ITT Technical Institute

IS3220T

Information Technology Infrastructure Security

Onsite Course

SYLLABUS

Credit hours: 4.5

Contact/Instructional hours: 72 (36 Theory Hours, 36 Lab Hours)

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

Prerequisites: IS3120T Network Communications Infrastructure or equivalent

Course Description:

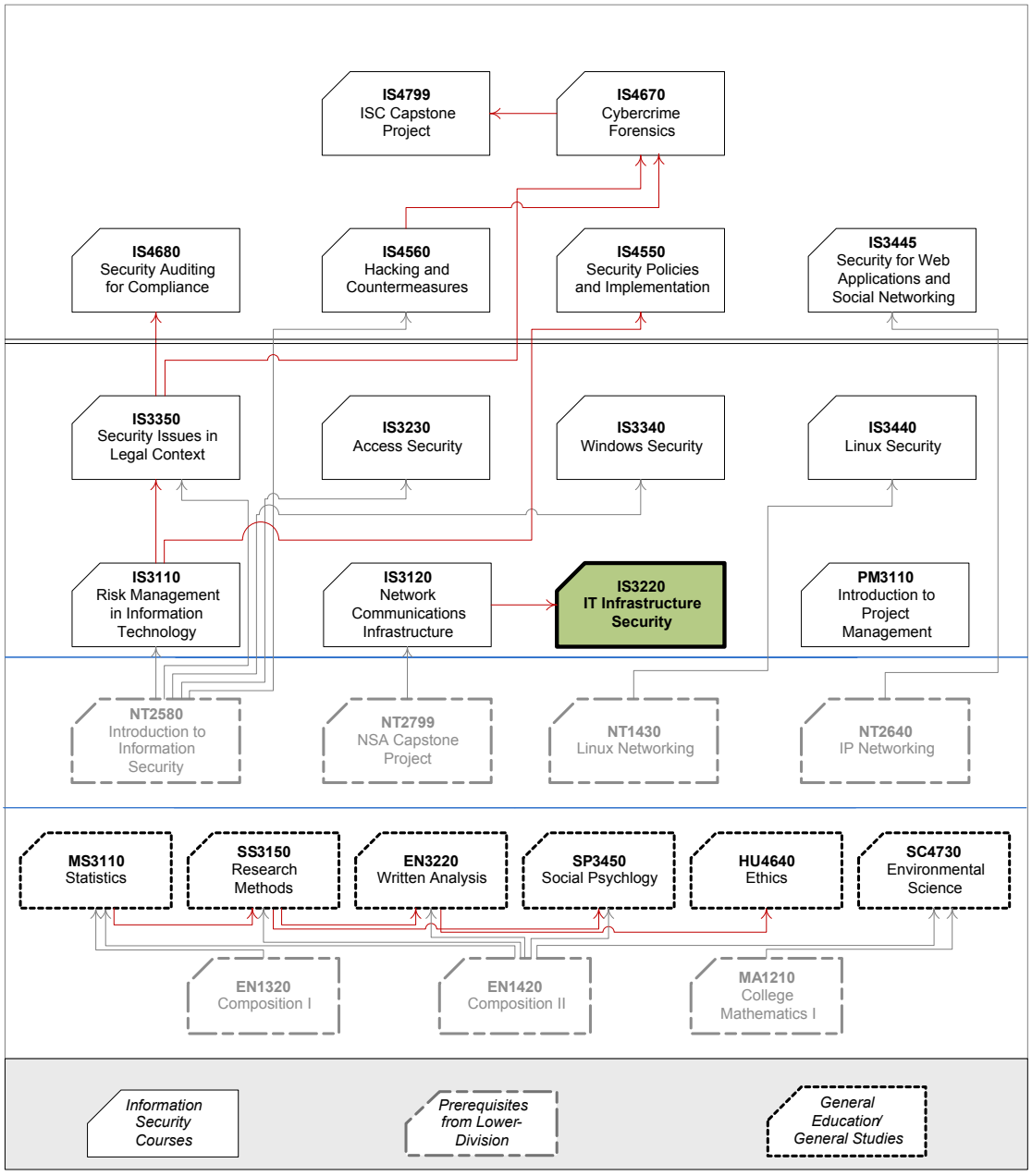
This course examines security challenges encountered on backbone networks in an information and communications infrastructure. Topics include methods of tightening infrastructure security, a variety of tools for monitoring and managing infrastructure security and commonly-used technologies, such as firewalls and VPNs.

