(http://conference.hitb.org/hitbsecconf2016ams)

Escape From The Docker-KVM-QEMU Machine

(http://conference.hitb.org/hitbsecconf2016ams/sessions/hitb-lab-mobile-application-security-for-ios-and-android/) (http://conference.hitb.org/hitbsecconf2016ams/agenda/) (http://conference.hitb.org/hitbsecconf2016ams/sessions/csp-oddities/)

KVM-Qemu and Docker containers are important components of virtualization technology and are widely used by mainstream cloud vendors.

KVM-Qemu is a full virtualization solution for Linux on x86 hardware which contains virtualization extensions (Intel VT or AMD-V) and devices emulated by QEMU in user components. Docker is an open-source and light-weight project that automates the development of applications inside software containers by providing an additional layer of abstraction and automation of operating-system-level virtualization on Linux servers. However, any vulnerabilities in these components will bring huge security risks to cloud computing system.

During this talk we will break the session down into two parts – in Part 1, Shengping Wang we will cover Docker escape technologies which involves the following aspects:

1. Docker's implementation principles
2. Exploitation of Linux kernel vulnerabilities
3. Container escape technology
4. **New methods of escape under the latest version of Docker**
5. Some amazing operations to kernel objects

We will show step-by-step how hackers can launch escape attacks and finally control the host to execute any command they want by utilizing Docker's features and existing Linux kernel vulnerabilities.

In Part 2, Xu Liu will talk about QEMU escape technology in which the following topics (and more) will be covered:

1. Analysis of memory layout of QEMU process under QEMU + KVM environment
2. **Several amazing security vulnerabilities of QEMU device emulator which were found by 360 Marvel Team**
3. **How to escape from the virtual machine by making use of the vulnerabilities and special memory mapping features**
4. **Other useful vulnerability exploitation methods of QEMU software.**

This talk is **brand-new and includes never before published material**.

CONFERENCE

LOCATION: **Track 1**
DATE: **May 26, 2016**
TIME: **11:45 am - 12:45 pm**

SHENGPING WANG

(HTTP://CONFERENCE.HITB.ORG/HITBSECCONF2016AMS/SPEAKERS/SHENGPING-WANG/)

XU LIU

(HTTP://CONFERENCE.HITB.ORG/HITBSECCONF2016AMS/SPEAKERS/XU-LIU/)

NIGHTS (http://www.zeronights.org/)

InfoSecConference @Tokyo CODE BLUE (https://m.facebook.com/codeblue.jp)

FRIENDS OF HITB

VULNERABILITY LAB (http://vulnerability-lab.com/)

OWASP The Open Web Application Security Project (https://www.owasp.org/index.php/Main_Page)

Hack In The Box - Keeping Knowledge Free for Over a Decade