IS317
Hacker Techniques, Tools and Incident Handling
[Onsite and Online]

Course Description:

This course is an introduction to hacking tools and incident handling. Areas of instruction include various tools and vulnerabilities of operating systems, software and networks used by hackers to access unauthorized information. This course also addresses incident handling methods used when information security is compromised.

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

Prerequisites: IT260 Networking Application Services and Security or equivalent

Credit hours: 4

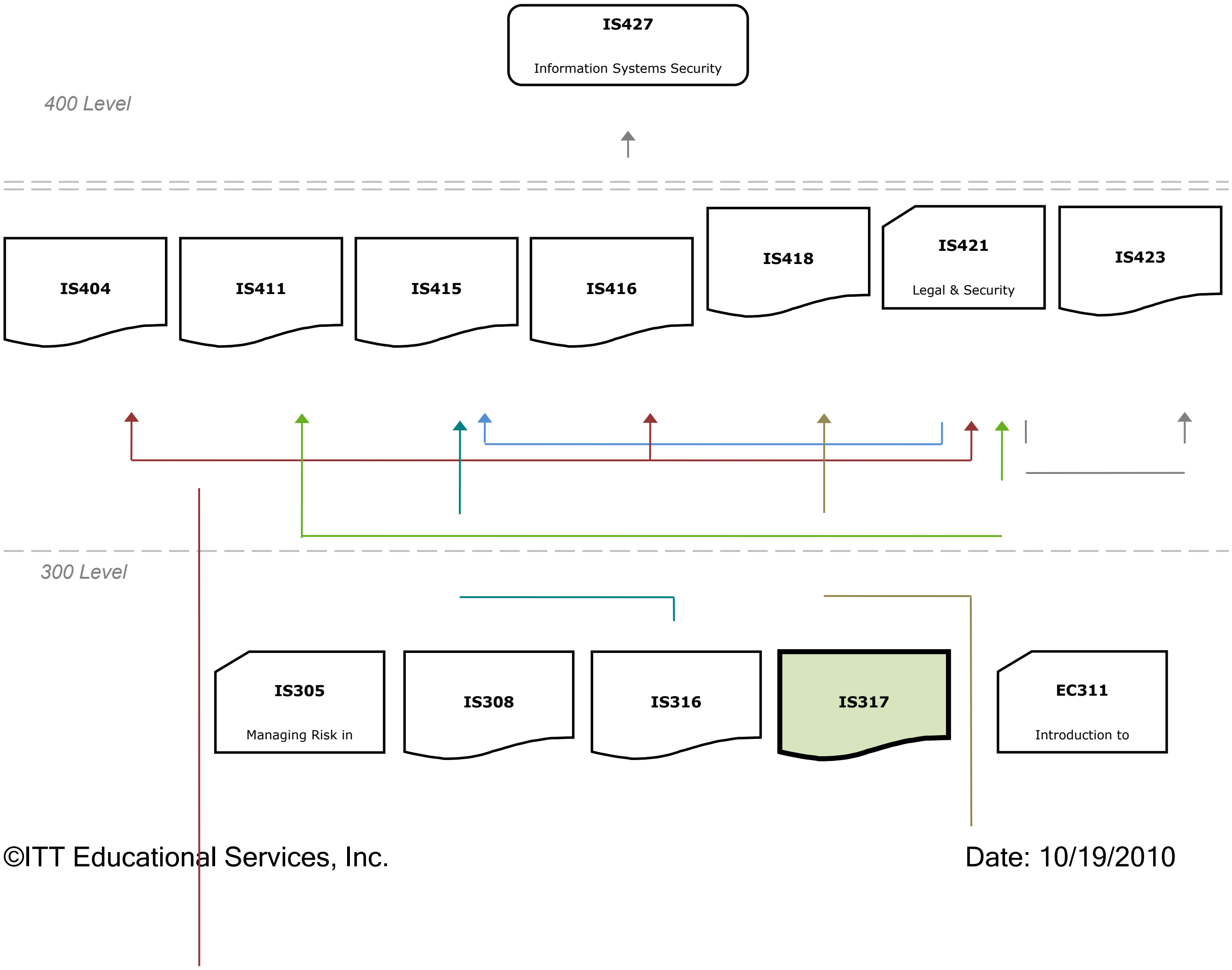
Contact hours: 50 (30 Theory Hours, 20 Lab Hours)