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. Network-centric TCP/IP protocols and applications
2. Network security risks, threats, and vulnerabilities
3. Firewall types, functions, uses, and deployment strategies
4. VPN types, functions, uses, and deployment strategies
5. Layered network security strategies
6. Secure network design
7. Best practices and strategies for network security and incident response

Course Objectives

1. Review essential Transmission Control Protocol/Internet Protocol (TCP/IP) behavior and applications used in IP networking.
2. Explain the fundamental concepts of network security.
3. Recognize the impact that malicious exploits and attacks have on network security.
4. Identify network security tools and discuss techniques for network protection.
5. Describe the fundamental functions performed by firewalls.
6. Assess firewall design strategies.
7. Describe the foundational concepts of VPNs.
8. Describe network security implementation strategies and the roles each can play within the security life cycle.
9. Appraise the elements of firewall and VPN implementation and management.
10. Identify network security management best practices and strategies for responding when security measures fail.

Learning Materials and References

Required Resources

Textbook Package	New to this Course	Carried over from Previous Course(s)	Required for Subsequent Course(s)
Stewart, James M. *Network Security, Firewalls, and VPNs*. 1st ed. Sudbury, MA: Jones & Bartlett, 2011.	■		
Printed IS3220 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 equipment-based labs that require a live, IP network. (For onsite only)	■	■	■
ISS Mock IT Infrastructure (2) – VM Server Farm (2 Microsoft Windows Servers and 2 Ubuntu Linux Servers) for classroom equipment-based VM labs. (For both onsite and online)	■	■	■
ISS Mock IT Infrastructure (2) – VM Workstation (Microsoft Windows XP Professional Workstation with Core ISS Apps and Tools) for classroom equipment-based VM labs. (For both onsite and online)	■	■	■

(1) The following presents the core ISS Cisco core backbone network components needed for some of the equipment-based 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

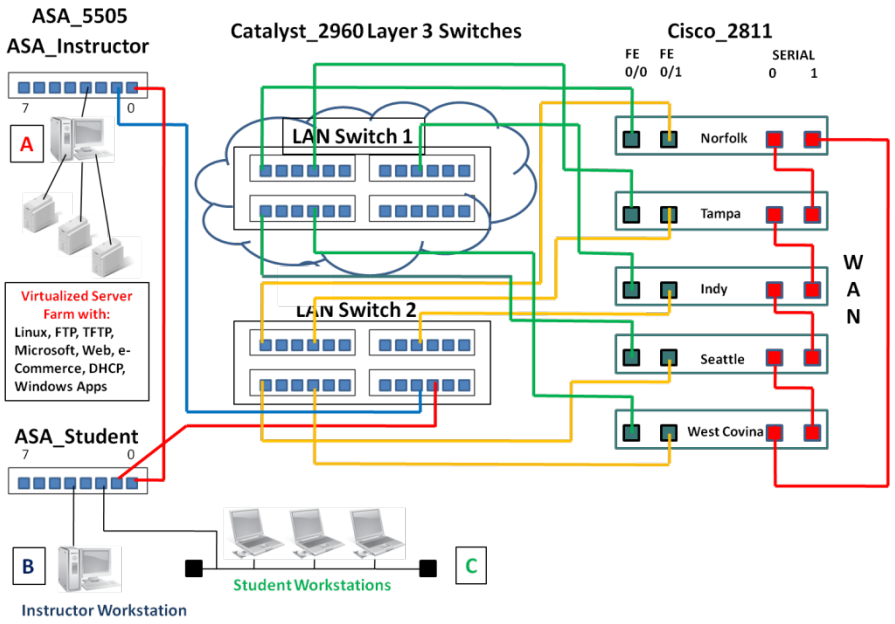


Figure 1 – ISS Cisco Core Backbone Network

(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:

