Firewalls and Network Security
(ITSY 2301)

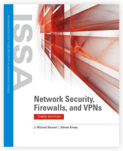
Credit: 3 semester credit hours (2 hours lecture, 4 hours lab)

Prerequisite/Co-requisite: None

Course Description

This course covers elements of firewall design, types of security threats and responses to security attacks, the use of Best Practices to design, implement, and monitor a network security plan, and the examination of security incident postmortem reporting and ongoing network security activities.

Required Textbook and Materials



1. ***Network Security, Firewalls, and VPNs, Third Edition,*** J. Michael Stewart; Denise Kinsey, PhD, CISSP, PMP; Jones & Bartlett, 2022. (www.jblearning.com.)
   a. The link to the bundle for the Third Edition of the eBook and the corresponding Cloud Labs is https://www.jblearning.com/catalog/productdetails/9781284184655. You may also use the keyword "Firewall" and select the Third Edition, then the bundle that includes the *eBook + Cloud Labs*. If you prefer a print book, there is a Paperback + Cloud Labs bundle at a higher cost.
   b. Check the Overview section for a **15% discount** once you have chosen your bundle. *This 15% discount only applies to the eBook/Cloud Labs combination bundle*.
   c. Create a log-in account at Jones & Bartlett if you did not create one during the purchase process. (*You may need to reset your password if you are unable to log back in*.)
   d. Once you have paid for the bundle and logged into Jones & Bartlett, go to My Account, then to Products. Click Lab Access for Network Security, Firewalls, and VPNs, Third Edition. Click Enter Course ID. You will need to get the Course ID from your instructor. This connects your Labs to your Blackboard.
   e. Go to this course’s Blackboard links to access the eBook and/or the Cloud Labs.
2. Computer Networking and Troubleshooting Technology and Cybersecurity students are required to have one 64 GB or larger capacity USB Flash Drive to be used for the duration of the time to complete their respective degree.

Course Objectives

Upon completion of this course, the student will be able to:

1. Demonstrate system security skills through firewall implementation and testing.
2. Use system tools, practices, and relevant technologies to implement a security plan.

3. Evaluate practices, tools, and technologies to identify security breaches, sources of attacks, and protect mission critical systems.
4. Establish an appropriate level of security based on an analysis of security logs.
5. Use relevant tools to secure a network, respond to and follow up on various types of attacks.

Course Outline

1. Fundamentals of Network Security
    a. What is network security?
    b. What are you trying to protect?
    c. Goals of Network Security
    d. How can you measure the success of network security?
    e. Why are written network security policies important?
    f. Who is responsible for network security?
    g. Enhancing the Security of Wired versus Wireless LAN Infrastructures
    h. Internal and External Network Issues
    i. Common Network Security Components used to Mitigate Threats
    j. TCP/IP Basics
2. Network Security Threats
    a. Hackers and their Motivation
    b. Favorite Targets of Hackers
    c. Threats from Internal Personnel and External Entities
    d. The Hacking Process
    e. Common IT Infrastructure Threats
    f. Malicious Code (Malware)
    g. Fast Growth and Overuse
    h. Wireless versus Wired
    i. Hijack and Replay Attacks
    j. Insertion Attacks
    k. Fragmentation Attacks
    l. Buffer Overflows
    m. Session Hijacking, Spoofing, and Man-in-the-Middle Attacks
    n. Covert Channels
    o. Network and Resource Availability Threats
    p. Hacker Tools
    q. Social Engineering
3. Common Network Topologies and Infrastructures
    a. What is a network topology?
    b. Types of Network Devices
    c. What differentiates logical and physical topologies?

d. Differences between Internet Protocol Version 4 (IPv4) and Internet Protocol Version 6 (IPv6)
e. Examples of Network Infrastructures and Related Security Concerns

