Security Workshop Introduction

APRICOT 2019 / Daejeon, Korea

2019.02.18-22

Introductions

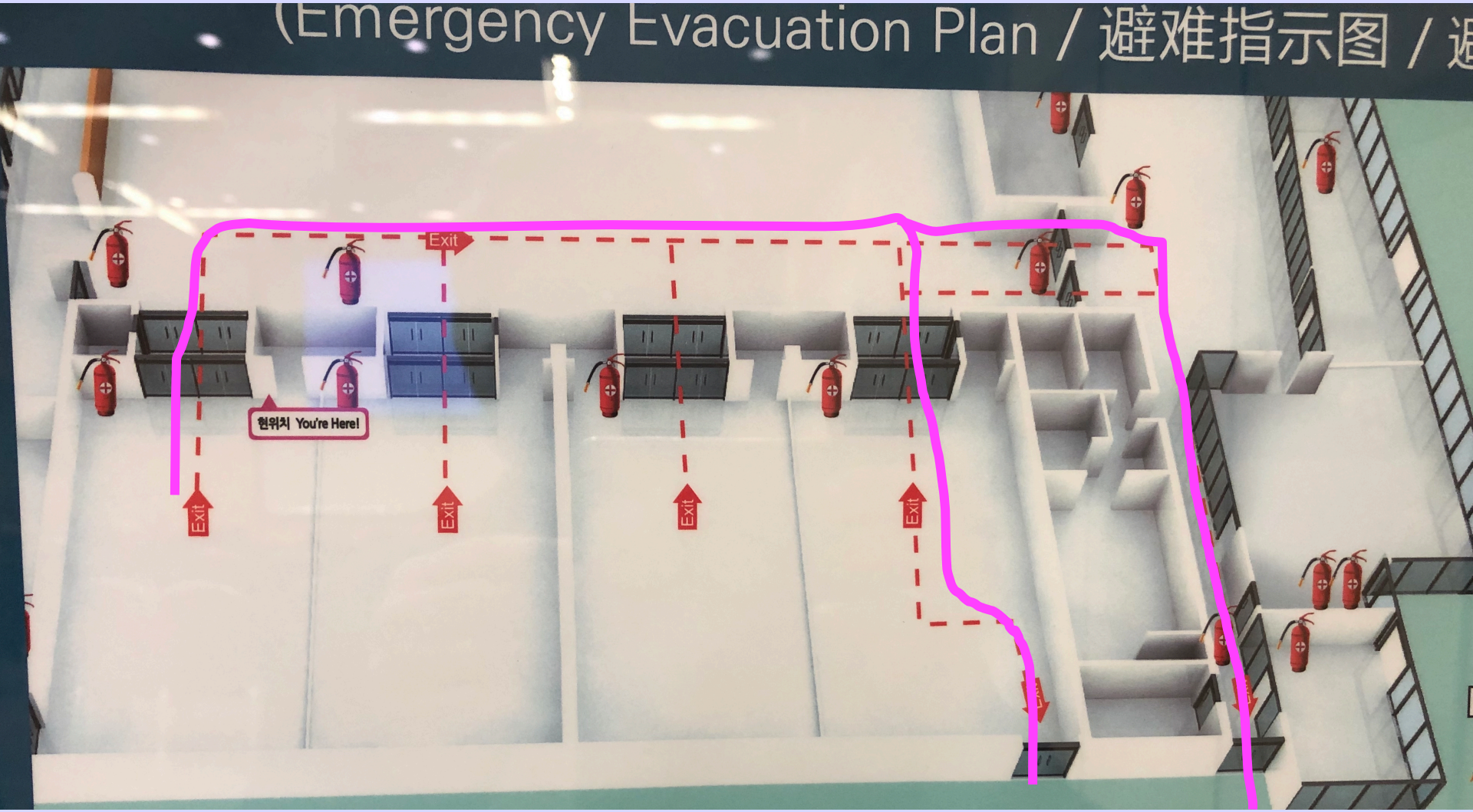
- Bhumika Sapkota - Classic Tech Pvt Ltd, Nepal
- Cristel Pelsser - Uni Strasbourg, France
- Keiichi Shima - Internet Initiative Japan, Japan
- Patrick Okui - Network Startup Resource Center, Uganda
- Randy Bush - Internet Initiative Japan, Japan, Arrcus, US

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
  - 12:30-13:30 – Lunch (LUNCH TICKET REQUIRED)
  - 13:30-15:00 – Session 3
  - 15:00-15:30 - Tea
  - 15:30-18:00 – Session 4
- Transport – You are on Your Own
- Administrative Support



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, …
- Someone could play a prank (joke) on you to teach you to think about security

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 Incremental as We Go

https://github.com/randyqx/apricot-sec2019

Software will be at

https://psg.com/a2019-sw/

Agenda – Day 1

- Introduction  we are here
- Assets and Threat Models
- Cryptography Overview
- Hashing
- PGP Introduction
- PGP 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://github.com/randyqx/apricot-sec2019

Normal WiFi

SSID is apricot

Password is wireless

Don't Abuse the Network

Virtual Machine WiFi

SSID is workshop

Password is iij/2497

Don't Abuse the Network