2023 Annual Conference & Exposition
Baltimore Convention Center, MD | June 25 - 28, 2023
The Harbor of Engineering Education for 130 Years
ASEE
Paper ID #37056

Early Integrating of Industry Certification Domains and Objectives into a Modern a Cybersecurity Degree Curriculum

Dr. Mahmoud K. Quweider, The University of Texas, Rio Grande Valley

M K Quweider is a Professor of Informatics and Engineering System (founding member of the Cyber Security Program) at the U. of Texas at RGV. He received his Ph.D. in Engineering Science (Multimedia and Imaging Specialty) and B.S. In Electrical Engineering, M.S. in Applied Mathematics, M.S. in Engineering Science, and M.S. in Biomedical Engineering all from the University of Toledo, Ohio. He also holds a Bachelor/Masters of English and a Masters of Business Administration from the University of Texas at Brownsville. After graduation, he was employed at several corporations including Pixera, a digital multimedia processing company in Cupertino, CA, 3COM, a networking and communication company in Schaumberg, IL, and Mercantec, an E-Commerce company in Naperville, IL. He is an IEEE Senior Member and has more than 40 publications in the field, and has served as a reviewer/moderator for several scientific and educational journals and conferences. He joined UTB in the Spring of 2000. His areas of interest include Imaging, Visualization and Animation, Networking and Cyber Security, Web Design, Computer Graphics, and Linguistics.

Dr. Liyu Zhang, The University of Texas, Rio Grande Valley

Liyu Zhang is an Associate Professor in the Department of Computer Science Department of Computer Science at the University of Texas Rio Grande Valley. He received his Ph. D. in Computer Science from the State University of New York at Buffalo in Septemb

Dr. Hansheng Lei

Early Integrating of Industry Certification Objectives into Modern Cyber Security Degree Curriculum

Abstract

We have recently created a new bachelor's degree in cyber security (B.Sc. CS) [1] to address the national and pressing needs for cybersecurity specialists, cyber-crime analysts, incident and intrusions analysts, IT auditors, and many other cyber security related fields. The new degree addresses not only the technical objective of the degree, but also the legal, corporate, policy, procedure, and human ones as well. To achieve such a wide range of objectives within the cyber security degree, a student is required to obtain two national certifications before they graduate. These certifications are embedded in the curricula and are an integral part of the degree.

In this paper, we present our academic and hands-on approach to these certifications. In particular, since these certifications are obtained by students with no expected extensive job experience or training, the choice of the certifications, the resources needed, and the academic approach to teaching them becomes very important. In the paper, we will present:

- The list of certifications that were carefully selected and the fields they cover:
    - Promoting vendor neutral certifications
    - Allowing customized certifications for experienced students.
- The complete degree plan with the embedded certification:
    - When to take the certification
    - What SLOs should be covered in courses leading to the certification
- The course developments for these certifications and how they are delivered:
    - Department-wide course template and resources
- Resources available to the students:
    - Internal and external
    - A live and ever-expanding compiled set of resources
- Practical and mock exams
- Compilation of ads by leading companies that require certifications as extra motivation for students.

By presenting our efforts, we hope that other institutions who are considering expanding their programs of study to include Cyber Security and Certifications can benefit from our experience by adopting best practices while avoiding pitfalls.

Keywords

Cyber Security, Vendor-Neutral Certification, Network+, Security+, Cloud+.

Introduction and Motivation

We have recently created a new bachelor's degree in cyber security (BSCS) that is part of a newly created department of Informatics and Engineering Systems (IES). Details of the degree are presented in [1] where we cover the overall objective and learning outcomes, courses details and the degree plan. According to the U.S. Bureau of Labor Statistics (BLS) [2,3], the field of Cyber Security is booming and is expected to grow 28% through 2026 and its market will reach more than $300B by 2024. Our degree takes a practical and wholistic approach toward preparing its graduates to join the industry and be productive from day one. This is achieved by having a great balance of legal, corporate, and technical computer skills. Unlike traditional degrees that are offered within the Engineering or the Computer Science department, our degree is hosted in a separate IES department. The degree plan requires the usual hefty dose of technical courses from Computer Science and Cyber Security. But additionally, it requires courses from Criminal Justice such as Introduction to Criminal Justice and Crime Evidence and Proof; and courses from Business such as Business and Technical Communications, Business Law, and Business Information Infrastructure. Fig. 1 shows the overall architecture of the Cyber Security degree, while Fig. 2 shows the details of the degree plan at the course and prerequisites level as approved by the Cyber Security program within the department.

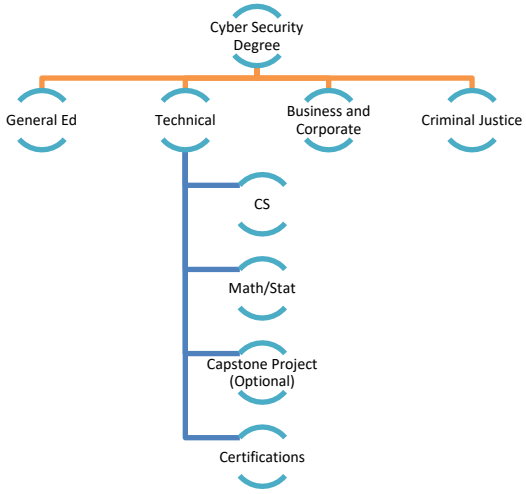


Figure 1. Cyber Security Degree Architecture

To complement education with training, the degree also requires students to pass two industry certifications before they graduate. The course number for each certification is CYBI-3101-xx where xx stands for the student's choice of certification such as Net+, Linux+, Security+, etc. A pool of certifications was carefully studied and approved, and we are currently in the process of developing a series of curricula and educational modules, web-based software, and a collection of external resources to ensure the success of our students when obtaining these certificates. There are also optional internship courses and a senior design course that we will discuss in future papers. Next, we present the details of the educational modules, software, and resources and how they are being integrated into the suitable courses as early as possible.

