IS404
Access Control, Authentication and Public Key Infrastructure (PKI) [Onsite]

Course Description:

This course introduces the concept of access control to information systems and applications. Access, authentication and accounting for end-users and system administrators will be covered. In addition, security controls for access control including tokens, biometrics, and use of public key infrastructures (PKI) will be covered.

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

Prerequisites: IT260 Networking Application Services and Security or equivalent

Credit hours: 4

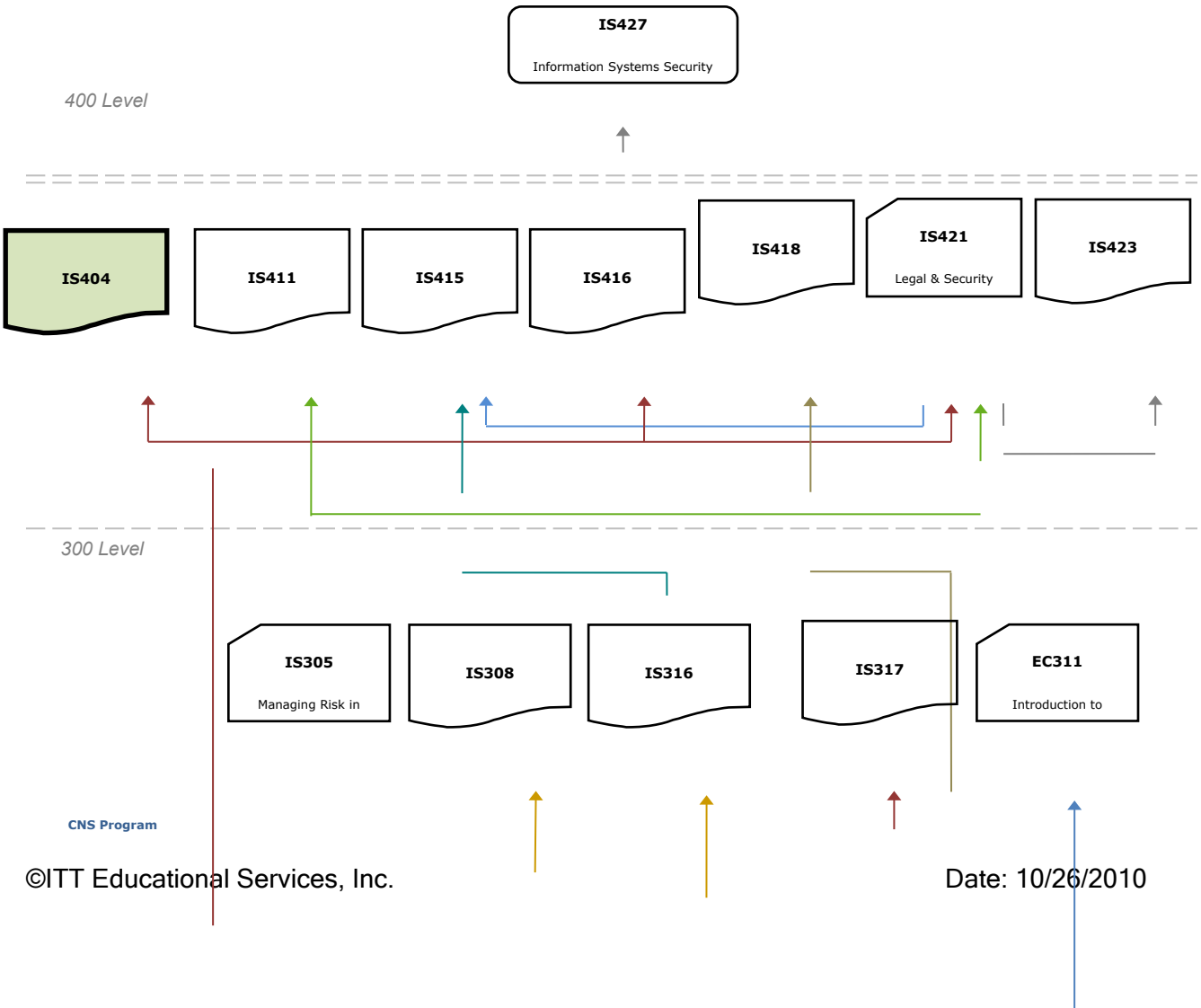
Contact hours: 50 (30 Theory Hours, 20 Lab Hours)

