IS418T
Securing Linux Platforms and Applications
[Onsite]

Course Description:

This course is an introduction to the securing of Linux platforms and applications. Areas of study include identifying and examining methods of securing Linux platforms and applications and implementing those methods.

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

Prerequisites: IT302T Linux System Administration or equivalent

Credit hours: 4

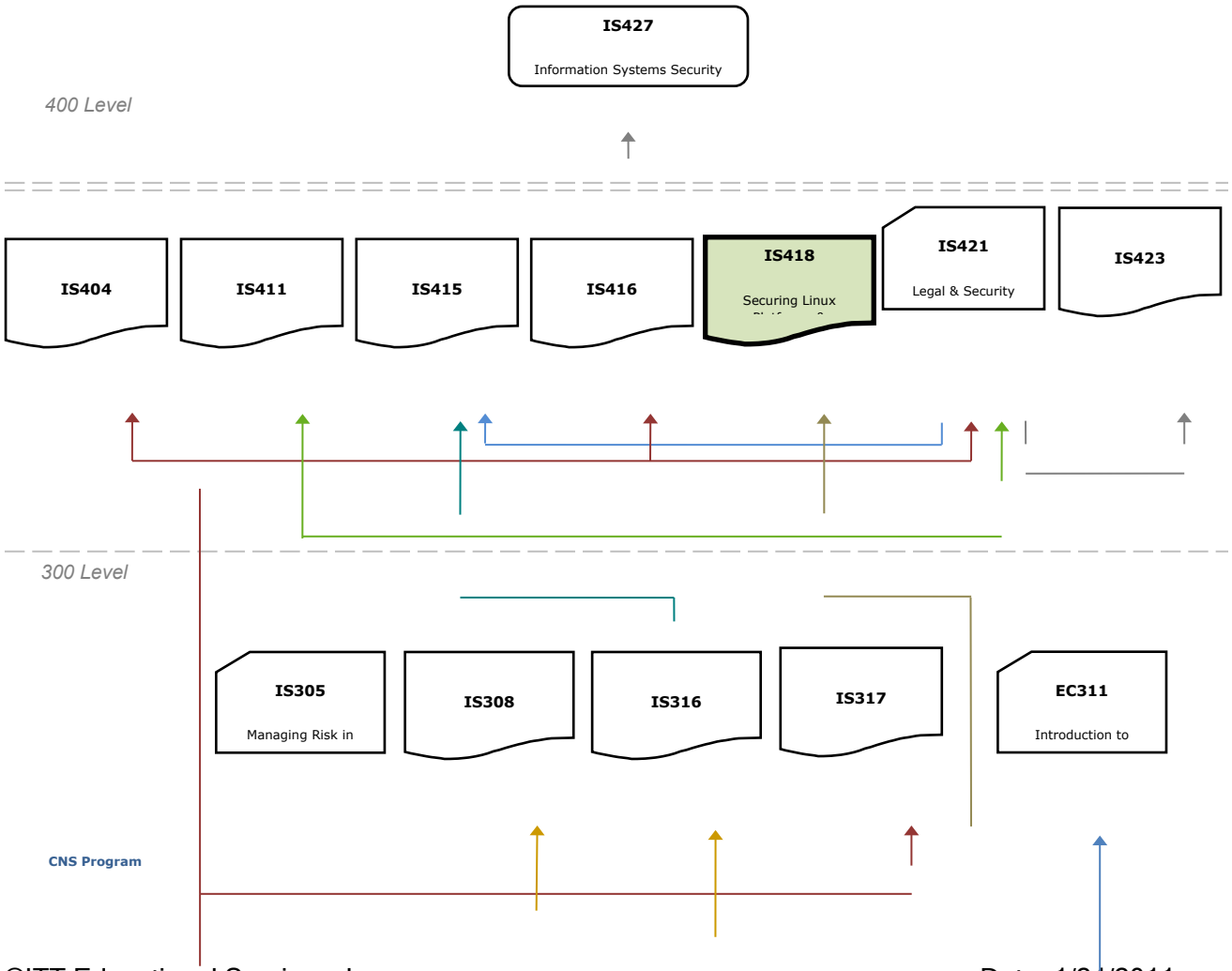
Contact hours: 60 (36 Theory Hours, 24 Lab Hours)