Certifications

It is critical that graduates of our Cyber Security program not only be fluent in the theoretical concepts of the field, but also be able to complement these concepts with industry training that promotes problem solving and critical thinking [5-6]. In surveying many pools of job advertisements for Cyber Security related fields, we noticed that applicants who obtained certifications are highly desirable by employers, and in fact many specifically list certain certifications as required. However, we did not know which certifications would be best to adopt for our degree and for our students who would mostly apply for entry level jobs. Current industry certifications are all over the place, some are awfully expensive to take, some are very technology specific, some require years of on-the-job experience, and others are not available everywhere. Considering that most of our students come straight out of high schools and that most of them are first-generation college students, we decided to go with vendor-neutral certifications. Some of these certifications include Linux+, Network+, Security+, and Cloud+ [7].

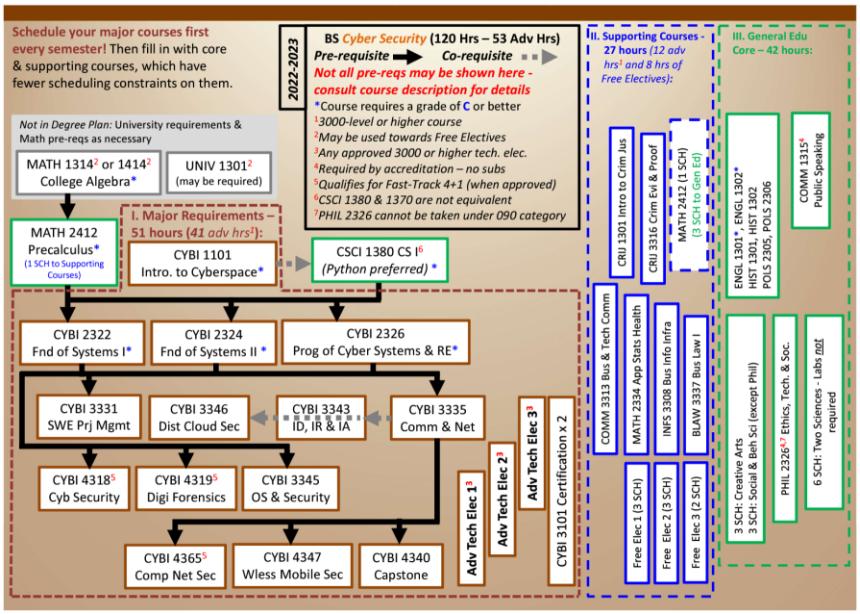


Figure 2. Cyber Security Degree Plan [4]

Vendor-neutral Certifications

Vendor-neutral, sometimes called vendor-agnostic, certifications focus on main concepts and general approaches used in a given field or technology. They highlight best practices and proficiency in different technology without being tied to a specific one. They provide a perfect fit for our graduating students in the CS program, presenting them as highly employable and more adaptable across a wide range of companies.

One of the independent, most reputable, and trusted vendor-neutral certification providers is CompTIA (The Computing Technology Industry Association). CompTIA "About US" [7] section describes the association as "a leading voice and advocate for the $5 trillion global information technology ecosystem; and the estimated 75 million industry and tech professionals who design, implement, manage and safeguard the technology that powers the world's economy."[https://www.comptia.org/about-us] It is considered by many as the number one vendor-neutral certification provider. CompTIA certificates usually meet industry-standard

requirements for hiring practices, including those for most IT jobs in government agencies. In the following, we summarized the top four certifications that we are advocating for our students. We selected them because each has a clear matching course in our degree plan where we can introduce the certificate objectives and goals and integrate them within class lectures and lab modules. CompTIA certifications align with IT infrastructure and cybersecurity career paths. It has four IT certification levels: Core, Infrastructure, Cybersecurity, and Professional. Network+ and Security+ are considered Core; Linux+ and Cloud+ are considered Infrastructure. The Cybersecurity level includes Cybersecurity Analyst CySA+, PenTest+, and CompTIA CASP which are intermediate/advanced certifications.

Table 1. Cyber Security Vendor-Neutral Certifications	
Certificate Name	• CompTIA Network+ • CompTIA Security+ • CompTIA Cloud+ • CompTIA Linux+

Linux+:

CompTIA Linux+ validates the skills administrators need to secure the enterprise, power the cloud, and keep systems running.

Skill Set

- System Management: Configure and manage software, storage, process, and services.
- Security: Understand best practices for permissions and authentication, firewalls, and file management.
- Scripting, Containers & Automation: Create simple shell scripts and execute basic BASH scripts, version control using Git, and orchestration processes.
- Troubleshooting: Analyze system properties and processes and troubleshoot user, application, and hardware issues

Network+:

CompTIA Network+ validates the technical skills needed to securely establish, maintain, and troubleshoot the essential networks that businesses rely on.

Skill Set

- Networking Fundamentals: Explain basic networking concepts including network services, physical connections, topologies and architecture, and cloud connectivity.
- Network Implementations: Explain routing technologies and networking devices; deploy ethernet solutions and configure wireless technologies.
- Network Operations: Monitor and optimize networks to ensure business continuity.
- Network Security: Explain security concepts and network attacks in order to harden networks against threats.
- Network Troubleshooting: Troubleshoot common cable, connectivity, and software issues related to networking.

Security+:

CompTIA Security+ is a global certification that validates the baseline skills necessary to perform core security functions and pursue an IT security career.

Skill Set

- Attacks, Threats, and Vulnerabilities: Focusing on more threats, attacks, and vulnerabilities on the Internet from newer custom devices that must be mitigated, such as IoT and

embedded devices, newer DDoS attacks, and social engineering attacks based on current events.

