Lecture Contact Hours: 32-36; Homework Hours: 64-72; Total Student Learning Hours: 96-108
Laboratory Contact Hours: 48-54; Homework Hours: 0; Total Student Learning Hours: 48-54

CUYAMACA COLLEGE
COURSE OUTLINE OF RECORD

COMPUTER AND INFORMATION SCIENCE 270 – PALO ALTO NETWORK SECURITY I

2 hours lecture, 3 hour laboratory, 3 units

Catalog Description
The Palo Alto Academy course feature hands-on lab training using Palo Alto Networks® next-generation firewalls. This course maps to certification exams that validate proficiency in managing Palo Alto Networks next-generation firewalls. Students learn the fundamentals of cybersecurity and identify the concepts required to recognize as well as mitigate attacks against enterprise networks and mission-critical infrastructure; general concepts involved in maintaining a secure network computing environment; students evaluate cybersecurity principles and demonstrate how to secure a network computing environment through the application of security controls~~;~~. Students will learn the nature and scope of today's cybersecurity challenges, strategies for network defense and detailed information about next-generation cybersecurity, students will also deploy a variety of security methodologies as well as technologies and concepts used for implementing secure network environments~~;~~. Students will gain a general understanding of how to install, configure and manage firewalls for the defense of enterprise network architecture. Students will also learn the theory and steps for setting up the security, networking, threat prevention, logging and reporting features of next-generation firewalls. This course is aligned with the U.S. National Initiative for Cybersecurity Education (NICE) framework.

Prerequisite
None

Recommended Preparation
CCNA 1-4, CCNA Security, Security +

Entrance Skills
Without the following skills, competencies and/or knowledge, students entering this course will be highly unlikely to succeed:
1) Basic Computer use and file navigation

Course Content
1) Routing Concepts
2) Physical Layer Security
3) Link-Layer Security
4) Network Layer Security
5) Transport Layer Security
6) Zone Traffic Defense
7) Designing a Security Posture
8) Mobile Device Security

Course Objectives
Students will be able to:
1) Discuss the nature and scope of today's cybersecurity challenges.
2) Apply strategies for network defense.
3) Analyze detailed information about next-generation cybersecurity approaches.
4) Describe security methodologies, technologies and concepts used for implementing a secure network environment.

5) Demonstrate knowledge of interconnected technologies.
6) Examine threat vectors, vulnerabilities and risks.
7) Apply subnet mask schemes for physical, logical and virtual networks.
8) Fully identify the functions of specific layers in the TCP/IP model.
9) Accurately explain cloud and virtual storage, backup, and recovery procedures.
10) Plan, design, implement and troubleshoot network infrastructure environments.
11) Formulate an industry-standard design to protect infrastructure against cybersecurity threats.
12) Apply advanced filtering methodologies, such as user, application and content identification, to protect against all known and unknown attack vectors.
13) Describe the basics of cryptography, including synchronous and asynchronous encryption; public key infrastructure, or PKI; and certificates.
14) Demonstrate the ability to assess and harden endpoints based on security policies.
15) Describe the uses of advanced malware research and analysis as they provide enhanced protection for enterprise networks.
16) Examine mobile and cloud-based connection technologies.
17) Compare industry-leading firewall platforms, architecture and defense capability related to Zero Trust security approaches and public cloud security.
18) Demonstrate and apply configuration of firewall initial access, interfaces, security zones, routing and more.
19) Analyze security policy administrative concepts related to source and destination network address translation.
20) Outline and construct security policies to identify known and unknown application software.
21) Differentiate, configure and deploy filtering technologies, such as antivirus, anti-spyware and file blocking.
22) Apply firewall certificate management policies.
23) Identify unknown malware, zero-day exploits and advanced persistent threats.
24) Configure and deploy zones, agents and security policies.
25) Differentiate and apply mobile device protection.
26) Implement and configure Application Command Center log forwarding and report monitoring.
27) Apply and monitor active/passive and active/active security device high availability.

Method of Evaluation
A grading system will be established by the instructor and implemented uniformly. Grades will be based on demonstrated proficiency in the subject matter determined by multiple measurements for evaluation, one of which must be essay exams, skills demonstration or, where appropriate, the symbol system.
1) Assignments, Quizzes, Final Project, and Exams.

Special Materials Required of Student
Internet connection
Flash drive

Minimum Instructional Facilities
Classroom with internet connection
Access to Cuyamaca Netlab

Method of Instruction
Lecture, Labs, and Out-of-Class Assignments

Out-of-Class Assignments
Utilizing Cuyamaca Netlab as a virtual Networking environment.

Texts and References

1) Required (representative example): The Cybersecurity e-book; Palo Alto Networks, 2019.
2) Supplemental: None

Exit Skills

Students having successfully completed this course exit with the following skills, competencies and/or knowledge:

1) Define an appropriate network security posture
2) Design the necessary policies for the security posture
3) Implement the Design in a Palo Alto appliance
4) Test the security posture of the installed Palo Alto appliance

Student Learning Outcomes

Upon successful completion of this course, students will be able to:

1) Analyze a network security problem, and design, implement, and test a solution through the successful completion of a semester-long project.
2) Collaborate in teams to allocate responsibility of the analysis, design and implementation of a final project.