

**TECHNICAL UNIVERSITY OF
MOLDOVA**

**PRACTICAL EXAMPLES
SOLVED TO BE
INTRODUCED IN
NETWORK SECURITY**

PRACTICAL GUIDE



CHIȘINĂU 2023



**TECHNICAL UNIVERSITY OF
MOLDOVA**

**FACULTY OF COMPUTERS,
INFORMATICS AND
MICROELECTRONICS**

**DEPARTMENT SOFTWARE
ENGINEERING AND AUTOMATICS**

NETWORK SECURITY

Practical examples solved to be introduced in network security

**Chişinău
Publisher „Tehnica-UTM”
2023**

CZU 004.72.056

P 48

The paper was discussed and approved for editing at the meeting of the council of the Faculty of Computers, Informatics and Microelectronics, process_no. 5 of. 28.04.2023

The practical guide is intended for the students from FCIM (Faculty of Computers, Informatics and Microelectronics) and FET (Faculty of Electronics and Telecommunications) who study the Networks Security course and aims to deepen their knowledge at seminars and for laboratory work.

The guide materials will assist you in developing the skills necessary to do the following: describe the security threats facing modern network infrastructures; secure Cisco devices; secure the network infrastructure; implement AAA on CISCO routers using a local router database and external AAA servers; mitigate threats to Cisco routers and networks using access control lists (ACLs); implement secure network design, management, and reporting; implement the Cisco IOS firewall feature set; mitigate common Layer 2 attacks; implement a site-to-site VPN; implement a remote access VPN.

Guide is focused on creating the global problem solvers needed to build, scale, secure, and defend the networks that used in our daily lives. The need for well-trained network security specialists continues to grow at an exponential rate.

The guide includes 44 examples of problems and tasks solved, the set of commands with description, 46 variants of exam preparation questions.

Authors: lecturer mag., Ludmila Peca
lecturer mag., Dinu Țurcanu

Reviewers: Associate professor, PhD. Dumitru Ciorbă
Associate professor, PhD. Natalia Burlacu

DESCRIEREA CIP A CAMEREI NAȚIONALE A CĂRȚII DIN RM

Peca, Ludmila, Țurcanu, Dinu.

Network security: Practical examples solved to be introduced in network security/
Ludmila Peca, Dinu Țurcanu; Technical University of Moldova, Faculty of Computers,
Informatics and Microelectronics, Department Software Engineering and Automatics.

– Chișinău: Tehnica-UTM, 2023. – 243 p.: fig., tab.

Aut. indicați pe vs. f. de tit. – Bibliogr.: p. 241-242 (16 tit.). – 50 ex.

ISBN 978-9975-45-941-9.

004.72.056

P 48

CONTENT

About:	5
Introduction:	6
EP1: Lab - Configure Secure Administrative Access	7
EP2: Packet Tracer - Configure Secure Passwords and SSH	17
EP3: Lab - Configure Network Devices with SSH	19
EP4: Lab - Configure Administrative Roles	24
EP5: Lab - Basic Device Configuration and OSPF Authentication	33
EP6: Packet Tracer - Configure OSPF Authentication	40
EP7: Packet Tracer - Configure and Verify NTP	42
EP8: Lab - Configure Cisco IOS Resilience Management and Reporting	44
EP9: Packet Tracer - Configure Cisco Devices for Syslog, NTP, and SSH Operations	55
EP10: Lab - Configure Local AAA Authentication	58
EP11: Packet Tracer - Configure Local AAA for Console and VTY Access	68
EP12: Lab - Install the Virtual Machine	70
EP13: Lab - Configure Server-Based Authentication with RADIUS	75
EP14: Packet Tracer - Configure Server-based AAA with TACACS and RADIUS	85
EP15: Packet Tracer - ACL Demonstration	88
EP16: Packet Tracer - Configure Named Standard IPv4 ACLs	91
EP17: Packet Tracer - Configure Numbered Standard IPv4 ACLs	93
EP18: Packet Tracer - Configure Extended ACLs - Scenario 1	96
EP19: Packet Tracer - Configure Extended IPv4 ACLs - Scenario 2	100
EP20: Packet Tracer - Configure IP ACLs to Mitigate Attacks	103
EP21: Packet Tracer - Configure IPv6 ACLs	106
EP22: Packet Tracer - Identify Packet Flow	108
EP23: Packet Tracer - Configure a ZPF	111
EP24: Lab - Configure ZPFs	115
EP25: Packet Tracer - Implement a Local SPAN	126
EP26: Packet Tracer - Implement Port Security	128
EP27: Packet Tracer - Investigate STP Loop Prevention	130
EP28: Lab - Configure STP Security	132
EP29: Packet Tracer - Implement STP Security	146
EP30: Packet Tracer - Layer 2 VLAN Security	149
EP31: Lab - Creating Codes	152
EP32: Lab - Exploring Encryption Methods	154
EP33: Lab - Hashing Things Out	158
EP34: Lab - Encrypting and Decrypting Data Using OpenSSL	161
EP35: Lab - Encrypting and Decrypting Data using a Hacker Tool	164
EP37: Lab - Examining Telnet and SSH in Wireshark	168
EP38: Lab - Certificate Authority Stores	171
EP39: Packet Tracer - Configure and Verify a Site-to-Site IPsec VPN	178
EP40: Lab - Configure a Site-to-Site VPN	183
EP41: Optional Lab - Configure ASA Basic Settings Using CLI	196

EP42: Packet Tracer - Configure ASA Basic Settings and Firewall Using the CLI 207
EP43: Optional Lab - Configure ASA Network Services, Routing, and DMZ with ACLs Using CLI 212
EP44: Lab - Configure ASA Basic Settings and Firewall Using ASDM 223
Exam Preparation Questions: 234
BIBLIOGRAPHY: 241

(EP) - Practical example

About:

Network security is a broad term that covers a multitude of technologies, devices and processes. In its simplest term, it is a set of rules and configurations designed to protect the integrity, confidentiality and accessibility of computer networks and data using both software and hardware technologies. Every organization, regardless of size, industry or infrastructure, requires a degree of network security solutions in place to protect it from the ever-growing landscape of cyber threats in the wild today.