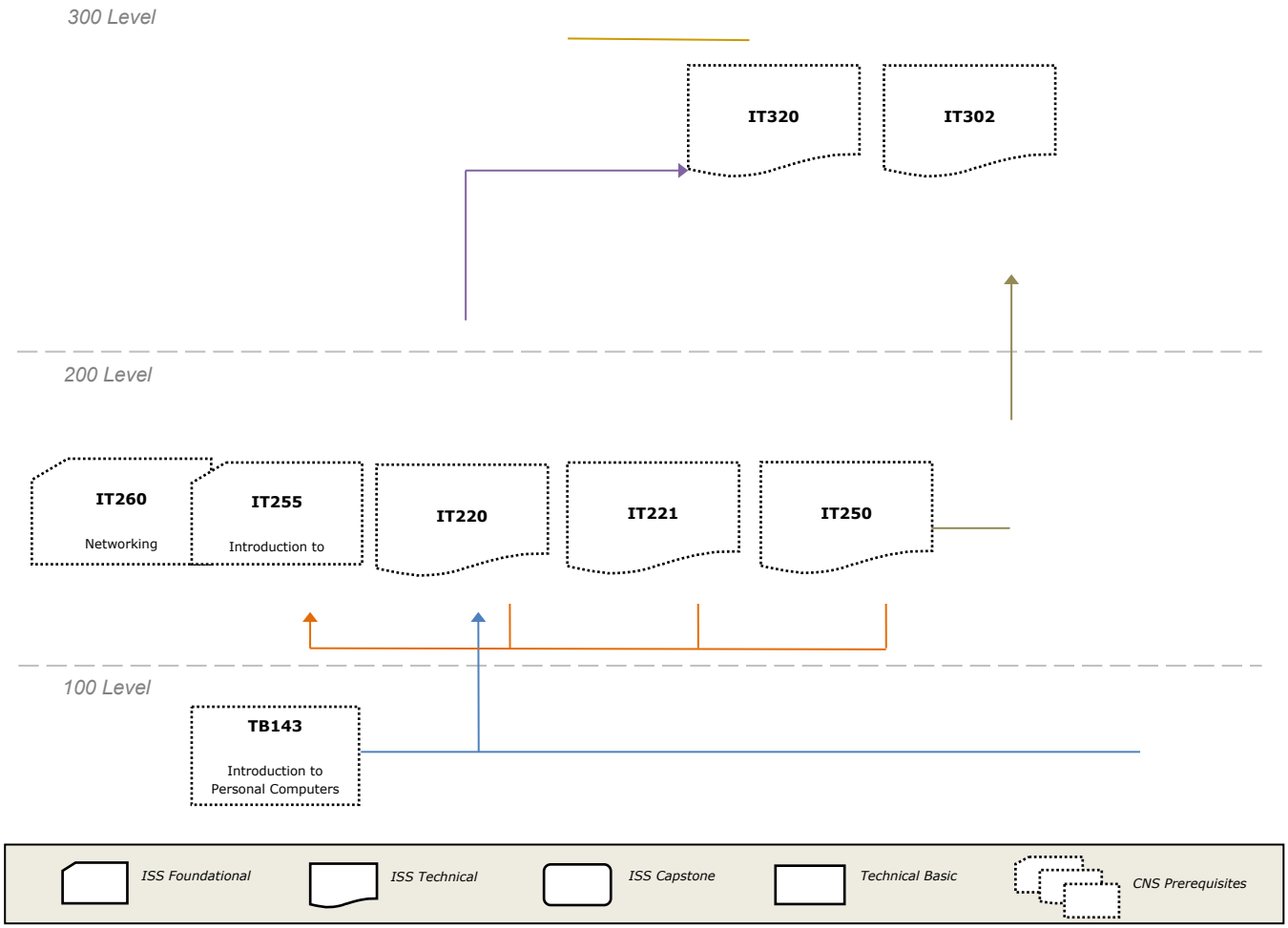
Where Does This Course Belong?

