IT255
Introduction to Information Systems Security
[Onsite]

Course Description:

This course provides an overview of security challenges and strategies of counter measures in the information systems environment. Topics include definition of terms, concepts, elements, and goals incorporating industry standards and practices with a focus on availability, vulnerability, integrity and confidentiality aspects of information systems.

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

Prerequisites: IT220 Network Standards and Protocols, IT221 Microsoft Network Operating System I, IT250 Linux Operating System

Credit hours: 4

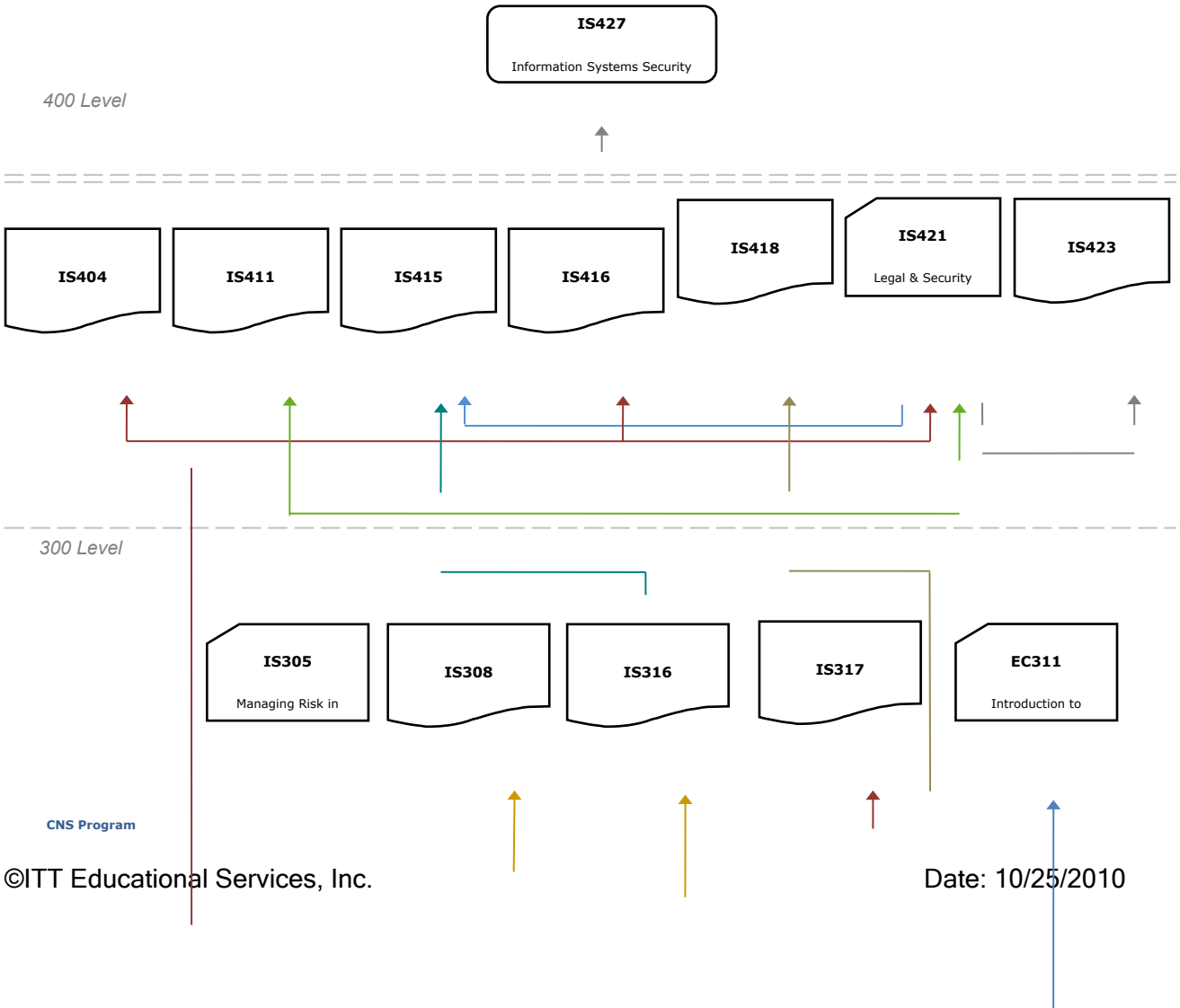
Contact hours: 50 (30 Theory Hours, 20 Lab Hours)