- Architecture and Design: Includes coverage of enterprise environments and reliance on the cloud, which is growing quickly as organizations transition to hybrid networks.
- Implementation: Expanded to focus on administering identity, access management, PKI, basic cryptography, wireless, and end-to-end security.
- Operations and Incident Response: Covering organizational security assessment and incident response procedures, such as basic threat detection, risk mitigation techniques, security controls, and basic digital forensics.
- Governance, Risk and Compliance: Expanded to support organizational risk management and compliance with regulations, such as PCI-DSS, SOX, HIPAA, GDPR, FISMA, NIST, and CCPA.

Cloud+:

CompTIA Cloud+ is a global certification that validates the skills needed to deploy and automate secure cloud environments that support the high availability of business systems and data.

Skill Set

- Attacks, Threats, and Vulnerabilities: Focusing on more threats, attacks, and vulnerabilities on the Internet from newer custom devices that must be mitigated, such as IoT and embedded devices, newer DDoS attacks, and social engineering attacks based on current events.
- Cloud Architecture & Design: Analyze the different cloud models to design the best solution to support business requirements.
- Cloud Security: Manage and maintain servers, including OS configurations, access control and virtualization.
- Cloud Deployment: Analyze system requirements to successfully execute workload migrations to the cloud.
- Operations & Support: Maintain and optimize cloud environments, including proper automation and orchestration procedures, backup and restore operations, and disaster recovery tasks.
- Troubleshooting: Troubleshoot capacity, automation, connectivity, and security issues related to cloud implementations.

Certification and Course Integration Methodologies:

With the set of certifications decided, we set out to identify the course(s) that are best to integrate the certification skill set in. In this paper, we present our methodologies as they apply to the Network+, which we used as the pilot project. We will report and disseminate results for other certifications as they are completed.

Course Material Revamping

With most of the faculty in the new Cyber Security Program coming from Computer Science background, it was imperative that we revamp the current course materials for any course that is foundational for the Certifications. Networking (CYBI-3335) and Computer and Network Security (CYBI-4365 were immediately identified for this process. For each course, a shift from theoretical concepts to a hands-on approach was adopted. The new revamped courses include:

- ***Additional*** material covering physical media and cables, connectors, and tools including:
    - Coaxial cables and connectors
    - Twisted-pair cabling standards including Cat 3, Cat 5, Cat 6/a, Cat 7/a.
    - Fiber cables and connectors.
    - Tools such as multimeters, punch down tool, tone generator and locator, crimper, butt set, time-domain reflectometry (TDR).
    - Hands-on labs with virtual machines, many of which are adopted from SEED [11], a well-documented and professionally created set of labs for security.
- Extensive set of labs:
    - Wireshark-based labs.
    - Packet-tracer labs.
- Reformatting certain exam question to a format similar to the certification questions.

This is an ongoing process and will continue as we gather more data and feedback from faculty as well as students who take the certifications.

Hands-on Labs & Lab Format

With regards to the labs, we have intentionally moved from programming-based assignments that explored client-server applications, mail application, and video application to more hands-on labs and tools that use Wireshark and Packet Tracer.

Wireshark labs

Wireshark [8] is a great packet analyzer tool to explore network protocols and the network stack. It is a multi-platform free packet analyzer used in our labs –it is stable, has a large user base and well-documented.

The set of Wireshark labs include:

- Introduction to Wireshark
- Filters with Wireshark
- UDP/TCP
- Congestion Control
- HTTP
- DNS
- SSL
- Wi-Fi

The labs are distributed over the Networking and the Computer Security courses. One thing we did for these labs was to convert the submission report into a set of questions similar to the ones in the Network+ certification. Appendix A shows a partial sample of a lab submission in the form of multiple-choice questions, submitted after completing the lab.

Packet Tracer Labs

PT [9] is a great tool to simulate a Network and to create Network diagrams. It allows students to investigate the hardware and the software involved in networking. We have come up with the following modules:

- Packet Tracer Basics
- VLANS

- SSH and Switch port Security
- Routing
- Outer on a Stick
- NAT
- Servers

For each lab, a set of PowerPoint slides as well as a recorded video has been created to allow students access to any time and any place. A sample of the first PT lab is given in Appendix B.

Software Development

We have developed a Flask-based [10] software framework that works with different certifications, with Network+ as the first one that is being completed. The overall architecture of the software is shown in Fig. 3. When completed, the software will be hosted in the cloud using GPC PaaS (App Engine Service) to allow for permanent hosting and to take advantage of the services Pass provides including the operating system, the middle ware, and the development environment. While still in its infancy, the software can be auto scaled and load-balanced under our selected hosting model.

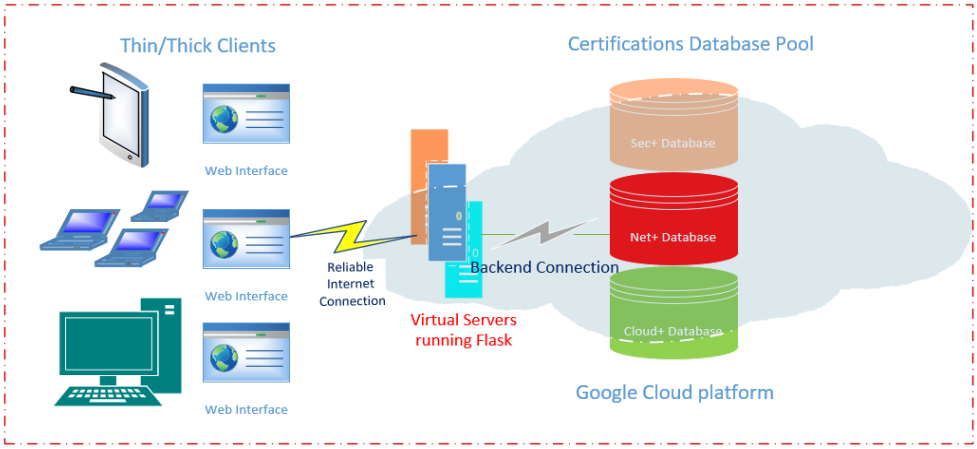


Figure 3. Certifications Software Framework

The framework is designed to allow for future expansion to any recommended certification. For any certification, the software has a web-based interface, accessible through a thin or thick client. The Web GUI interface allows for different functionalities supported at the server side with the help of a backend database. The functionalities include:

- Registration with login/logout.
- Generation of sample exams.
- Management of exam database.
- Listing of Acquired resources.
- Testimonials/recommendations from previous students

Following, we give a brief description of every functionality.

