I. INTRODUCTION

A. Identify elements of firewall design, types of security threats and responses to security attacks. Use Best Practices to design, implement, and monitor a network security plan. Examine security incident postmortem reporting and ongoing network security activities.

B. This course serves as a required or elective course on various degree plans. Curriculum plans for degrees and certificates are listed in the current Central Texas College catalog.

C. The delivery method of this course may be traditional lecture/lab, blended lecture/lab, or online.

D. Prerequisites: ITNW 1358 Network+

II. LEARNING OUTCOMES

Upon successful completion of this course, Firewalls and Network Security, the student will be able to:

A. Demonstrate system security skills through firewall implementation and testing. (C5, C6, C8, C15, C19, C20).

B. Use system tools, practices, and relevant technologies to implement a security plan. (C1, C5, C6, C8, C19, C20, F1, F3, F8, F9, F12).

C. Evaluate practices, tools, and technologies to identify security breaches, sources of attacks, and protect mission critical systems. (C1, C5, C6, C8, C19, C20, F1, F3, F8, F9, F12).

D. Establish an appropriate level of security based on an analysis of security logs. (C5, C6, C8, C15, C19, C20).

E. Use relevant tools to secure a network, respond to and follow up on various types of attacks. (C1, C5, C6, C8, C19, C20, F1, F3, F8, F9, F12).

December 2018
III. INSTRUCTIONAL MATERIALS

A. The instructional materials identified for this course are viewable through www.cted.edu/books

B. Lecture Classes also require at least one USB storage device. (2-4 GB preferred).

IV. COURSE REQUIREMENTS

A. Attend both lecture and lab or in the case of online delivery, be actively engaged in Blackboard and maintain constant progress.

B. Be prepared to participate in discussion, team projects/assignments and take unannounced assessments relating to the lecture materials.

C. Complete all exams/assessments.

D. Submit all assignments on time.

V. ASSESSMENTS

A. Student content mastery will be evaluated in the following areas:
   • Assessments (midterm exam, quizzes, projects, discussion etc.)
   • Final Assessment (final exam and/or semester project, participation)

B. Scheduled and unscheduled assessments will be given at the discretion of the instructor.

C. Exams/assessments may be composed of both subjective and objective questions plus computer output.

D. A student must take all exams/assessments. Both online and on campus students who know in advance that they will be absent due to school sponsored trips, military duty or orders, or any other valid reason, must arrange to take an early exam/assessment. Unexpected absences due to illness or other extenuating circumstances will require the student to contact the instructor about make-up work in lieu of the missed exam/assessment.

E. Students with unexcused absences will be given a zero for each missed assignment.
VI. SEMESTER GRADE COMPUTATIONS

<table>
<thead>
<tr>
<th>Course Requirements</th>
<th>Points</th>
<th>Points</th>
<th>Grade</th>
<th>Quality Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assignments</td>
<td>300</td>
<td>900-1000</td>
<td>A-Superior</td>
<td>4</td>
</tr>
<tr>
<td>Assessments</td>
<td>300</td>
<td>800-899</td>
<td>B-Above Average</td>
<td>3</td>
</tr>
<tr>
<td>Final Assessment</td>
<td>400</td>
<td>700-799</td>
<td>C-Average</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>TOTAL</td>
<td>1000</td>
<td>600 - 699 D-Passing, but unsatisfactory</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>900-1000</td>
<td>A-Superior</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>800-899</td>
<td>B-Above Average</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>700-799</td>
<td>C-Average</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>600 - 699</td>
<td>D-Passing, but unsatisfactory</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 -599</td>
<td>F-Failure</td>
<td>0</td>
</tr>
</tbody>
</table>

VII. NOTES AND ADDITIONAL INSTRUCTIONS FROM THE INSTRUCTOR

A. Information on the following Academic Policies, as described in the CTC Course Catalog will be followed:
   1. Withdrawals
   2. Grading
   3. Class Attendance and Course Progress
   4. Scholastic Honesty

B. Cell Phones and Pagers: Students will silence cell phones and mobile devices while in the classroom or lab.

C. Americans with Disabilities Act (ADA): Disability Support Services provide services to students who have appropriate documentation of a disability. Students requiring accommodations for class are responsible for contacting the Office of Disability Support Services (DSS) located on the central campus. This service is available to all students, regardless of location. Review the website at www.ctcd.edu/disability-support for further information. Reasonable accommodations will be given in accordance with the federal and state laws through the DSS office.

