IS416
Securing Windows Platforms and Applications
[Onsite]

Course Description:

This course discusses security implementations for various Windows platforms and applications. Areas of study involve identifying and examining security risks, security solutions and tools available for various Windows platforms and applications.

Prerequisite(s) and/or Corequisite(s):

Prerequisites: IT260 Networking Application Services and Security or equivalent

Credit hours: 4

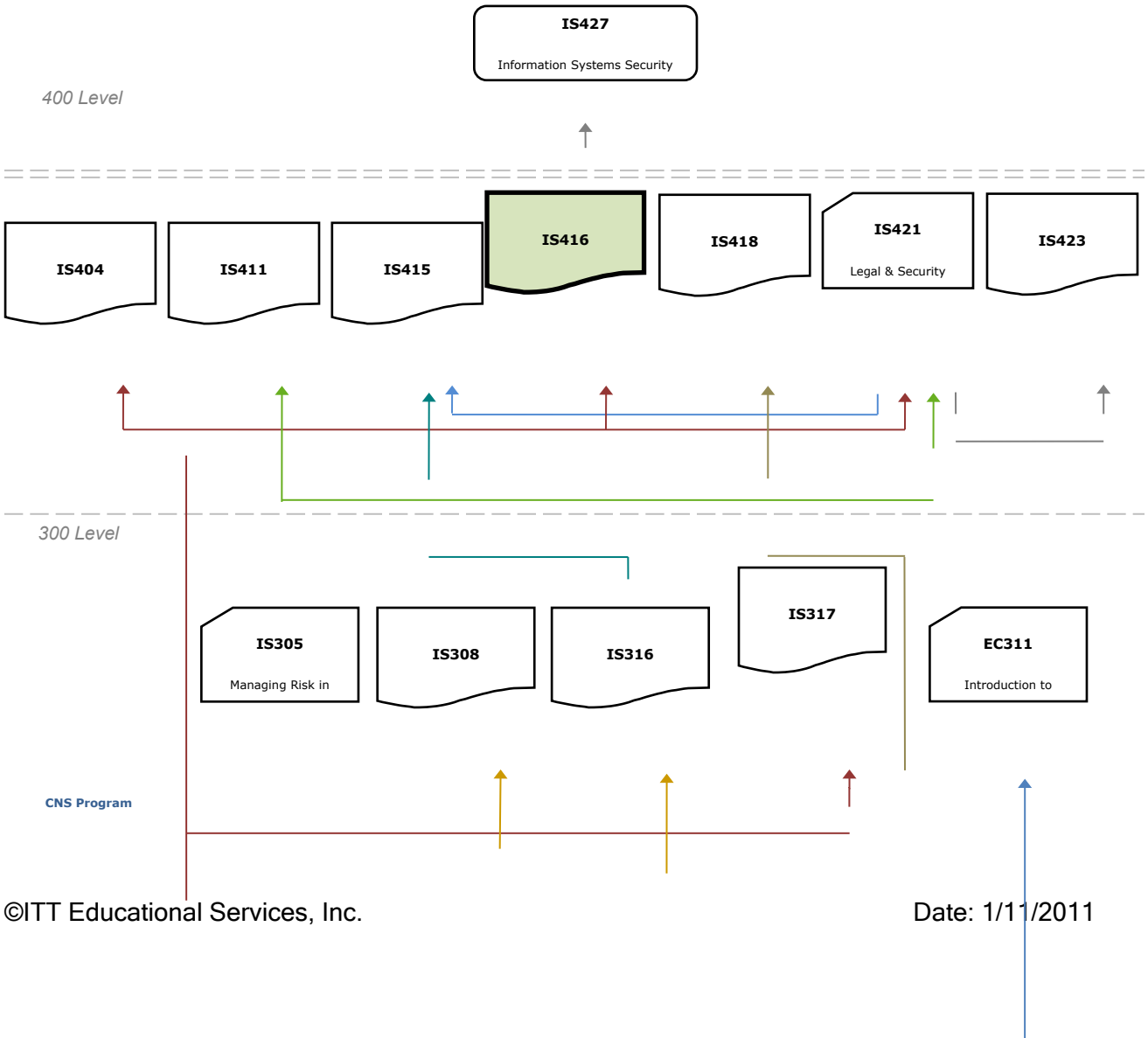
Contact hours: 50 (30 Theory Hours, 20 Lab Hours)