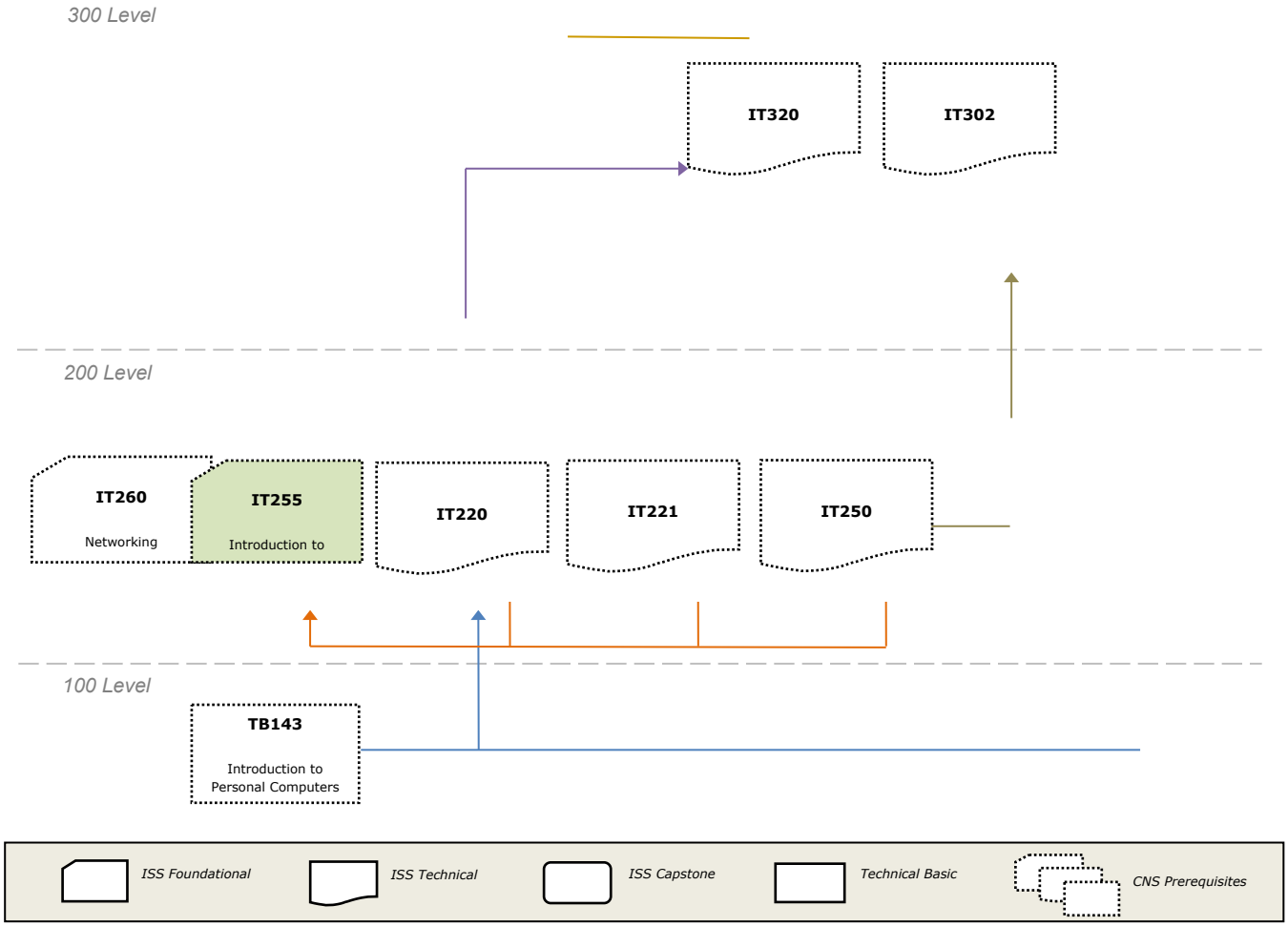
Where Does This Course Belong?

