INTERAMERICAN UNIVERSITY OF PUERTO RICO
GUAYAMA CAMPUS
DEPARTMENT OF NATURAL SCIENCES AND TECHNOLOGY

SYLLABUS

I. GENERAL INFORMATION

Course Title : NETWORK SECURITY DESIGN
Code and Number : CSNS 6230
Credits : credits (3)

II. DESCRIPTION

Analysis of the design elements for security in networks and implementation of safety techniques and their tools. Design of safe network's for remote access and small and medians wireless. CSNS requirements 5222 and 6110.

III. OBJECTIVES

It is expected that upon completion of the course, the student will be able to:

1. Describe the components of the " SAFE" methodology.
2. To substantiate the design of the "SAFE" methodology.
3. Plan the design of a network using the "SAFE" methodology.
4. Design a small secure network.
5. Design a secure medium network.
6. Design secure remote access networks.
7. Design secure wireless networks.
8. Analyze the events that occur in a network within layers 2, 3, 4 and 7 of the OSI "Open Systems Interconnection" model.
9. Analyze the need for scalable secure network designs.

IV. THEMATIC CONTENT

A. "SAFE" methodology

1. What is the " SAFE" methodology?
2. Uses of the " SAFE" methodology.
    a. Companies.
    b. VPN "Virtual Private Networks".
    c. Medium networks.
    d. Wireless networks.
    e. Telephony systems.

B. Design fundamentals of the " SAFE" methodology.

1. Design philosophy.
2. Policy design.
3. Implementation of security in existing or new infrastructures.
4. Reports
5. Access to critical resources.
6. Design adapted to types of threats.

C. Design concepts of the " SAFE" methodology.

1. Secure architectures.
2. Safety inspection in the design.
3. Types of whites.
    a. routers.
    b. switches.
    c. customers.
    d. networks.
    e. applications.

D. Classification of attacks.

1. Rudimentary attacks.
2. Sophisticated attacks.
3. Methodology to avoid rudimentary attacks.
4. Methodology to avoid sophisticated attacks.

E. Perimeter security

F. Design of a small secure network.

1. Fundamentals.
2. Components.

3. Design guides.
4. Analysis and design methodology.

G. Implementation of a small secure network .

1. Team.
2. Interfaces.
3. Interaction between networks.
4. Security in the service.
5. Implementation plan.
6. Optional implementations.

H. Design of a secure medium-sized network .

1. Fundamentals.
2. Components.
3. Design guides.
4. Analysis and design methodology.

I. Implementation of a secure medium-sized network .

1. Team.
2. Interfaces.
3. Interaction between networks.
4. Security in the service.
5. Implementation plan.

J. Design of secure remote access networks .

1. Fundamentals.
2. Components.
3. Design guides.
4. Analysis and design methodology.

K. Design of secure enterprise networks .

1. Fundamentals.
2. Distribution of components.
    a. Administration.
    b. Structural.
    c. Base.

d. Servers.

3. Design guides.

4. Analysis and design methodology.

L. Design of local access wireless networks .

1. Fundamentals.

2. Components.

3. Design guides.

4. Analysis and design methodology.

V. TEXTBOOKS

Chung, J., Pueblas, M., Nadimi, A., Hamilton, D., Farrington, S, et al. (2013). Cisco *SAFE reference* guide: *Cisco validated design guide*. Cisco Systems.

Moyle, E., Kelley, D. (2020). *Practical Cybersecurity Architecture: A guide to creating and implementing robust designs for cybersecurity architects.* Packt Publishing.