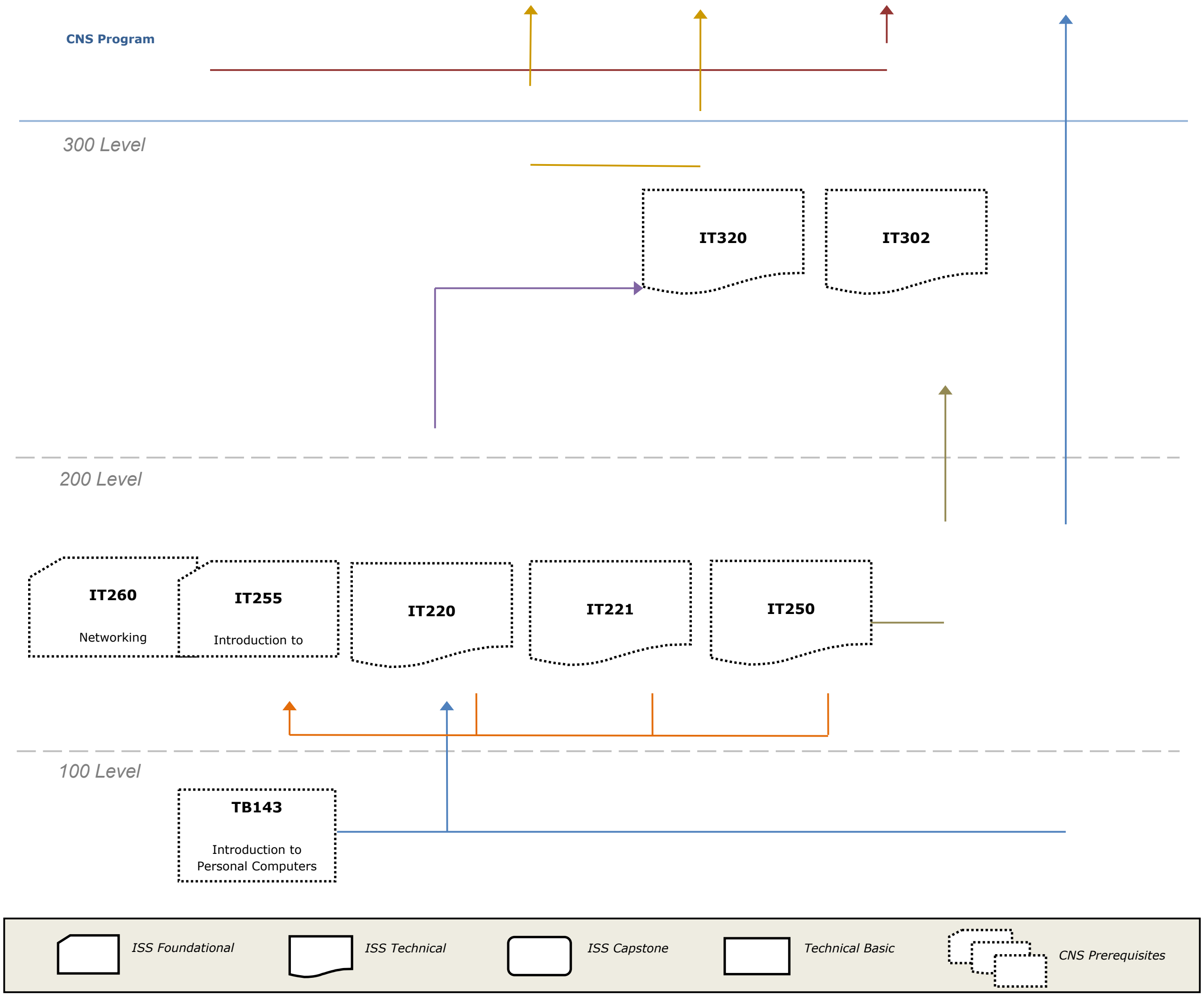
Where Does This Course Belong?

