ITT Technical Institute

IS4560T

Hacking and Countermeasures

Onsite Course

SYLLABUS

Credit hours: 4.5

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

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

Prerequisites: NT2580T Introduction to Information Security or equivalent

Course Description:

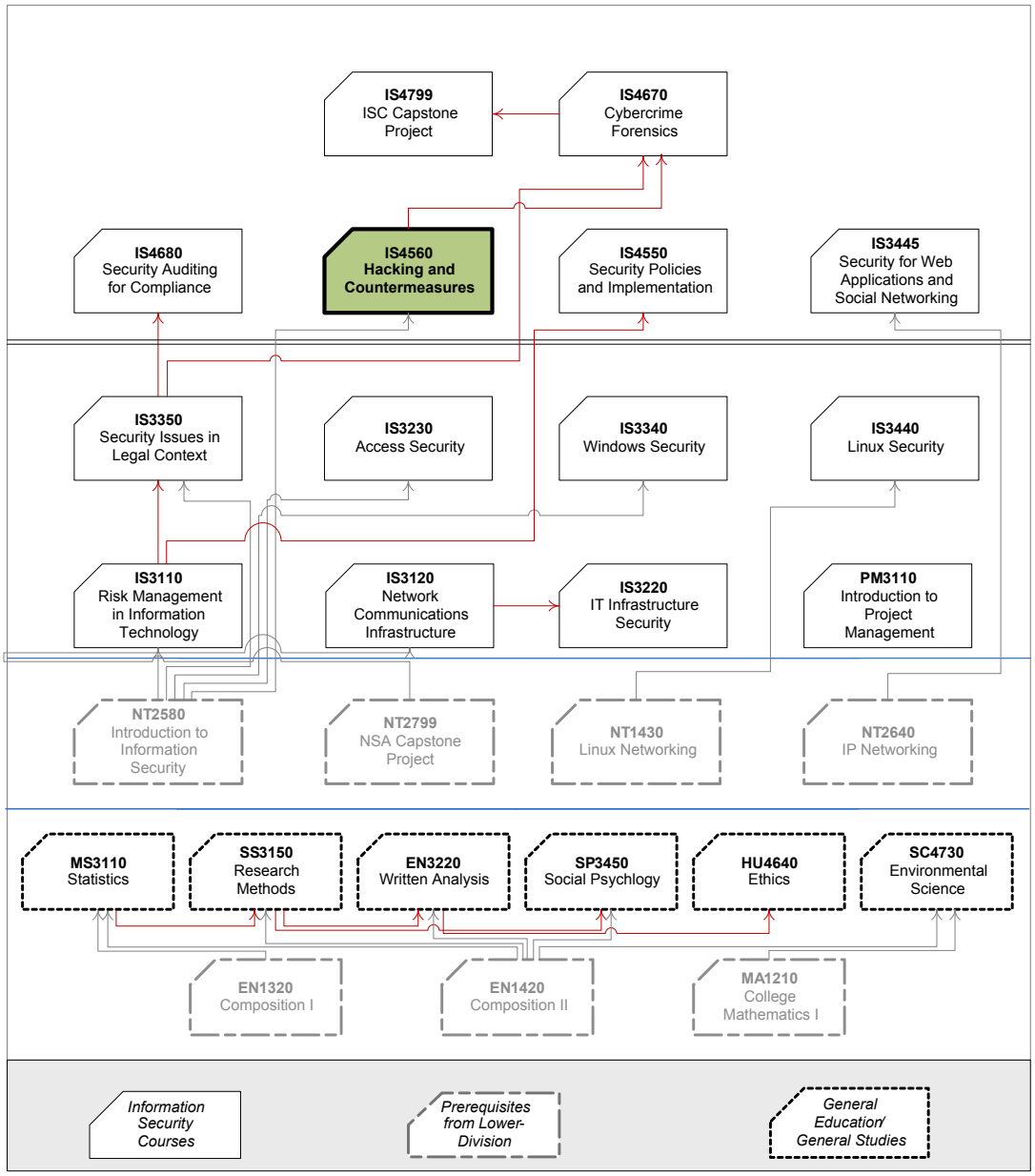
This course explores hacking techniques and countermeasures. Topics include network systems penetration tools and techniques for identifying vulnerabilities and security holes in operating systems and software applications. Students will practice ethical hacking procedures to attempt unauthorized access to target systems and data, and incident handling procedures in the case of an information security compromise.