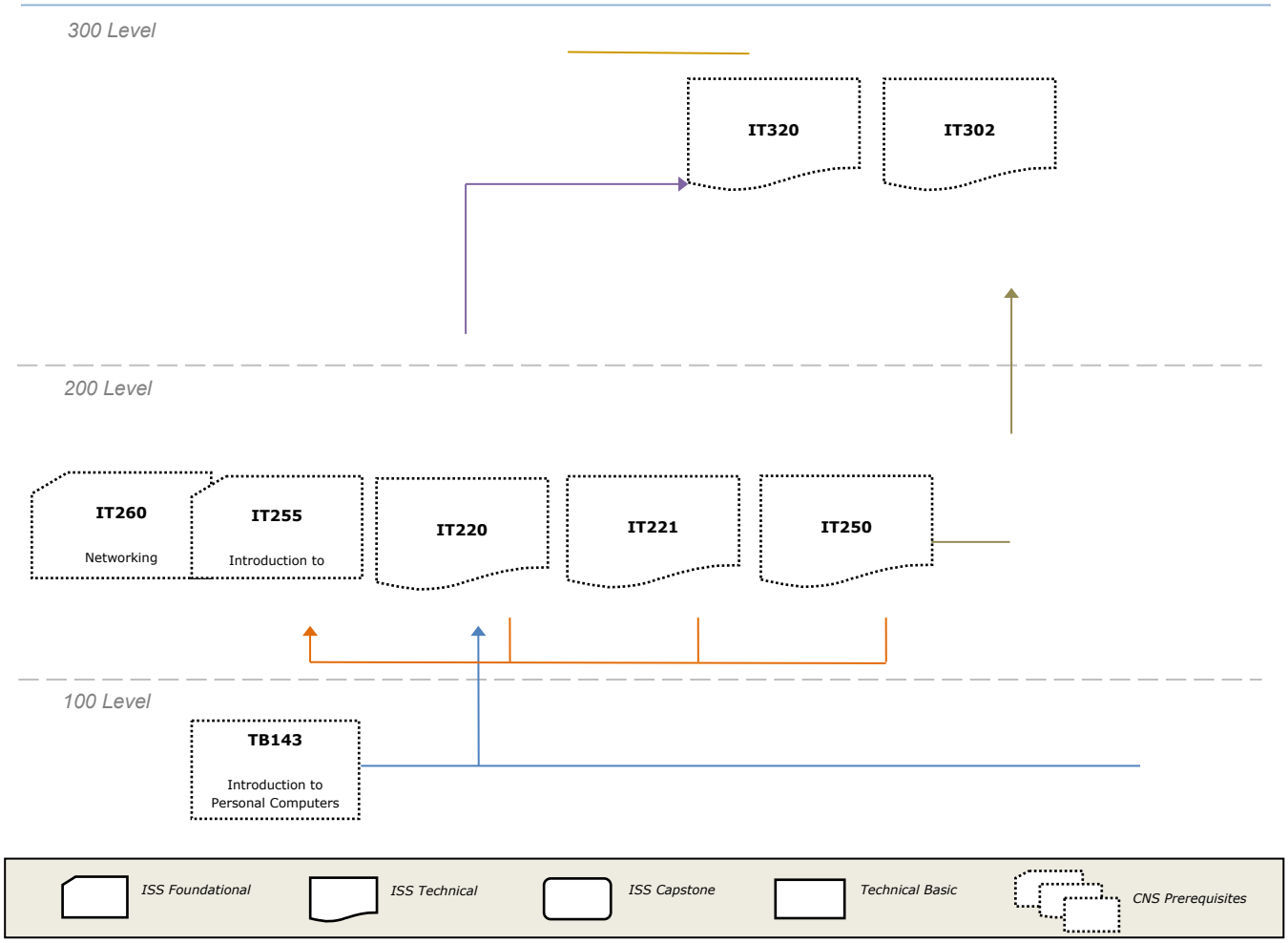
Where Does This Course Belong?

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

Course Description

This course is an introduction to the securing of Linux platforms and applications. Areas of study include identifying and examining methods of securing Linux platforms and applications and implementing those methods.