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:




CNS 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. 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.

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)
Oriyano, Sean-Philip and Michael Gregg. *Hacker Techniques, Tools, and Incident Handling*. 1st ed. Sudbury, MA: Jones & Bartlett, 2010.	▪		
Printed IS317 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)	▪	▪	▪
Companion DVD-IS317 (3) - Additional VMs, Apps, Tools needed for the Student VM workstation to perform the labs			▪

Textbook Package	New to this Course	Carried over from Previous Course(s)	Required for Subsequent Course(s)
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.

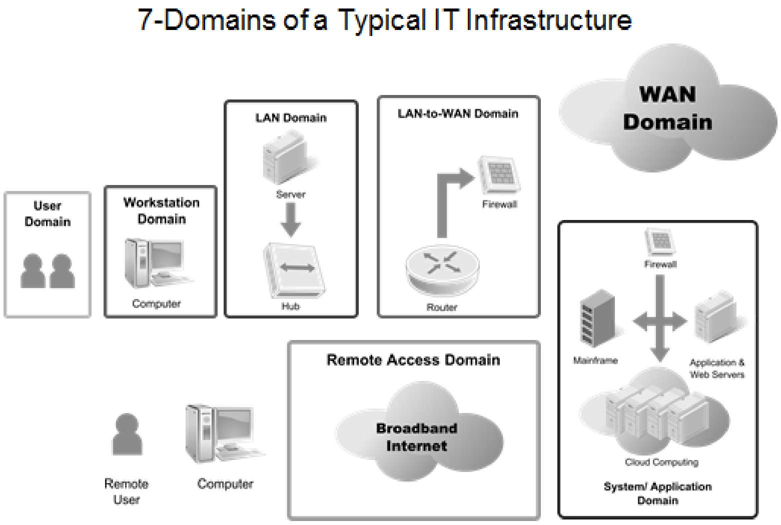


Figure 1 – Seven Domains of Information Systems Security Responsibility

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.