Main Interface

As shown in Fig. 4, the main web interface allows for registering a user, generating an exam, managing the database, get a list of certification-related resources, and read what previous students had to say about the certification and any recommendations they provide.

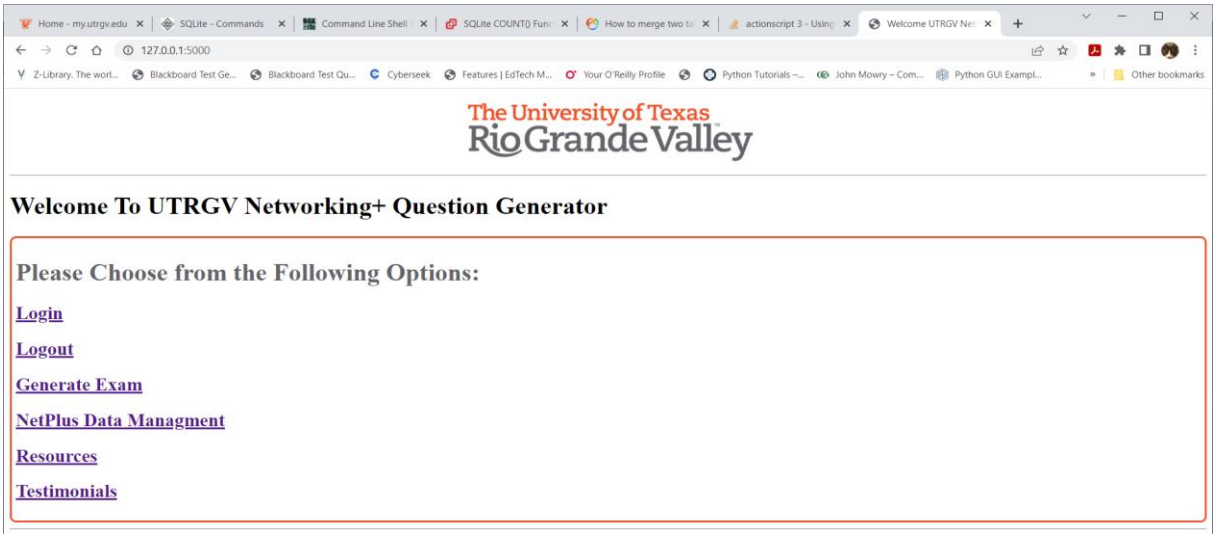


Figure 4. Framework Main Web Interface

Exam Generation & Feedback

As shown in Fig. 5,6, a registered student is allowed to generate an exam and answer questions one by one with detailed feedback provided after each question. When a student answers a question, the feedback shows the correct answer with an explanation of why the answer is the correct one and the other answers are not. The objective of the question is also displayed to allow the student to focus on his/her strengths and weaknesses. We currently don't track the student grade, but that will be fixed when the final code is released. We will also have more options under exam generation to tailor it for generating questions for a given objective or questions with specific key words.