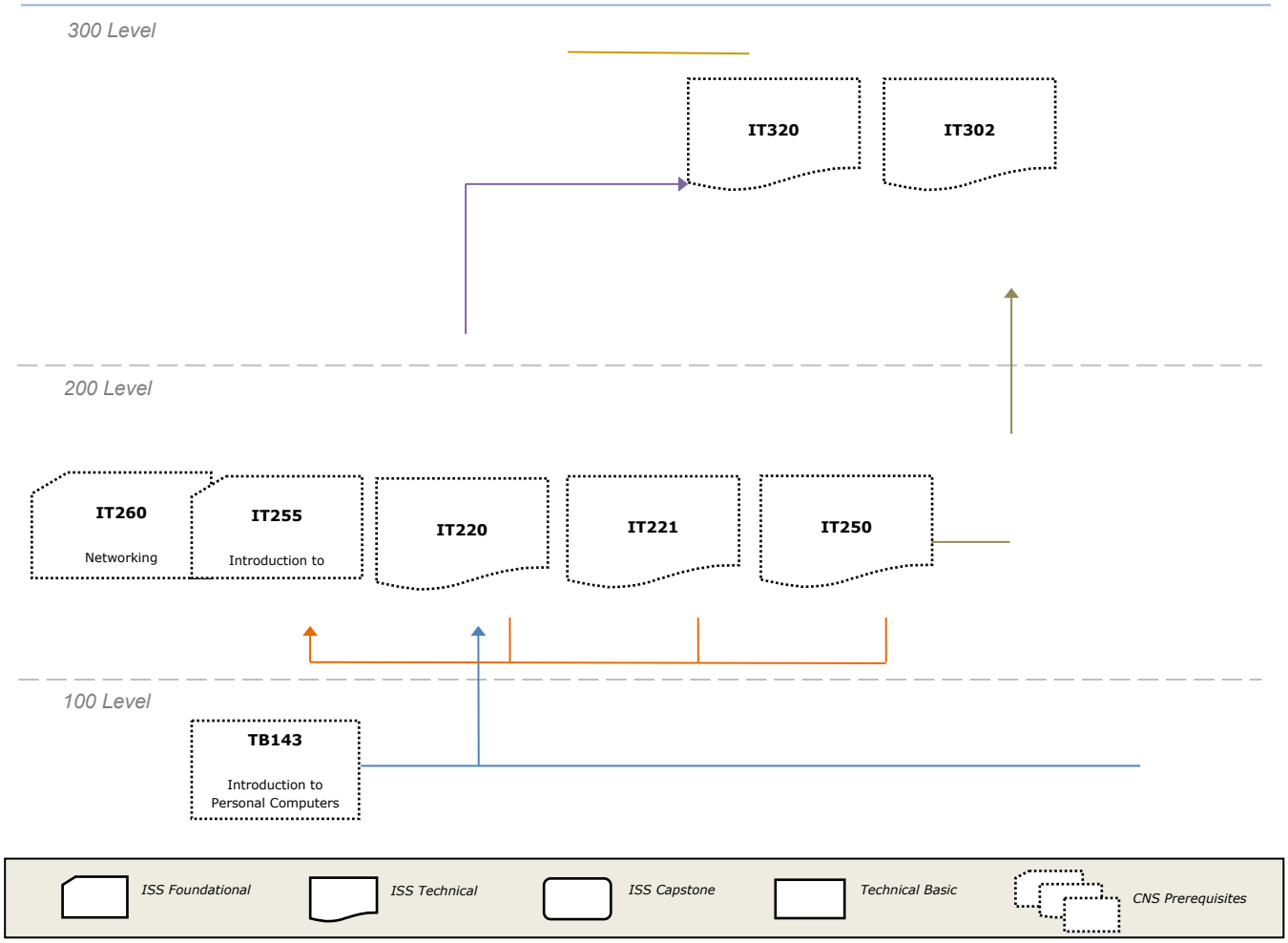
Where Does This Course Belong?

This course is required for the Bachelor of Science in Information Systems Security program. This program covers the following core areas:

- Foundational Courses
- Technical Courses
- BSISS Project

The following diagram demonstrates how this course fits in the program:




300 Level
IT320
IT302
200 Level
IT260
Networking
IT255
Introduction to
IT220
IT221
IT250
100 Level
TB143
Introduction to
Personal Computers
ISS Foundational
ISS Technical
ISS Capstone
Technical Basic
CNS Prerequisites

Course Summary

Course Description

This course discusses security implementations for various Windows platforms and applications. Areas of study involve identifying and examining security risks, security solutions and tools available for various Windows platforms and applications.