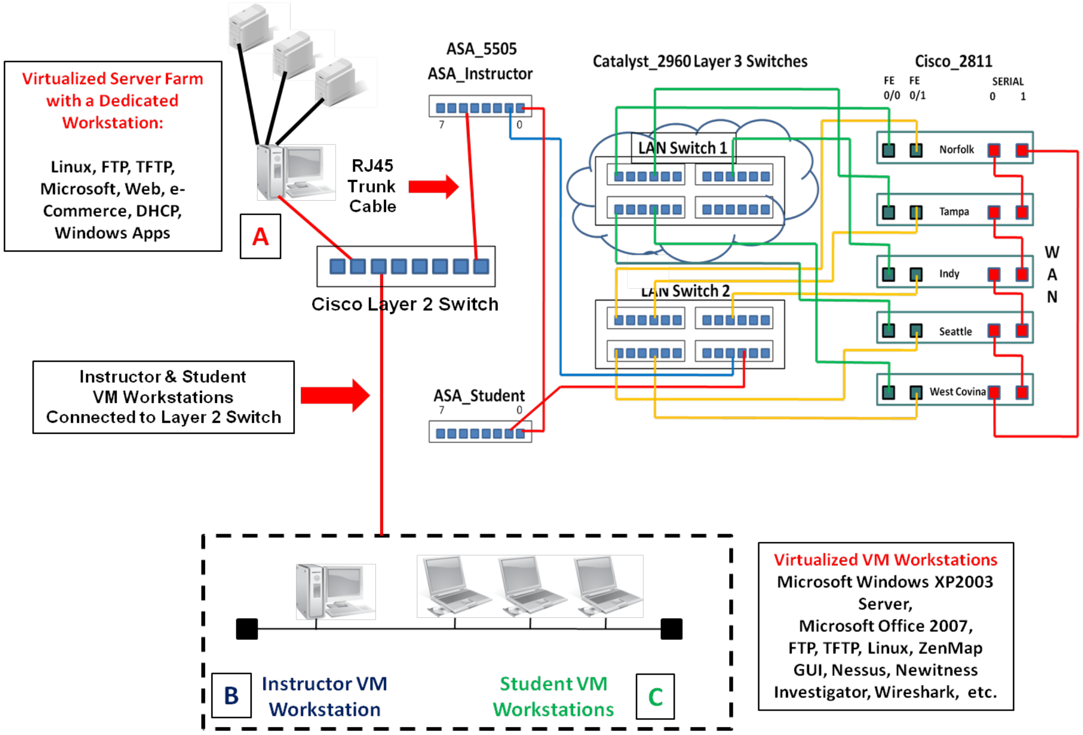

Virtualized Server Farm with a Dedicated Workstation:
Linux, FTP, TFTP, Microsoft, Web, e-Commerce, DHCP, Windows Apps
A
RJ45 Trunk Cable
ASA_5505
ASA_Instructor
7
0
Catalyst_2960 Layer 3 Switches
LAN Switch 1
LAN Switch 2
Cisco_2811
FE 0/0
FE 0/1
SERIAL 0 1
Norfolk
Tampa
Indy
Seattle
West Covina
W A N
Cisco Layer 2 Switch
Instructor & Student VM Workstations Connected to Layer 2 Switch
ASA_Student
7
0
B
Instructor VM Workstation
Student VM Workstations
C
Virtualized VM Workstations
Microsoft Windows XP2003 Server,
Microsoft Office 2007,
FTP, TFTP, Linux, ZenMap GUI, Nessus, Newitness Investigator, Wireshark, etc.

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)

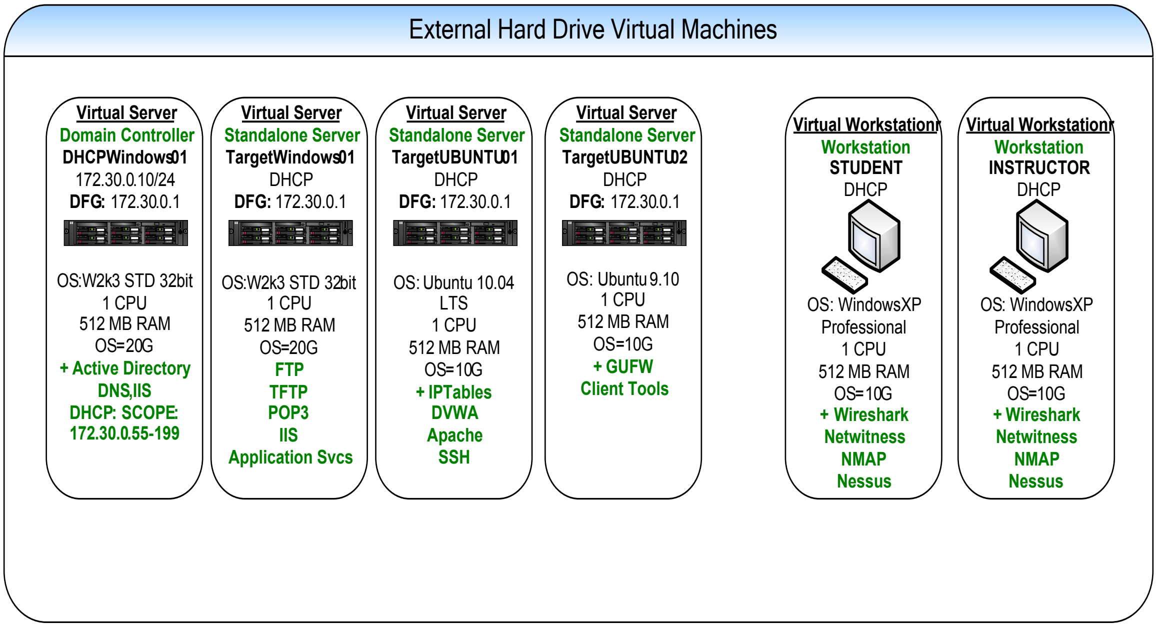


Figure 3 – VM Server Farm and VM Workstations

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)