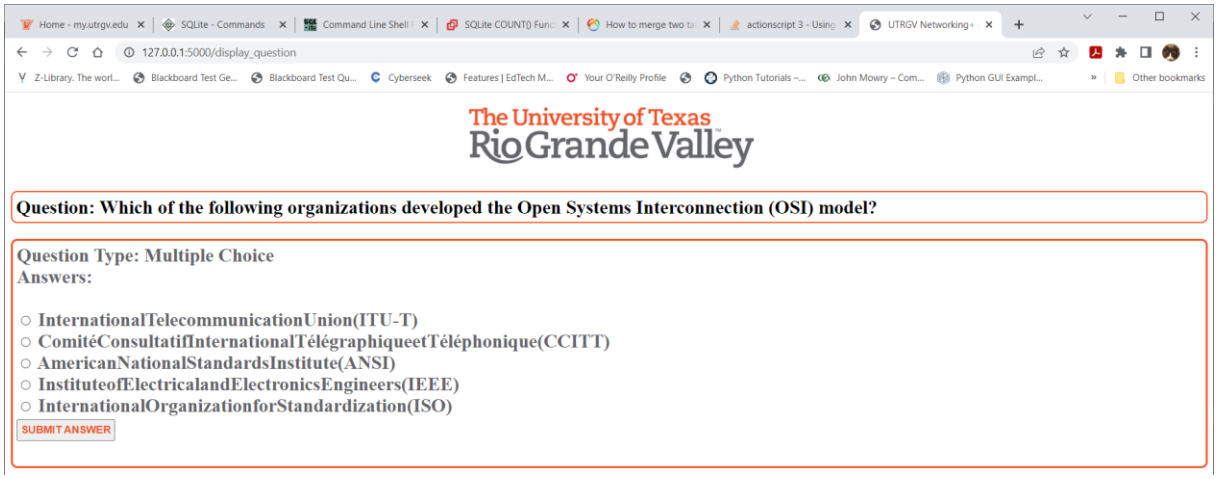


Figure 5. Exam Generation

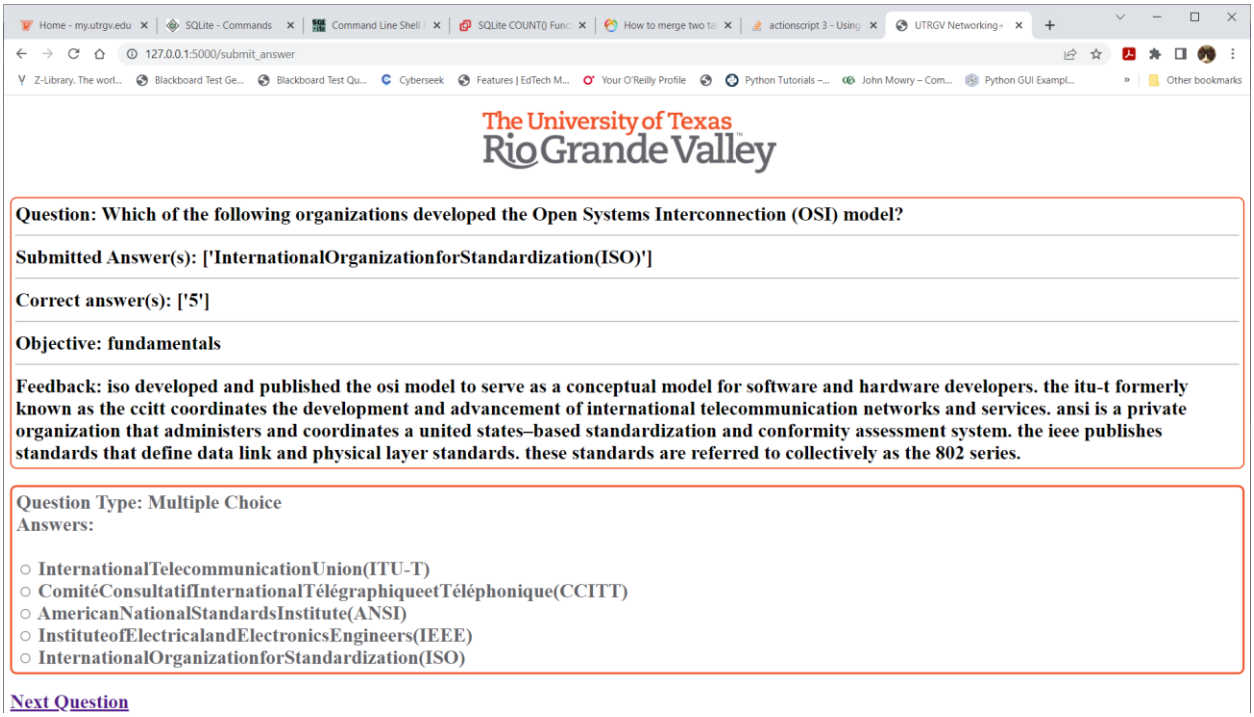


Figure 6. Question Feedback

Data Management

While the university has a vast pool of great resources for the students to use including Coursers, LinkedIn Learning, and the on-line Digital library, students are always finding resources that fit their needs and way of studying for the exam. We chose to embrace the resources that students find helpful for passing the exam. Therefore, during the Certification course offering, any resource that students identify is added to the resources page of the software.

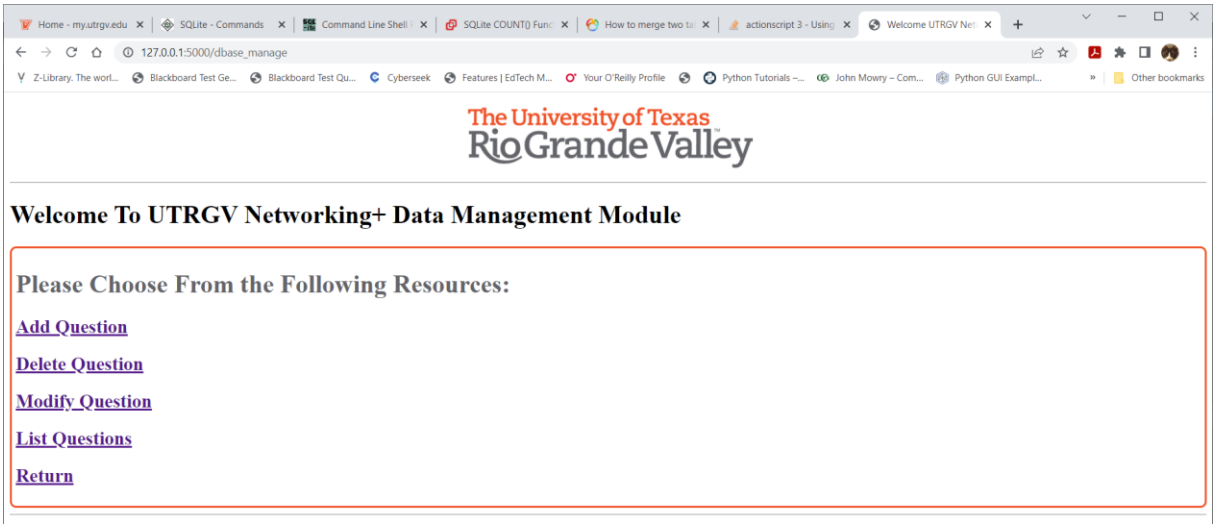


Figure 7. Exam Pool Database Management

Resources

While the university has a vast pool of great resources for the students to use including Coursers, LinkedIn Learning, and the on-line Digital Library, students are always finding resources that fit

their needs and way of studying for the exam. We chose to embrace the resources that students find helpful for passing the exam. Therefore, during the certification course offering, any resource that students identify is added to the resources page of the software.

