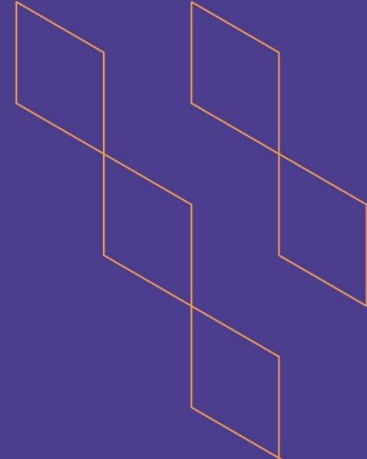




T-104
2022

Course Specification



| |
|--|
| Course Title: Network Security |
| Course Code: IT11004 |
| Program: Bachelor of Information Technology |
| Department: Information Technology |
| College: Faculty of Computer Science and IT |
| Institution: AlBaha University |
| Version: V2022 |
| Last Revision Date: 29 March 2023 |



Table of Contents:

| Content | Page |
|---|------|
| A. General Information about the course | 3 |
| 1. Teaching mode (mark all that apply) | 4 |
| 2. Contact Hours (based on the academic semester) | 4 |
| B. Course Learning Outcomes (CLOs), Teaching Strategies and Assessment Methods | 5 |
| C. Course Content | 6 |
| D. Student Assessment Activities | 7 |
| E. Learning Resources and Facilities | 8 |
| 1. References and Learning Resources | 8 |
| 2. Required Facilities and Equipment | 8 |
| F. Assessment of Course Quality | 8 |
| G. Specification Approval Data | 9 |



A. General information about the course:

Course Identification

1. Credit hours: 3

2. Course type

a. University College Department Track Others

b. Required Elective

3. Level/year at which this course is offered: 10th

4. Course general Description

The Network Security course provides students with an in-depth understanding of the principles and practices of securing and managing computer networks. The course covers the concepts, tools, and techniques necessary for securing and administering modern computer networks, including wired and wireless networks, cloud-based systems, and mobile devices.

5. Pre-requirements for this course (if any):

6. Co- requirements for this course (if any):

7. Course Main Objective(s)

1. Understand the basic principles of network security, including network architecture, protocols, and services.
2. Identify and assess potential network security threats, including malware, phishing, and denial-of-service attacks, and develop appropriate security measures to mitigate these threats.
3. Design and implement secure computer networks using appropriate security measures, including firewalls, intrusion detection systems, and other tools.
4. Develop proficiency in network administration, including network management, troubleshooting, and performance optimization.
5. Evaluate the effectiveness of network security measures, policies, and procedures in real-world scenarios, and recommend improvements as necessary.
6. Analyze and evaluate network security threats and recommend appropriate solutions.
7. Develop comprehensive network security policies and procedures.
8. Synthesize various network security measures to create a cohesive and effective security strategy.
9. Demonstrate the ability to communicate effectively and collaborate with peers on network security and administration topics.
10. Understand ethical and legal considerations related to network security and administration, including data privacy and confidentiality.



1. Teaching mode (mark all that apply)

| No | Mode of Instruction | Contact Hours | Percentage |
|----|--|---------------|------------|
| 1. | Traditional classroom | 33 | 100% |
| 2. | E-learning | | |
| 3. | Hybrid <ul style="list-style-type: none"> • Traditional classroom • E-learning | | |
| 4. | Distance learning | | |

2. Contact Hours (based on the academic semester)

| No | Activity | Contact Hours |
|----|-------------------|---------------|
| 1. | Lectures | 22 |
| 2. | Laboratory/Studio | 22 |
| 3. | Field | |
| 4. | Tutorial | |
| 5. | Others (specify) | |
| | Total | 44 |



B. Course Learning Outcomes (CLOs), Teaching Strategies and Assessment Methods

| Code | Course Learning Outcomes | Code of CLOs aligned with program | Teaching Strategies | Assessment Methods |
|------|---|-----------------------------------|--|--|
| 1.0 | Knowledge and understanding | | | |
| 1.1 | Define the basic concepts of network security, including network architecture, protocols, and services. | K1 | <ul style="list-style-type: none"> Lectures Assignments Lab Exercises | <ul style="list-style-type: none"> Quizzes Midterm Exams Final Exam |
| 1.2 | Identify various types of network security threats, such as malware, phishing, and denial-of-service attacks. | K2 | <ul style="list-style-type: none"> Lectures Assignments Lab Exercises | <ul style="list-style-type: none"> Quizzes Midterm Exams Final Exam |
| 1.3 | Explain the principles of threat modeling and risk assessment in the context of network security. | K2 | <ul style="list-style-type: none"> Lectures Assignments Lab Exercises | <ul style="list-style-type: none"> Quizzes Midterm Exams Final Exam |
| 2.0 | Skills | | | |
| 2.1 | Design and implement secure computer networks using appropriate security measures, including firewalls, intrusion detection systems, and other tools. | S1 | <ul style="list-style-type: none"> Lectures Assignments Lab Exercises | <ul style="list-style-type: none"> Quizzes Midterm Exams Lab Exam Final Exam |
| 2.2 | Evaluate the effectiveness of network security measures, policies, and procedures in real-world scenarios, and recommend improvements as necessary. | S2 | <ul style="list-style-type: none"> Lectures Assignments Lab Exercises | <ul style="list-style-type: none"> Quizzes Midterm Exams Lab Exam Final Exam |
| 2.3 | Demonstrate proficiency in network administration, including network management, troubleshooting, and performance optimization. | S3 | <ul style="list-style-type: none"> Lectures Assignments | <ul style="list-style-type: none"> Quizzes Midterm Exams Lab Exam Final Exam |
| 3.0 | Values, autonomy, and responsibility | | | |



| Code | Course Learning Outcomes | Code of CLOs aligned with program | Teaching Strategies | Assessment Methods |
|------|---|-----------------------------------|---|---|
| 3.1 | Communicate effectively and collaborate with peers on network security and administration topics. | V1 | <ul style="list-style-type: none"> • Assignments • Oral Presentations | <ul style="list-style-type: none"> • Reports • Presentations • Class Discussions |
| 3.2 | | | | |
| ... | | | | |