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

Major Instructional Areas

1. Access control policy framework
2. Risk mitigation with sound access controls
3. Information technology (IT) infrastructure access control requirements and implementation
4. PKI and encryption
5. Security controls in an IT infrastructure
6. Authentication solutions

Course Objectives

1. Define authorization and access to an IT infrastructure based on an access control policy framework.
2. Mitigate risk to an IT infrastructure's confidentiality, integrity, and availability with sound access controls.
3. Analyze how a data classification standard impacts an IT infrastructure's access control requirements and implementation.
4. Develop an access control policy framework consisting of best practices for policies, standards, procedures, and guidelines to mitigate unauthorized access.
5. Define proper security controls within the User Domain to mitigate risks and threats caused by human behavior.
6. Implement appropriate access controls for information systems within IT infrastructures.
7. Design appropriate authentication solutions throughout an IT infrastructure based on user types and data classification standards.
8. Implement a secure remote access solution.
9. Implement PKI and encryption solutions to ensure the confidentiality of business communications.

10. Mitigate risk from unauthorized access to IT systems through proper testing and reporting.

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)
Ballad, Bill, Tricia Ballad, and Erin Banks. *Access Control, Authentication, and Public Key Infrastructure.* 1st ed. Sudbury, MA: Jones & Bartlett, 2011.	▪		
Printed IS404 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			

Textbook Package	New to this Course	Carried over from Previous Course(s)	Required for Subsequent Course(s)
Microsoft Windows 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)	■	■	■
Companion DVD-IS404 (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.

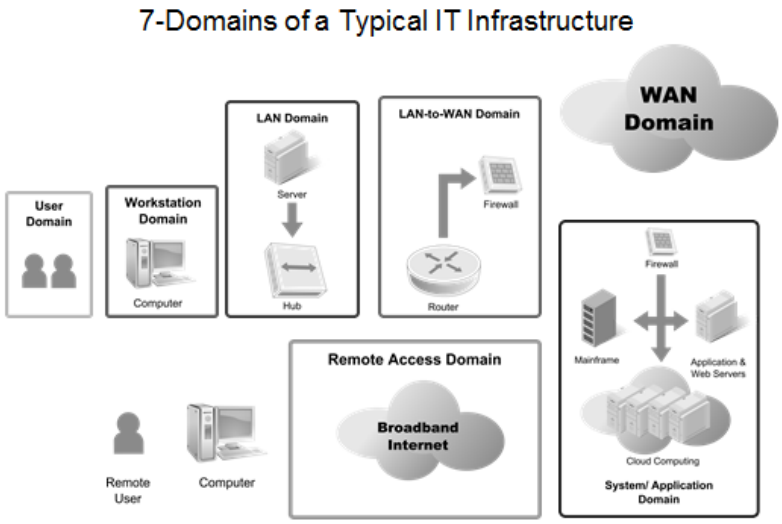


Figure 1 – Seven Domains of Information Systems Security Responsibility

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.