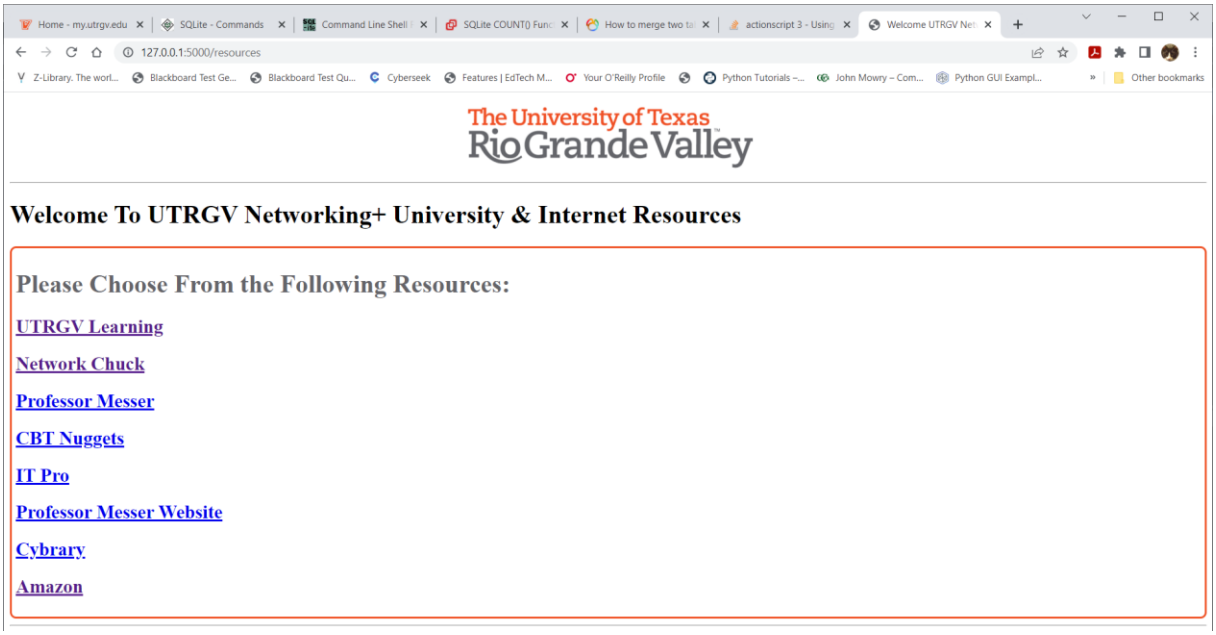


Figure 8. Certification Resources

Testimonials/Debriefing

After taking the certification exam, we send our students a simple questionnaire to answer. A sample of such a questionnaire is given in Table 2.

Table 2. Sample Questionnaire
1. How was the exam, what helped the most?
2. What advice do you give to other students?
3. Was the material I posted helpful?
4. What resources you found very helpful?
5. What can we do to prep students more?
6. Can you tutor future students to take the exam?
7. What courses prepared the most for the exam?
8. What courses prepared you the least for the exam?
9. Could you have handled two certifications in one semester?

Data from questionnaires is used to create a feedback mechanism that helps the faculty and future students. For example, faculty could use the feedback to modify and update their teaching materials, and students can benefit from feedback from their colleagues. A sample of feedback from a student is given in Fig. 9.

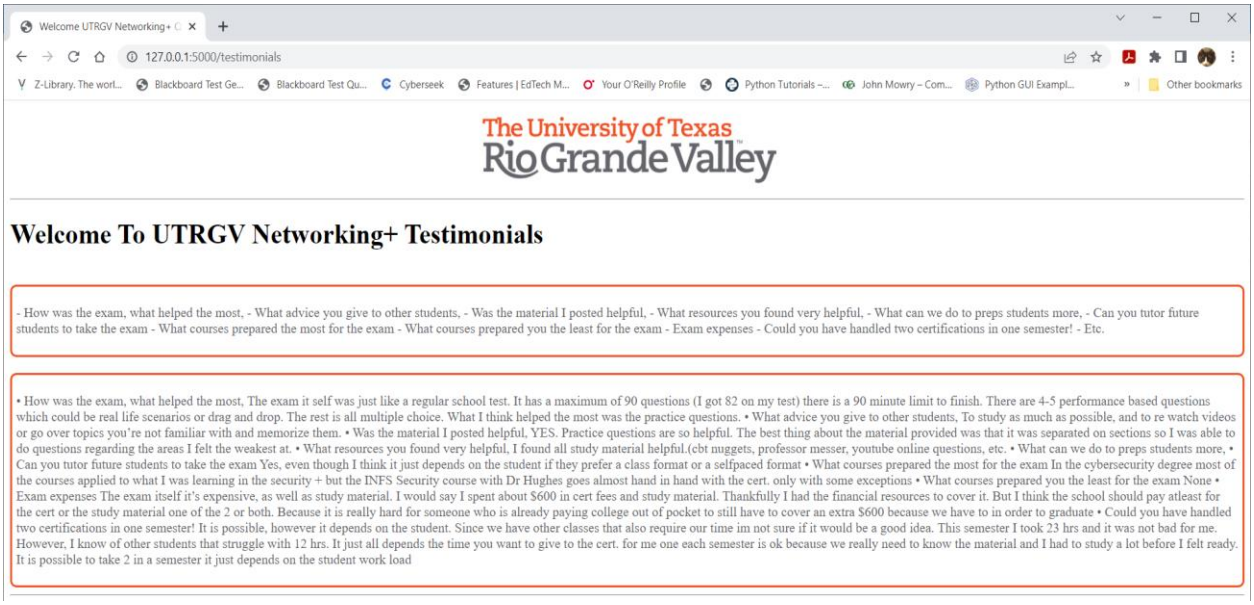


Figure 9. Certification Testimonials

Certification Exam and Question Visualization

Visualization is an important tool in helping students answer exam questions with confidence and ease. During the Certification course, students are presented with sample questions and mock exams to train them for the real exam. We found ourselves using the Google search to find explaining diagrams related to the question at hand. That is when we decided to complement each question with proper visualization where appropriate. The TA assigned to the class, along with the students joined in this collective effort and we are currently adding this visualization to all the PowerPoint slides we use in class. Another project that will be offered to students to do is to incorporate these visualizations into the database of questions. A sample of these questions with visualization are given in Fig. 10/11.

1. After starting work as the network administrator of Wingtip Toys, you discover that all of the switches in the company's datacenter have support for remote management, with built-in Simple Network Management Protocol (SNMP) agents in each port. Which of the following tasks must you perform to be able to gather information from the agents on those switches and display it on a central console? (Choose all that apply.)