Major Instructional Areas

1. Threats to Linux operating systems and other open source applications and mitigation of risks
2. Core components to secure Linux platform
3. User account management and software management plan
4. Network applications security
5. Linux kernel and techniques
6. Security breach response and recovery

Course Objectives

1. Identify threats to the Linux operating system and other open source applications.
2. Configure the basic settings to secure a Linux platform.
3. Explain user account management and the principle of least privilege to protect and secure the system and its data.
4. Examine the flexibility of various options with file permissions and filesystem settings and how granular control isolates data access.
5. Describe security solutions to mitigate vulnerabilities in Linux services and the appropriate steps to mitigate the risks.

6. Assess how firewall, Transmission Control Protocol (TCP) Wrappers, and Security Enhanced Linux (SELinux) complement one another to secure network applications.
7. Assess the architecture of the Linux kernel and techniques used to enact a more secure kernel.
8. Evaluate the importance of maintaining a software management plan.
9. Establish a system baseline with monitoring and logging to detect anomalies.
10. Analyze the best practices to respond and recover from a security breach (incident).

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)
Jang, Michael. *Security Strategies in Linux Platforms and Applications*. 1st ed. Sudbury, MA: Jones & Bartlett, 2011.	▪		
Printed IS418 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	▪	▪	▪

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

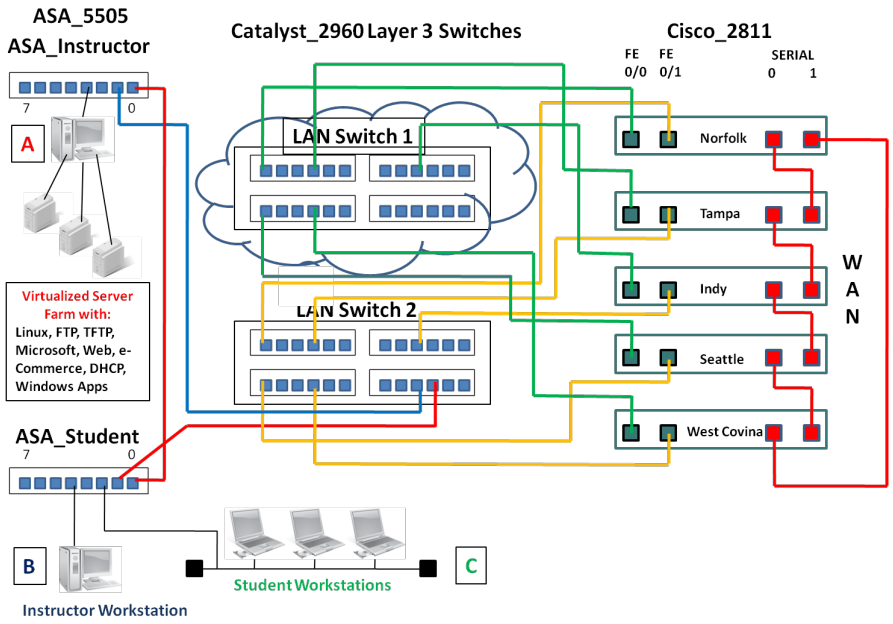


Figure 1 – ISS Cisco Core Backbone Network

(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:

