



|  |                        |
|--|------------------------|
| <b>Faculty: Information Technology</b> |                        |
| <b>Department: Cybersecurity</b>       | <b>Program: Master</b> |
| <b>Academic year:</b>                  | <b>Semester:</b>       |

## Course Plan

### First: Course Information

|                                      |  |                        |                       |                     |
|--------------------------------------|--|------------------------|-----------------------|---------------------|
| <b>Course No.:</b><br><b>1506735</b> | <b>Course Title: Advance</b><br><b>Network Security</b>  | <b>Credit Hours: 3</b> | <b>Theoretical: 3</b> | <b>Practical: 0</b> |
| <b>Prerequisite No. and Title:</b>   |  | <b>Section No.:</b>    | <b>Lecture Time:</b>  |                     |
| <b>Level in JNQF</b>                 | <b>9</b>   |                        |                       |                     |
| <b>Type Of Course:</b>               | <div><input type="checkbox"/> <b>Obligatory University Requirement</b><input type="checkbox"/> <b>Elective University Requirement</b></div> <div><input type="checkbox"/> <b>Obligatory Faculty Requirement</b><input type="checkbox"/> <b>Elective Faculty Requirement</b></div> <div><input checked="" type="checkbox"/> <b>Obligatory Specialization Requirement</b><input type="checkbox"/> <b>Elective Specialization Requirement</b></div> <div><input type="checkbox"/> <b>Ancillary course</b></div> |                        |                       |                     |
| <b>Type of Learning:</b>             | <div><input checked="" type="checkbox"/> <b>Face-to-Face Learning</b></div> <div><input type="checkbox"/> <b>Blended Learning (2 Face-to-Face + 1 Asynchronous)</b></div> <div><input type="checkbox"/> <b>Online Learning (2 Synchronous+ 1 Asynchronous)</b></div>   |                        |                       |                     |

### Second: Instructor's Information

|                            |               |                          |                |                  |                 |
|----------------------------|---------------|--------------------------|----------------|------------------|-----------------|
| <i>Course Coordinator:</i> |               |                          |                |                  |                 |
| <i>Name:</i>               |               | <i>Academic Rank:</i>    |                |                  |                 |
| <i>Office Number:</i>      |               | <i>Extension Number:</i> |                | <i>Email:</i>    |                 |
| <i>Course Instructor:</i>  |               |                          |                |                  |                 |
| <i>Name:</i>               |               | <i>Academic Rank:</i>    |                |                  |                 |
| <i>Office Number:</i>      |               | <i>Extension Number:</i> |                | <i>Email:</i>    |                 |
| <i>Office Hours:</i>       | <i>Sunday</i> | <i>Monday</i>            | <i>Tuesday</i> | <i>Wednesday</i> | <i>Thursday</i> |

### Third: Course Description

This course introduces fundamental concepts and techniques underlying the science and art of network security, with a primary focus on network security vulnerability assessment and penetration testing, secure network architecture design, and network security services and mechanisms. Examples of attack techniques and tools are introduced, as well as adequate countermeasures against these attacks.

### Fourth: Course Objectives

1. Introducing the student to fundamental concepts and techniques underlying the science and art of network security.
2. Providing the student with a good grasp of network vulnerability assessment techniques, as well as secure architecture design and countermeasure.
3. Developing the student's ability to identify for a target network the security requirements, and extract adequate security policy.
4. Expanding the student's skills to design and implement appropriate protection strategies and countermeasures for a target network.
5. Providing the student with the skills to conduct penetration testing for an existing enterprise network and develop and implement adequate remediation plan.