4. Network Design Considerations
   a. Network Design and Defense in Depth
   b. Protocols
   c. Common Types of Addressing
   d. Controlling Communication Pathways
   e. Intrusion Detection Systems and Intrusion Prevention Systems
   f. Hardening Systems
   g. Equipment Selection
   h. Authentication, Authorization, and Accounting
   i. Communication Encryption
   j. Hosts: Local-Only or Remote and Mobile
   k. Redundancy
   l. Endpoint Security
   m. Risk Assessment and Management
   n. What are zones of risk?
5. Firewall Fundamentals
   a. What is a firewall?
   b. Why do you need a firewall?
   c. How Firewalls Work and What Firewalls Do
   d. Types of Firewalls
   e. Individual and SOHO Firewall Options
   f. Uses for Host Software Firewalls
   g. Uses for Commercial Software Network Firewalls
   h. Uses for Hardware/Appliance Firewalls
   i. Next-Generation Firewalls
   j. What are virtual firewalls?
   k. Dual-Homed and Triple-Homed Firewalls
   l. Ingress and Egress Filtering
   m. Types of Filtering
   n. Selecting the Right Firewall for your Needs
   o. The Difference between Buying and Building a Firewall
6. Firewall Implementation
   a. Examining your Network and its Security Needs
   b. Proper Firewall Implementation Procedure
   c. Constructing, Configuring, and Managing a Firewall
   d. pfSense
   e. pfSense Requirements

   f. Planning a Firewall Implementation with pfSense
   g. Installing the pfSense Firewall
   h. Configuring a Firewall with pfSense
   i. Elements of Firewall Deployment
   j. Testing and Troubleshooting
7. Firewall Deployment Considerations
   a. Common Security Strategies for Firewall Deployments
   b. Authentication, Authorization, and Accounting
   c. Placement of Network Hardware Firewalls
   d. Benefit and Purpose of Reverse Proxy
   e. Use and Benefit of Port Forwarding
   f. Considerations for Selecting a Bastion Host OS
   g. Monitoring and Logging
   h. Understanding and Interpreting Firewall Logs and Alerts
   i. Intrusion Detection Systems and Intrusion Prevention Systems
   j. Security Event and Information Management
   k. Evaluating Needs and Solutions in Designing Security
   l. What happens when security gets in the way of doing business?
8. Configuring Firewalls
   a. Firewall Rules
   b. Composing Firewall Rules
   c. Ordering Firewall Rules
   d. What should you allow and what should you block?
   e. Essential Elements of a Firewall Policy
   f. Limitations of Firewalls
   g. Improving Performance
   h. The Downside of Encryption with Firewalls
   i. Firewall Enhancements
   j. Management Interfaces
9. VPN Fundamentals
   a. What is a virtual private network?
   b. What are the benefits of deploying a VPN?
   c. What are the limitations of a VPN?
   d. What are effective VPN policies?
   e. VPN Deployment Models and Architecture
   f. Tunnel versus Transport Mode
   g. The Relationship between Encryption and VPNs
   h. What is VPN authentication?
   i. What is VPN authorization?

10. VPN Management
    a. VPN Management Best Practices
    b. Developing a VPN Policy
    c. Developing a VPN Deployment Plan
    d. VPN Threats and Exploits
    e. Commercial versus Open-source VPNs
    f. Differences between Personal and Enterprise VPNs
    g. Balancing Anonymity and Privacy
    h. Protecting VPN Security to Support Availability
    i. The Importance of User Training
    j. VPN Troubleshooting
11. VPN Technologies
    a. Differences between Software and Hardware Solutions
    b. Differences between Layer 2 and Layer 4 VPNs
    c. Internet Protocol Security (IPSec)
    d. Layer 2 Tunneling Protocol (L2TP)
    e. Secure Sockets Layer (SSL)/Transport Layer Security (TLS)
    f. Secure Shell (SSH) Protocol
    g. Establishing Performance and Stability for VPNs
    h. Using VPNs with Network Address Translation (NAT)
    i. Types of Virtualization
12. VPN Implementation
    a. Operating System-Based VPNs
    b. VPN Appliances
    c. Remote Desktop Protocol
    d. Using Remote Control Tools
    e. Using Remote Access
    f. Remote Desktop Services
    g. Microsoft DirectAccess
    h. DMZ, Extranet, and Intranet VPN Solutions
    i. Internet Café VPNs
    j. Online Remote VPN Options
    k. The Tor Application
    l. Planning a VPN Implementation
    m. VPN Implementation Best Practices