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:





Course Summary

Major Instructional Areas

1. Information Systems Security fundamentals
2. Seven domains of a typical Information Technology (IT) infrastructure
3. Risks, threats, and vulnerabilities found in a typical IT infrastructure
4. Security countermeasures for combating risks, threats, and vulnerabilities commonly found in an IT infrastructure
5. $(ISC)^2$ Systems Security Certified Practitioner (SSCP®) Common Body of Knowledge – SSCP® domains
6. Six domains of the CompTIA Security+ certification

Course Objectives

1. Explain the concepts of information systems security as applied to an IT infrastructure.
2. Describe how malicious attacks, threats, and vulnerabilities impact an IT infrastructure.
3. Explain the role of access controls in implementing a security policy.
4. Explain the role of operations and administration in effective implementation of security policy.
5. Explain the importance of security audits, testing, and monitoring to effective security policy.
6. Describe the principles of risk management, common response techniques, and issues related to recovery of IT systems.
7. Explain how businesses apply cryptography in maintaining information security.
8. Analyze the importance of network principles and architecture to security operations.
9. Explain the means attackers use to compromise systems and networks and defenses used by organizations.

10. Apply international and domestic information security standards and compliance laws to real-world implementation in both the private and public sector.

SCANS Objectives

SCANS is an acronym for the 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)
Kim, David, and Michael G. Solomon. *Fundamentals of Information Systems Security*. 1st ed. Sudbury, MA: Jones & Bartlett, 2011.	▪		
Printed IT255 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 Windows Standard Servers 2003 and 2 Ubuntu Linux Servers) 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)
ISS Mock IT Infrastructure (2) – VM Workstation (Windows XP Professional Workstation with Core ISS Apps and Tools) for classroom hands-on VM labs. (For both onsite and online)	▪	▪	▪
Companion DVD-IT255 (3) - Additional VMs, Apps, Tools needed for the Student VM workstation to perform the labs for this course. (For both onsite and online)	▪		▪

ISS Mock IT Infrastructure

The ISS Mock IT infrastructure was designed to mimic a real-world IT infrastructure consisting of the seven domains of a typical IT infrastructure.

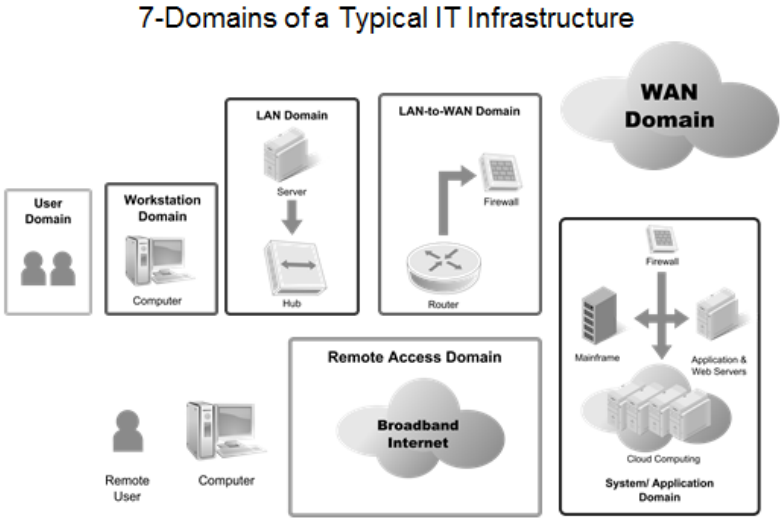


Figure 1 – Seven Domains of Information Systems Security Responsibility

The ISS Mock IT infrastructure consists of the following three major components:

- Cisco Core Backbone Network
- VM Server Farm
- VM Instructor and Student Workstations

At the core of the ISS Mock IT infrastructure is a Cisco core backbone network using the CNS curriculum equipment (Cisco 2811/2801 routers, ASA5505s, and Catalyst 2950/2960 switches). The use of the Cisco core backbone network for both CNS and ISS provides a real-world, representation of a typical IT infrastructure. This also requires proper preparation and loading of IOS image files and configuration files into/from the Cisco router and a TFTP server.

Some ISS courses and labs require the use of the Cisco core backbone network when an IP network infrastructure is needed as part of the hands-on lab activity. This will be indicated in the “Required Setup & Tools” section of each laboratory within each ISS course lab manual.