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. Evolution of computer hacking
2. The role of information security professionals
3. Hacking tools and techniques
4. Vulnerabilities exploited by hackers
5. Incident response
6. Defensive technologies

Course Objectives

1. Explain the history and current state of hacking and penetration testing, including ethical and legal implications.
2. Describe cryptology.
3. Identify common information gathering tools and techniques.
4. Analyze system vulnerabilities exploited by hackers.
5. Perform web and database attacks.
6. Remove trojans, backdoors, and malware from infected systems.
7. Perform network traffic analysis and sniffing by using appropriate tools.
8. Analyze wireless network vulnerabilities exploited by hackers.
9. Perform incident handling by using appropriate methods.
10. Compare and contrast defensive technologies.

Learning Materials and References

Required Resources

Textbook Package	New to this Course	Carried over from Previous Course(s)	Required for Subsequent Course(s)
Oriyano, Sean-Philip and Michael Gregg. *Hacker Techniques, Tools, and Incident Handling*. 1st ed. Sudbury, MA: Jones & Bartlett, 2010.	■		
Printed IS4560 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 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)	■	■	■

(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

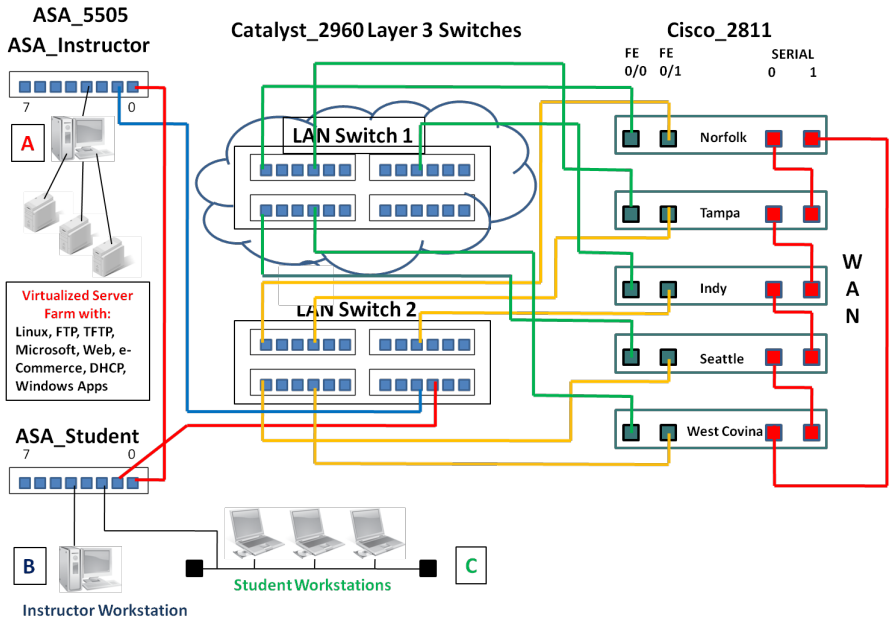


Figure 1 – ISS Cisco Core Backbone Network

(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:

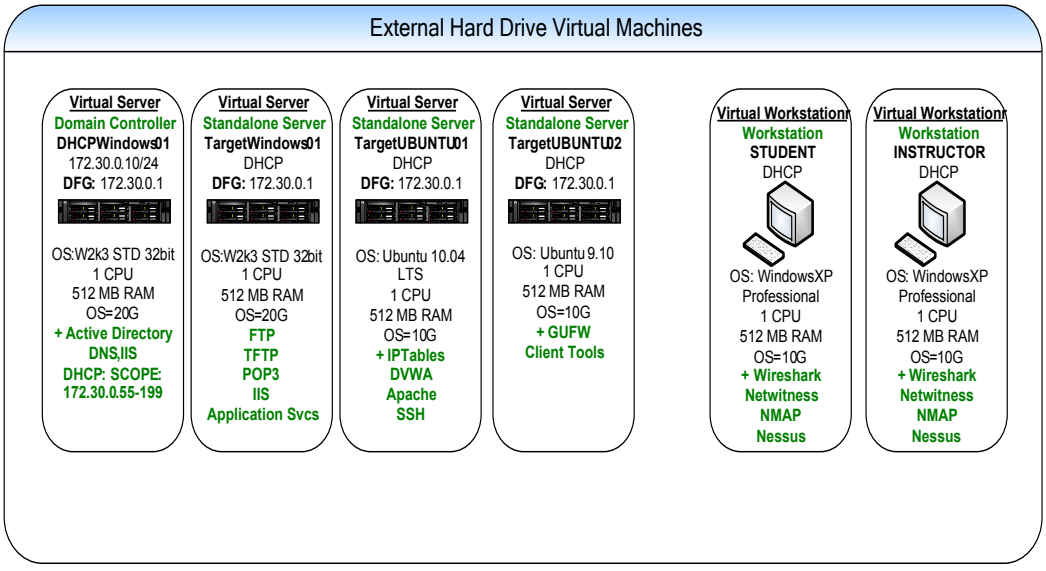


Figure 2 – ISS Core VM Server Farm & VM Workstations

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 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 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®[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:

Books
Books24X7
CRCnetBASE
Periodicals
ProQuest
EbscoHost
Reference
School of Information Technology

- Harold F. Tipton, et al

Information Security Management Handbook, 6th ed. (Chapter 76)

- Tim Greene
  "SSL hack vulnerability details to emerge; Black Hat demo to show even extended validation certificates are vulnerable to man-in-the-middle attacks", *Network World (Online)*, Jul 16, 2009.

- Peter Galli
  "Red Hat rolls out Global Desktop", *eWeek*, May 2007, Vol. 24 Issue 17, (Page 14-14), (*AN 25060492*)

- Cliff Saran
  "Wal-Mart opts for Linux platform to cut costs through virtualisation", *Computer Weekly*, Feb 2007, (Page 12-12), (*AN 24336710*)

Other References

- DShield
  Security threat trends and current information
  http://www.dshield.org/indexd.html (accessed May 25, 2010).

- Insecure.org
  Security tools and documentation
  http://insecure.org/ (accessed May 25, 2010).

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

Keywords:
Asymmetric Encryption
Black Hat Hackers
Cryptanalysis
Cryptographic System
Cryptographic Technologies
Cryptographic Tools
Data Gathering Techniques
Encryption
Ethical Hacking

Ethical Laws and Standards for Penetration Testers

Footprinting

Hacking

Hashing

Information Gathering

Nessus®

Nmap

Penetration Testing

Pretty Good Privacy (PGP)

Symmetric Encryption

Vulnerability Scanning

White Hat Hackers

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	Introduction to Hacking and Penetration Testing, Ethics and the Law	*Hacker Techniques, Tools, and Incident Handling*: ▪ Chapter 1	Assignment	1.1	Developments in Hacking, Cybercrime, and Malware	1
			Lab	1.2	Develop an Attack & Penetration Test Plan	2
2	Cryptology in Information Security	*Hacker Techniques, Tools, and Incident Handling*: ▪ Chapter 1 ▪ Chapter 3	Assignment	2.1	Cryptography	1
				2.2	Vulnerability of a Cryptosystem	1
			Lab	2.3	Implement Hashing & Encryption for Secure Communications	2
3	Information Gathering and Footprinting	*Hacker Techniques, Tools, and Incident Handling*: ▪ Chapter 5	Assignment	3.1	Information Gathering Plan	1
				3.2	Data Gathering and Footprinting Protection Plan	1
			Lab	3.3	Perform Data Gathering and Foot-printing on a Targeted Website	2