VI. ACTIVITIES

A. Individual Works
B. Discussion Forum
C. Readings
D. Other

VII. EVALUATION

	Punctuation	% of Final Grade
Exam 1	100	18.1%
Exam 2	100	18.1%
Final Exam	100	18.1%
Forum Discussions	50	9.099%
Secure Network Design Project	200	36.7%
Total	550	100.00 %

VIII. " STUDENT LEARNING ASSESSMENT" TECHNIQUES

1. Evaluation rubric secure network design project.

IX. SPECIAL NOTES

A. Auxiliary Services or Special Needs

Students requiring additional services or special assistance must request these at the beginning of the course or as soon as they learn that they need them, through the appropriate register at the Dean's Office.

B. Honesty, Fraud and Plagiarism

The lack of honesty, fraud, plagiarism and any other inadequate behavior in relation to academic work constitute major infractions sanctioned by General Student Regulations. Major infractions according to General Student Regulations, may result in suspension from the University for a definite period of time greater than one year or the permanent expulsion from the University, among other sanctions.

C. Use of Electronic Devices

Cellular (mobile) telephones and any other electronic device that could interrupt the teaching-learning process or disrupt a milieu favorable for academic excellence will be deactivated. Critical situations will be dealt with in an appropriate manner. The use of electronic devices that permit the accessing, storing or sending of data during tests or examinations is prohibited.

D. Compliance with the provisions of Title IX

The Federal Higher Education Law, as amended, prohibits discrimination based on sex in any academic, educational, extracurricular, athletic activity or in any other program or employment, sponsored or controlled by an institution of higher education regardless of whether it is carried out. inside or outside the institution's premises if the institution receives federal funds.

In accordance with current federal regulations, an Assistant Title IX Coordinator has been appointed in our academic unit who will provide assistance and guidance in relation to any alleged incident that constitutes discrimination based on sex or gender, sexual harassment or sexual assault. You can contact the Auxiliary Coordinator by calling 787-864-2222, extension 2247, or by email at arcilia.rivera@guayama.inter.edu.

The Normative Document entitled Norms and Procedures for Attending Alleged Violations of the Provisions of Title IX is the document that contains the institutional rules to channel any complaint that is presented based on this type of allegation. This document is available on the website of the Inter American University of Puerto Rico (www.inter.edu).

X. BIBLIOGRAPHY

Reference Books

Ackerman.P. (2021). *Industrial cybersecurity: Efficiently monitor the cybersecurity posture of your ICS environment.* (2nd ed.). Packt Publishing.

Al-Shawi, M. (2015). *CCDE study guide*. Cisco Press.

Bertaccini, M. (2022). Cryptography Algorithms: *A guide to algorithms in blockchain, quantum cryptography, zero-knowledge protocols, and homomorphic encryption.* Packit Publishing.

Bodungen, C., (2016). *Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets & Solutions*. McGraw Hill.

Bruno, A., & Jordan, S. (2020). C*CNP Enterprise Design ENSLD 300-420 Official Cert Guide: Designing Cisco Enterprise Networks (Certification* Guide). Cisco Press.

Cole, And. (2009). *Network security bible.* John Wiley and Sons.

Dowd, M., McDonald, J., & Schuh, J. (2006). *The art of* software *security assessment: Identifying and preventing software vulnerabilities.* Addison Wesley Professional.

Donohue, D., & White, R. (2014). *The art of network architecture: Business driven design*. Cisco Press.

Fry, C., & Nystrom, M. (2009). *Security monitoring*. O'Reilly.

Graham, E. (2021). Practical Network Security Monitoring: Using Free Software. BabyBook.

Gregg, M, & Kim, D. (2005). *Inside network security assessment: Guarding your IT infrastructure.* Sams Publishing.

Holden, G. (2006). *Guide to network defense and countermeasures.* . (2nd ed.). Course Technology.

Hooda, S.K., Kapadia, S., & Krishnan, P. (2014). *Using TRILL, FabricPath and VXLAN: Designing massively scalable data centers (MSDC) with overlays (Network Technology).* Cisco Press.

Jackson, C. (2010). *Network security auditing.* Indianapolis, IN: Cisco Press.