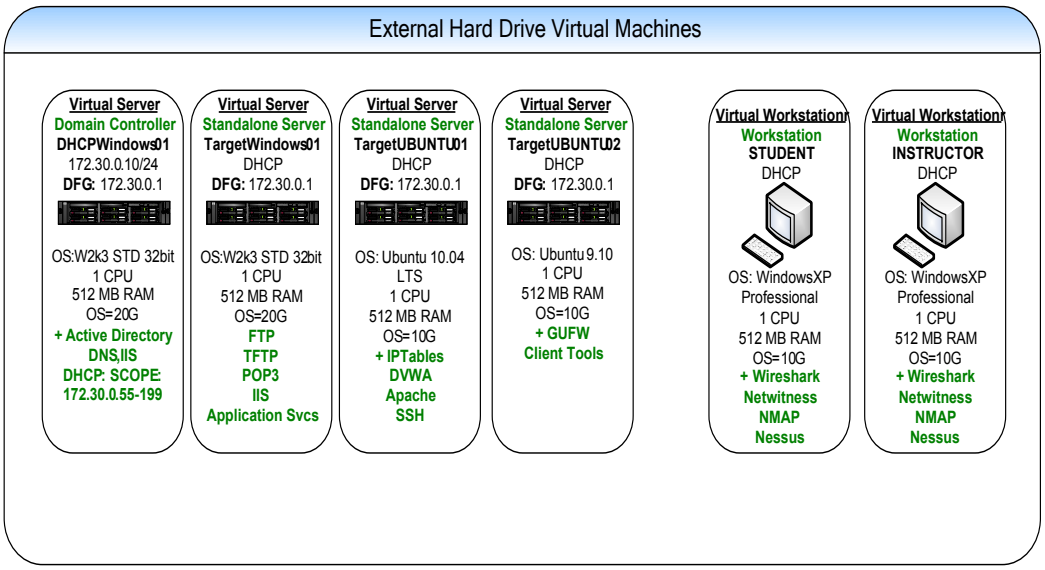


Figure 2 – ISS Core VM Server Farm & VM Workstations

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 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:

Books

Books24X7

Ebrary

NetLibrary

Periodicals

EbscoHost

ACM Digital Library

Bill Childers

“Virtualization Shootout: VMware server vs. VirtualBox vs. KVM”, *Linux Journal*, Nov2009, Vol. 2009 Issue 187

Brian Hatch, et al

Hacking Exposed Linux, 3rd ed. (Chapters 2, 13 and Appendix B)

Christian B. Lahti, et al

Sarbanes-Oxley IT Compliance Using COBIT and Open Source Tools (Chapters 3 and 4)

Craig Hunt

Linux Network Servers: Craig Hunt Linux Library (Chapters 3, 6 and 9)

Ellick M. Chan, et al

“BootJacker: compromising computers using forced restarts”, *Proceedings of the 15th ACM conference on Computer and communications security*, 2008, (Pages 555-564)

James Stanger, et al

Hack Proofing Linux: A Guide to Open Source Security (Chapter 2)

Jeramiah Bowling

“The tao of Linux security: five lessons for a secure deployment”, *Linux Journal*, Jan2008, Vol. 2008 Issue 165

Kyle Rankin

"Hack and /: Linux troubleshooting, Part I: high load", *Linux Journal*, Mar2010, Vol. 2010 Issue 191

Kyle Rankin

"Introduction to forensics", *Linux Journal*, Jan2008, Vol. 2008 Issue 165

Marco Fioretti

"How to setup and use tripwire", *Linux Journal*, Jun2006, Vol. 2006 Issue 146, (Page 6)

Mick Bauer

"Paranoid penguin: brutally practical Linux desktop security", *Linux Journal*, Oct2009, Vol. 2009 Issue 186

Mick Bauer

"Paranoid penguin: secured remote desktop/application sessions", *Linux Journal*, Sep2008, Vol. 2008 Issue 173

Moshe Bar

Linux Internals (Chapter 2)

Richard Petersen

Linux: The Complete Reference, 6th ed. (Chapters 10, 20 and 32)

Robb H. Tracy

Linux+ Certification Study Guide (Chapters 6 and 7)

Robert Love

Linux Kernel Development, 2nd ed. (Chapter 2)

Roderick Smith

Degunking Linux (Chapter 6)

Scott Andrew Maxwell

Linux Core Kernel Commentary, 2nd ed. (Chapters 3 and 11)

Shadab Siddiqui

Linux Security (Chapters 2, 3, 5, 12 and 13)

William C. Benton

“Kernel korner: Loadable kernel module exploits”, *Linux Journal*, Sep2001, Vol. 2001 Issue 89, (Page 7)

Professional Associations

- The Linux Foundation

  This Web site provides Linux-related unified resources and services that enable open source platforms to compete with closed platforms.
  http://www.linuxfoundation.org/ (accessed June 1, 2010).

- Linux Professional Institute
  This Web site provides advocation and assistance in professional use of Linux, open source, and free software.

  http://www.lpi.org/ (accessed June 1, 2010).

Other References

- Institute for Security and Open Methodologies (ISECOM)

  This Web site provides certification, training support, project support services, and practical methods on security and integrity.

  http://www.isecom.org/osstmm/ (accessed June 1, 2010).

- Filesystem Hierarchy Standard

  This Web site serves as a reference for UNIX distribution developers, package developers, and system implementers.

  http://www.pathname.com/fhs/ (accessed June 1, 2010).

