Course Programme

Network traffic monitoring with ntop
ntop is the ideal network monitoring solution for companies of all sizes that need simple, effective and cost-efficient monitoring of their network traffic. It provides detailed traffic insights to improve network availability and security, and more quickly identify and resolve performance bottlenecks and issues. With extensive features and advantages over classic providers, ntop is increasingly popular choice for sysadmins and security teams who need comprehensive and reliable network monitoring to quickly and effectively visualize, analyze and continuously monitor network data.

Training program:

Module 1: Introduction to ntop

In this module, participants will learn the basics of ntop and the new version ntopng and how it is used in network environments. Participants receive an overview of the new functions and improvements and can install and configure them directly on a test system.

- Welcome and introduction of the trainer
- Introduction of ntop and ntopng, functionalities
- First introduction to an ntop architecture
- Traffic analysis

a) Packet (Port mirror, SPAN, TAP)
b) Collection of flows (sFlow, NetFlow, IPFIX)

- Explanation of packets and flows
- SNMP and active monitoring

Module 2: Installation and Licensing

- Supported platforms and operating systems
- Installation of the ntop solutions ntopng and nprobe
- Licensing

a) License models
b) Differences in license models
c) Maintenance

- License creation

a) Explanation of the system ID
b) Creating and importing the license

- Starting ntopng as a service

a) Introduction to ntopng's configuration file

- nBox
- Hardware sizing

Module 3: Network Traffic Monitoring

This section focuses on network traffic monitoring and shows students how to use ntop to monitor and analyze network traffic. They learn how to collect traffic statistics, create traffic flow diagrams and examine traffic logs.

- Flow collection

    - How to collect rivers
    - Configuration nProbe as NetFlow exporter
    - Configuration nProbe as NetFlow collector
    - Integration of ntopng with nProbe
        - Active hosts and flows and their lifecycle
        - Alarms, anomalies, network and security issues
        - Collecting large groups of devices: Observation Points
        - PCAP data collection
        - Using ntop to monitor network traffic
        - Creation of custom reports and charts
        - Capacity planning and optimization of network resources
        - ntop integration with other network monitoring tools and solutions
    - External recipients and endpoints

Module 4: Performance optimization with ntop

In this module, participants will learn how to optimize the performance of ntopng to achieve better performance and scalability on their network. Various optimization techniques such as caching, data compression and indexing of data are covered

- Basics of performance optimization with ntop
- Retain historical data

    - Time series
    - Flows

      -Alerts
        - Flow data stores (ClickHouse, MySQL, Elasticsearch)
        - Configuration for optimal performance and scalability
        - Use of caching techniques to improve performance

    - Monitor performance and identify bottlenecks
    - Access to historical data:
- Flow explorer
- Package and data drill down (n2disk)
    - Troubleshooting and troubleshooting
    - Date retention

Module 5: Network Security Features

Here, participants learn how to detect and ward off attacks using the security functions of ntopng. Various attack scenarios such as DDoS attacks or malware infections are played out and the participants learn how to recognize and resolve them. Implementing network security policies and monitoring network performance and availability are also covered.

- Detect and prevent network attacks with ntopng
- Running through attack scenarios such as DDoS attacks and malware infections
- Implementation of network security policies
- Monitoring network performance and availability

Module 6: ntopng administration and maintenance

This module covers administration and maintenance of ntopng, including configuring security settings, updating ntopng, and performing backups and restores. The management of user accounts and rights is also covered.

Feedback round

In this module, participants have the opportunity to share their experiences and opinions on the training and to give feedback. They can share their positive experiences and suggestions for improvement to improve future training.

- Feedback and experiences from participants
- Suggestions for improvement for future training