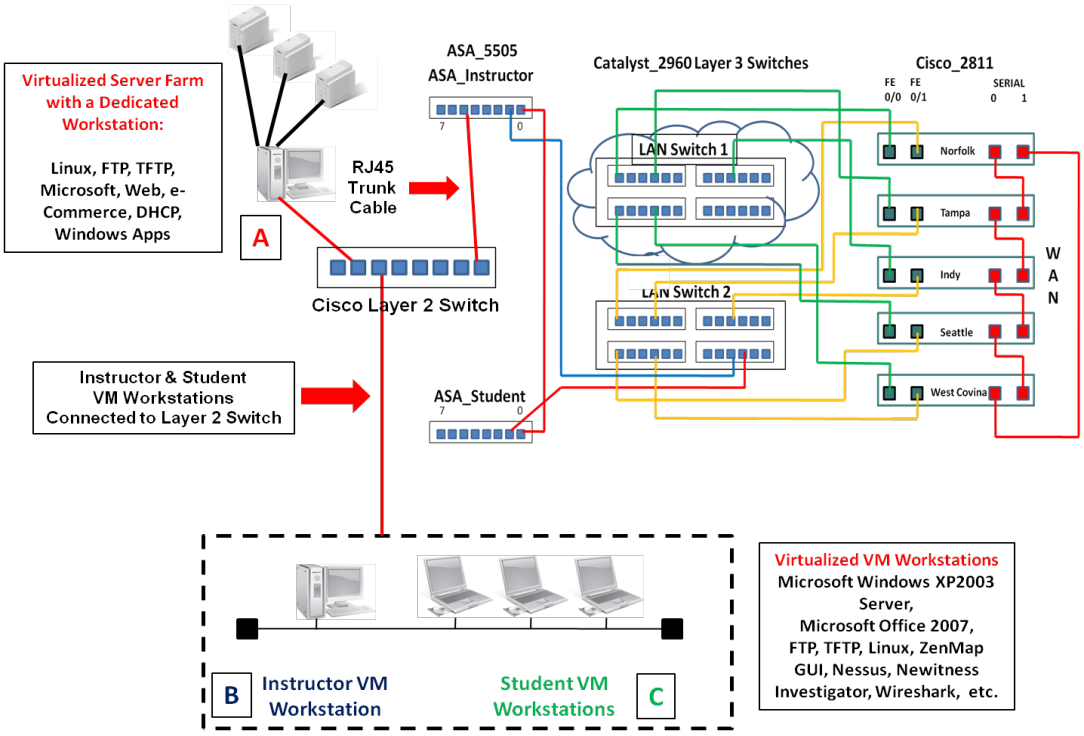


Figure 2 – ISS Mock IT Infrastructure

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)

