CyberNEST
(Next Evolution of Security Training)

Enhancing Cybersecurity Education: An Immersive and Integrated Experiential Learning

Sebastian Hayes & Albert Tay

CyberNEST

- Develop a cutting-edge Cybersecurity simulator with immersive and realistic learning experiences.
- Implement strategic stages with varying difficulty levels to simulate real-world scenarios.
- Empower learners with practical skills and insights essential for thriving in the dynamic landscape of Cybersecurity.

CES

(Church Education System)

SOC

(Security Operations Center)

Penetration Testing

Testing a system, application, or website to find and validate security concerns.

Security Event Monitoring and Development

Working with our log data to create monitoring, dashboards, and alerts for known security issues.

Security Incident Investigation and Response

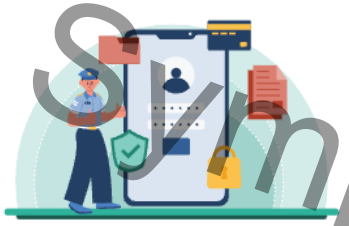
Day to day information security incident work. Includes phishing, account compromise, system compromise, and other security issues.

Threat Hunting

Working with our log data to understand what normal is so that we can recognize the abnormal early in an attack.

Vulnerability Management

Detection of, tracking, and reporting on unpatched security vulnerabilities.



Security Risk Management

Assessment of systems and applications to discover configuration and processes gaps against campus IT and cybersecurity controls. Risk based reporting of those gaps.

Training and Communications

Posters, training, fake phishing exercises, articles, and websites to promote security awareness.

Curriculum Integration

- Higher Education
  - Class Assignments within existing courses
  - Dedicated elective classes for hands on learning
- K-12
  - Introduction to Cybersecurity
  - Cyber day or week long camps
- Organizations
  - Initial training for new hires
  - Skill training for existing employees

Benefits

- Aids problem-solving skill development
- Fills instructional gaps and targets specific cybersecurity skills
- Provides a safe environment for experiential learning
- Fosters long-term memory retention
- Encourages learning from mistakes

Feedback

- The large amount of config files and services I became familiar with.
- I thought this lab was kind of fun. I appreciated the gamification of the points and scoreboard.
- I loved the exposure to a more practical application of having to use Linux to understand what is happening on the machine, rather than just making a file and changing some permissions

Future Expansion

Security Operations

Participants obtain the knowledge, skills, and tools necessary to effectively manage and oversee security operations within an organization, encompassing threat detection, incident response, security monitoring, log analysis, SIEM implementation, threat intelligence integration, and collaboration with relevant stakeholders to ensure the continuous protection and the mitigation of security risks in diverse and dynamic environments.

Penetration Testing

Designed to gain practical skills in identifying cybersecurity vulnerabilities through simulated attacks and assessments. Participants engage in hands-on simulations, covering reconnaissance, vulnerability assessment, exploitation, and reporting.

Future Expansion

Web Systems & Security

Participants engage in the testing and fortification of web-based applications and systems through simulated attacks and hardening techniques, with the goal of evaluating and reinforcing the resilience of web infrastructure against potential threats and vulnerabilities.

Designed to equip participants with essential knowledge, practical skills, and best practices in operating systems, networking, security, monitoring, backup, virtualization, automation, troubleshooting, and problem resolution.

System Administration

Future Expansion

Cyber Policy Implementation

The practical application of cybersecurity policies within organizational frameworks, encompassing policy development, enforcement strategies, risk assessment, compliance frameworks, incident response protocols, governance structures, and stakeholder communication to ensure effective protection of digital assets and mitigate cyber threats.

Participants delve into the systematic identification, assessment, prioritization, and mitigation of security vulnerabilities in information systems, covering vulnerability scanning tools, risk analysis, patch management, and the development of proactive strategies to safeguard organizational assets against potential threats in dynamic and evolving cyber landscapes.

Vulnerability Management

Conclusion

- Offer immersive and realistic learning experiences for diverse audiences and skill levels
- Aid in developing problem-solving skills and target specific cybersecurity skills
- Simulations will grow to include, system administration, web security and systems, cyber policy implementation, and vulnerability management.
- Foster long-term memory retention and encourages learning from mistakes
- We aim to shape the next generation of cybersecurity professionals and contribute to a safer digital environment.

Q&A

Have more questions?

Please contact Sebastian at sebastian.hayes@byu.edu