

**COLLEGE OF INFORMATION TECHNOLOGY**

**DEPARTMENT OF INFORMATION TECHNOLOGY**

**COURSE SYLLABUS/ SPECIFICATION**

**Course Code & Title:** ITCS 443 - SecurityServices

**Weight:** (2- 2 - 3)

**Prerequisite:** ITCS 404

**NQF Level Allocated:** Level 8

**NQF Notional Hours / Credits:** 120 notional hours/ 12 NQF credit

**Description:** This course provides layers of protection that helps to address both known and emerging threats at Windows Server 2016. Students will learn how to secure your infrastructure and see how protections were build to mitigate an array of attack vectors and to deal with overall threat of ongoing attacks inside the datacenter. Explore ways to configure network security, including firewalls, and look at secure virtualization, like encryption-supported virtual machines. Further, students will learn security service concepts such as threat detection, privileged identity, desired state configuration and more.

**Objective:**

1. To know the current nature of the security threat landscape
2. To design new security architecture and features of Windows Server 2016 that mitigate threats
3. To identify the insights into the security services bundled with Windows Server 2016 latest edition
4. To get knowledge of the supporting security external infrastructure
5. To understand the new security features of Hyper-V
6. To learn about Desired State Configuration (DSC)
7. To determine usage scenarios for Encrypting File System (EFS)

**Semester:**

**Instructor (s):**

**Office Telephone: Email (s):**

**Intended Learning Outcomes (ILOs):**

|  |  |  |
| --- | --- | --- |
| 1. **Knowledge and Understanding** | | **NQF Descriptor/ Level** |
| **A1** | **Concepts and Theories:** Demonstrate, critical and understanding of concepts, and specialized theories relating to security services and related infrastructure using various tools and methods. | Knowledge: theoretical understanding  [Level 8] |
| **A2** | **Contemporary Trends, Problems and Research:**  Demonstrate critical understanding of major current issues of security services, and research on new trends in protecting information. | Knowledge: theoretical understanding  [Level 8] |
| **A3** | **Professional Responsibility: N/A** |  |

|  |  |  |
| --- | --- | --- |
| 1. **Subject-specific Skills** | | **NQF Descriptor/ Level** |
| **B1** | **Problem Solving:**  Identify real life problems and Design the solution pertains to security services. Gather, and organize material from various sources independently (including library, electronic and online resources), and critically evaluate its significance. | Knowledge: Practical Application  [Level 8] |
| **B2** | **Modeling and Design:** Design the infrastructure and services by choosing specialized appropriate components and models that satisfy security specifications. | Knowledge: Practical Application  [Level 8] |
| **B3** | **Application of Methods and Tools:** Apply appropriate security management tools to implement secure infrastructure virtualization, JIT, JET, PAWS, threat detection solutions. | Knowledge: Practical Application  [Level 8] |

|  |  |  |
| --- | --- | --- |
| 1. **Critical-Thinking Skills** | | **NQF Descriptor/ Level** |
| **C1** | **Analytic skills:** Critically analyze specialized case studies and recommend suitable solutions. | Generic Problem solving & Analytical skills [Level 8] |
| **C2** | **Synthetic:** Integrate appropriate information security components into one effective security system | Generic Problem solving & Analytical skills [Level 8] |
| **C3** | **Creative Thinking and innovation:** Demonstrate creativity in the development of effective security systems to control the problems of information systems. | Generic Problem solving & Analytical skills [Level 8] |

|  |  |  |
| --- | --- | --- |
| 1. **General and Transferable Skills (other skills relevant to employability and personal development)** | | **NQF Descriptor/ Level** |
| **D1** | **Communication:** Express and communicate complex ideas related to security services in written and oral forms. | Communication, ICT and Numeracy skills [Level 8] |
| **D2** | **Teamwork and Leadership:** Demonstrate the ability to work as a group member/leader and share the ideas together | Competence: Autonomy, Responsibility and context  [Level 8] |
| **D3** | **Organizational and Developmental Skills:**  Demonstrate the ability to organize ideas and effectively allocate time given in given assignments and projects | Competence: Autonomy, Responsibility and context  [Level 8] |
| **D4** | **Ethics and Social Responsibility:** Demonstrate an understanding of the role of culture as it applies to ethics in information security | Competence: Autonomy, Responsibility and context  [Level 8] |