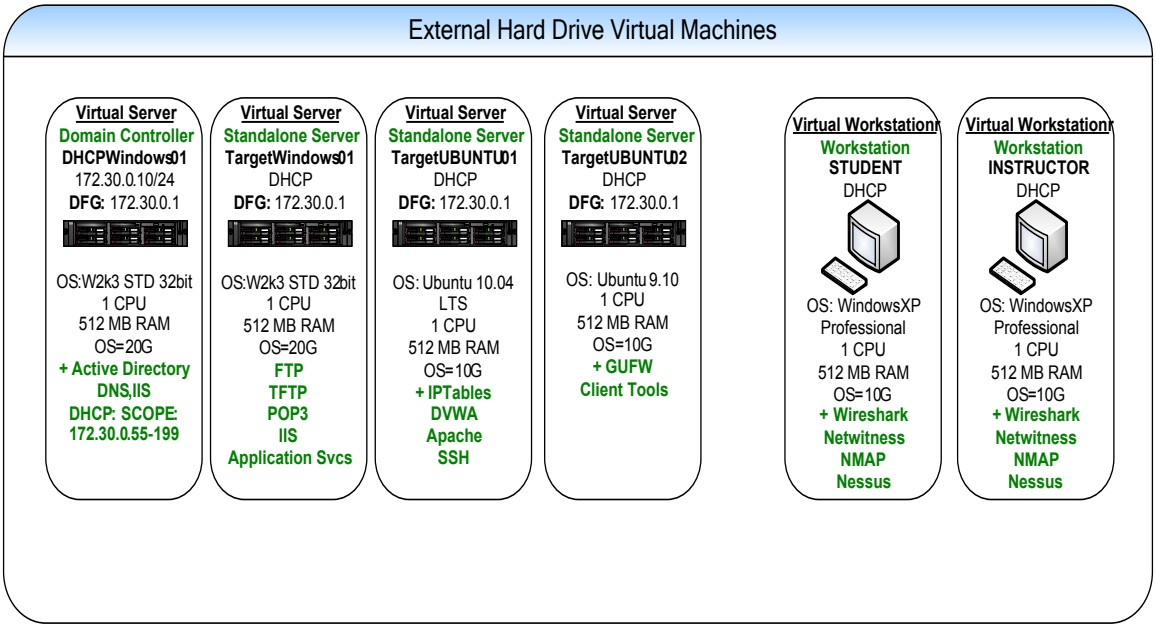


Figure 3 – VM Server Farm and VM Workstations

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)

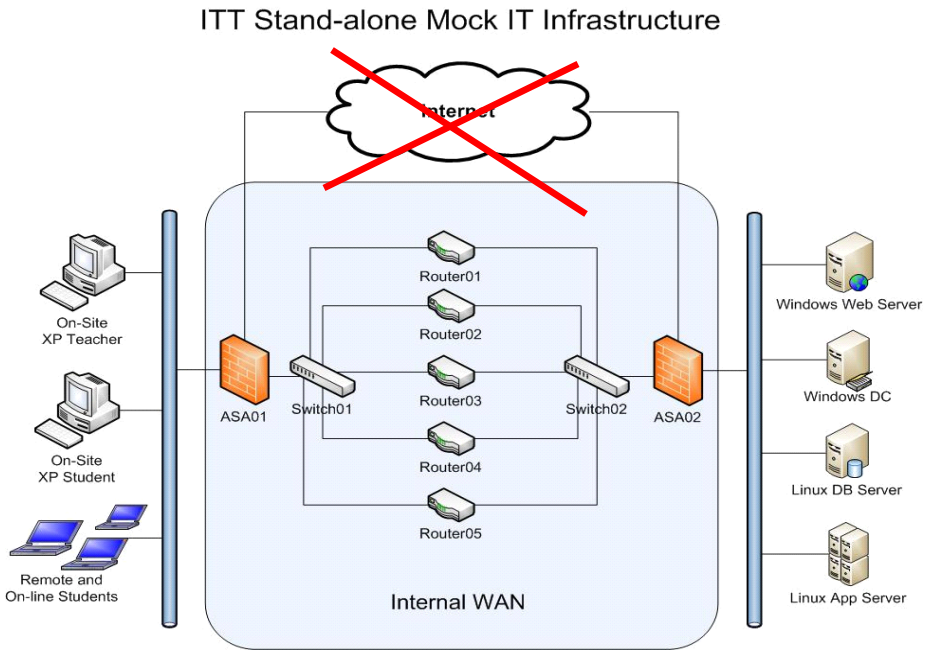


Figure 4 - Mock IT Infrastructure High-level Diagram

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

Periodicals

EbscoHost

ProQuest

- "Brocade; Survey Results Demonstrate Need for Integrated Approach to Network Security; Point Products Fall Short", *Network Business Weekly*, Apr 5, 2010.

- Bruce J. Fried, et al

  Human Resources in Healthcare: Managing for Success, 2nd ed. (Chapter 4)

- "Certified Ethical Hacker is Big News for Local Small Business: The Academy of Computer Education", *Business Wire*, Dec 22, 2008.

- Craig S. Wright

  The IT Regulatory and Standards Compliance Handbook: How to Survive Information Systems Audit and Assessments (Chapter 3)

- Dobromir Todorov

Mechanics of User Identification and Authentication: Fundamentals of Identity Management (Chapter 1, 2 and 3)

- "e-DMZ Security Selected as 2010 SC Magazine Best Regulatory Compliance Solution", *Business Wire*, Mar 8, 2010.