Major Instructional Areas

1. Windows security vulnerabilities
2. Microsoft Windows hardening strategies
3. Windows system monitoring techniques
4. Back up and restore operations
5. Security incident handling tactics

Course Objectives

1. Explain security features of the Microsoft Windows operating systems.
2. Implement secure access controls when setting up Microsoft Windows in a given organization.
3. Set up encryption in a given organization to secure Windows environment.
4. Install controls to protect a given Windows system from malware.
5. Apply Group Policy controls and profile and audit tools to keep Windows systems secure.
6. Perform backup and restore operations on a given Windows system.
7. Design techniques to protect given Windows networks and systems from security vulnerabilities.

8. Design techniques to protect given Windows application software from security vulnerabilities.
9. Apply best practices for handling a given Microsoft Windows system and application incident.
10. Apply best practices while managing changes to Windows and its applications.

SCANS Objectives

SCANS is an acronym for Secretary's Commission on Achieving Necessary Skills. The committee, appointed by the National Secretary of Labor in 1990, created a list of skills and competencies that continue to be a valuable resource for individuals developing their careers in a high-tech job market. For more information on the SCANS objectives, visit The U.S. Department of Labor Employment and Training Administration: www.doleta.gov.

Learning Materials and References

Required Resources

Textbook Package	New to this Course	Carried over from Previous Course(s)	Required for Subsequent Course(s)
Solomon, Michael. *Security Strategies in Windows Platforms and Applications.* 1st ed. Sudbury, MA: Jones & Bartlett, 2010.	■		
Printed IS416 Student Lab Manual	■		
ISS Mock IT Infrastructure (1) – Cisco Core Backbone Network consisting of Cisco 2811 routers, 2950/2960 catalyst switches, ASA 5505s for classroom hands-on labs that require a live, IP network. (For onsite only)	■	■	■
ISS Mock IT Infrastructure (2) – VM Server Farm (2 Microsoft Windows XP2003 Standard Servers and 2 Ubuntu Linux Servers) for classroom hands-on VM labs. (For both onsite and online)	■	■	■
ISS Mock IT Infrastructure (2) – VM Workstation (Microsoft Windows XP2003 Professional Workstation with Core ISS Apps and Tools) for classroom hands-on VM labs. (For both onsite and online)	■	■	■
			■

Textbook Package	New to this Course	Carried over from Previous Course(s)	Required for Subsequent Course(s)
Companion DVD-IS416 (3) - Additional VMs, Apps, Tools needed for the Student VM workstation to perform the labs for this course. (For both onsite and online)	▪		

(1) The following presents the core ISS Cisco core backbone network components needed for some of the hands-on labs for onsite delivery only. (Note: video labs will be used for online delivery):

- Cisco 2811 Routers
- Cisco 2950/2960 Catalyst Switches
- Cisco ASA 5505 Security Appliances
- Simulated WAN Infrastructure
- EGP using BGP4 or IGP using EIGRP
- Layer 2 Switching with VLAN Configurations
- Telnet and SSH version 2 for Remote Access
- Inside and Outside VLANs
- DMZ VLAN