**Course Structure (Outline)**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Week** | **Hours** | | **ILOs** | **Topics** | **Teaching Method** | **Assessment Method** |
| **Lec.** | **Lab** |
| 1 | 4 | - | A1 | Introduction | Lecture / Class Discussion |  |
| 2 | 2 | 2 | A1 | **Server Hardening Solutions**  Configure disk and file encryption | Lecture/ Class Discussion | In-Lab  Exercises |
| 3 | 2 | 2 | A1, B1, B3 | **Implement Server Hardening Solutions**  Implement malware protection  Protect credentials | Lecture/ Lab Demonstra- tion / In-Class Supervised work | In-Lab  Exercises / Case study |
| 4 | 2 | 2 | A1, B1, B3 | **Implement Server Hardening Solutions**  Create security baselines | Lecture/ Lab Demonstra- tion / In-Lab Supervised Work | In-Lab  Exercises/ Case study |
| 5 | 2 | 2 | A1,A2, B2,D1, D3 | **Secure a Virtualization Infrastructure**  Design Guarded Fabric solution | Lecture/ In-Class Supervised work / Lab Demonstra- tion | In-Lab  Exercises / Assignment - 1  (Week 5) |
| 6 | 2 | 2 | B3,C1 | **Secure a Virtualization Infrastructure**  Synthesize the shielded and encryption-supported VMs | Lecture / In-Class Supervised work / Lab Demonstra- tion | In-Lab  Exercises |
| 7 | 2 | 2 | A1, B2 | **Secure a Network Infrastructure**  Configure Windows Firewall | Lecture/ In-Class Supervised work / In-Lab Supervised Work | In-Lab  Exercises |
| 8 | 2 | 2 | B3,C1,C2,D3 | **Secure a Network Infrastructure**  Implement a Software Defined Datacenter Firewall  Secure network traffic | Lecture/ In-Class Supervised work / Lab Demonstration | In-Class  Exercises |
| 9 | 2 | 2 | A1, B2, B3 | **Manage Privileged Identities**  Design and Implement  Just-In-Time (JIT) Administration | Lecture/ In-Class Supervised work / Lab Demonstration / In-Lab Supervised Work | In-Lab  Exercises / Assignment 2 |
| 10 | 2 | 2 | A1, B1,B2, C1, C2 | **Manage Privileged Identities**  Implement Just-Enough-Administration (JEA)  Analyze the implementation of Privileged Access Workstations (PAWs) and User Rights Assignments | Lecture/ In-Class Supervised work / Lab Demonstration | In-Lab Exercises / Major Test (Week 10) |
| 11 | 2 | 2 | A1, B2, B3 | **Manage Privileged Identities**  Local Administrator Password Solution (LAPS) | Lecture / In-Class Supervised work | In-Class  Exercises |
| 12 | 2 | 2 | B3,C1,C2,D3 | **Threat Detection Solutions**  Configure advanced audit policies | Lecture/ In Class Supervised work / In Lab supervised work | In-Lab  Exercises |
| 13 | 2 | 2 | A1, B3,C1,C2,D3 | **Threat Detection Solutions**  Install and configure Microsoft Advanced Threat Analytics (ATA)  Determine threat detection solutions using Operations Management Suite (OMS) | Lecture/ Lab Demonstra- tion | Assignment-3 (Week 13) |
| 14 | 2 | 2 | B3,C1,C2,D3 | **Workload-Specific Security**  Secure application development and server workload infrastructure  Secure file services infrastructure and Dynamic Access Control (DAC) | Lecture/ Lab Demonstra- tion / Class Discussion |  |
| 15 | 2 | 2 | A2, B1,B2,B3, C1,C2,C3,D1, D2,D3,D4 | Student Projects | Project Supervision | Evaluation of Project Presentations and Reports |
| 16 |  |  | A1,B1,B2, C1,C3,D4 | All topics |  | Final Exam |

**Teaching Materials:**

|  |  |
| --- | --- |
| **Textbook(s):** | Warner, Timothy L., and Craig Zacker. (2016), Securing Windows Server. Microsoft Press. |
| **Handout(s):** | Available on Moodle i.e. <http://www.ahlia.edu.bh/moodle> |
| **Reference(s):** | Palmer, Michael. [(2017](file:///\\\\\\\\92017)), Hands-On Microsoft Windows Server, Cengage Learnin.  Liu, Dale, and Remco Wisselink. (2016), Securing Windows Server. |

**Assessment**

|  |  |  |  |
| --- | --- | --- | --- |
| **Method of Assessment** | **Description** | **Learning Outcomes** | **Weighting** |
| Major Test | The major test is a written 90 minutes test. It will cover topics studied in the first 10 weeks. The majority of the test’s questions are problem solving, short answer, and analysis questions. | A1, B1, B2, C1, D4 | 20% |
| Assignments | Three assignments to be given. The assignments will assess students’ skills in differentiating, and analyzing security service techniques. | A2, B2, C1, D1, D3 | 20% |
| Project | Student will work as groups of 2-4 members to develop a security system as a project. This will go through several phases in which the student should analyze, and design a security system for a real world application. | A2, B1, B2, B3, C1, C2, C3, D1, D2, D3, D4 | 20% |
| Final Exam | The final exam is a comprehensive,  written exam and will be of two hours. It will consist of analysis, design, short-answer and essay questions. | A1, B1, B2, C1, C3, D4 | 40% |
| In-Lab Exercises | Exercises will help the students in understanding  and digesting all the course topics. | B1, B3, C1, C2 | Formative |
| Case Studies | Different security project cases are  analyzed and studied. | B1, D4 | Formative |
| **Overall** |  |  | **100%** |

|  |  |
| --- | --- |
| **Admissions** | |
| **Minimum number of students** | **5** |
| **Maximum number of students** | **20** |

|  |
| --- |
| **Ahlia University values academic integrity. Therefore, all students must understand the meaning and consequences of cheating, plagiarism and other academic offences under the Code of Student Conduct and Disciplinary Procedures (see** [www.ahlia.edu.bh/integrity](http://www.ahlia.edu.bh/integrity) **for more information).** |