Credit hours: 4.5
Contact/Instructional hours: 60 (30 Theory Hours, 30 Lab Hours)
Prerequisite(s) and/or Corequisite(s):
Prerequisites: NT1430 Linux Networking or equivalent
Course Description:
This course examines threats, vulnerabilities and other security issues in Linux operating systems and applications in the Linux environment. Students will practice using different methods, tools and techniques to secure Linux operating systems and applications.
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. 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.
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).
Learning Materials and References

### Required Resources

<table>
<thead>
<tr>
<th>Textbook Package</th>
<th>New to this Course</th>
<th>Carried over from Previous Course(s)</th>
<th>Required for Subsequent Course(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Printed IS3440 Student Lab Manual</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>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)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>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)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>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)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(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
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:

**External Hard Drive Virtual Machines**

<table>
<thead>
<tr>
<th>Virtual Server</th>
<th>Domain Controller</th>
<th>DHCP/Windowd1</th>
<th>TargetWindowd1</th>
<th>TargetUbuntu1</th>
<th>TargetUbuntu2</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS:</td>
<td>W2K3 STD 32bit</td>
<td>1 CPU</td>
<td>512 MB RAM</td>
<td>OS=9G</td>
<td>OS=10G</td>
</tr>
<tr>
<td></td>
<td>+ Active Directory</td>
<td></td>
<td></td>
<td>POP3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DNS/IS</td>
<td></td>
<td></td>
<td>Application Svs</td>
<td>ISP</td>
</tr>
<tr>
<td></td>
<td>DHCP: SCOPE</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>172.30.0.55-199</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Virtual Server**

- **Standalone Server**
  - **TargetWindowd1**
    - DHCP: 172.30.0.1
  - **TargetUbuntu1**
    - DHCP: 172.30.0.1
  - **TargetUbuntu2**
    - DHCP: 172.30.0.1

**Virtual Workstation**

- **STUDENT**
  - **DHCP**
  - **OS:** Ubuntu 10.04 LTS
  - 1 CPU
  - 512 MB RAM
  - OS=10G
  - + GUI

- **INSTRUCTOR**
  - **DHCP**
  - **OS:** WindowsXP Professional
  - 1 CPU
  - 512 MB RAM
  - OS=10G
  - + GUI

**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
   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
   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  

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

James Stanger, et al
Hack Proofing Linux: A Guide to Open Source Security (Chapter 2)

Jeramiah Bowling

Kyle Rankin

Kyle Rankin

Marco Fioretti

Mick Bauer

Mick Bauer

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

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 advocacy 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.

- 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:

<table>
<thead>
<tr>
<th>DO</th>
<th>DON’T</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Do take a proactive learning approach</td>
<td>• Don’t assume there is only one correct answer to a question</td>
</tr>
<tr>
<td>• Do share your thoughts on critical issues and potential problem solutions</td>
<td>• Don’t be afraid to share your perspective on the issues analyzed in the course</td>
</tr>
<tr>
<td>• Do plan your course work in advance</td>
<td>• Don’t be negative towards the points of view that are different from yours</td>
</tr>
<tr>
<td>• Do explore a variety of learning resources in addition to the textbook</td>
<td>• Don’t underestimate the impact of collaboration on your learning</td>
</tr>
<tr>
<td>• Do offer relevant examples from your experience</td>
<td>• Don’t limit your course experience to reading the textbook</td>
</tr>
<tr>
<td>• Do make an effort to understand different points of view</td>
<td></td>
</tr>
</tbody>
</table>
### DO

- Do connect concepts explored in this course to real-life professional situations and your own experiences

### DON'T

- Don’t postpone your work on the course deliverables – work on small assignment components every day

