Organising institution

Università degli Studi di Padova
Dipartimento di Ingegneria dell'Informazione - DEI
Prof. Nicola Laurenti

Visiting Professor

Alexandru Soceanu
Hochschule Munchen (Munich University of Applied Sciences), Germany

Course Title and Description

Secure Networks

The project consists of 4 seminars on Secure Network Management. Laboratory activities under the supervision of prof. Soceanu will follow the lectures. Finally, part of the exam of the Master course will be on the contents
Of these seminars and prof. Soceanu will collaborate also in this phase.

The detailed programme is the following:

Learning objectives:
After completing this short intensive practical oriented course, students will be able to:
- understand the role and the objectives of network management (NM) for an organization
- learn how to investigate standard/private Management Information Bases (MIB)
- implement and analyse the most up to date used type of secure NM monitoring protocol:
SNMPv3
- generate and investigate network attacks on network traffic and network components
- use Next Generation tools and techniques: NGFW, NGIPS, RADIUS, NGSIEM for protecting the network by having hands on commercial protection tools as i.e.: NGFW from Palo Alto Networks, NGSIEM from SPLUNK and NGIPS from SNORT

Syllabus:
Topic 1. Review Computer Networking Knowledge: TCP/IP Stack, Routing-Algorithms, -Protocols RIPv2, OSPF, Routing-Tables
Topic 2. Network Management Information Bases (MIBs): Reference Model: Monitor-Agent, Legacy Network Management Functionality, Distributed Network Management, Visualization Access and Security (EVAS) Concept, Standard and Private MIBs structure, MIB II, Structure of Management Information (SMI) using ASN.1 language
Topic 3. Network Monitoring Protocols: SNMPv2-Protocols, NetFlow Protocol and NetFlow Collector based on NfSen Server, Network Management Server OpenNMS
Topic 4. Secure Network Monitoring: SNMPv1&v2 Security aspects, Secure SNMPv3, SNMPv3 configuration, Network Visibility using SIEM technology, Applied SIEM technology for Network Security, Case study using SPLUNK application.
Topic 5. Attacks to Network Security: Network type of attacks: Reconnaissance (Recon), Denial of Service (DoS), Tools for generating network attacks: SCAPY (Python based) and Metasploit.
Topic.6. Managing Computer Network Security: Network Security Overview (Confidentiality, Integrity, Availability Model), Next Generation FW (NGFW), Next Generation IPS (NGIPS), Network Access Control (NAC), FreeRADIUS, Sandbox, Network Access Decision Control using Policy Engines, Case Studies.
4 x Lab Assignments used for support the project:
All the assignments will be carried out using the virtual lab container with already preinstalled network components and open source/commercial software tools.The completion the assignments are mandatory for being admitted to project presentation.

	Collaborative Project: A project will be assigned to the students. It will be carried out in a collaborative manner by teams of 2 students. The project is mandatory for evaluating the achieving the learning objectives of the short practical “Secure Network Management” course.
Period	01/11/2021 – 15/12/2021
Course Level	Master degree courses in ICT for Internet and Multimedia, in Cybersecurity and in Computer Engineering