C. Course Content

| No | List of Topics | Contact Hours |
|----|--|---------------|
| 1. | Network Security Fundamentals: This topic covers the basic principles of network security, including types of security threats, network security policies, and security protocols. | 4 |
| 2. | Cryptography: This topic covers the principles of cryptography and encryption, including symmetric and asymmetric encryption, hashing, and digital signatures. | 2 |
| 3. | Access Control and Authentication: This topic covers the principles of access control and authentication, including authentication mechanisms, access control models, and biometric authentication. | 2 |
| 4. | Firewalls and Intrusion Detection Systems: This topic covers the operation and benefits of firewall and intrusion detection systems, including types of firewalls, intrusion detection and prevention techniques, and monitoring and analysis of network traffic. | 2 |
| 5. | Virtual Private Networks (VPNs): This topic covers the principles of VPNs, including the different types of VPNs, their benefits, and implementation strategies. | 2 |
| 6. | Wireless Network Security: This topic covers the principles of wireless network security, including security protocols, encryption, and authentication mechanisms. | 2 |
| 7. | Cloud Security: This topic covers the principles of cloud security, including security concerns, threat modeling, and implementation strategies. | 2 |
| 8. | Threats and Vulnerabilities: This topic covers the types of security threats and vulnerabilities that can affect computer networks, such as malware, phishing, and denial-of-service attacks. | 2 |
| 9. | Network Monitoring and Incident Response: This topic covers the principles of network monitoring and incident response, including threat analysis, risk assessment, and incident management. | 2 |



| | | |
|-------|---|----|
| 10. | Security Policies and Procedures: This topic covers the development of comprehensive network security policies and procedures, including the importance of documentation, risk management, and compliance with industry regulations and standards. | 2 |
| Total | | 22 |

D. Students Assessment Activities

| No | Assessment Activities * | Assessment timing (in week no) | Percentage of Total Assessment Score |
|-----|-------------------------------|--------------------------------|--------------------------------------|
| 1. | Homework and class discussion | Weekly | 10% |
| 2. | Midterm | 5th week | 15% |
| 3. | Quiz | 9th Week | 15% |
| 4. | Lab Exam | 10th Week | 20% |
| 5. | Final Exam | 11th Week | 40% |
| ... | Total | | 100% |

*Assessment Activities (i.e., Written test, oral test, oral presentation, group project, essay, etc.)





E. Learning Resources and Facilities

1. References and Learning Resources

| | |
|--------------------------|---|
| Essential References | Network Security: Private Communication in a Public World Subsequent Edition by Charlie Kaufman, Radia Perlman, Mike Speciner ISBN-10 : 0130460192 |
| Supportive References | Network Security Essentials: Applications and Standards" by William Stallings (6th Edition), Publisher Pearson, ISBN-10 : 9780134527338 |
| Electronic Materials | <ul style="list-style-type: none"> • Access to the Saudi Digital Library (SDL). • ACM (Association for Computer Machinery) web site - http://www.acm.org/ • ACM SIGCSE (Special Interest Group on Computer Science Education) resource website: http://www.sigcse.org/SIGresources • IEEE Computer Society web site: http://www.computer.org/portal/web/guest/home |
| Other Learning Materials | None |

2. Required Facilities and equipment

| Items | Resources |
|--|---|
| facilities (Classrooms, laboratories, exhibition rooms, simulation rooms, etc.) | <ul style="list-style-type: none"> • A classroom or lecture hall with whiteboard for 25 students. • A laboratory with 25 computers. |
| Technology equipment (projector, smart board, software) | Wireshark, Nmap, Kali linux |
| Other equipment (depending on the nature of the specialty) | |

F. Assessment of Course Quality

| Assessment Areas/Issues | Assessor | Assessment Methods |
|--------------------------------------|---|---|
| Effectiveness of teaching | <ul style="list-style-type: none"> • Students • Peer Reviewer • Program Leaders | <ul style="list-style-type: none"> • Survey (indirect) • Peer review (direct) • Class visit (direct) |
| Effectiveness of students assessment | <ul style="list-style-type: none"> • Students • Exam Evaluation Committee • Course Coordinator | <ul style="list-style-type: none"> • Survey (indirect) • Exam Review (direct) review of course file (direct) |
| Quality of learning resources | <ul style="list-style-type: none"> • Faculty • Students | Survey (indirect) |





| Assessment Areas/Issues | Assessor | Assessment Methods |
|---|--|---|
| The extent to which CLOs have been achieved | <ul style="list-style-type: none"> Faculty Program Leaders or Course Coordinator | <ul style="list-style-type: none"> Exams (direct) Exit Exams (direct) |
| Other | | |

Assessor (Students, Faculty, Program Leaders, Peer Reviewer, Others (specify))

Assessment Methods (Direct, Indirect)

G. Specification Approval Data

| | |
|--------------------|------------|
| COUNCIL /COMMITTEE | |
| REFERENCE NO. | |
| DATE | 29/01/2023 |