## Fifth: Learning Outcomes

| <i>Level descriptor according to (JNQF)</i> | <i>CILOs Code</i> | <i>CILOs</i><br>If any CLO will not be assessed in the course, mark NA.   | <i>Associated PILOs Code</i><br>Choose one PILO for each CILO* | <i>Assessment method</i><br>Choose at least two methods   |
|---|-------------------|---|--|---|
| <b>Knowledge</b>                            | <b>K1</b>         | Provide the students with the uses and benefits of network security.  | <b>PK1</b>   | <ul style="list-style-type: none"> <li>• Mid-term Exam</li> <li>• Final Exam</li> <li>• Research</li> </ul> |
|   | <b>K2</b>         | Describe the methods used to assess network vulnerability, as well as design secure network architecture.                                     | <b>PK2</b>   | <ul style="list-style-type: none"> <li>• Mid-term Exam</li> <li>• Final Exam</li> <li>• Research</li> </ul> |
|   | <b>K3</b>         | Demonstrate of methodologies and techniques to identify for a target network the security requirements, and extract adequate security policy. | <b>PK3</b>   | <ul style="list-style-type: none"> <li>• Mid-term Exam</li> <li>• Final Exam</li> <li>• Research</li> </ul> |
|   | <b>K4</b>         | Describe different techniques for dealing with network security.  | <b>PK4</b>   | <ul style="list-style-type: none"> <li>• Mid-term Exam</li> <li>• Final Exam</li> <li>• Research</li> </ul> |
| <b>Skills</b>                               | <b>S1</b>         | design and implement appropriate protection strategies and countermeasures for a target network.  | <b>PS1</b>   | <ul style="list-style-type: none"> <li>• Mid-term Exam</li> <li>• Final Exam</li> <li>• Research</li> </ul> |
|   | <b>S2</b>         | Provide the student with the skills to conduct penetration testing for an existing enterprise network   | <b>PS2</b>   | <ul style="list-style-type: none"> <li>• Mid-term Exam</li> <li>• Final Exam</li> <li>• Research</li> </ul> |
|   | <b>S3</b>         | Understand the available techniques and methods for network security.   | <b>PS3</b>   | <ul style="list-style-type: none"> <li>• Mid-term Exam</li> <li>• Final Exam</li> <li>• Research</li> </ul> |
|   | <b>S4</b>         | Conduct independent research to better comprehend a certain topic or stay current with field developments.                                    | <b>PS4</b>   | <ul style="list-style-type: none"> <li>• Mid-term Exam</li> <li>• Final Exam</li> </ul>                     |

|                     |           |   |            |   |
|---------------------|-----------|---|------------|---|
|                     |           |   |            | <ul style="list-style-type: none"> <li>• Research</li> </ul>  |
| <b>Competencies</b> | <b>C1</b> | Utilize different techniques for dealing with N security  | <b>PC3</b> | <ul style="list-style-type: none"> <li>• Mid-term Exam</li> <li>• Final Exam</li> <li>• Research</li> </ul> |
|                     | <b>C2</b> | Develop effective communication skills with the students to deliver the required skills and providing them with knowledge about network security. | <b>PC4</b> | <ul style="list-style-type: none"> <li>• Mid-term Exam</li> <li>• Final Exam</li> <li>• Research</li> </ul> |

\*CILOs: Course Intended Learning Outcomes; PILOs: Program Intended Learning Outcomes; For each CILO, the PILO could be the same or different.

## Sixth: Learning Resources

|   |   |                                   |               |                              |
|---|---|-----------------------------------|---------------|------------------------------|
| <b>Main Reference:</b>                    | <b>Computer Security – Art and Sciences</b>   |                                   |               |                              |
| <b>Author: Matt Bishop</b>                |   | <b>Issue No.:<br/>2nd edition</b> | <b>Print:</b> | <b>Publication Year:2019</b> |
| <b>Additional Sources &amp; Websites:</b> | <ul style="list-style-type: none"><li>• The Basics of Hacking and Penetration Testing - Ethical Hacking and Penetration Testing Made Easy.</li><li>• Computer Network Security</li></ul>                    |                                   |               |                              |
| <b>Teaching Type:</b>                     | <input checked="" type="checkbox"/> Classroom <input checked="" type="checkbox"/> Laboratory <input type="checkbox"/> Workshop <input type="checkbox"/> MS Teams <input checked="" type="checkbox"/> Moodle |                                   |               |                              |

## Seventh: Course Structure

| Lecture Date        | Course Intended Teaching Outcomes (CILOs) | Topics  | Teaching Procedures * | Teaching Methods**                        | References***                 |
|---------------------|---|---|-----------------------|---|-------------------------------|
| <b>Week 1</b>       | C2, K1                                    | -Network Security Overview<br>- Introduction of fundamental security principles and concepts                                    | Face-to-Face          | Lecturing                                 | Textbook-ch1                  |
| <b>Week 2</b>       | C2, K1                                    | Network Protocols and Addressing Schemes  | Face-to-Face          | Lecturing, Research Assignments           | Textbook-ch1, Research Papers |
| <b>Week 3</b>       | S1, K2, K3, K4                            | Network Attacks and Penetration Testing   | Face-to-Face          | Lecturing, Research Assignments           | Textbook-ch2                  |
| <b>Week 4</b>       | S1, K2, K3, K4                            | Authentication Systems and Protocols  | Face-to-Face          | Practice, Lecturing, Research Assignments | Textbook-ch2                  |
| <b>Week 5</b>       | S1, K2, K3, K4                            | Port scanning, denial of service, attack on authentication system   | Face-to-Face          | Practice, Lecturing, Research Assignments | Textbook-ch2                  |
| <b>Week 6</b>       | S2, K2, K3, K4                            | Web Applications Attacks<br>-Code injection<br>-SQL injection<br>-Cross-Site Scripting  | Face-to-Face          | Practice, Lecturing, Research Assignments | Textbook-ch3                  |
| <b>Week 7</b>       | S2, K2, K3, K4                            | Malicious Software<br>-Trojan horses<br>- Rootkits<br>- Viruses<br>- Worms<br>- Botnets<br>- Exploit Kits (EKs)<br>- Ransomware | Face-to-Face          | Practice, Lecturing, Research Assignments | Textbook-ch4                  |
| <b>Midterm Exam</b> |   |   |                       |   |                               |

