

Security Workshop

Introduction

BhutanNOG / Thimphu

2017.06.06-9

Introductions

- Alisha Garung - Bhutan Telecom
- Randy Bush - Internet Initiative Japan
- 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, ...?

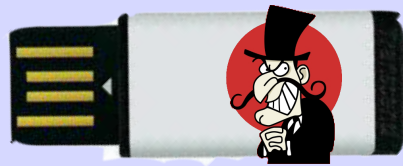
Logistics

- 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

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

<https://github.com/randyqx/bhutannog-sec2017/tree/master>

Software is at

<https://psg.com/btnog-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://github.com/randyqx/bhutannog-sec2017/tree/master>

WiFi

SSID is **APRICOT**

Password is **wireless**

Don't Abuse the Network