**SECU8010**

**Midterm Examination Review – Week 7**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

The Midterm Examination for SECU8010 will be held on Week 7 during your regular class time and will be an online quiz through eConestoga Quizzes and may consist of the following types of possible questions:

* **True and False Questions**
* **Multiple Choice Questions**
* **Multi-Select Questions**
* **Long (Written) Answer Questions**
* **Matching Questions**
* **Ordering Questions**

You will need to use the Respondus Lockdown Browser on your laptop computer along with the WebCam for this exam (same one used for the Academic Integrity Quiz). All material covered to date (lecture slides, lab slides, videos, links, assignments and past assessments) is fair game for the midterm.

The midterm is worth 30% of your final grade and you will have two (2) hours in which to complete it.

During the exam, you are not permitted to have your smartphones within reach and must keep your eyes on your own work and no communication (except with the proctor) is allowed.

**Disclaimer:** This review is NOT meant to substitute for your individual study of ALL of the material covered to date. It is only being provided as a high-level look back at the past six weeks on the main topics covered in each lesson.

**Lesson #1: Ethical Hacking**

* What is computer security?
  + Common Terminology – Vulnerability, Exploit, Threat,
* Computer security principles
  + Process not a product, continual effort
  + Technology, people, environment
* How are we protecting systems?
  + Obscurity
  + Software processes, physical processes,
* Hacking
  + Someone who circumvents computer security and uses their resourcefulness to solve problems.
* Why do we need computer security?
  + Risks: loss of hardware, software, disruption of service, information, money
* Confidentiality, Integrity and Availability

**Lesson #2: The Cybersecurity Landscape**

* Terminology
  + Vulnerability, Exploit, Threat, Attack
* Security Elements
  + Authentication, Authorization, and Auditing
* Classifying Attacks
  + Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege,
* Network Infrastructure Attacks
  + Sniffing, ARP Spoofing, Man-in-the-Middle, SYN Flood, DDOS, Eavesdropping,
* Application Attacks
  + Code injection attacks, Race conditions
* Web Application Attacks
  + SQL Injection, Cross Site Scripting, Parameter Manipulation, Phishing

**Lesson #3: Malware & Injections**

* + Malware
    - Backdoors, Botnets, Downloaders
    - Information stealing, launchers, rootkits
    - Scareware, Ransomware, Spam-Sending, Worms / Virus', Trojan Horse, Blended
    - Targets: Mass malware, targeted malware
  + Malware Analysis
    - Focus on key features, try more than one tool – Malware is constantly improving
    - Static Analysis – view Malware without looking at its code
    - Dynamic Analysis – execute the Malware and monitor its effects
  + PHP Injection
    - Application level vulnerability – attack through PHP code
  + SQL Injection
    - Possibilities: add new data, modify data, gain access to a user's system capabilities.
    - Defence: Use prepared statements written in PHP with bound variables, filter input, no sweeping privileges, datatype parameters, encrypt sensitive data, configure database error reporting

**Lesson #4: The Confidentiality, Integrity and Availability Framework**

* + Confidentiality
    - What is Confidentiality?
    - Failures in Confidentiality
    - Controlling Confidentiality
  + Integrity
    - What is Integrity?
    - Failures in Integrity
    - Controlling Integrity
  + Availability
    - What is Availability?
    - Failures in Availability
    - Controlling Availability

**Lesson #5: Encryption**

* + Symmetric key encryption
    - DES, AES
  + Asymmetric key encryption
    - Public Key Encryption - RSA
  + Public Key Infrastructure (PKI)
  + Hybrid approach
  + Digital signatures
    - Opposite of Public Key Encryption
  + Network security threats:
    - Interruption
    - Interception
    - Modification
    - Fabrication
    - Passive attacks – prevented by using encryption
    - Active attacks
* End to End Encryption vs. Link Encryption
* Key Exchange
* Certificates
* Digital Signatures

**Lesson #6: Encryption**

* + Digital Signatures
  + Certificates
    - Certificate Lifecycle
  + Key Exchanges
    - Diffie-Hellman Key Exchange