Unit #	Unit Title	Assigned Readings	Graded Activities			
			Grading Category	#	Activity Title	Grade Allocation (% of all graded work)
4	Port Scanning, Vulnerability Scanning, and System Exploits	*Hacker Techniques, Tools, and Incident Handling*: ▪ Chapter 6 ▪ Chapter 7	Assignment	4.1	Top Ports and Rising Ports Review	1
			Lab	4.2	Compromise and Exploit a Vulnerable Microsoft Workstation/Server	2
			Project	4.3	Project Part 1: Current Security Threats†	3
5	Web and Database Attacks	*Hacker Techniques, Tools, and Incident Handling*: ▪ Chapter 9	Discussion	5.1	Web Server Vulnerability Analysis	5
			Assignment	5.2	Web Application Attacks Prevention	1
			Lab	5.3	Perform a Website & Database Attack by Exploiting Identified Vulnerabilities	2
			Project	5.4	Project Part 2: Vulnerabilities in Information Technology (IT) Security†	3
6	Identifying and Combating Trojans, Backdoors, and Malware	*Hacker Techniques, Tools, and Incident Handling*: ▪ Chapter 10 ▪ Chapter 11	Assignment	6.1	Malware Lifecycle	1
			Lab	6.2	Identify & Mitigate Malware & Malicious Software on a Linux Workstation	2
			Exam	6.3	Mid-Term Exam	15

Unit #	Unit Title	Assigned Readings	Graded Activities			
			Grading Category	#	Activity Title	Grade Allocation (% of all graded work)
7	Network Traffic Analysis and Sniffing	*Hacker Techniques, Tools, and Incident Handling*: ▪ Chapter 12	Assignment	7.1	Network Traffic and Exploit Identification	1
			Lab	7.2	Conduct a Network Traffic Analysis & Baseline Definition	2
			Project	7.3	Project Part 3: Investigate Findings on the Malware†	3
8	Wireless Security	*Hacker Techniques, Tools, and Incident Handling*: ▪ Chapter 8	Discussion	8.1	Security Features of Wireless Technologies	5
			Assignment	8.2	Wireless Exploit Research	1
			Lab	8.3	Audit and Implement a Secure WLAN Solution	2
			Project	8.4	Project Part 4: Analysis of Intrusion Detection System (IDS) Traffic with Inbound Attacks†	3
9	Incident Response	*Hacker Techniques, Tools, and Incident Handling*: ▪ Chapter 14	Assignment	9.1	Gaps in Incident Response	1
			Lab	9.2	Perform Incident Response for Linux and Microsoft Workstations	2

Unit #	Unit Title	Assigned Readings	Graded Activities			
			Grading Category	#	Activity Title	Grade Allocation (% of all graded work)
10	Defensive Technologies and Techniques	*Hacker Techniques, Tools, and Incident Handling*: ▪ Chapter 4 ▪ Chapter 15	Assignment	10.1	Controls	1
			Lab	10.2	Design and Implement SNORT as an Intrusion Detection System (IDS)	2
			Project	10.3	Project Part 5: Malware Infection†	3
11	Course Review and Final Examination	N/A	Project	11.1	Project Part 6: Defense Plan to Prevent Attacks†	3
			Exam	11.2	Final Exam	25

† Candidate for ePortfolio

Evaluation and Grading

Evaluation Criteria

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

Category	Weight
Assignment	12%
Discussion	10%
Lab	20%
Project	18%
Exam	40%
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)