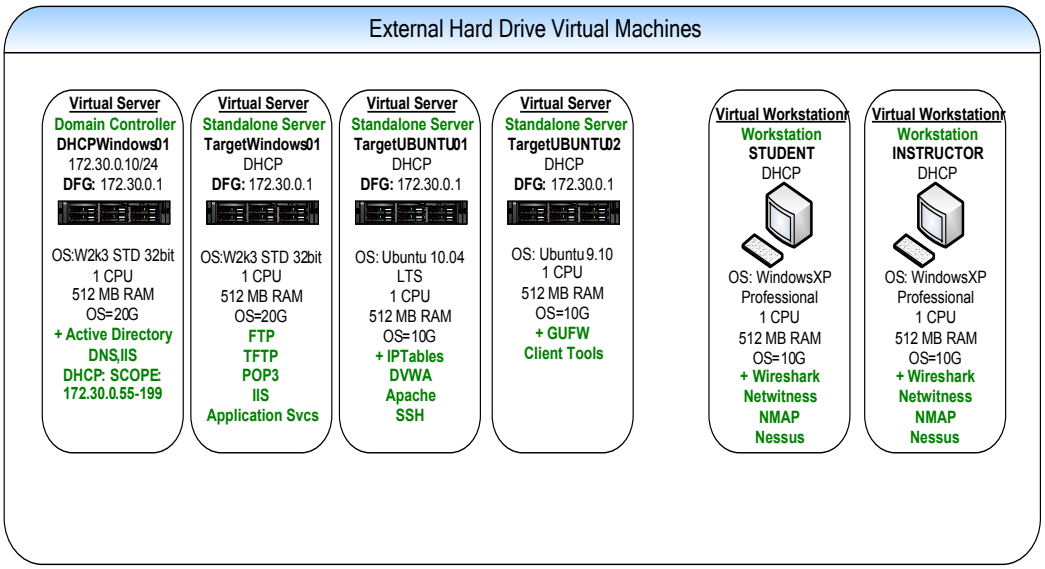


Figure 2 – ISS Core VM Server Farm & VM Workstations

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.

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

1. New VM for server farm: “VulnerableXP01”. This VM is a vulnerable Microsoft Windows Server 2003 Standard Edition 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®[1]

[1] Nessus® is a Registered Trademark of Tenable Network Security, Inc.

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:

- Michael Rash, *Linux Firewalls: Attack Detection and Response With Iptables, Psad, and Fwsnort*
- Debra L. Shinder, et al , *Scene of the Cybercrime*, 2nd ed.
- Thomas Shinder, *The Best Damn Firewall Book Period*, 2nd ed.
- James M. Stewart, et al., *CISSP: Certified Information Systems Security Professional Study Guide*, 4th ed.
- John R. Vacca, et al, *Firewalls: Jumpstart for Network and Systems Administrators*
- Anne Henmi (ed)., *Firewall Policies and VPN Configurations* (Chapters 2 and 5)
- Seymour Bosworth, et al., *Computer Security Handbook*, 5th ed. (Chapters 3, 21 and 26)

Search in:

Books > Books 24x7

Periodicals . EbscoHost

Professional Associations

- CERT

  This Web site provides assistance in understanding and handling security vulnerabilities. It also provides research tools on long-term changes in networked systems and gives training assistance to improve security.

  http://www.cert.org/ (accessed June 22, 2010)

- National Institute of Standards and Technology (NIST)

This Web site provides access to subject matter experts and also facilitates in research. It also provides career-building resources and opportunities.
http://www.nist.gov/index.html (accessed June 22, 2010)

- National Security Agency/Central Security Service (NSA/CSS)
  This Web site provides guidance on information assurance security solutions and also provides insights on risks, vulnerabilities, mitigations, and threats. It also provides information on cryptologic support.
  http://www.nsa.gov/index.shtml (accessed June 22, 2010)

- SANS: Computer Security Training, Network Research & Resources
  This Web site provides information on computer security training through several delivery methods like live and virtual conferences, mentors, online, and onsite. It also provides certification and numerous free security resources.
  http://www.sans.org/ (accessed June 22, 2010)

Other References

- Common Vulnerabilities and Exposures (CVE)
  http://cve.mitre.org/ (accessed June 22, 2010)

- Information Assurance Support Environment (IASE): Security Technical Implementation Guides (STIGS)
  http://iase.disa.mil/stigs/stig/index.html (accessed June 22, 2010)

- Information Assurance Support Environment (IASE): Security Checklists
  http://iase.disa.mil/stigs/checklist/index.html (accessed June 22, 2010)

- Mark Paulding, Department of Defense Proposes New Information Security Requirements for Contractors", *HL Chronicle of Data Protection*, Mar2010
  http://www.hhdataprotection.com/articles/information-security/ (accessed April 26, 2010)

- Chris May, et al., Advanced Information Assurance Handbook
  http://www.cert.org/archive/pdf/aia-handbook.pdf (accessed April 26, 2010)

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

Information Search

Use the following keywords to search for additional online resources that may be used for supporting your work on the course assignments:

Attacker
C-I-A, C-I-A triad
Confidentiality, Integrity, Availability
Defense in depth
Demilitarized zone
DMZ
Filtering
Firewall
Firewall Design
Firewall Management
Firewall Security
Hacker
Intrusion Detection System (IDS)
Intrusion Prevention System (IPS)
IP
Malware
NetWitness Investigator
Network Protocol, Networking Protocol
Network Security
Packet Filter
Policy, Policies
Protocols
Proxy Firewall
Router
Security
Security Policies
Stateful Firewall
Switch
TCP/IP
Threats
Trojan Horse
Virtual Private Network (VPN)
Virus

VPN Design

VPN Management

VPN Security

Vulnerabilities

Web Server

Worm

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.

Important: Keep the deliverables you completed for earlier units as you may need them for working on the tasks assigned in later units of this course.

