RN Trust
The Digital Trust Company

NETWORK FORENSICS (5 DAYS)

The course will provide participants with advanced knowledge of networks, computer network sources of evidence and the forensic analysis of network artefacts. Participants will learn about the underlying principles of computer networks and enhance their ability to conduct forensic examinations of data collected from computer networks including network devices, servers and hosts.

Course Objectives:

By the end of this workshop, all the students will be able to:

- Understand legal concepts in digital evidence
- Understand legal aspects of data collecting
- Conduct physical interception
- Capture traffic with open source tools
- Make active acquisition (capturing traffic from live memory)
- Analyze captured traffic
- Capture and analyze wireless traffic
- Detect and analyze network intrusion
- Aggregate, correlate and analyze event logs
- Recognize switches, routers, and firewalls – their fundamentals and relevance to network forensics
- Understand the importance of network tunneling

Prerequisites:

Participants should have basic knowledge of digital forensics and network protocols, models, security. Highly recommended experience with Linux basic navigation.

Syllabus

DAY 1

Day one starts with short overview of digital forensics and network topology basic elements. Day continues with some practical investigative strategies followed by real case scenarios. The second part of the day one is dedicated to identification of evidence, handling the evidence and legal aspects of data collecting. Day one ends with physical interception of network traffic and introduction to several tools for traffic acquisition, majority of them from open source. All necessary software will be installed, and basic features explained.

I. Strengthening our technical fundamentals

- Defining network forensics
- Network models
- Internet protocol (ip)
- Transmission control protocol (tcp)
- User datagram protocol (udp)
- Internet application protocols

II. Practical investigative strategies

- Practical investigative strategies
- Network security goals
- Real-world cases
- Footprints
- Concepts in digital evidence

III. Laying hands on the evidence

- Identifying sources of evidence
- Learning to handle the evidence
- Legal aspects of data collecting
- Physical interception
- Traffic acquisition software (open source tools)
  - ❖ Collecting network traffic
  - ❖ Collecting network logs

DAY 2

Day two begins with active acquisition of RAM memory. Captured traffic is subjected to traffic analysis divided into two major disciplines: packet and statistical flow analysis. Each part ends with relevant case study. Traffic analysis results are presented with visualization tools which help participants find connections between targets. At the end of day two network forensics analysis goes wireless. Participants are introduced to IEEE Layer 2 Protocol Series, wireless protection and security and wireless access points. They are getting familiar with the most common attacks within wireless environment.

I. Active acquisition (capturing traffic from live memory)

II. Traffic analysis

- Packet analysis
  - ❖ Protocol analysis
  - ❖ Packet analysis
  - ❖ Flow analysis
  - ❖ Higher layer traffic analysis

III. Going wireless

- The IEEE Layer 2 Protocol Series
- Understanding wireless protection and security
- Wireless Access Points (WAPs)
- Common attacks
- Case study

- ❖ Case study
- Statistical flow analysis
  - ❖ Process overview
  - ❖ Sensors
  - ❖ Flow record export protocols
  - ❖ Analysis
  - ❖ Case study
- Analysis visualization
- PRTG network monitor

DAY 3

Day starts with wireless traffic capture and analysis. Day continues with network intrusion detection and analysis. Differences between NIDS and NIPS are explained on real scenarios. Participants are introduced into SNORT. Day three ends with case study related to the learned topics.

I. Capturing and analysing wireless traffic

- Sniffing challenges in a WiFi world
- Configuring our network card
- Sniffing packets
- Analysing wireless packet capture

II. Network intrusion detection and analysis

- Understanding network intrusion detection systems (NIDS)
- Understanding network intrusion prevention systems (NIPS)
- Differentiating between NIDS and NIPS
- Modes of detection
- NIDS/NIPS evidence acquisition
- Using SNORT for network intrusion detection and prevention
- Comprehensive packet logging
- Security Information and Event Management (SIEM)
- Case study

DAY 4

Day four is dedicated to understanding log formats, their sources, collection and analysis. Network logs are analyzed using Splunk. Day continues with explanation of switches, routers, firewalls and their importance in network forensics analysis. Finally, at the end of day participants learn about proxies and their analysis from the network forensic point of view.

I. Event log aggregation, correlation, and analysis

- Understanding log formats
- Sources of logs
- Network log architecture
- Collecting and analysing evidence
- Analysing network logs using Splunk
- Case study

II. Switches, routers, and firewalls

- Storage media
- Interfaces
- Logging
- Different types of firewalls
- Interpreting firewall logs

III. Web proxies

- Roles proxies play
- Types of proxies
- Evidence
- Squid
- Web proxy analysis
- Encrypted web traffic
- Case study

DAY 5

Day five starts with network tunneling principles, types and vulnerabilities. After that, participants are introduced to network virtualization and possibilities that are offered through virtualization tools. Finally, students get the list of open source tools for network traffic capture and analysis. The workshop ends with the final exam, survey and certification ceremony for the successful students.

I. Network tunnelling

- Understanding VPNs
- How does tunnelling work
- Types of tunnelling protocols
- Various VPN vulnerabilities and logging

II. Network virtualization

III. Open source tools for network traffic capture and analysis

IV. Final exam

V. Survey and certification ceremony