava

Regional Director

Conferences

Spoken

Nullcon
c0c0n
RootConf
ClubHack

Trained

Blackhat (US/EU/Asia)
Nullcon
c0c0n

Tools Presented

Blackhat Arsenal (US/EU/Asia)
Defcon
Demolabs 2017

Open-Source Projects

AndroidTamer

A single point of reference for all Android Professionals (https://androidtamer.com)

CodeVigilant

An opensource code review project aimed at finding, reporting, helping in fixing and disclosing security (https://codevigilant.com)

Background

An Engineering graduate from 2008, he has been working with computers and opensource software since 2000. He moderated a linux user group in Bhopal and was active in other major linux user groups across India during 2000-2008. He has worked with various corporates like TechMahindra, Infosys and PA Consulting before joining NotSoSecure. He has been running and maintaining the opensource project AndroidTamer since 2011. He is active with the information security community null, where he also mentors local talent as well as for the Offensive Web Testing Framework (OWTF). He is also an active contributor to the Open Web Application Security Project (OWASP) and reviews and contributes to various technical documentation, including Mobile Security Testing Guide, Mobile ASVS and Web Testing Guide.

What he does for NSS

Anant is responsible for NotSoSecure's entire operations in India and the technical aspects of the company's work. Managing the NotSoSecure team of Information Security specialists, he works primarily on client cases from the UK and the US with the delivery of technical work. He is also a lead trainer on NotSoSecure training courses and responsible for strategy and the general direction of the company moving forward. The key feature of his work is that he provides practical, effective solutions that allow clients to undertake their normal business operations in the most secure possible environment by establishing a holistic approach to security.

What he likes about his work

A computer and software specialist by nature, he is constantly stimulated by the technical environment of his work and the excellent working relationships he has established with his team of like-minded individuals. This allows him to manage a varied caseload of collaborative working and then come up with solutions to a wide range of security issues.

In his own words

Every day something new happens and your knowledge becomes outdated.
If you don't constantly keep your knowledge up-to-date, you're going to lose.
So if something is new, you need to say: "Let's learn about it" — and put
your best foot forward with as much capabilities as you can. In this work, you
need that willingness to go the extra mile.

Prices *Including 5days lunch

1st Early bird discount : JPY 480,000 **Deadline :May 25th, 2018**

2nd Early bird discount : JPY 540,000 **Deadline :June 22th, 2018**

Regular : JPY 600,000 (All prices are not including tax)

WHAT STUDENTS SHOULD BRING

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.

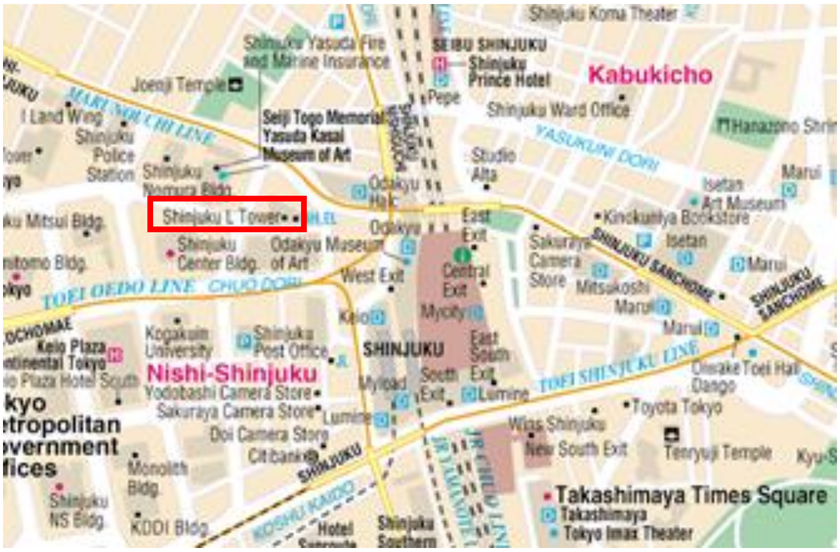
We also provide a dedicated Kali VM to each attendee on the hacklab. So, you don't need to bring any VMs with you. All you need is admin access to install the VPN client and once connected, you are good to go!

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.

ACCESS



3 minutes on foot from JR Shinjuku Station West Exit.

Go straight ahead from the West exit underground shopping mall (Odakyu Ace North building on your right) and turn right at the end (Subaru Building).

Take an escalator to the 2nd floor and take the elevator to the 12th floor.

Inquiry
CSET Show Management Office
(NANO OPT Media,Inc.)
TEL : +81-3-6258-0590 FAX : +81-3-6258-0598
Email: contact@f2ff.jp