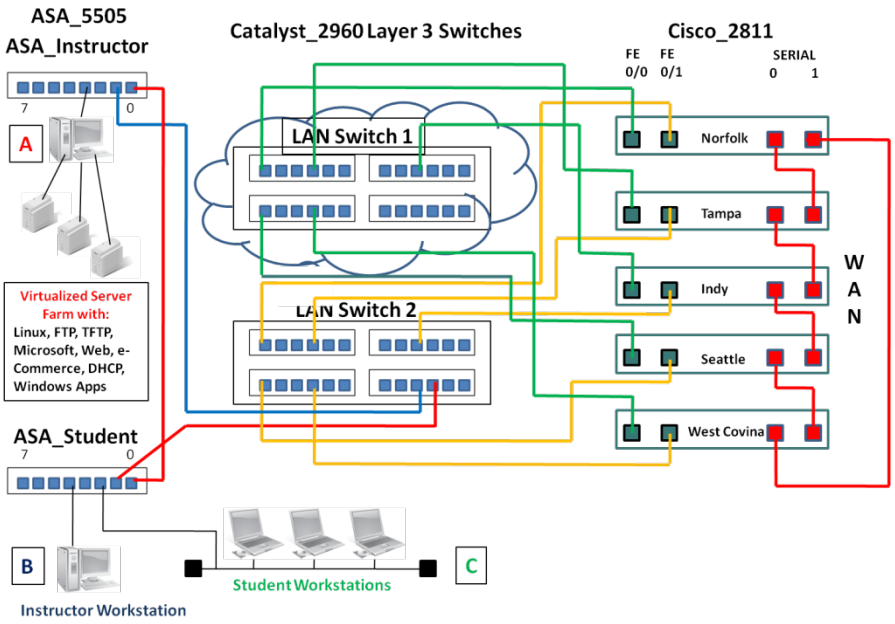


Figure 1 – ISS Cisco Core Backbone Network

(2) The following lists the core ISS VM server farm and VM workstation OS, applications, and tools required for this course for both onsite and online course deliveries:

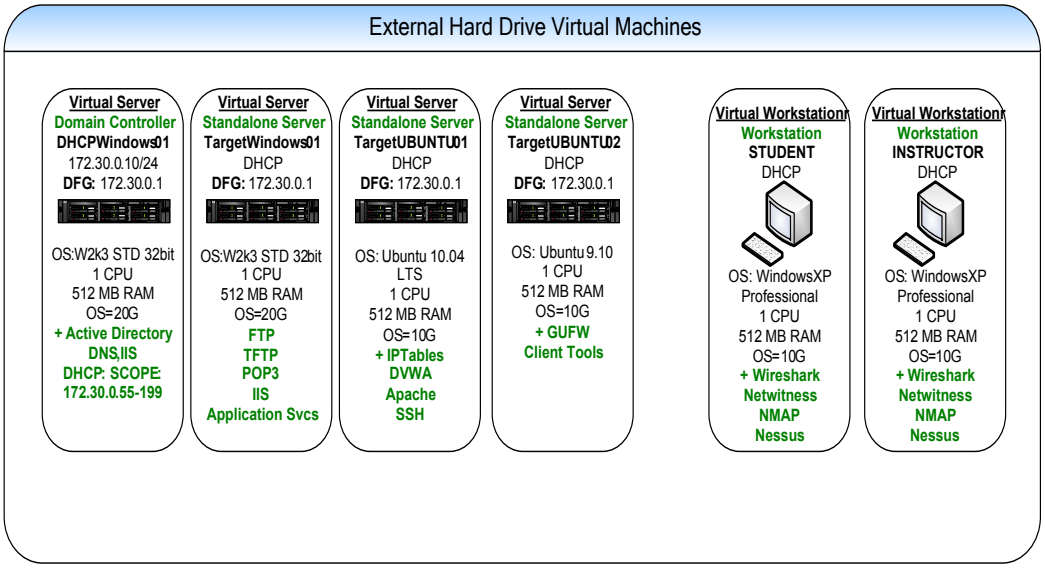


Figure 2 – ISS Core VM Server Farm & VM Workstations

(3) The following lists the new VMs, applications, and tools required to perform the hands-on labs for this course for both onsite and online deliveries:

1. New VM for server farm: “VulnerableXP01”. This VM is a vulnerable Microsoft Windows XP 2003 Standard Edition server used for performing attacks.

2. New VM for server farm: “Backtrack01”. A Backtrack 4 Ubuntu Server pre-loaded with the following applications and tools:

   a. Metasploit with required plug-ins
   b. Kismet
   c. Aircrack-ng
   d. Airsnort
   e. Snort
   f. MySQL
   g. BASE

3. New VM that Replaces the Old “TargetUbuntu01” VM on the VM server farm. An Ubuntu Server 10.4 VM pre-loaded with the following applications and tools:

   a. Damn Vulnerable Web App (DVWA)
   b. ClamAV Installed
   c. Rootkit Hunter: http://www.rootkit.nl/projects/rootkit_hunter.html
   d. Chrootkit: http://www.chkrootkit.org/
   e. Appropriate rootkit tools can be found at:

      http://www.packetstormsecurity.org/UNIX/penetration/rootkits/indexdate.html

   f. Infected with EICAR
   g. tcpdump

h. Common Linux tools such as strings, sed and grep

4. Tools Directory: A directory called "tools" which contains the binary installation files for each tool covered in the course, including:

   a. Infected with EICAR
   b. ClamAV Installed
   c. Rootkit Hunter: http://www.rootkit.nl/projects/rootkit_hunter.html
   d. Chrootkit: http://www.chkrootkit.org/
   e. Appropriate rootkit tools can be found at: http://www.packetstormsecurity.org/UNIX/penetration/rootkits/indexdate.html
   f. Wireshark
   g. Netwitness Investigator
   h. FileZilla FTP client/Server
   i. Putty SSH client
   j. Nessus
   k. Zenmap
   l. MD5sum
   m. SHA1sum
   n. GnuPG (Gnu Privacy Guard)
   o. OpenSSL
   p. VMware Player

