GAVILAN COLLEGE
5055 Santa Teresa Blvd
Gilroy, CA 95023

Course Outline

COURSE: CSIS 187 DIVISION: 50 ALSO LISTED AS:

TERM EFFECTIVE: Spring 2022 CURRICULUM APPROVAL DATE: 06/8/2021

SHORT TITLE: FIREWALLS & NETWORK SECURITY

LONG TITLE: Firewalls and Network Security

Units	Number of Weeks	Type	Contact Hours/Week	Total Contact Hours
3	18	Lecture:	3	54
		Lab:	0	0
		Other:	0	0
		Total:	3	54

COURSE DESCRIPTION:

This course provides students with the information needed to manage network Firewalls. In addition, students will learn to identify advanced threats by using integrated security policies, profiling application, intrusion prevention, web filtering, and signatures to protect networks against emerging threats. This course; along with CSIS 179, 184, and 186; prepares you to take the professional industry CompTIA CySA+ certification exam. This course has the option of a letter grade or pass/no pass. ADVISORY: CSIS 179.

PREREQUISITES:

COREQUISITES:

CREDIT STATUS: D - Credit - Degree Applicable

GRADING MODES
- L - Standard Letter Grade
- P - Pass/No Pass

REPEATABILITY: N - Course may not be repeated

SCHEDULE TYPES:
- 02 - Lecture and/or discussion
- 05 - Hybrid
- 71 - Dist. Ed Internet Simultaneous
- 72 - Dist. Ed Internet Delayed

STUDENT LEARNING OUTCOMES:

By the end of this course, a student should:

1. Explain firewalls and their features.

2. Apply techniques used by firewalls to counteract vulnerabilities.

3. Perform installation and configuration of common firewalls.

CONTENT, STUDENT PERFORMANCE OBJECTIVES, OUT-OF-CLASS ASSIGNMENTS

Curriculum Approval Date: 06/8/2021

9 Hours

Content: INTRODUCTION TO FIREWALLS - Introduction to Firewalls, Firewall Basics, TCP/IP for Firewalls

Student Performance Objectives: State what a firewall is and discuss what a firewall can be reasonably expected to do. Explain software firewalls, integrated firewalls, and appliance firewalls. Explain how TCP/IP functions from the perspective of firewall administration. Review the various protocols, applications, and services in the TCP/IP world. Create security zones. Configure basic interface types. Perform basic Interface Management configurations.

18 Hours

Content: HOW FIREWALLS WORK - Personal and Desktop Firewalls, Broadband Routers and Firewalls, Cisco PIX Firewall and ASA Security Appliance, Linux-Based Firewalls, Application Proxy Firewalls, Where Firewalls Fit in a Network

Student Performance Objectives: Identify firewalls that can be found or installed on laptop and desktop systems. Connect your firewall to a User-ID agent. Install a software User-ID agent on a Windows host. Discuss what a broadband router/firewall is, how it works, and how and where it should be implemented. Create a virtual router. Provide an overview of some PIX capabilities as well as how to configure the system initially. Provide an overview of configuring Linux-based firewalls. Explain what an application proxy is, how it works, and how and where it should be implemented. Discuss the basic features and functionality necessary to perform a basic configuration on the Microsoft ISA Server 2004 firewall. Discuss different types of firewall design architectures, including dual firewall and different types of DMZ implementations. Explore the different types of firewalls and where each type of firewall best fits in the network. Create a self-signed SSL certificate. Configure the firewall as a forward-proxy using decryption rules.

25 Hours

Content: MANAGING AND MAINTAINING FIREWALLS - Firewall Security Policies, Managing Firewalls, What is My Firewall Telling Me, Troubleshooting Firewalls, Going Beyond Basic Firewall Features

Student Performance Objectives: Review how the firewall security policies are configured. Describe and demonstrate how to provide for secure management access. Describe basic network security vulnerabilities. Create a security policy to allow basic internet connectivity. Configure security profiles. Create a security profile group. Discuss and utilize some management tools used to manage personal and small firewalls. Identify the types of logging supported by most firewalls and the kind of information that can be gleaned from that information. Explain how to read the information provided by the logs and how that information can be used for forensics analysis. Identify the top 10 things to look for in log files. Examine how to build a checklist that you can use to troubleshoot traffic flow through the firewalls. Explore the advanced features that firewalls can provide, while at the same time illustrating the limitations of firewalls in providing these advanced features. Create a certificate signing request (CSR). Create a self-signed CA certificate.

2 Hours

Final

METHODS OF INSTRUCTION:

Lecture, Computer Demonstrations, Presentations, Guided Practice

OUT OF CLASS ASSIGNMENTS:

Required Outside Hours: 40

Assignment Description:

Read textbook and study for quizzes and exams.

Required Outside Hours: 68

Assignment Description:

Homework: Complete hands-on problem solving assignments and projects.

For Example: Create security zones. Configure basic interface types. Perform basic Interface Management configurations. Connect your firewall to a User-ID agent. Install a software User-ID agent on a Windows host. Create a virtual router. Create a self-signed SSL certificate. Configure the firewall as a forward-proxy using decryption rules. Demonstrate how to provide for secure management access. Create a security policy to allow basic internet connectivity. Configure security profiles. Create a security profile group. Utilize some management tools used to manage personal and small firewalls. Examine how to build a checklist that you can use to troubleshoot traffic flow through the firewalls. Explore the advanced features that firewalls can provide. Create a certificate signing request (CSR). Create a self-signed CA certificate.

METHODS OF EVALUATION:

Problem-solving assignments

Percent of total grade: 30.00 %

Percent range of total grade: 30% to 40% Homework Assignments, Projects

Skill demonstrations

Percent of total grade: 40.00 %

Percent range of total grade: 30% to 50% Hands-On Exercises

Objective examinations

Percent of total grade: 30.00 %

Percent range of total grade: 20% to 40% Multiple Choice, True/False, Matching Items, Completion

REPRESENTATIVE TEXTBOOKS:

J. Michael Stewart, Denise Kinsey. Network Security, Firewalls, and VPNs; Third Edition. Burlington, Massachusetts: Jones & Bartlett Learning,2020.

ISBN: 10 - 1284183653; 13 - 978-1284183658

Reading Level of Text, Grade: 12+ Verified by: MS Word

Required Other Texts and Materials

OR Firewall Fundamentals by Wes Noonan and Ido Dubrawsky, Cisco Press

ARTICULATION and CERTIFICATE INFORMATION

Associate Degree:
CSU GE:
IGETC:
CSU TRANSFER:
Not Transferable
UC TRANSFER:
Not Transferable

SUPPLEMENTAL DATA:

Basic Skills: N
Classification: Y
Noncredit Category: Y
Cooperative Education: N
Program Status: 1 Program Applicable
Special Class Status: N
CAN:
CAN Sequence:
CSU Crosswalk Course Department:
CSU Crosswalk Course Number:
Prior to College Level: Y
Non Credit Enhanced Funding: N
Funding Agency Code: Y
In-Service: N
Occupational Course: C
Maximum Hours:
Minimum Hours:
Course Control Number: CCC000625381
Sports/Physical Education Course: N
Taxonomy of Program: 070810