Kamhoua, C.A., Njilla, L.L., Kott, A., & Shetty, S. (2020). *Modeling and Design of Secure Internet of Things.* IEEE Press.

Kendrick, T. (2009). *Identifying and managing* project *risk: Essentials tools for failure-proofing your project.* (2nd ed.). AMACOM.

Layton, T.P. (2006). *Information security: Design, implementation, measurement, and compliance.* Auerbach Publications.

Rajnovic, D. (2010). *Computer incident and product vulnerability handling.* Indianapolis, IN: Cisco Press.

Smith, P. (2021). *Pentesting Industrial Control Systems: An ethical hacker's guide to analyzing,*

compromising, mitigating, and securing industrial processes. Packit Publishing.

Tantsura, J., & White, R. (2015). *Navigating network complexity: Next generation routing with SDN, Service Virtualization, and Service Chaining*. Addison-Wesley.

Thomatis, M. (2015). *Network design cookbook: Architecting Cisco networks*. Lulu.com.

Tiso, J. (2011). *Foundation learning guide: Designing Cisco network service architectures (ARCH).* Cisco Press.

Trost, R. (2009). *Practical intrusion analysis: Prevention and detection for the twenty-first century.* Addison-Wesley Professional.

White, R., & Donohue, D. (2014). *The art of network architecture: Business-driven design (Network Technology)*. Cisco Press.

Oppenheimer, P. (2010). *Top down network design*. (3rd ed.). Indianapolis, IN: *Cisco* Press.

Electronic Resources, Journals and Published Conferences

Caldwell, Z. B. (2022). The Case for a Security Metric Framework to Rate Cyber Security Effectiveness for Internet of Medical Things (IoMT). In *Women Securing the Future with TIPPSS for Connected Healthcare* (pp. 63-81). Springer, Cham.

Kulik, T., Dongol, B., Gorm Larsen, P. et al. (2022). A Survey of Practical Formal Methods for Security. *Form. ASP. Comput. Just Accepted* (January 2022).

Paim de Jesus, W., Alves da Silva, D., de Sousa Júnior, R.T., & Lopes da Frota, F.V.. (2014). Analysis of SDN Contributions for Cloud Computing Security. In *Proceedings of the 2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing* (UCC '14). IEEE Computer Society, Washington, DC, USA, 922-927.

Rajaboyevich, G. S., Rustamovna, S. H., & Mahmud, G. A. (2022). Characterizing Honeypot -Captured Cyber-attacks: Statistical Framework and Case Study. I*nternational Journal of Innovative Analyses and Emerging Technology*, 2(5), 63-67.

Sengupta, S. (2011). Cloud data center networks: technologies, trends, and challenges. In *Proceedings of the ACM SIGMETRICS joint international conference on Measurement and modeling of computer systems* (SIGMETRICS '11). ACM, New York, NY, USA, 355-356.

Tripathi, S., Chickering, R., & Gainsley, J. (2015). Distributed Control Plane For High Performance Switch-based VXLAN Overlays. In *Proceedings of the Eleventh ACM/IEEE Symposium on Architectures for networking and communications systems* (ANCS '15). IEEE Computer Society, Washington, DC, USA, 185-186.

Veaudry, K. (2022). Identification of Barriers to Practicing Cybersecurity by Non-information System Trained Home Users: A Qualitative Study (Doctoral dissertation, Colorado Technical University).

Wilson, S. V. (2022). Cybersecurity and Higher Education: A Review of Cyber Vulnerabilities and Their Impact on Colleges and Universities.

Yao, J., Wang, Z., Yin, X., Shi, X., Wu, J., & Li, W . (2014). Model Based Black-Box Testing of SDN Applications. In *Proceedings of the 2014* CoNEXT *on* Student Workshop(CoNEXT Student Workshop '14). ACM, New York, NY, USA, 37-39.

Revised: June 2022, Prof. Luis Sánchez, Associate Professor in Computer Science