Technology
Arts Sciences
TH Köln

Course
NSA - Network Security and Automation

Version: 7 | Last Change: 09.12.2022 13:03 | Draft: 0 | Status: vom verantwortlichen Dozent freigegeben

General information

Long name	Network Security and Automation
Approving CModule	NSA_BaTIN, NSA_BaET
Responsible	Prof. Dr. Andreas Grebe Professor Fakultät IME
Level	Bachelor
Semester in the year	summer semester
Duration	Semester
Hours in self-study	60
ECTS	5
Professors	Prof. Dr. Andreas Grebe Professor Fakultät IME
Requirements	Knowledge and Competences of Module Networks and Protocols (NP) alternate requorements: knowledge and competences of IP networking courses or CCNA (ITN and RSE) Networking Fundamentals TCP/IP Protocol Family ISO/OSI Model and Protocols IPv4/IPv6 Addressing, Subnetting, and Routing Switching Techniques TCP/UDP Transport Techniques Application Protocols Network Implementation Competences (Client, Server, Switch, Router)
Language	German
Separate final exam	Yes

Final exam

Details

In a final examination (written, optionally oral), the students demonstrate their competences in summary form. The exam comprises the following sub-areas, in which six taxonomy levels (reproduce, understand, apply, analyze, synthesize, and evaluate) are included.
1.) A good command of basic concepts, concepts and techniques. Typical tasks are multiple-choice questions, open questions, evaluation of statements regarding their correctness.
2.) Application of planning and valuation techniques. Typical tasks are planning tasks of networks or subsystems.
3.) Examination of proposed solutions for correctness, identification of errors in statements or given networks. Typical tasks include the analysis of given network architectures and system statements.

Minimum standard

Achievement of the individual minimum score per exam, typically 50% of maximum score.

Exam Type

In a final examination (written, optionally oral), the students demonstrate their competences in summary form. The exam comprises the following sub-areas, in which six taxonomy levels (reproduce, understand, apply, analyze, synthesize, and evaluate) are included.
1.) A good command of basic concepts, concepts and techniques. Typical tasks are multiple-choice questions, open questions, evaluation of statements regarding their correctness.
2.) Application of planning and valuation techniques. Typical tasks are planning tasks of networks or subsystems.
3.) Examination of proposed solutions for correctness, identification of errors in statements or given networks. Typical tasks include the analysis of given network architectures and system statements.

Lecture / Exercises

Learning goals

Knowledge

Fundamentals for the construction of hierarchically structured networks, corporate networks with redundancy techniques, wireless LAN (WLAN), cross-location communication, WAN techniques. Introduction to network security with details on attacks, security targets, cryptographic procedures, encryption, packet filters, secure infrastructures, virtual private networks. Introduction to distributed network management and service quality techniques. Techniques for network virtualization, software-defined networking and network automation.

Excerpt of the contents:
Hierarchical networks, redundancy, STP, EtherChannel, FHRP, Single-area and Multiarea OSPF, OSPF security technologies, WLAN, WAN connection, PPP, xDSL
Network security with security goals, cryptographic methods, algorithms, packet filters, ACL, NAT, FireWall, DMZ, VPN, IPsec
SNMP, Syslog, QoS - Quality of Service
Software Defined Networking (SDN), SDN Controller, Cloud, Virtualization, Ansible, JSON, YAML, REST API

Skills

Students acquire the skills to analyse medium-sized, cross-location corporate networks using suitable tools, to select suitable architectures and to plan and implement corresponding networks. They name and identify hazard situations for corporate networks. Suitable security mechanisms are to be

selected, designed and implemented. Tasks and methods of software-controlled networks including virtualization are known and mechanisms for network automation are planned and implemented.

Expenditure classroom teaching

Type	Attendance (h/Wk.)
Lecture	2
Exercises (whole course)	2
Exercises (shared course)	0
Tutorial (voluntary)	0

Separate exam

none

Practical training

Learning goals

Knowledge

Identify, structure and classify concepts and technologies for medium-sized, cross-location corporate networks. Master network analysis techniques and tools, know network design steps and methods for network planning. Identify security-relevant network gaps and know suitable measures for network security and their implementation. Know the tasks of network automation and virtualisation and master their implementation for suitable network areas.

Skills

Planning, implementation and analysis of VLAN architectures, WLAN networks, cross-site VPN and packet filter firewall.
Implementation and analysis of network management with SNMP and Syslog.
Implementation and analysis of network automation on network elements (e.g. router, switch, host, SDN controller) via REST API with Phython scripting or Ansible YAML scripting.

Expenditure classroom teaching

Type	Attendance (h/Wk.)
Practical training	1

Tutorial (voluntary)	0

Separate exam

Exam Type

working on practical scenarion (e.g. in a lab)

Details

There are several lab dates with different tasks.
The following tasks have to be completed for each date:
Independent solution of the preparatory self-learning tasks (homework).
Solution of the network design, implementation and analysis tasks in a small team (typically 2 students), if necessary with the help of assistance.
Optional participation in Cisco Academy CCNA (Cisco Certified Network Associate) modules is possible. The successful completion of selected CCNA 1 and CCNA 2 labs is recognized for the internship.

Minimum standard

Successful participation in all lab dates, correct solution of all self-learning tasks and completion of all tasks of the lab date.