Onsite students will perform hands-on labs using this Cisco core backbone network and the VM server farm and VM workstations.

Online students will watch video only labs when the Cisco core backbone network is used and will perform hands-on labs using the VM server farm and VM workstations.

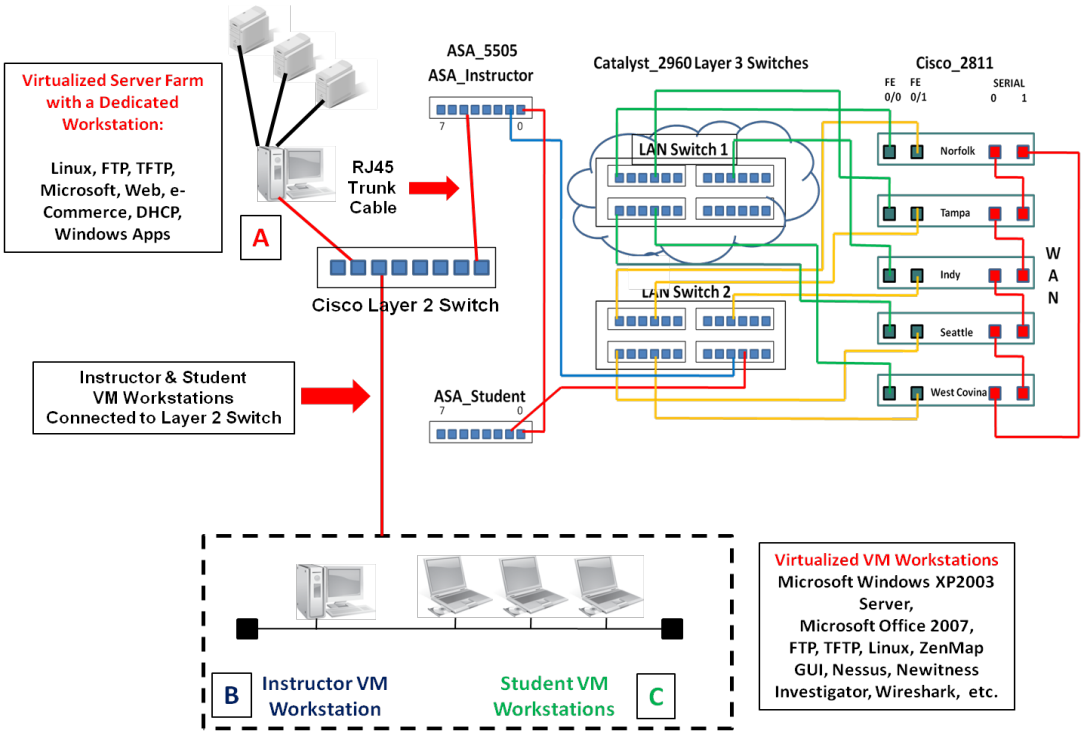


Figure 2 – ISS Mock IT Infrastructure

The second component is the virtualized server farm. This virtualized (VM) server farm ("A") consists of Microsoft Windows and Ubuntu Linux servers running native, as well as, open source and freeware applications and services. The purpose of the VM server farm is to mimic production services and applications where the Instructor has full control over the implementation of the VM server farm based on what the lab requires. Future ISS courses will have new VMs containing pertinent applications and tools. Note that the VM Server farm can connect to either ASA_Instructor (172.30.0.0/24) or ASA_Student (172.31.0.0/24) as long as the DHCP host range and IP default gateway router definitions are set properly. See figure 3 below.

The third component is the Instructor ("B") VM workstation and Student VM workstations ("C") with client applications and tools pre-installed. See figure 3 below.

The following notes are implementation recommendations:

- Install the VM server farm (“A”) and VM workstations (“B” and “C”) on either ASA_Instructor or ASA_Student as long as you specify the correct IP network lease address pool on the DHCP server and specify the correct IP default gateway router definition
- The DHCP server, “WindowsDHCP01” is already pre-configured to support the 172.30.0.0, 255.255.255.0 / ASA_Instructor subnet with an IP default gateway router of 172.30.0.1, 255.255.255.0
- Install the VM server farm on a dedicated classroom workstation with 2 Gig RAM (required) / 4 Gig RAM (recommended)