Grade Scale

90 – 100	A
80 – 89	B
70 – 79	C
60 – 69	D
0 – 59	F

Course Evaluation

Final grades will be calculated according to the following criteria:

Labs	30%
Study Guides	10%
Tests	30%
Final Exam	30%

Course Requirements

1. Demonstrate proficiency through hands-on labs as assigned.
2. Completion of Study Guides as assigned.

Course Policies

1. No food, drinks, or use of tobacco products in class.
2. Electronic devices not being used for the class, such as phones and headphones, must be turned off while in class. Any device usage during class may result in a deduction of points on an assignment or test.
3. Do not bring children to class.
4. Certification: If s student passes the certification test that is associated with this class you will receive an "A" on the final exam and credit for 25% of your labs. If you have missed a previous test you must still take the final exam to substitute for that grade.
5. Attendance Policy: Three absences are allowed. If a student is tardy to class or departs early three (3) times, it will be equal to one (1) absence. Each absence beyond three absences will result in a 2-point deduction from your final grade.
6. If you wish to drop a course, the student is responsible for initiating and completing the drop process. If you stop coming to class and fail to drop the course, you will earn an 'F' in the course.
7. Tools: Return all tools and/or software to their designated place.
8. A grade of 'C' or better must be earned in this course for credit toward degree requirement:
9. Additional course policies, as defined by the individual course instructor, will be outlined in the course addendum and provided by the instructor.

Disabilities Statement

The Americans with Disabilities Act of 1990 and Section 504 of the Rehabilitation Act of 1973 are federal anti-discrimination statutes that provide comprehensive civil rights for persons with disabilities. LIT provides reasonable accommodations as defined in the Rehabilitation Act of 1973, Section 504 and the Americans with Disabilities Act of 1990, to students with a diagnosed disability. The Special Populations Office is located in the Eagles' Nest Room 129 and helps foster a supportive and inclusive educational environment by maintaining partnerships with faculty and staff, as well as promoting awareness among all members of the Lamar Institute of Technology community. If you believe you have a disability requiring an accommodation, please contact the Special Populations Coordinator at (409) 839-2018. You may also visit the online resource at Special Populations - Lamar Institute of Technology (lit.edu).

Technical Requirements (for courses using Blackboard)

The latest technical requirements, including hardware, compatible browsers, operating systems, software, Java, etc. can be found online at:

https://help.blackboard.com/Learn/Student/Getting_Started/Browser_Support/Browser_Checker.

A functional broadband internet connection, such as DSL, cable, or Wi-Fi is necessary to maximize the use of the online technology and resources.

Starfish

LIT utilizes an early alert system called Starfish. Throughout the semester, you may receive emails from Starfish regarding your course grades, attendance, or academic performance. Faculty members record student attendance, raise flags and kudos to express concern or give praise, and you can make an appointment with faculty and staff, all through the Starfish home page. You can also log in to Blackboard or MyLIT and click on the Starfish link to view academic alerts and detailed information. It is the responsibility of the student to pay attention to these emails and information in Starfish and consider taking the recommended actions. Starfish is used to help you be a successful student at LIT.

For more information: https://www.lit.edu/student-success/starfish

Student Code of Conduct Statement

It is the responsibility of all registered Lamar Institute of Technology students to access, read, understand and abide by all published policies, regulations, and procedures listed in the LIT Catalog and Student Handbook. The LIT Catalog and Student Handbook may be accessed at www.lit.edu or obtained in print upon request at the Student Services Office. Please note that the online version of the LIT Catalog and Student Handbook supersedes all other versions of the same document.

Certification Requirement

CNTT and Cyber Security majors are required to earn certification in one of the following areas prior to graduation.

- A+ Certification
- Network+ Certification
- Security+ Certification
- Linux+ Certification
- Cisco Certified Network Associate (CCNA)