Note #1: ISS onsite students can obtain their removable hard drive directly from their ITT campus. ISS online students will be required to download the core ISS VM server farm and VM workstations directly to their personal computer for installation. The ITT Onsite or Online Instructor will provide students with the specific instructions and procedures for how to obtain the core ISS VM server farm and workstation image files during the first week of class.

Note #2: Installation instructions for installing these new VMs, applications and tools will be provided by the ISS onsite or online Instructor during day 1/ week 1 of the course.

Recommended Resources

Books, Professional Journals

Please use the following author's names, book/article titles and/or keywords to search in the ITT Tech Virtual Library for supplementary information to augment your learning in this subject:

Books

Periodicals

EbscoHost

Books24X7

- Brian Komar

Windows Server 2008 PKI and Certificate Security.

- Erik Larkin

"Advanced Antivirus". *PC World*, Jan2010, Vol. 28 Issue 1, (Pages 80-86), *(AN 47157049)*

- Harold F. Tipton, et al

Information Security Management Handbook, 6th ed.

- ISACA

Cybercrime: Incident Response and Digital Forensics.

- Jeremy Moskowitz

Group Policy: Fundamentals, Security, and Troubleshooting.

- Jesper M. Johansson, et al

Windows Server 2008 Security Resource Kit.

- Mitch Tulloch, et al

Windows 7 Resource Kit.

- Steve Seguis

Microsoft Windows Server 2008 Administration.

Keywords:

Access Control
Access Science
Back Up
Encryption
Group Policy Control
Malware
Microsoft Windows Security
Restore
Security Incidents
Vulnerabilities

Course Plan

Instructional Methods

This course is designed to promote learner-centered activities and support the development of cognitive strategies and competencies necessary for effective task performance and critical problem solving. The course utilizes individual and group learning activities, performance-driven assignments, problem-based cases, projects, and discussions. These methods focus on building engaging learning experiences conducive to development of critical knowledge and skills that can be effectively applied in professional contexts.

Suggested Learning Approach

In this course, you will be studying individually and within a group of your peers. As you work on the course deliverables, you are encouraged to share ideas with your peers and instructor, work collaboratively on projects and team assignments, raise critical questions, and provide constructive feedback.

Use the following advice to receive maximum learning benefits from your participation in this course:

DO	DON'T
▪ Do take a proactive learning approach ▪ Do share your thoughts on critical issues and potential problem solutions ▪ Do plan your course work in advance ▪ Do explore a variety of learning resources in addition to the textbook ▪ Do offer relevant examples from your experience ▪ Do make an effort to understand different points of view ▪ Do connect concepts explored in this course to real-life professional situations and your own experiences	▪ Don't assume there is only one correct answer to a question ▪ Don't be afraid to share your perspective on the issues analyzed in the course ▪ Don't be negative towards the points of view that are different from yours ▪ Don't underestimate the impact of collaboration on your learning ▪ Don't limit your course experience to reading the textbook ▪ Don't postpone your work on the course deliverables – work on small assignment components every day

Course Outline

Unit #	Unit Title	Assigned Readings	Graded Activities			
			Grading Category	#	Activity Title	Grade Allocation (% of all graded work)
1	Microsoft Windows Security Features	*Security Strategies in Windows Platforms and Applications*: ▪ Chapter 1 ▪ Chapter 2	Assignment	1.1	Adding Active Directory	2
			Lab	1.2	Configure Active Directory and Implement Department and User Access Controls	2

Unit #	Unit Title	Assigned Readings	Graded Activities			
			Grading Category	#	Activity Title	Grade Allocation (% of all graded work)
			Assignment	1.3	Executive Summary Report	3
2	Setting up Windows Systems with Secure Access Controls	*Security Strategies in Windows Platforms and Applications*: ▪ Chapter 3	Assignment	2.1	Recommendations for Access Controls	2
			Lab	2.2	Implement Access Control Lists to Secure Folders and Read/Write/Access to Files	2
			Assignment	2.3	Procedure Guide on Access Controls	3
3	Setting up Windows Systems Using Encryption and Application Rules	*Security Strategies in Windows Platforms and Applications*: ▪ Chapter 4	Assignment	3.1	Encryption and BitLocker Activity	2
			Lab	3.2	Enable Encryption on a Microsoft Workstation to Ensure Confidentiality	2
			Assignment	3.3	Communication Policy Procedure Guide	3
4	Setting up Controls to Protect Windows Systems from Malware	*Security Strategies in Windows Platforms and Applications*: ▪ Chapter 5	Assignment	4.1	Identifying Types of Malware Infection	2
			Lab	4.2	Identify and Remove Malware and Malicious Software on a Microsoft Workstation	2
			Assignment	4.3	Malware Policy Procedure Guide	3