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	▪ 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
▪ 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 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	Essential TCP/IP Network Protocols and Applications	*Network Security, Firewalls, and VPNs:* ▪ Chapter 1 ▪ Chapter 2 ▪ Chapter 5	Discussion	1.1	Familiar Protocols	1
			Lab	1.2	Analyze Essential TCP/IP Networking Protocols	2
			Assignment	1.3	Clear-Text Data in Packet Trace	2
Course Project and associated deliverables are introduced in Units 1 - 2.						
2	Network Security Basics	*Network Security, Firewalls, and VPNs:* ▪ Chapter 1	Discussion	2.1	Familiar Domains	1
			Lab	2.2	Network Documentation	2
			Assignment	2.3	Selecting Security Countermeasures	2
3	Network Security Threats	*Network Security, Firewalls, and VPNs:* ▪ Chapter 4 ▪ NIST SP 800-30: Risk Management Guide for Information Technology Systems (http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf)	Discussion	3.1	Social Engineering Defense Issues	1
			Lab	3.2	Network Discovery & Security Scanning Using ZenMap GUI (*Nmap*)	2

Unit #	Unit Title	Assigned Readings	Graded Activities			
			Grading Category	#	Activity Title	Grade Allocation (% of all graded work)
4	Network Security Tools and Techniques	*Network Security, Firewalls, and VPNs:* ▪ Chapter 5 ▪ Chapter 7 ▪ Chapter 15	Discussion	4.1	Host-Based vs. Network-Based IDSs/IPSs	1
			Lab	4.2	Perform a Software Vulnerability Scan & Assessment with Nessus®[2]	2
			Assignment	4.3	Identify Unnecessary Services From a Saved Vulnerability Scan	2
			Project	4.4	Network Survey	4
5	Firewall Fundamentals	*Network Security, Firewalls, and VPNs:* ▪ Chapter 2	Discussion	5.1	Ingress and Egress Filtering	1
			Lab	5.2	Configure a Microsoft Windows Workstation Internal Firewall	2
			Assignment	5.3	Select the Proper Type of Firewall	2
6	Firewall Design Strategies	*Network Security, Firewalls, and VPNs:* ▪ Chapter 7 ▪ Chapter 8	Discussion	6.1	Firewall Security Strategies	1
			Lab	6.2	Design a De-Militarized Zone (DMZ) for a LAN-to-WAN Ingress/Egress	2
7	VPN Fundamentals	*Network Security, Firewalls, and VPNs:* ▪ Chapter 3 ▪ Chapter 11 ▪ Chapter 12	Discussion	7.1	Developing a VPN Policy and Enforcing VPN Best Practices	1
			Lab	7.2	Implement a VPN Tunnel for Secure Remote-Access	2
			Assignment	7.3	Create a VPN Connectivity Troubleshooting Checklist	2
			Project	7.4	Network Design	5

[2] Nessus is a Registered Trademark of Tenable Network Security, Inc.

Unit #	Unit Title	Assigned Readings	Graded Activities			
			Grading Category	#	Activity Title	Grade Allocation (% of all graded work)
8	Network Security Implementation Strategies	*Network Security, Firewalls, and VPNs:* ▪ Chapter 5	Discussion	8.1	System Hardening	1
			Lab	8.2	Design a Layered Security Strategy for an IP Network Infrastructure	2
			Assignment	8.3	Security Concerns and Mitigation Strategies	2
9	Firewall Implementation and Management	*Network Security, Firewalls, and VPNs:* ▪ Chapter 9 ▪ Chapter 10 ▪ Chapter 13 ▪ Chapter 14	Discussion	9.1	Firewall Implementation Planning	1
			Lab	9.2	Construct a Linux Host Firewall and Monitor for IP Traffic	2
			Assignment	9.3	Remote Access Security Plan and Documentation	2
10	Network Security Management	*Network Security, Firewalls, and VPNs:* ▪ Chapter 6 ▪ Chapter 15 ▪ NIST SP 800-61: Computer Security Incident Handling Guide (http://www.nist.gov/customcf/get_pdf.cfm?pub_id=51289)	Discussion	10.1	Incident Response Strategies	1
			Lab	10.2	Design and Implement Security Operations Management Best Practices	2
			Assignment	10.3	Postincident Executive Summary Report	2
11	Course Review and Final Examination	N/A	Project	11.1	Network Security Plan†	20

Unit #	Unit Title	Assigned Readings	Graded Activities			
			Grading Category	#	Activity Title	Grade Allocation (% of all graded work)
			Exam	11.2	Exam	25

† **Candidate for ePortfolio**

Evaluation and Grading

Evaluation Criteria

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

Category	Weight
Discussion	10
Lab	20
Assignment	16
Project	29
Exam	25
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)