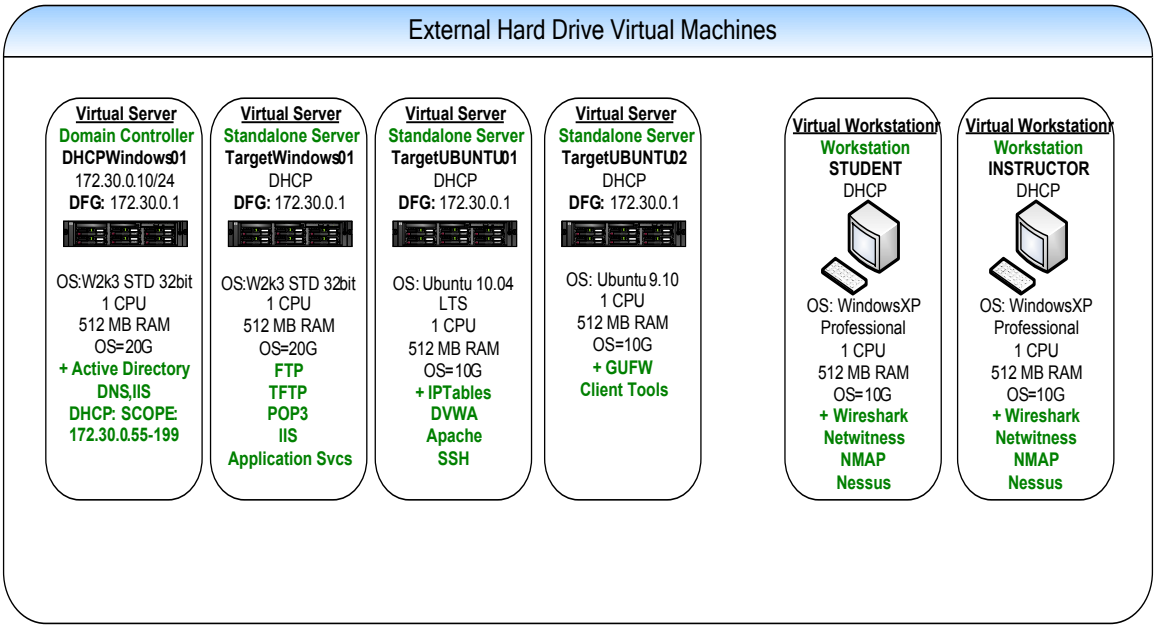


Figure 3 – VM Server Farm and VM Workstations

To support the delivery of the ISS curriculum, use of ITT Technical Institute’s Microsoft software licenses are used where needed for Microsoft server and workstation VMs. The VM server farm is physically housed on a USB hard drive allowing for physical installation to a dedicated VM server farm workstation.

All student workstations must be physically isolated from the rest of the classroom workstations given that some ISS courses and hands-on labs require disconnection from the ITT internal network.

ISS hands-on labs require the Instructor or Student to install their hard drive into a physical workstation in the classroom. VMware Player v3.x is used to enable the VM servers and/or VM workstations. Use of a DHCP server provides all IP host addresses to the VM workstations. Ideally, the VM server farm workstation should have 4 Gig of RAM in order to load and run more than 2 VM servers. The Instructor and Student VM workstations can have 2 Gig RAM to load to VM workstation with applications and tools.

The VM server farm should be connected to the layer 2 switch along with the Instructor VM and Student VM workstations. From here you can run an RJ45-RJ45 trunk cable connecting the layer 2 switch to ASA_Instructor (this is the default configuration using 172.30.0.0/24). This way the VM server farm and DHCP server can be accessed by either the Instructor or Student VM workstations.

Figure 4 below shows a high-level diagram of the ISS “Mock” IT Infrastructure representing both the network and server elements. Do not connect the ISS “Mock” IT infrastructure to the internal ITT Technical Institute network or public Internet. Special partitioning and separation of those classroom workstations (on its own layer 2 classroom switch) used for ISS hands-on labs is required given the intrusive applications and tools used by ISS hands-on labs. This will facilitate easy connection/disconnection to the ITT internal network.