D. Instructor Discretion: The instructor reserves the right of final decision in course requirements and may make changes to the course outline and/or assignments as needed.

E. Civility: Individuals are expected to be aware of what a constructive educational experience is and be respectful of those participating in a learning environment. Failure to do so can result in disciplinary action up to and including expulsion.
VIII. COURSE OUTLINE

A. Unit One: Fundamentals of Network Security and Firewalls

1. Unit Objectives: Upon successful completion of this unit the student will be able to:
   a. Describe the key concepts and terms associated with network security.
   b. Describe the importance of a written security policy and explain how the policies help mitigate risk exposure and threats to a network infrastructure.
   c. Define network security roles and responsibilities and who within an IT organization is accountable for these security implementations.
   d. Identify examples of network security concerns or threats that require enhanced security countermeasures to properly mitigate risk exposure and threats.
   e. Describe the security requirements needed for wired versus wireless LAN infrastructures to provide an enhanced level of security.
   f. Compare and contrast common network security components and devices and their use throughout the IT infrastructure.
   g. Define firewalls.
   h. Explain the need for firewalls.
   i. Describe types of firewalls, including network router/interface firewall, hardware appliance firewall, and host software firewall.
   j. Explain standard filtering methods, including static packet filtering, NAT services, application proxy filtering, circuit proxy filtering, dynamic packet filtering, stateful inspection filtering, and content filtering.
   k. Define the meaning of ingress and egress filtering.
   l. Compare and contrast software and hardware firewalls.
   m. Illustrate on a typical business network diagram possible placement for a firewall.
   n. Compare and contrast dual- and triple-homed firewalls.

2. Learning Activities:
   a. Read Chapters 1 and 2. (C5, C6, C8, C19, F1, F5, F11)
   b. Complete the assigned quiz, assignment, and lab. (C5, C6, C8, C19, F1, F5, F11)

3. Unit Outline: Follow the sequence of unit objections.

B. Unit Two: VPN Fundamentals and Network Security Threats

1. Unit Objectives: Upon successful completion of this unit the student will be able to:
   a. Define VPNs.
   b. Explain the business and personal uses of VPNs.
c. Describe the pros and cons of VPNs.
d. Illustrate deployment models or architectures of VPNs, including an edge router, a corporate firewall, a VPN appliance, a remote access server, a site-to-site VPN and supporting devices, and a host-to-host VPN and supporting devices.
e. Differentiate between a transport-mode VPN and a tunnel-mode VPN.
f. Describe the importance to VPNs of encryption, authentication, and authorization.
g. Describe the motivations of hackers and other malicious computer network intruders.
h. Compare and contrast threats from internal and external sources.
i. Describe how accidents, natural disasters, and ignorance affect network security.
j. Explain the risk posed by malicious code.
k. Express the effects of wired and wireless connectivity on network security.
l. Describe common network security exploits and attacks, including replay attacks, insertion attacks, fragmentation attacks, buffer overflow attacks, XSS attacks, man-in-the-middle attacks, hijacking attacks, spoofing attacks, covert channels, DoS, DDoS, botnet attacks, and social engineering attacks.
m. Demonstrate how hacker tools exploit vulnerable targets.

2. Learning Activities:
   a. Read Chapters 3 and 4. (C5, C6, C8, C19, F1, F5, F11)
   b. Complete the assigned quiz, assignment, and lab. (C5, C6, C8, C19, F1, F5, F11)

3. Unit Outline: Follow the sequence of the unit objectives.

C. Unit Three: Network Security Implementation and Management

1. Unit Objectives: Upon successful completion of this unit the student will be able to:
   a. Describe elements of network security design.
   b. Compare and contrast public and private addressing as well as static and dynamic addressing.
   c. State the importance of system hardening.
   d. Describe why authentication, authorization, accounting, and encryption are essential for network security.
   e. Identify the security concerns of local hosts as well as remote and mobile hosts.
   f. Define the elements of node security.
   g. List examples of network security "best practices".
   h. Describe the importance of physical security.
   i. Compose a procedure for incident response.
j. Define and explain key components of an effective network security installation.
k. Describe the methods of network security assessment.