## Course Outline

<table>
<thead>
<tr>
<th>Unit #</th>
<th>Unit Title</th>
<th>Assigned Readings</th>
<th>Graded Activities</th>
<th>Grade Allocation (% of all graded work)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Grading Category</td>
<td>#</td>
</tr>
<tr>
<td>1</td>
<td>Introduction to Linux Security</td>
<td><em>Security Strategies in Linux Platforms and Applications:</em></td>
<td>Discussion</td>
<td>1.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Chapter 1</td>
<td>Lab</td>
<td>1.2</td>
</tr>
<tr>
<td>2</td>
<td>Securing a Linux Platform—Core Components</td>
<td><em>Security Strategies in Linux Platforms and Applications:</em></td>
<td>Discussion</td>
<td>2.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Chapter 2</td>
<td>Lab</td>
<td>2.2</td>
</tr>
<tr>
<td>3</td>
<td>User Account Management</td>
<td><em>Security Strategies in Linux Platforms and Applications:</em></td>
<td>Quiz</td>
<td>3.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Chapter 4</td>
<td>Lab</td>
<td>3.2</td>
</tr>
<tr>
<td>4</td>
<td>Securing the Linux Filesystem</td>
<td><em>Security Strategies in Linux Platforms and Applications:</em></td>
<td>Discussion</td>
<td>4.1</td>
</tr>
<tr>
<td>Unit #</td>
<td>Unit Title</td>
<td>Assigned Readings</td>
<td>Graded Activities</td>
<td></td>
</tr>
<tr>
<td>-------</td>
<td>------------------------------------------</td>
<td>-----------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Securing Common Linux Services</td>
<td>Security Strategies in Linux Platforms and Applications:</td>
<td>Lab 4.2 Apply Hardened Linux File System Security Controls 2</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Chapter 6</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Chapter 8</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Chapter 9</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Project 4.3 Project Part1: Executive Summary† 8</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Chapter 7</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Lab 5.2 Apply Hardened Security for Linux Services &amp; Applications 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Securing the Linux Kernel</td>
<td>Security Strategies in Linux Platforms and Applications:</td>
<td>Quiz 7.1 Quiz 3 3</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Chapter 10</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Lab 7.2 Apply Hardened Security for the Linux Kernel 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Project 7.3 Project Part 2: Executive Summary† 8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unit #</td>
<td>Unit Title</td>
<td>Assigned Readings</td>
<td>Graded Activities</td>
<td></td>
</tr>
<tr>
<td>--------</td>
<td>------------------------------------</td>
<td>-----------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Unit Title</strong>: Software Management</td>
<td><strong>Grading Category</strong></td>
<td><strong>#</strong></td>
</tr>
<tr>
<td>8</td>
<td>Software Management</td>
<td><strong>Assigned Readings</strong>; <em>Security Strategies in Linux Platforms and Applications</em>:</td>
<td>Discussion 8.1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Chapter 11</td>
<td>Lab 8.2</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Linux System Logging and Monitoring</td>
<td><strong>Assigned Readings</strong>; <em>Security Strategies in Linux Platforms and Applications</em>:</td>
<td>Quiz 9.1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Chapter 12</td>
<td>Lab 9.2</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Incident Response and Recovery</td>
<td><strong>Assigned Readings</strong>; <em>Security Strategies in Linux Platforms and Applications</em>:</td>
<td>Discussion 10.1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Chapter 14</td>
<td>Lab 10.2</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Project 10.3</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Course Review and Final Examination</td>
<td>N/A</td>
<td>Project 11.1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Exam 11.2</td>
<td></td>
</tr>
</tbody>
</table>
Evaluation and Grading

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

<table>
<thead>
<tr>
<th>Category</th>
<th>Weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lab</td>
<td>20</td>
</tr>
<tr>
<td>Project</td>
<td>32</td>
</tr>
<tr>
<td>Discussion</td>
<td>12</td>
</tr>
<tr>
<td>Quiz</td>
<td>12</td>
</tr>
<tr>
<td>Exam</td>
<td>24</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>

Grade Conversion
The final grades will be calculated from the percentages earned in the course, as follows:

<table>
<thead>
<tr>
<th>Grade</th>
<th>Percentage</th>
<th>Credit</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>90–100%</td>
<td>4.0</td>
</tr>
<tr>
<td>B+</td>
<td>85–89%</td>
<td>3.5</td>
</tr>
<tr>
<td>B</td>
<td>80–84%</td>
<td>3.0</td>
</tr>
<tr>
<td>C+</td>
<td>75–79%</td>
<td>2.5</td>
</tr>
<tr>
<td>C</td>
<td>70–74%</td>
<td>2.0</td>
</tr>
<tr>
<td>D+</td>
<td>65–69%</td>
<td>1.5</td>
</tr>
<tr>
<td>D</td>
<td>60–64%</td>
<td>1.0</td>
</tr>
<tr>
<td>F</td>
<td>&lt;60%</td>
<td>0.0</td>
</tr>
</tbody>
</table>

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)