The default DHCP setting are:

172.30.0.0/24 (IP Network Number with 255.255.255.0 Subnet Mask)

172.30.0.1 /25 (IP Default Gateway Router)

172.30.0.55 – 172.30.0.199 (DHCP Address Lease Pool)

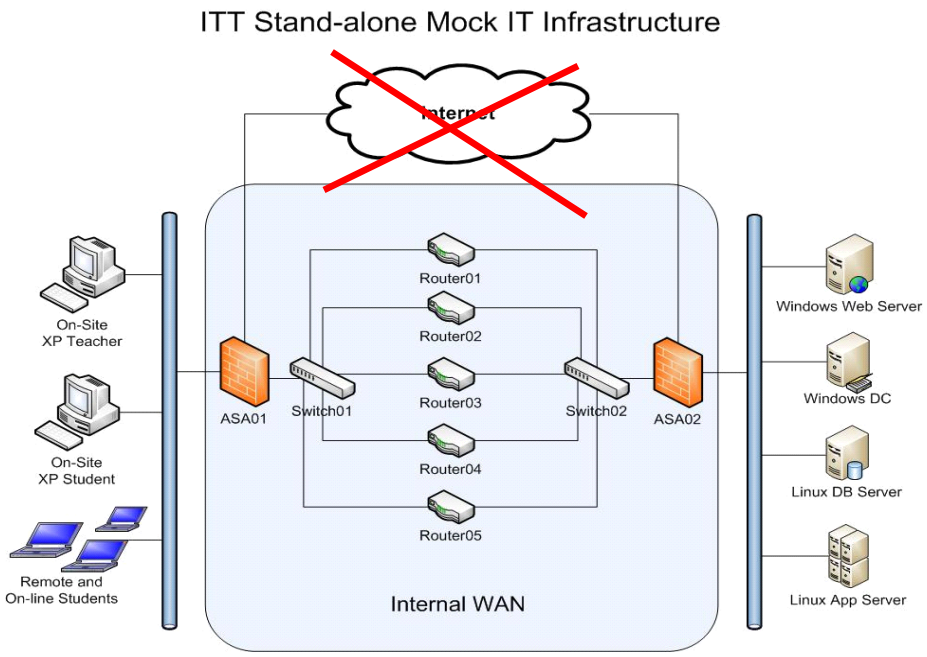


Figure 4 - Mock IT Infrastructure High-level Diagram

The latest version of the ISS Mock IT Infrastructure Installation & Setup Guide (in PDF format) can be found in two different locations: (**ISS Mock IT Infrastructure_v 3 7_101006_dk final.pdf)**

- The www.jblearning.com\ITT instructor portal:
  The ISS Mock IT Infrastructure Installation and Setup Guide can be found in each course's \Labs sub-folder as follows:
  \ISxxx\Labs\Mock IT Infrastructure\..., where xxx=ISS Course Number
- The ITT Faculty Portal:
  The Mock IT Infrastructure Installation and Setup Guide and can be found here:
  \ITT Faculty Portal\IT Shared Documents\ISS\Mock Infrastructure Setup v3.7\...

Note #1: 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.

(1) 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 Windows 2003 Server VM and is used as a target device.
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 #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

Books24X7

CRCnetBASE

Periodicals

ProQuest

EbscoHost

Reference

School of Information Technology

- Sandy Bacik

  Building an Effective Information Security Policy Architecture (Chapter 3)

- Michael Howard, et al

  The Security Development Lifecycle: SDL: A Process for Developing Demonstrably More Secure Software (Chapter 1)

- Maura A. van der Linden

  Testing Code Security (Chapters 5 and 8)

- Thomas R. Peltier

Information Security Risk Analysis, 2nd ed. (Chapter 2)

- John Wylder

  Strategic Information Security (Chapter 13)

- Eric A. Fisch, et al

  Secure Computers and Networks; analysis, design, and implementation (Chapters 1, 2, 5, 6, 10, 13, 14 and 15)

- William Stepka

  "Profiling Hackers: The Science of Criminal Profiling as Applied to the World of Hacking", *Security Management*, Mar 2010, Vol. 54 Issue 3, (Page 80)

- Xin Luo, et al

  "Awareness Education as the Key to Ransomware Prevention", *Information Systems Security*, Jul/Aug 2007, Vol. 16 Issue 4, (Pages 95-202), (*AN 26520074*)