2. **Learning Activities:**
   a. Read Chapters 5 and 6. (C5, C6, C8, C19, F1, F5, F11)
   b. Complete the assigned quiz, assignment, and lab. (C5, C6, C8, C19, F1, F5, F11)

3. **Unit Outline:** Follow the sequence of the unit objectives

D. **Unit Four:** Firewall Basics and Deployment Considerations

1. **Unit Objectives:** Upon successful completion of this unit the student will be able to:
   a. Construct examples of common firewall rules.
   b. Design a policy to guide effective firewall monitoring and logging.
   c. Discuss the limitations and weaknesses of firewalls.
   d. Describe methods to manage firewall performance.
   e. Define the concerns of encryption related to firewalls.
   f. Evaluate the benefits and drawbacks of firewall enhancements.
   g. Demonstrate how to access and use firewall management interfaces.
   h. Compose a firewall policy defining what to allow and what to block.
   i. Describe various firewall security strategies.
   j. Define the pros and cons of reverse proxy and port forwarding.
   k. Explain the important of a bastion host.
   l. Assess the business impact of security over availability and performance.

2. **Learning Activities:**
   a. Read Chapter 7 and 8. (C5, C6, C8, C19, F1, F5, F11)
   b. Complete the assigned quiz, assignment, and lab. (C5, C6, C8, C19, F1, F5, F11)

3. **Unit Outline:** Follow the sequence of the unit objectives

E. **Unit Five:** Firewall Management and Using Common Firewalls

1. **Unit Objectives:** Upon successful completion of this unit the student will be able to:
   a. Describe firewall management "best practices".
   b. Select the best firewall for a given network scenario.
   c. Demonstrate the use of tools for managing and monitoring a firewall.
   d. Troubleshoot, correct, and document common firewall problems.
   e. Write a firewall installation plan.
f. Configure and document the Windows Firewall on Windows.
g. Set up a broadband connection device firewall.

2. Learning Activities:
a. Read Chapter 9 and 10. (C5, C6, C8, C19, F1, F5, F11)
b. Complete the assigned quiz, assignment, and lab. (C5, C6, C8, C19, F1, F5, F11)

3. Unit Outline: Follow the sequence of the unit objectives

F. Unit Six: VPN Management and technologies

1. Unit Objectives: Upon successful completion of this unit the student will be able to:
a. Describe VPN "best practices".
b. Write a VPN policy.
c. Describe the issues involved with deployment, placement, and implementation of a VPN.
d. Appraise the threats and attacks against VPNs.
e. Contrast the needs and features of personal and enterprise or network VPNs.
f. Compare anonymity and privacy.
g. Compose an introductory VPN training program for users.
h. Formulate a procedure for troubleshooting VPNs.
i. Contrast hardware and software VPN solutions.
j. Describe VPN protocols, their uses, features, and problems.
k. Explain the problem of using VPNs with NAT.
l. Evaluate hardware VPN devices.

2. Learning Activities:
a. Read Chapter 11 and 12. (C5, C6, C8, C19, F1, F5, F11)
b. Complete the assigned quiz and assignment. (C5, C6, C8, C19, F1, F5, F11)

3. Unit Outline Follow the sequence of the unit objectives

G. Unit Seven: Firewall Implementation and real-World VPN’s

1. Unit Objectives: Upon successful completion of this unit the student will be able to:
a. Install a host software firewall.
b. Create a remote-control VPN using Remote Desktop
c. Evaluate hardware VPN devices.
d. Experiment with TOR.
e. Set up an Internet cafe VPN client.
f. Assess online remote-control products, such as GoToMyPC and LogMeIn.
g. Configure and document settings for an IPSec VPN.

2. **Learning Activities:**
   a. Read Chapter 13 and 14. (C5, C6, C8, C19, F1, F5, F11)
   b. Complete the assigned quiz and assignment. (C5, C6, C8, C19, F1, F5, F11)

3. **Unit Outline:** Follow the sequence of the unit objectives

---

H. **Unit Eight: Perspectives, Resources, and the Future**

1. **Unit Objectives:** Upon successful completion of this unit the student will be able to:
   a. Discuss the different types of integrated and specialized firewalls, as well as the advantages and disadvantages of each.
   b. List additional sources of information related to network security.
   c. Describe emerging IT and security trends and their impact on network security.
   d. Identify challenges and advantages presented by the new technologies and emerging threats to network security.
   e. Describe the features which are different between an IDS and an IPS.
   f. Discuss the future of network security, firewalls and VPNs.

2. **Learning Activities:**
   a. Read Chapter 15. (C5, C6, C8, C19, F1, F5, F11)
   b. Complete the assigned quiz and assignment. (C5, C6, C8, C19, F1, F5, F11)

3. **Unit Outline:** Follow the sequence of the unit objectives