- Eric Cole, et al

  Network Security Bible (Chapter 5)

- Harold F. Tipton, et al

  Information Security Management Handbook, 6th ed. (Chapters 19, 30, 87 and 106)

- Harold F. Tipton, et al

  Official (ISC)2 Guide to the CISSP CBK (Domains 1 and 2)

- Jay Kelley, et al

  Network Access Control for Dummies (Chapter 15)

- Jeremy Moskowitz

  Group Policy: Management, Troubleshooting, and Security: For Windows Vista, Windows 2003, Windows XP, and Windows 2000 (Chapter 1)

- John R. Vacca

  Public Key Infrastructure: Building Trusted Applications and Web Services (Chapter 1)

- Joseph Steinberg, et al

  SSL VPN: Understanding, Evaluating, and Planning Secure, Web-Based Remote Access

- M.E. Kabay

  "Extensive Catalog Provides Security Controls for Contemporary Security Requirements", *Network World (Online)*, Nov 2, 2009.

- Michael Coles, et al

  Expert SQL Server 2008 Encryption (Chapter 1)

- Neil Wyler, ed.
  Juniper Networks Secure Access SSL VPN Configuration Guide (Chapter 9)

- "NetworkedPlanet: 50 Percent of Employees Admit to Losing Documents on the Company Network", *M2 Presswire*, Apr 12, 2010.

- Peter Stephenson
  "Applying Evolved Policy", *SC Magazine*, Oct 2009, Vol. 20 Issue 10, (Page 39)

- Poonam Khanna
  "Two-Factor Authentication is Key to Sound ID Management: Schmidt", *Computing Canada*, Jun 17, 2005, Vol. 31 Issue 9, (Page 10)

- Robert E. Larson, et al

  CCSP: Cisco Certified Security Professional Certification All-in-One Exam Guide (Chapter 4)

- "Secure Computing Shares Research Innovations and Best Practices In Email, Web and Domain Authentication; Technologists Discuss Reputation Systems and Authentication Protocols at 2007 Authentication Summit", *PR Newswire*, Apr 17, 2007.

- Seymour Bosworth, et al

  Computer Security Handbook, 5th ed. (Chapters 23, 67 and 69)

- Steve Manzuik, et al

  Network Security Assessment: From Vulnerability to Patch (Chapter 2)

- Yan Zhang, et al
  Handbook of Research on Wireless Security (Chapter XLIV)

Professional Associations

- International Association of Privacy Professionals (IAPP)

  This Web site provides opportunity to interact with a community of privacy professionals and to learn from their experiences. This Web site also provides valuable career advice.

  https://www.privacyassociation.org/ (accessed April 22, 2010)

- International Information Systems Security Certification Consortium, Inc., (ISC)²®

This Web site provides access to current industry information. It also provides opportunities in networking and contains valuable career tools.

http://www.isc2.org/ (accessed April 22, 2010)

- ISACA

This Web site provides access to original research, practical education, career-enhancing certification, industry-leading standards, and best practices. It also provides a network of like-minded colleagues and contains professional resources and technical/managerial publications.

http://www.isaca.org/template.cfm?section=home (accessed April 22, 2010)

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

Keywords:

Access Control Policy Framework

Authentication Solutions

Compliance

Data Classification Standards

Data Classification Policy

Encryption

Information Systems Security

Internet/Web Access

Layered Security Control

Multi-Factor Authentication Process

Network Diagram

Penetration Test

PKI

Remote Access Method

Remote Access Solution

Remote Workers and Employees

Risk Mitigation

Security Breach

Unauthorized Access

User Domain

U.S. and State Compliance Laws

Vulnerability Scan Report

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	▪ 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

DO	DON'T
▪ Do connect concepts explored in this course to real-life professional situations and your own experiences	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	Introduction to Access Control, Authentication, and PKI	*Access Control, Authentication, and Public Key Infrastructure*: ▪ Chapter 1	Assignment	1.1	Identification, Authentication, and Authorization Techniques	1
			Lab	1.2	Assess the Impact on Access Controls for a Regulatory Case Study	2
			Assignment	1.3	Impact of U.S. Federal and State Compliance Laws	2
2	Risk Mitigation Using Sound Access Controls	*Access Control, Authentication, and Public Key Infrastructure*:	Assignment	2.1	Infrastructure Control Areas Within the Seven Domains	1

