

Security Workshop

Introduction

APRICOT / Thành phố Hồ Chí Minh

2017.02.20-24

Introductions

- Cristel Pelsser - University Strasbourg
- Fakrul (pappu) Alam - APNIC
- Randy Bush - Internet Initiative Japan
- Toai Vi - VNNIC
- Yoshinobu (Maz) Matsuzaki - Internet Initiative Japan

Introduce Yourself Loudly, Please

- Your Name
- Country / City
- Where do you work?
- ISP, Enterprise, Government, ...?
- What you do: SysAdmin, Programmer, ...?

Logistics

- Timing
 - 09:00-10:30 - Session 1
 - 10:30-11:00 - Tea
 - 11:00-12:30 - Session 2
 - 13:00-14:00 - Lunch
 - 14:00-15:30 - Session 3
 - 15:30-16:00 - Tea
 - 16:00-18:00 - Session 4
- Transport - You are on Your Own
- Administrative Support

AUT Emergency Instructions

- WG level 4 and above to take the nearest stairway exit and exit out at the level 4 doors onto St Paul Street.
- WG level 3 to use the nearest stairwell exit and gather at 55 Wellesley Street car park.
- In case of an emergency, please follow the instruction of AUT security and the AUT staff members.
- Instructions are also printed on many walls scattered around the building.

No tea/coffee cups are permitted in the workshop rooms. Water bottles will be provided and these are OK.

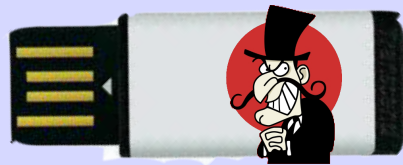
Please do not fix any
signage to walls/windows

Lunch vouchers are to the total value of \$75 (\$15 per day) and can be used at NewsFeed Café on L3 or Counter Café in the WF Building. These vouchers cannot be topped up or redeemed for cash and must be returned to registration at the end of the week or we are charged a \$5 per card replacement fee.

Security

- Please be responsible for your own items. It is recommended you do not leave valuable items in the classrooms
- This is a security workshop, you should secure your kit, phone, ...

In Other Workshops, We
Circulate a USB Stick with
the Presentations



But we do NOT Exchange
USBs in a Security
Workshop


Agenda and Download Presos

<https://wiki.rg.net/wiki/Apricot2017Sec>

Software is at

<https://psg.com/aprisc-sw/>

Agenda - Day 1

- Introduction  we are here
- Assets and Threat Models
- Social Engineering, and Who to Trust
- Cryptography
- PGP Introduction & Lab

Agenda - Day 2

- SSH & SSH Lab
- WireShark
- VPNs, IPsec, & TLS
- OpenVPN and pfSense

Agenda - Day 3

- Network Infrastructure
 - Routers & Switches
 - Filtering
 - Configuration & Archiving
- Sick Host Detection
- Logging and Monitoring
- Anomaly Detection & Firewalls
- IDS / Snort

Agenda - Day 4

- DNS
- Protecting Hosts
- Virus, Mail, and Browsing
 - Anti-Virus
 - Safe Mail Practices
 - Safe Browsing Practices
- Inter-Host Protocols
 - Personal and File Encryption
 - Secure File Transfer
 - Covert Channels

Agenda - Day 5

- Inter-Network Cooperation
- Overflow from previous days

Materials

<https://wiki.rg.net/wiki/Apricot2017Sec>

WiFi

SSID is **APRICOT**

Password is **wireless**

Don't Abuse the Network