Unit #	Unit Title	Assigned Readings	Graded Activities			
			~~Grading~~ Category	#	Activity Title	Grade Allocation (% of all graded work)
5	Maintaining Windows System Security with Group Policy Controls	*Security Strategies in Windows Platforms and Applications*: ▪ Chapter 6 ▪ Chapter 7	Assignment	5.1	Auditing Tools for Windows System	2
			Lab	5.2	Configure Access to Folders & Files Using Microsoft GPO Manager & Use MBSA to Identify the Current Security Baseline Definition	2
			Assignment	5.3	Security Audit Procedure Guide	3
6	Performing Backup and Restore Operations on Windows Systems	*Security Strategies in Windows Platforms and Applications*: ▪ Chapter 8	Discussion	6.1	Minimizing Recovery Time Strategies	5
			Lab	6.2	Perform a Microsoft Windows Server & Workstation Backup and Restoration	2
			Assignment	6.3	Procedure Guide on Restoring a System	3
7	Analyzing Windows Networks and Systems for Security Vulnerabilities	*Security Strategies in Windows Platforms and Applications*: ▪ Chapter 9 ▪ Chapter 10 ▪ Chapter 11	Assignment	7.1	Security Administration Requirements Policy	2
			Lab	7.2	Harden a Microsoft Workstation Using Security Configuration Wizard & Manual Configurations	2
			Assignment	7.3	Hardening Windows Authentication, Networking, and Data Access	4

Unit #	Unit Title	Assigned Readings	Graded Activities			
			~~Grading~~ Category	#	Activity Title	Grade Allocation (% of all graded work)
8	Analyzing Windows Application Software for Security Vulnerabilities	*Security Strategies in Windows Platforms and Applications*: ▪ Chapter 12	Assignment	8.1	Policy for Securing Windows Environment	2
			Lab	8.2	Apply Security Hardening on Windows Microsoft Server & Microsoft Client Applications	2
			Assignment	8.3	Best Procedures to Secure Windows Applications	4
9	Handling and Managing Security Incidents of Windows Systems	*Security Strategies in Windows Platforms and Applications*: ▪ Chapter 13	Assignment	9.1	Evidence Collection Policy	2
			Lab	9.2	Perform Digital Evidence Collection & Documentation as per the Chain of Custody	2
			Assignment	9.3	Windows Incident Handling Tools	4
10	Applying Best Practices in Managing Changes to Windows Systems and Applications	*Security Strategies in Windows Platforms and Applications*: ▪ Chapter 14 ▪ Chapter 15	Discussion	10.1	Best practices in Managing Changes to Windows Systems and Applications	5
			Lab	10.2	Perform a Security Baseline Definition using MBSA to Harden a Microsoft Server	2

Unit #	Unit Title	Assigned Readings	Graded Activities			
			Grading Category	#	Activity Title	Grade Allocation (% of all graded work)
			Assignment	10.3	Software Development Management Policies	4
11	Course Review and Final Examination	N/A	Exam	11.1	Final Exam	20

Evaluation and Grading

Evaluation Criteria

The graded assignments will be evaluated using the following weighted categories:

Category	Weight
Discussion	10
Assignment	50
Lab	20
Exam	20
TOTAL	**100%**

Grade Conversion

The final grades will be calculated from the percentages earned in the course, as follows:

Grade	Percentage	Credit
A	90–100%	4.0
B+	85–89%	3.5
B	80–84%	3.0
C+	75–79%	2.5
C	70–74%	2.0
D+	65–69%	1.5
D	60–64%	1.0
F	<60%	0.0

Academic Integrity

All students must comply with the policies that regulate all forms of academic dishonesty, or academic misconduct, including plagiarism, self-plagiarism, fabrication, deception, cheating, and sabotage. For more information on the academic honesty policies, refer to the Student Handbook.

(End of Syllabus)