- Avinash W. Kadam

  "Information Security Policy Development and Implementation", *Information Systems Security*, Sep/Oct 2007, Vol. 16 Issue 5, (Pages 246-256), (*AN 27625696*)

- Peter O. Okenyi, et al

  "On the Anatomy of Human Hacking", *Information Systems Security*, Nov 2007, Vol. 16 Issue 6, (Pages 302-314), (*AN 27979547*)

- Patricia A. Bonner

"Quick Reference to HIPAA Compliance", *Benefits Quarterly*, 2010 First Quarter, Vol. 26 Issue 1, (Page 58), (*AN 47616062*)

- Chris Nowell

  "Regulatory Compliance - the Wonderful World of FISMA", *Information Systems Security*, Sep/Oct 2007, Vol. 16 Issue 5, (Pages 278-280), (*AN 27625693*)

- Mimi Herrmann

  "Security Strategy: From Soup to Nuts", *Information Security Journal: A Global Perspective*, Jan 2009, Vol. 18 Issue 1, (Pages 26-32), (*AN 36353502*)

- Ryan Sherstobitoff, et al

  "You Installed Internet Security on Your Network: Is Your Company Safe?" *Information Systems Security*, Jul/Aug 2007, Vol. 16 Issue 4, (Pages 188-194), (*AN 26520075*)

Professional Associations

The following is a list of vendor neutral professional organizations and their respective certifications:

- CISA, CISM, CGEIT, CRISC Certifications
  http://www.isaca.org/ (accessed May 26, 2010).

- CISSP® and SSCP® Information Systems Security Certifications
  http://www.isc2.org/ (accessed May 26, 2010).

- CSIH Certification
  http://www.cert.org/ (accessed May 26, 2010).

- FISMA Training and Certification
  http://www.fismacenter.com/ (accessed May 26, 2010).

- SANS GIAC Certifications
  http://www.sans.org/ (accessed May 26, 2010).

- Security + Certification
  http://www.comptia.com/ (accessed May 26, 2010).

The following is a list of vendor-specific professional certifications:

- CCSP Certification
  http://www.cisco.com/ (accessed May 26, 2010).

- Check Point Firewall Specialist Certifications
  http://www.checkpoint.com/ (accessed May 26, 2010).

- MSCE Security Certification
  http://www.microsoft.com/ (accessed May 26, 2010).

- RSA Training and Certifications
  http://www.rsa.com/ (accessed May 26, 2010).

- Symantec Security Specialist Certifications
  http://www.symantec.com/ (accessed May 26, 2010).

Other References

- CVE List
  http://cve.mitre.org/ (accessed May 26, 2010).

- National Cyber Alert System
  http://www.us-cert.gov/cas/alldocs.html (accessed May 26, 2010).

- National Vulnerability Database
  http://nvd.nist.gov/ (accessed May 26, 2010).

- SANS Top 20 Threats/Vulnerabilities
  http://www.sans.org/top-cyber-security-risks/?ref=top20 (accessed May 26, 2010).

- CERT® Coordination Center
  http://www.cert.org/ (accessed May 26, 2010).

- US Computer Emergency Readiness Team
  http://www.us-cert.gov/ (accessed May 26, 2010).

- US Department of Homeland Security
  http://www.dhs.gov/ (accessed May 26, 2010).

- US National Institute of Standards & Technology
  http://www.nist.gov/ (accessed May 26, 2010).

NOTE: All links are subject to change without prior notice.

Keywords:

Availability

Business Continuity

Business Impact Analysis

Compliance Laws

Confidentiality

Cryptography

Disaster Recovery

Incident Response

Information Security

Information Systems Security

Integrity

IT Risks, Threats, Vulnerabilities

IT Security Assessment

IT Security Audit

Malicious Code

Malware

Network Security

Risk Management

Security Breaches

Security Controls

Security Countermeasures

Security Incidents

Security Management

Security Monitoring

Security Operations

Security Testing

Telecommunications Security

Unauthorized Access

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 the 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	▪ 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 points of view that are different from yours ▪ Don't underestimate the impact of collaboration on your learning