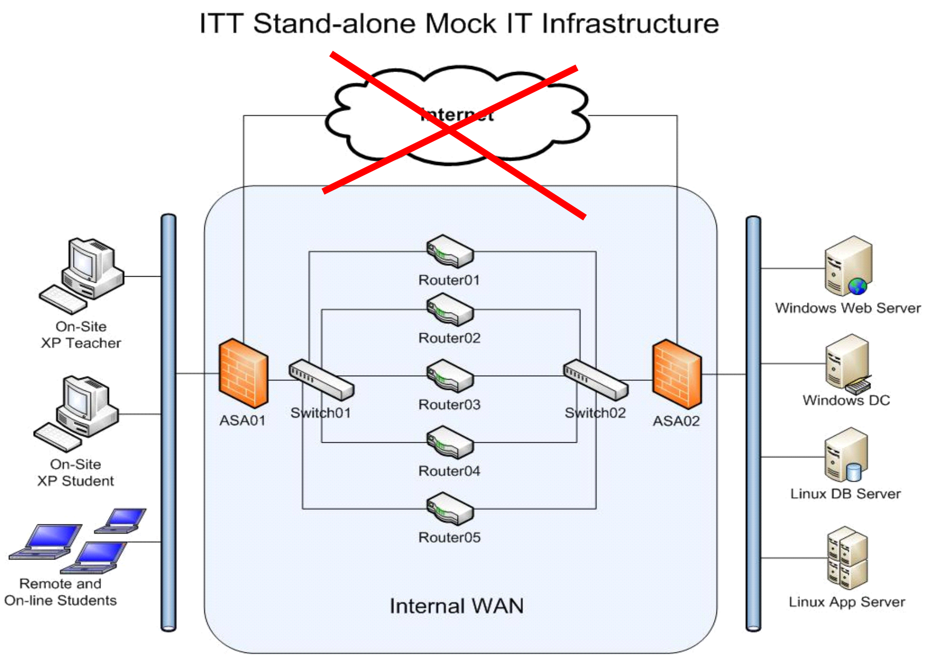


Figure 4 - Mock IT Infrastructure High-level Diagram

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 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

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	▪ 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	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	Implement Hashing & Encryption for Secure Communications	1
			Lab	2.3	Practical Encryption and Hashing	2
3	Information Gathering and Footprinting	*Hacker Techniques, Tools, and Incident Handling*: ▪ Chapter 5	Assignment	3.1	Information Gathering Plan	1
				3.2	Perform Data Gathering and Foot-printing on a Targeted Website	1
			Lab	3.3	Data Gathering and Footprinting	2
4	Port Scanning, Vulnerability	*Hacker Techniques, Tools, and Incident Handling*:	Assignment	4.1	Top Ports and Rising Ports Review	1

Unit #	Unit Title	Assigned Readings	Graded Activities			
			Grading Category	#	Activity Title	Grade Allocation (% of all graded work)
	Exploits	▪ Chapter 6 ▪ Chapter 7	Lab	4.2	Compromise and Exploit a Vulnerable Microsoft 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	Perform a Website & Database Attack by Exploiting Identified Vulnerabilities	1
			Lab	5.3	Web and Database Attacks	2
			Project	5.4	Project Part 2: Vulnerabilities in Information Technology (IT) Security	3
6	Identifying and Combating Trojans, Back Doors, 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
			Mid-Term 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 & 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 & Microsoft Workstations	2
10	Defensive Technologies and Techniques	*Hacker Techniques, Tools, and Incident Handling*:	Assignment	10.1	Controls	1
			Lab	10.2	Design & Implement	2

Unit #	Unit Title	Assigned Readings	Graded Activities			
			Grading Category	#	Activity Title	Grade Allocation (% of all graded work)
		▪ Chapter 4 ▪ Chapter 15			SNORT as an Intrusion Detection System (IDS)	
			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

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%
Mid-Term Exam	15%
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)