|                   |                    |  |              |   |                               |
|-------------------|--------------------|--|--------------|---|-------------------------------|
| <b>Week 8</b>     | S3, K2, K3, K4     | <i>Firewall Systems</i><br>- Classes of firewall<br>- Firewall configurations and architectures<br>- Network Address Translation (NAT)<br>- Linux IP Tables                | Face-to-Face | Practice, Lecturing, Research Assignments | Textbook-ch 6                 |
| <b>Week 9</b>     | S3, K2, K3, K4     | <i>Intrusion Detection Systems (IDS)</i><br>- IDS models, architectures, and tools<br>- Intrusion Prevention Systems (IPS)<br>- IDS/IPS performance metrics and evaluation | Face-to-Face | Lecturing                                 | Textbook-ch 7                 |
| <b>Week 10</b>    | S1, K2, K3, K4     | <i>Virtual Private Network (VPN)</i><br>- Network Layer Security<br>- IPSec protocol<br>- VPN Technology<br>- Secure Network Architecture                                  | Face-to-Face | Lecturing                                 | Textbook-ch8                  |
| <b>Week 11</b>    | S2, K2, K3, K4     | <i>Biometrics Systems</i><br>- Biometric system components<br>- Biometric performance metrics and evaluation techniques  | Face-to-Face | Practice, Assignments                     | Textbook-ch9                  |
| <b>Week 12</b>    | C1, C2, S3, S4, K1 | -- Technologies overview:<br><i>fingerprint, face, gait, keystroke dynamic</i>   | Face-to-Face | Lecturing                                 | Textbook-ch9                  |
| <b>Week 13</b>    | C1, C2, S3, S4, K1 | <i>Security Policies</i><br>- Notions and examples of security policies and models: Bell-LaPadulla, Biba, Chinese  | Face-to-Face | Lecturing                                 | Textbook-ch5, Research Papers |
| <b>Week 14</b>    | C1, C2, S3, S4, K1 | -Basic access control model, reference monitor concept, security kernel.<br>- Role-based access control model  | Face-to-Face | Practice, Lecturing, Research Assignments | Textbook-ch5                  |
| <b>Final Exam</b> |                    |  |              |   |                               |

\*Teaching procedures: (Face-to-Face, synchronous, asynchronous).

\*\* Teaching methods: (Lecture, video....).

\*\*\* Reference: (Pages of the book, recorded lecture, video....)

## Eighth: Assessment Methods

| Methods                 | Online Learning | Blended Learning | Face-To-Face Learning | Specific Course Output to be assessed<br>**If any CILO will not be assessed in the course, mark NA. |    |    |    |    |    |    |    |    |    |
|-------------------------|-----------------|------------------|-----------------------|---|----|----|----|----|----|----|----|----|----|
|                         |                 |                  |                       | K1  | K2 | K3 | K4 | S1 | S2 | S3 | S4 | C1 | C1 |
| First Exam              |                 |                  |                       |   |    |    |    |    |    |    |    |    |    |
| Second Exam             |                 |                  |                       |   |    |    |    |    |    |    |    |    |    |
| Mid-term Exam           |                 |                  | 30                    |   | ✓  |    | ✓  | ✓  | ✓  | ✓  |    |    | ✓  |
| Participation           |                 |                  |                       |   |    |    |    |    |    |    |    |    |    |
| Asynchronous Activities |                 |                  |                       |   |    |    |    |    |    |    |    |    |    |
| Quizzes                 |                 |                  |                       |   |    |    |    |    |    |    |    |    |    |
| Assignments/ Research   |                 |                  | 30                    | ✓   | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  |
| Group presentation      |                 |                  |                       |   |    |    |    |    |    |    |    |    |    |
| Final Exam              |                 |                  | 40                    | ✓   | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  |
| Total out of 100        |                 |                  | 100                   |   |    |    |    |    |    |    |    |    |    |

## Ninth: Course Policies

- All course policies are applied to all teaching patterns (online, blended, and face-to-face Learning) as follows:
  - a. Punctuality.
  - b. Participation and interaction.
  - c. Attendance and exams.
- Academic integrity: (cheating and plagiarism are prohibited).

| Approval           | Name | Date | Signature |
|--------------------|------|------|-----------|
| Head of Department |      |      |           |
| Faculty Dean       |      |      |           |