DO	DON'T
▪ Do connect concepts explored in this course to real-life professional situations and your own experiences	▪ 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	Information Systems Security Fundamentals	*Fundamentals of Information Systems Security*: ▪ Chapter 1	Lab	1.1	Perform Reconnaissance & Probing Using ZenMap GUI (Nmap)	2
			Assignment	1.2	Match Risks/Threats to Solutions	1
				1.3	Impact of a Data Classification Standard	1
2	Application of Security Countermeasures to Mitigate Malicious Attacks	*Fundamentals of Information Systems Security*: ▪ Chapter 3 ▪ Chapter 4	Lab	2.1	Conduct a Vulnerability Assessment Scan Using Nessus®	2
			Project	2.2	Project Part 1: Multi-Layered Security Plan	6
			Assignment	2.3	Calculate the Window of Vulnerability	1
				2.4	Microsoft Environment Analysis	1
3	Appropriate Access Controls for Systems, Applications,	*Fundamentals of Information Systems Security*:	Lab	3.1	Enable Windows Active Directory and User Access Controls	2

Unit #	Unit Title	Assigned Readings	Graded Activities			
						Grade Allocation
			Grading Category	#	Activity Title	(% of all graded work)
			Discussion	3.2	Access Control Models	4
			Assignment	3.3	Remote Access Control Policy Definition	1
4	Effective Implementation of Security Policy	*Fundamentals of Information Systems Security*: ▪ Chapter 6	Lab	4.1	Configure Group Policy Objects and Microsoft Baseline Security Analyzer (MBSA)	2
			Assignment	4.2	Enhance an Existing IT Security Policy Framework	1
				4.3	Acceptable Use Policy (AUP) Definition	1
5	Importance of Testing, Auditing, and Monitoring	*Fundamentals of Information Systems Security*: ▪ Chapter 7	Lab	5.1	Perform Protocol Capture & Analysis Using Wireshark & Netwitness Investigator	2
			Assignment	5.2	Testing and Monitoring Security Controls	1
				5.3	Define an Acceptable Use Policy (AUP)	1
6	Role of Risk Management, Response, and Recovery for IT	*Fundamentals of Information Systems Security*:	Lab	6.1	Perform Business Continuity Plan Implementation Planning	2

Unit #	Unit Title	Assigned Readings	Graded Activities			
						Grade Allocation
			Grading Category	#	Activity Title	(% of all graded work)
	Systems, Applications, and Data	▪ Chapter 8	Assignment	6.2	BCP, DRP, BIA, and Incident Response Plan Mix and Match	4
				6.3	Quantitative and Qualitative Risk Assessment Analysis	1
7	Role of Cryptography in Maintaining Confidentiality and Privacy of Data	*Fundamentals of Information Systems Security*: ▪ Chapter 9	Lab	7.1	Relate Windows Encryption and Hashing to Confidentiality & Integrity	2
			Assignment	7.2	Select Appropriate Encryption Algorithms	1
				7.3	Design an Encryption Strategy	1
8	Networks and Communications and their Inherent Weaknesses	*Fundamentals of Information Systems Security*: ▪ Chapter 10	Lab	8.1	Perform a Web Application Attack Using Cross Site Scripting & Remediate	2
			Assignment	8.2	Network Hardening	1
				8.3	Network Security Applications and Countermeasures	1

Unit #	Unit Title	Assigned Readings	Graded Activities			
						Grade Allocation
			Grading Category	#	Activity Title	(% of all graded work)
9	Mitigation of Risk and Threats from Attacks and Malicious Code	*Fundamentals of Information Systems Security*: ▪ Chapter 11	Lab	9.1	Perform a Virus Scan and Malware Identification Scan and Eliminate Threats	2
			Assignment	9.2	List Phases of a Computer Attack	1
				9.3	Summary Report on a Malicious Code Attack	1
10	Information Security Standards and Compliance Laws	*Fundamentals of Information Systems Security*: ▪ Chapter 12 ▪ Chapter 15	Lab	10.1	Craft an Information Security Policy	2
			Assignment	10.2	Examine Real-World Implementations of Security Standards and Compliance Laws	1
				10.3	Small- to Medium-Sized Business Analysis	4
11	Course Review and Final Examination	N/A	Project	11.1	Project Part 2: Student SSCP® Domain Research Paper	15
			Exam	11.2	Final Exam	30

Evaluation and Grading

Evaluation Criteria

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

Category	Weight
Assignment	25%
Lab	20%
Project	21%
Discussion	4%
Exam	30%
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)