- A. Install the network management software on a network computer.
- B. Install a Management Information Base (MIB) on each of the switches.
- C. Install an agent on the console computer.
- D. Install an MIB on the console computer.
- E. Purchase a network management product.

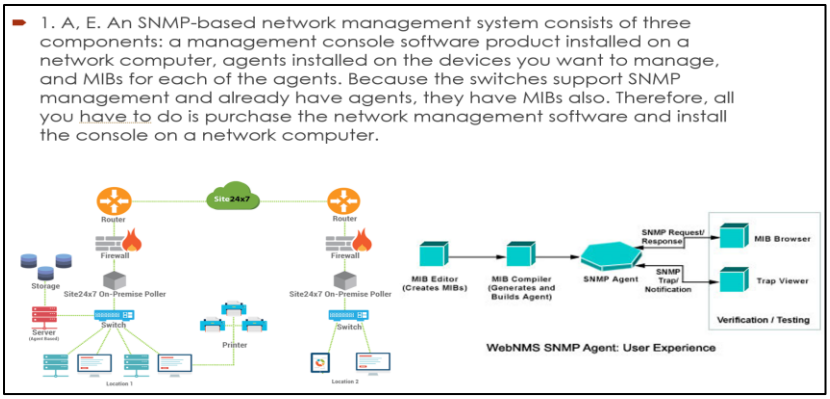


Figure 10. Exam Pool Question with Added Visualization

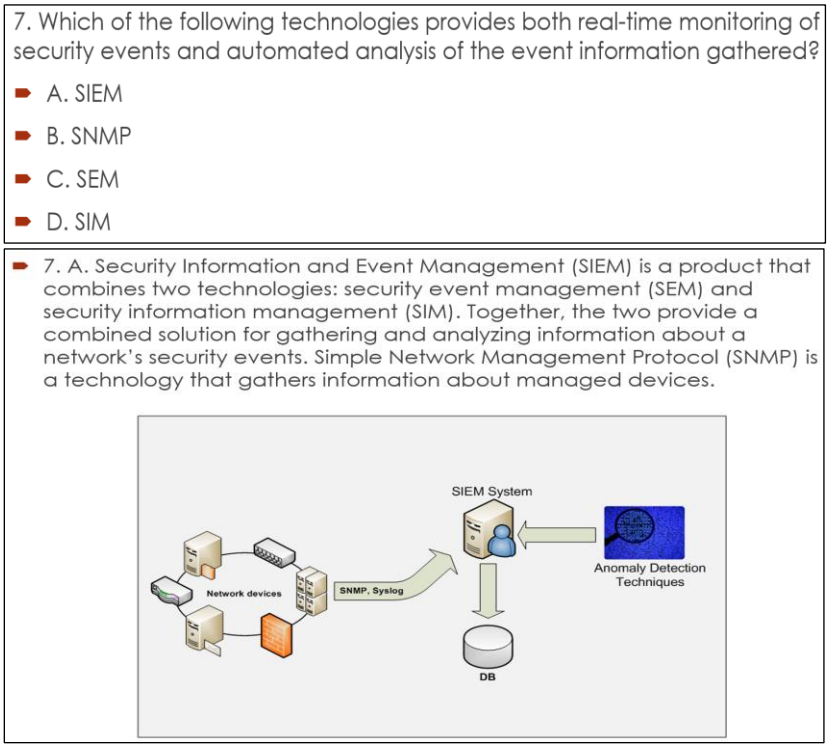


Figure 11. Exam Pool Question with Added Visualization

Discussion

As certifications have become the cornerstone of our newly formed degree, you can see that a tremendous effort has been dedicated to ensuring the success of our students as they take the certification exam. Several methodologies were adopted and integrated early in our curriculum to help the students have confidence and tools by the time they attempt the exam. We have even instituted voucher reimbursement program for the first attempt of each certification up to two. The multifaceted strategy of curriculum revamping, use of hands-on labs, implementing a certification software frame, adding visualization to pool questions, and the making available a set of resources and testimonials should be a great aid to the students. We are currently collecting data about each certification exam attempted and we hope to analyze the data and present the results in future work.

Conclusions and Future Work

In this paper we presented several integration methodologies of the certification objectives into our cyber security degree. The methodologies aim is to better prepare the student in passing the industry certification required for their graduation. They include Adding hands-on and practical material current courses; converting certain labs into a format compatible with that of the exams; developing a software that has an expandable pool of questions that target all objectives of the exam. Through a Graphical User Interface, the software allows for adding/modifying/editing of questions to fit the strengths and weaknesses of current students; The software has a set of resources that are recommended by current students. We also set out to improve the current pool of questions by adding visualizations where appropriate. We also added a testimonial/recommendations section specifically from our students who were debriefed after the exams in the hope that it will guide and inspire future students. Future work will report and analyze future data from all recommended certifications.

Acknowledgment

I would like to thank my TA Nick Perales and my current certification students Lourdes Perez, Alex Sanchez, and Tyler Landgraf for many constructive discussions during the certification mockup questions and for their comments regarding the design and implementation of the software.

References

1. Quweider, MK, et. al., (2022, August), *Crafting a Degree, Empowering Students, securing a Nation: The Creation of a Modern Cyber Security Degree for the 21st Century* Paper presented at 2022 ASEE Annual Conference & Exposition, Minneapolis, Minnesota. https://peer.asee.org/41292
2. https://www.bls.gov/ooh
3. www.chronicle.com/article/Cybersecurity-Rising/239270.
4. https://www.utrgv.edu/cyberspace/academics/index.htm.
5. Swain, N. (2014, June), *A Multi-Tier Approach to Cyber Security Education, Training, and Awareness in the Undergraduate Curriculum (CSETA)* Paper presented at 2014 ASEE Annual Conference & Exposition, Indianapolis, Indiana. 10.18260/1-2--19964
6. Ahmad, A. (2016, June), *Articulation of Certification for Manufacturing* Paper presented at 2016 ASEE Annual Conference & Exposition, New Orleans, Louisiana. 10.18260/p.26278
7. https://www.comptia.org/about-us
8. https://www.wireshark.org/
9. https://www.netacad.com/courses/packet-tracer
10. https://flask.palletsprojects.com/en/2.2.x
11. https://seedsecuritylabs.org/

Appendix: Partial Sample Lab

Computer Networks Lab

Name:

Lab: HTTP-01

You have one hour to complete the lab.