- National Security Agency/Central Security Service (NSA/CSS)

  This Web site provides guidance on information assurance, security solutions, and insights on risks, vulnerabilities, mitigations, and threats. It also provides information on cryptologic support.

  http://www.nsa.gov/ (accessed June 1, 2010).

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

Keywords:

Accounts and Account Policies

Backup Plan

Custom Kernel

Data Access

Discretionary Access Control (DAC)

Encryption

File Permissions

File System Hierarchy (FHS)

File System Settings

Granular Control

Iptables

Linux Kernel

Linux Operating Systems

Linux Platforms

Linux Security

Linux Techniques

Loadable Kernel Modules (LKM)

Mandatory Access Control (MAC)

Network Applications

Packet Forwarding

Principle of Least Privilege

Public-Facing Web Server

SELinux

Security Breach

Software Management Plan

User Account Management

Web and Database Server

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)

Unit #	Unit Title	Assigned Readings	Graded Activities			
						Grade Allocation
			Grading Category	#	Activity Title	(% of all graded work)
1	Introduction to Linux Security	*Security Strategies in Linux Platforms and Applications*: ▪ Chapter 1	Discussion	1.1	Securing a Linux System	2
			Lab	1.2	Install a Core Linux Operating System on a Server	2
2	Securing a Linux Platform—Core Components	*Security Strategies in Linux Platforms and Applications:* ▪ Chapter 2 ▪ Chapter 3	Discussion	2.1	Identifying Layers of Access Control in Linux	2
			Lab	2.2	Configure Basic Security Controls on a Fedora Linux Server	2
3	User Account Management	*Security Strategies in Linux Platforms and Applications:* ▪ Chapter 4	Quiz	3.1	Quiz 1	3
			Lab	3.2	Apply Hardened User Account Management & Security Controls	2
4	Securing the Linux Filesystem	*Security Strategies in Linux Platforms and Applications:* ▪ Chapter 5	Discussion	4.1	Compromising an Online System	2
			Lab	4.2	Apply Hardened Linux File System Security Controls	2
			Project	4.3	Project Part1: Executive Summary	8

Unit #	Unit Title	Assigned Readings	Graded Activities			
						Grade Allocation
			Grading Category	#	Activity Title	(% of all graded work)
5	Securing Common Linux Services	*Security Strategies in Linux Platforms and Applications:* ▪ Chapter 6 ▪ Chapter 8 ▪ Chapter 9	Quiz	5.1	Quiz 2	3
			Lab	5.2	Apply Hardened Security for Linux Services & Applications	2
6	Using Layered Security for Access Control	*Security Strategies in Linux Platforms and Applications:* ▪ Chapter 7	Discussion	6.1	Determining Firewall Rules	2
			Lab	6.2	Apply Hardened Security for Controlling Access	2
7	Securing the Linux Kernel	*Security Strategies in Linux Platforms and Applications:* ▪ Chapter 10	Quiz	7.1	Quiz 3	3
			Lab	7.2	Apply Hardened Security for the Linux Kernel	2
			Project	7.3	Project Part 2: Executive Summary	8
8	Software Management	*Security Strategies in Linux Platforms and Applications:* ▪ Chapter 11	Discussion	8.1	Using Community and Vendor Support for Managing Software	2

Unit #	Unit Title	Assigned Readings	Graded Activities			
						Grade Allocation
			Grading Category	#	Activity Title	(% of all graded work)
			Lab	8.2	Implement Best Practices for Secure Software Management	2
9	Linux System Logging and Monitoring	*Security Strategies in Linux Platforms and Applications:* ▪ Chapter 12 ▪ Chapter 13	Quiz	9.1	Quiz 4	3
			Lab	9.2	Implement Best Practices for Security Logging & Monitoring	2
10	Incident Response and Recovery	*Security Strategies in Linux Platforms and Applications:* ▪ Chapter 14	Discussion	10.1	Creating a Backup Plan	2
			Lab	10.2	Define Linux OS & Application Backup & Recovery Procedures	2
			Project	10.3	Project Part 3: Executive Summary	8
11	Course Review and Final Examination	N/A	Project	11.1	Project Part 4: Executive Summary of the Project	8
			Exam	11.2	Final Exam	24

Evaluation and Grading

Evaluation Criteria

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

Category	Weight
Lab	20
Project	32
Discussion	12
Quiz	12
Exam	24
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)