Unit #	Unit Title	Assigned Readings	Graded Activities			
						Grade Allocation
			Grading Category	#	Activity Title	(% of all graded work)
		▪ Chapter 2	Lab	2.2	Design Infrastructure Access Controls for a Network Diagram	2
			Assignment	2.3	Improving Security Through Layered Security Control	2
3	Data Classification	*Access Control, Authentication, and Public Key Infrastructure*: ▪ Chapter 3	Quiz	3.1	Quiz 1	2
			Lab	3.2	Identify & Classify Data for Access Control Requirements	2
			Assignment	3.3	Implementation of a Data Classification Policy	2
4	Developing Access Control Policy Framework	*Access Control, Authentication, and Public Key Infrastructure*: ▪ Chapter 4 ▪ Chapter 5	Discussion	4.1	Security Breach Evaluation	5
			Lab	4.2	Implement Organizational-Wide Access Controls	2
			Assignment	4.3	Implementation of an Organization-Wide Security Plan	2
5	Managing Human	*Access Control, Authentication,*	Quiz	5.1	Quiz 2	2

Unit #	Unit Title	Assigned Readings	Graded Activities			
						Grade Allocation
			Grading Category	#	Activity Title	(% of all graded work)
		▪ Chapter 6 ▪ Chapter 7	Lab	5.2	Enhance Security Controls for Access to Sensitive Data	2
			Assignment	5.3	Implementing Comprehensive Human Resources Risk Management Plan	2
6	Implementing Infrastructure Controls	*Access Control, Authentication, and Public Key Infrastructure*: ▪ Chapter 8	Assignment	6.1	Aligning Account Types and Privileges	1
			Lab	6.2	Enhance Security Controls for File System Access Controls	2
			Assignment	6.3	Managing Microsoft Account and File Systems Access Controls	2
7	Authentication Methods and Requirements	*Access Control, Authentication, and Public Key Infrastructure*: ▪ Chapter 10	Quiz	7.1	Quiz 3	2
			Lab	7.2	Design a Multi-factor Authentication Process	2
			Assignment	7.3	Implementation of Authentication Process	2

Unit #	Unit Title	Assigned Readings	Graded Activities			
						Grade Allocation
			Grading Category	#	Activity Title	(% of all graded work)
8	Securing Remote Access	*Access Control, Authentication, and Public Key Infrastructure*: ▪ Chapter 11 ▪ Chapter 12	Discussion	8.1	Remote Access Method Evaluation	5
			Lab	8.2	Align Appropriate Remote Access Solutions Based on Data Sensitivity	2
			Assignment	8.3	Internet/Web Access Management	2
9	PKI and Encryption	*Access Control, Authentication, and Public Key Infrastructure*: ▪ Chapter 13	Quiz	9.1	Quiz 4	2
			Lab	9.2	Apply Encryption to Mitigate Risk Exposure	2
			Assignment	9.3	PKI and Encryption at Work	2
10	Unauthorized Access Risk Mitigation Techniques	*Access Control, Authentication, and Public Key Infrastructure*: ▪ Chapter 14	Assignment	10.1	Scope of Work for Penetration Test	1
			Lab	10.2	Use Reconnaissance, Probing, & Scanning to Identify Servers and Hosts	2
			Assignment	10.3	Developing a Vulnerability Scan Report	2
11	Course Review and	N/A	Exam	11.1	Final Exam	20

Unit #	Unit Title	Assigned Readings	Graded Activities			
						Grade Allocation
			Grading Category	#	Activity Title	(% of all graded work)
	Final Examination		Project	11.2	Access Control Proposal	18

Evaluation and Grading

Evaluation Criteria

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

Category	Weight
Discussion	10
Assignment	24
Lab	20
Project	18
Quiz	8
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)