You must complete the original lab on your own before attempting this quiz.

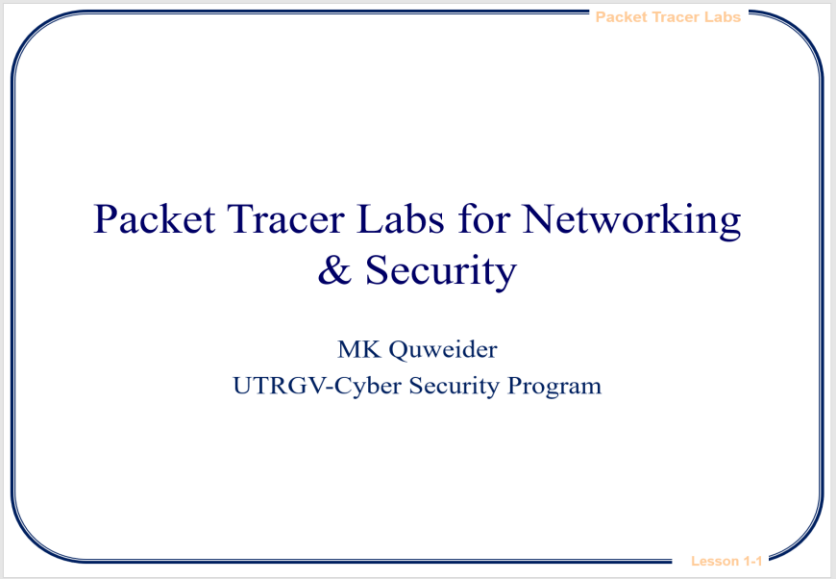
You are allowed to run the Wireshark while completing this lab.

The following questions are similar to ***Network+ type of questions*** and are relate to trace named: http-ethereal-trace-1.

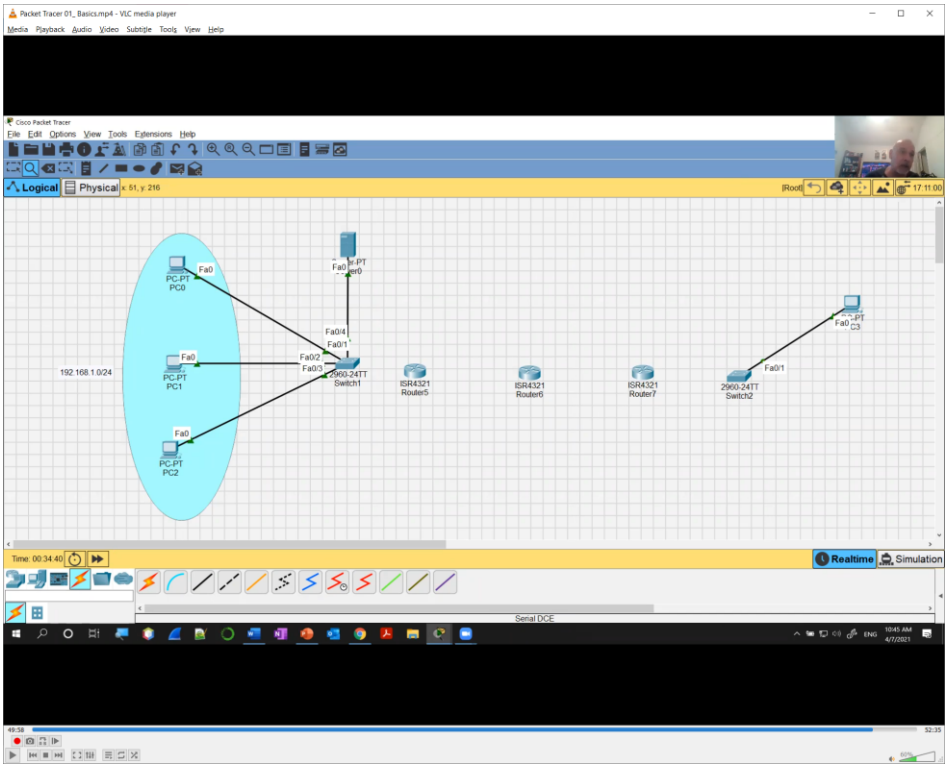
1. If you set the http filter, how many packets you will see:
    a. 3
    b. 4
    c. 5
    d. 6
2. If you set the SNMP filter, how many packets you will see:
    a. 3
    b. 4
    c. 5
    d. 6
3. For HTTP packet number 10 (Frame 10),), the total size of the packet is:
    a. 555
    b. 439
    c. 541
    d. 1395
4. For HTTP packet number 10 (Frame 10), the requesting user agent is:
    a. User-Agent: Mozilla/5.0
    b. User-Agent: Firefox/5.0
    c. User-Agent: Chrome/5.0
    d. User-Agent: Safari/5.0
5. For HTTP packet number 10 (Frame 10), the request version (Http version) is:
    a. HTTP 1.0
    b. HTTP 1.1
    c. HTTP 2.0
    d. HTTP 2.1
6. For HTTP packet number 10 (Frame 10), the source IP is given as:
    a. 192.168.1.12
    b. 192.168.1.102
    c. 128.119.245.10
    d. 128.119.245.12

Appendix B: Packet Tracer Videos

PT Basics Lab



PT Basics PowerPoint Slides



PT Basics Video Recording