## Course Competency

### Competency 1: The student will demonstrate an understanding of key electronic security terminology and techniques by:

1. Identifying the necessary components to ensure a system is secure (i.e. confidentiality, integrity, and availability).
2. Defining the principle of easiest penetration and its implications on secure design.
3. Identifying and providing examples of the four primary threats that all attacks can be categorized into (i.e. interception, interruption, modification, and fabrication).
4. Enumerating the three requirements for any attack to occur (i.e. method, opportunity, and motive).
5. Comparing and contrasting the three primary goals of computer security (i.e. confidentiality, integrity, and availability) and explaining why there is often a trade off in implementing these goals.
6. Identifying the primary vulnerabilities within hardware, software, and data.
7. Enumerating the most common types of computer criminals (i.e. amateurs, crackers/hackers, career criminals, governments and terrorists).
8. Enumerating the methods of defense (i.e. prevent, deter, deflect, detect, and recover).
9. Identify and use professional terminology and hacker slang.
**Competency 2:** The student will demonstrate an understanding of elementary cryptography by:

1. Demonstrating a basic understanding of binary representations of data.
2. Defining key terminology used in cryptography (e.g. plaintext, ciphertext, keys, cipher, encipher, cryptosystem, cryptanalysis, etc).
4. Describing, implementing and using a basic substitution cipher (e.g. Caesar cipher).
5. Describing, implementing and using a basic permutation cipher (e.g. Caesar cipher).
6. Explaining why one-time pads are considered to have perfect, unbreakable encryption as well as why they are difficult to implement.
7. Enumerating and explaining Shannon’s five characteristics of “good ciphers”.
8. Enumerating the properties required of “trustworthy encryption systems”.
9. Defining, comparing, and contrasting the difference between confusion and diffusion.
10. Defining, comparing, and contrasting the difference between stream ciphers and block ciphers.
11. Using cryptoanalytic techniques to break simple substitution and permutation ciphers.
12. Defining the purpose of and using hashing algorithms (e.g. MD5, SHA, etc).

**Competency 3:** demonstrate an understanding of symmetrical encryption by:

- **Critical thinking**
- **Information Literacy**

1. Describing the environment that led to the development of the Data Encryption Standard (DES).
2. Identifying and explaining the purpose of each stage of the DES algorithm.
3. Explaining why the input and output permutation in DES do not improve the security.
4. Enumerating the weaknesses of the DES algorithm.

*Updated Spring 2021*
5. Explaining how 3DES mitigates some of the inherent flaws of the DES algorithm, as well as why 2DES would not have been sufficient.
6. Using the DES algorithm to encrypt a data file.
7. Describing the environment that led to the development of the Advanced Encryption Standard (AES).
8. Comparing and Contrasting the DES and AES algorithms.
9. Using the DES and AES algorithms to encrypt and decrypt data.

**Competency 4:** The student will demonstrate an understanding of asymmetrical encryption by:

- Information Literacy

| 1. Identifying the inherent difficulties with symmetric encryption and explaining how asymmetric encryption helps to mitigate those difficulties.  
| 2. Describing the steps required to perform the Rivest, Shamir, Adleman (RSA) encryption algorithm.  
| 3. Using the RSA algorithm to encrypt and decrypt data.  
| 4. Describing a key exchange algorithm or protocol (e.g. Diffie-Hellman).  
| 5. Defining, explaining, and using common hashing functions such as MD5/SHA.  

**Competency 5:** The student will demonstrate an understanding of networking and computer security basics by:

- Critical thinking
- Information Literacy

| 1. Describing the difference between local and wide area networks.  
| 2. Performing packet level inspection using a tool such as Wireshark.  
| 3. Performing basic network forensics using tools such as IPCnf, Ping, Tracerout, Netstat, and NSLookup.  
| 4. Exploring common intrusion detection systems.  
| 5. Defining and identifying distributed denial of service attacks.  
| 6. Identifying and employing methods of active and passive scanning (e.g. nmap).  

Updated Spring 2021
<table>
<thead>
<tr>
<th><strong>Competency 6:</strong> The student will demonstrate an understanding of program level security by:</th>
<th></th>
<th>Information Literacy</th>
</tr>
</thead>
</table>
| 1. Identifying early methods of preventative program security including penetrate and patch and tiger teams and their inherent flaws.  
2. Define, describe, and identify the various forms of non-malicious program errors within a code sequence (e.g. buffer overflow, string injection, time of check / time of use, incomplete mediation, etc).  
3. Enumerate, Compare and Contrast the different forms of malicious code (e.g. Virus, Trojan Horse, Logic Bomb, Time Bomb, Trapdoor, Worm, Rabbit, etc).  
4. Describe the attack vectors that can take place after a program is compromised (e.g. shellcode injection, variable dumping, etc). |  |  |

<table>
<thead>
<tr>
<th><strong>Course Competency 7:</strong> The student will demonstrate an understanding of legal and ethical issues related to electronic security by:</th>
<th></th>
<th>Information Literacy</th>
</tr>
</thead>
</table>
| 1. Identify ethical, professional responsibilities, risks and liabilities in electronic, computer, and network environments.  
2. Describing mandatory access control and how covert channels can be used to subvert such control.  
3. Defining and Describing the Orange Book and its successors.  
5. Discussing the impact of emerging technologies such as RFID, electronic voting, and VOIP.  
6. Presenting or debating a case study of an ethical dilemma related to electronic security and/or privacy. |  |  |

<table>
<thead>
<tr>
<th><strong>Course Competency 8:</strong> The student will demonstrate an ability to interpret and present research in the area of electronic security by:</th>
<th></th>
<th>Information Literacy</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Describing the latest developments in computer and network security.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Updated Spring 2021
2. Locating, reading, and presenting a recent journal or conference paper presented at an IEEE or ACM accepted conference.
3. Presenting or debating a case study on electronic security (e.g. industrial espionage, cyberterrorism and information warfare, or weapons of cyber warfare).