Network Security and Packet Analysis Workshop

Dates: 8-12 December 2019
Venue: Yala Durbar Venue, Shankhamul, Lalitpur
Conference Page: **https://npnog.org.np/npnog5/programs/**

Synopsis

- The objective of this workshop is to examine the elements involved in establishing and maintaining security for a network, and building an understanding and familiarity with the operations.
- Device and network infrastructure security is also examined with a focus on establishing robust, stable, and secure networks.
- It also includes an introductory level packet analysis for those who are performing incident response and investigation. Participants will explore tools such as wireshark, bro, tcpdump and others for dissecting network packets related to security incidents.
- The workshop will also look at - Why we keep seeing news headlines about major networks not being reachable because traffic got rerouted to somewhere else? BGP mishaps are very common and frighteningly very easy. Examples are malicious route hijacking, mis-origination (fat fingers), and bad filters (route leaks). We need better mechanism(s) to ensure no one can inject false information into the global routing system that easily.
- We will look at current tools/techniques, how rPKI is just a piece in the puzzle, and what we should do to secure the internet routing instead of waiting for an ideal solution that fixes all issues.

Target Audience

- Engineers, Network Managers and Operators, and Security policy makers who are interested in network security and want to gain an understanding of the threats they face and how to mitigate such threats.

Pre-requisites

- It is assumed that participants have a basic understanding of network operations, Internet technologies, OSI reference model and TCP/IP.

Workshop topics

- Network security fundamentals
- Vulnerabilities and Mitigation on different layers of the TCP/IP stack
- Cryptography and PKI
- Device and Infrastructure Security
- Operational Security and Policies
- Intrusion detection and prevention
- Packet capture and analysis
- Honeypots and honeynet
- VPNs
- Cryptomining/cyrptojacking

- Resource PKI
- Route Origin Validation

Other requirements

- Participants are advised to bring their own laptop computers with high-speed Wi-Fi (802.11a/g/n/ac) and administrative access to system. It is also recommended that laptops have Intel i5 or i7 processor, >=8GB of RAM and 30GB of free hard disk space.

Workshop Items

- Agenda (includes links to presentations and schedule)
- Instructors: Bikash Bhattarai (Dristi Tech), Tashi Phuntsho (APNIC)