Today's network architecture is complex and is facing a threatful environment that is always changing and attackers that are always trying to find ways to exploit vulnerabilities. These vulnerabilities can exist in a broad number of areas, including devices, data, applications, users and locations. For this reason, there are many network security management tools and applications in use today that address individual threats and exploits and also regulatory non-compliance. When just a few minutes of downtime can cause widespread disruption and massive damage to an organization's bottom line and reputation, it is essential that these protection measures are in place.

The guide of solved practical exercises is developed according to the study programs in the course Networks Security for the Technical University of Moldova.

Each paper concludes with comprehension verification questions, which include the minimum knowledge required to perform the laboratory work that will be presented to students by the teacher.

The guide is intended for students enrolled in the specialties where the Networks Security course can be found in the curriculum, full-time or part-time mode of study.

The support that contains solved practical examples is as an Appendix for the lessons recorded for the Networks Security university course on the eLearning platform of the Technical University of Moldova, access link:

<https://lectii.utm.md/courses/retele-de-calculatoare-computer-networks/>

https://www.researchgate.net/publication/367041027_Computer_networks_Practical_examples_solved_to_be_introduced_in_computer_networks

This guide is intended to supplement the didactic-methodical support of the Network Security discipline included in the study programmes of several specialties within the Technical University of Moldova.

Introduction:

Networks are routinely attacked. A quick Internet search for network attacks will return many articles about network attacks, including news about organizations that have been compromised, the latest threats to network security, attack mitigation tools, and more.

Network security directly relates to the business continuity of an organization. Network security breaches can disrupt e-commerce, cause loss of business data, threaten people's privacy and compromise information integrity. These breaches can result in lost revenue for corporations, intellectual property theft, lawsuits, and even threaten public safety.

Maintaining a secure network ensures the safety of network users and protects business interests. Keeping a network secured requires vigilance from an organization's network security professionals. The latterly must be constantly aware of new and evolving network threats and attacks, as well as device and application vulnerabilities.

Internal threats have the potential to cause greater damage than external threats because internal users have direct access to the building and its infrastructure devices. Employees may also have knowledge of the corporate network, its resources, and its confidential data.

Network security professionals must implement tools and apply techniques to mitigate both external and internal threats, in order to protect organization's data, as well as implement various data loss prevention controls that combine strategic, operational and tactical measures.

BIBLIOGRAPHY:

1. Ludmila Peca, Dinu Țurcanu. Computer networks: Practical examples solved to be introduced in computer networks. ISBN 978-9975-45-812-2. Chișinău, Publisher „Tehnica-UTM”, 2022.
2. Balchunas, Aaron. Cisco CCNA Study Guide. 2014;
3. CISCO CCNA Network Security course;
4. CISCO CCNA Cybersecurity Operations course;
5. CISCO CCNA Security course;
6. Kurose, James F., and Keith W. Ross. Computer Networking: A Top-Down Approach. 7th ed., Pearson, 2017.
7. Stallings, William. Network Security Essentials: Applications and Standards. 6th ed., Pearson, 2017.
8. Dinu Țurcanu, Natalia Spinu, Serghei Popovici, Tatiana Țurcanu. Cybersecurity of the Republic of Moldova: a retrospective for the period 2015-2020. Journal of Social Sciences, Vol. IV, no. 1 (2021), pp. 74 – 83.
9. Stevens, W. Richard. TCP/IP Illustrated, Volume 1: The Protocols. Addison-Wesley Professional, 2011.
10. Rodica Bulai, Dinu Țurcanu, Dumitru Ciorbă. Education in Cybersecurity. Central and Eastern European eDem and eGov Days 2019 - Conferința "Central and Eastern European eDem and eGov Days ", Budapesta, Hungary, 2-3 mai 2019.
11. Dinu Țurcanu, Serghei Ppovici, Tatiana Țurcanu, “Digital signature: advantages, challenges and strategies,” Journal of Social Sciences, Vol. III, no. 4 (2020), pp. 62 - 72.
12. Carolina Timco, Larisa Bugaian, Dinu Țurcanu, “Governance of the Technical University of Moldova in the digital era,” Journal of Social Sciences, Vol. II, no. 2 (2019), pp. 19 - 27.
13. D. Țurcanu, Rodica Siminiuc, V. Bostan & T. Țurcanu, “Impact of the Covid-19 Pandemic on the Use of Microsoft 365 and Learning Outcomes at the Technical University of Moldova,” International Conference on Nanotechnologies and Biomedical Engineering, ICNBME 2021: 5th International Conference on Nanotechnologies and Biomedical Engineering, pp. 456–462.
14. Dinu Țurcanu, Rodica Siminiuc, Viorel Bostan, “The Impact of the COVID-19 Pandemic on the Use of Digital Technologies in Ensuring the Efficient e-Learning Process at the Technical University of Moldova”, Creative Education, 2020, 11, <https://www.scirp.org/journal/ce>, DOI: 10.4236/ce.2020.1110154, pp.2116–2132.

15. Sanders, Chris. "Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems." 3rd ed., No Starch Press, 2017.
16. ȚURCANU, Dinu; CHIHAI, Andrei; RUSSU, Gabriel. Ghid metodic pentru lucrări de laborator la disciplina "Rețele de calculatoare". Partea întâia. Chișinău, UTM, 2012.