Password Technical College
44 Calle Dr. Santiago Veve
San Germán, PR 00683
http://passwordtech.edu20.org

Syllabus

COURSE GENERAL INFORMATION

Course Title: Network Security
Code: CYLI 2030
Contact Hours: 60 hrs.
Credits: 2.0
Out of Class Hours: 15 hrs.
Term: October 19, 2022 to November 8, 2022
Teacher: Joel Vargas Ramos
Email: jvargas@passwordpr.com

Course Description

Today's organizations are challenged with responding rapidly to emerging network security threats. Security personnel configure and monitor various network security threat mitigation measures, such as device hardening, intrusion prevention systems, and firewalls, to protect data assets and network systems from attack. The purpose of this course is to provide skills and knowledge in the field of network security.

Objective

Network Security helps students develop the skills needed for entry-level network security career opportunities. It provides a theoretically rich, hands on introduction to network security, in a logical sequence driven by technologies. The goals of the Network Security course are as follows:

- Provide an in depth, theoretical understanding of network security.
- Provide students with the knowledge and skills necessary to design and support network security.
- Provide an experience-oriented course that employs industry-relevant instructional approaches to prepare students for entry-level jobs in the industry.

Password Technical College
44 Calle Dr. Santiago Veve
San Germán, PR 00683
http://passwordtech.edu20.org

Skills Distribution

- Explain the various types of threats and attacks.
- Explain the tools and procedures to mitigate the effects of malware and common network attacks.
- Configure command authorization using privilege levels and role-based CLI.
- Implement the secure management and monitoring of network devices.
- Configure AAA to secure a network.
- Implement ACLs to filter traffic and mitigate network attacks on a network.
- Implement Zone-Based Policy Firewall using the CLI.
- Explain how network-based Intrusion Prevention Systems are used to help secure a network.
- Explain endpoint vulnerabilities and protection methods.
- Implement security measures to mitigate Layer 2 attacks.
- Explain how the types of encryption, hashes, and digital signatures work together to provide confidentiality, integrity, and authentication.

ASSESSMENTS

- Anatomy of Malware
- Research Network Standards
- Social Engineering
- Network Threat

LABORATORIES

- Configure VPN Transport Mode
- Qualys SSL Labs
- Router and Resilience
- Comic Strip

Password Technical College
44 Calle Dr. Santiago Veve
San Germán, PR 00683
http://passwordtech.edu20.org

Chapters	Modules
Module 1. Securing Networks	• Network Topology • Current State of Affairs
Module 2. Network Threats	• Who is Attacking Our Network? • Threat Actor Tools • Malware
Module 3. Mitigating Threats	• Defending the Network • Network Security Policies • Security Tools, Platforms, and Services
Module 4. Secure Device Access	• Secure the Edge Router • Configure Secure Administrative Access • Configure SSH
Module 5. Assign Administrative Roles	• Configure Privilege Levels • Configure Role-Based CLI • Assign Administrator Role
Module 6. Device Monitoring and Management	• Lock Down a Router Using Auto Secure • Routing Protocol Authentication • Secure Management and Reporting
Module 7. Authentication, Authorization and Accounting (AAA)	• Configure Local AAA Authentication • Configure Server-Based Authorization and Accounting • Authentication, Authorization and Accounting (AAA)
Module 8. Access Control Lists	• Introduction to Access Control Lists • Mitigate Attacks with ACLs

Password Technical College
44 Calle Dr. Santiago Veve
San Germán, PR 00683
http://passwordtech.edu20.org

Module 9: Firewall Technologies	• Secure Networks with Firewalls • Firewalls in Network Design
Module 10: Zone-Based Policy Firewalls	• ZPF Operation • Configure a ZPF
Module 11: IPS Technologies	• IPS Implementations • IDS and IPS Characteristics
Module 12: IPS Operation and Implementation	• IPS Signatures • IPS Operation and Implementation

Password Technical College
44 Calle Dr. Santiago Veve
San Germán, PR 00683
http://passwordtech.edu20.org

Evaluation Criteria

CRITERIA	Grade total
Mid-Term Exam	100
Final Exam	100
Quizzes	100
Laboratories 1-4	100
Assessment 1-4	100
Forums 1-5	100
Attendance	100
Total	**700**

*5 Points less for each non-excused absence.

Assignments are always due in class on the day designated. You are responsible for any work lost due to technical problems, etc. Late papers will lose a letter grade for each day that they are late. Any exceptions must be properly documented and discussed in advance for an extension to be arranged.

Educational Resources

- Neo LMS (2022). Network Security. *passwordtech.edu20*.

  https://passwordtech.edu20.org/

- Cisco Network Academy (2022). Network Security. *Netacad*.

  https://www.netacad.com/

Notes

• ***Reasonable Accommodation*:** Any student who requires a reasonable accommodation should do the request at the beginning of the course or as soon as he / she acquires knowledge of what it requires, through the Professor in charge and this notifying the Academic Director.

• ***Honesty, fraud, plagiarism:*** The lack of honesty, fraud, plagiarism and / or any other inappropriate behavior in relation to the student's academic performance constitute violations of the Institution's Catalog, its Rules of Conduct and Student Duties. Major infractions, as determined by the Catalog, may result in the suspension of the Institution for a definite time or permanent expulsion as stipulated in the Norms of Conduct and Duties of the Student.