



This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the [Creative Commons Attribution 3.0 Unported License](http://creativecommons.org/licenses/by/3.0/deed.en_US).

Authoring Organization: Moraine Valley Community College

Written by: Susan Sands

Copyright: © National Information Security, Geospatial Technologies Consortium (NISGTC)

Development was funded by the Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48; The National Information Security, Geospatial Technologies Consortium (NISGTC) is an entity of Collin College of Texas, Bellevue College of Washington, Bunker Hill Community College of Massachusetts, Del Mar College of Texas, Moraine Valley Community College of Illinois, Rio Salado College of Arizona, and Salt Lake Community College of Utah.

This workforce solution was funded by a grant awarded by the U.S. Department of Labor's Employment and Training Administration. The solution was created by the grantee and does not necessarily reflect the official position of the U.S. Department of Labor. The Department of Labor makes no guarantees, warranties or assurances of any kind, express or implied, with respect to such information, including any information on linked sites, and including, but not limited to accuracy of the information or its completeness, timeliness, usefulness, adequacy, continued availability or ownership.

**IT Security Essentials Syllabus**

Please provide a complete syllabus. All elements of the syllabus are required unless noted as “if applicable.”

|  |  |
| --- | --- |
| **Course Title:** IT Security Essentials (Security+) | **Course Number** (If applicable): LAN-153 |
| **COURSE DESCRIPTION:** This course introduces the basic principles of network security. The student will be introduced to computer network vulnerabilities and threats and how to safeguard computer networks from those vulnerabilities and threats. This course will expose the student to network security planning, network security technology, network security organization and the legal and ethical issues associated with network security. This course is designed to prepare the successful student for the CompTIA Security+ certification.  |
| **PREREQUISITES:** Basic Networking knowledge or consent of instructor |
| **REQUIRED MATERIALS: None** |
| **ADDITIONAL RESOURCES** (if applicable): |
| **LEARNING OUTCOMES/COMPETENCIES:****Computer Network Defense**1. Knowledge of access authentication methods. (CND8)
2. Knowledge of basic system, network, and operating system hardening techniques. (CND13)
3. Knowledge of data backup, types of backups (e.g., full, incremental), and recovery concepts and tools. (CND29)
4. Knowledge of incident response and handling methodologies. (CND61)
5. Knowledge of Information Assurance principles and tenets (confidentiality, integrity, availability, authentication, non-repudiation). (CND63)
6. Knowledge of network security architecture, including the application of Defense-In-Depth principles. (CND85)
7. Knowledge of network traffic analysis methods. (CND87)
8. Knowledge of security management. (CND110)
9. Knowledge of VPN security. (CND148)
10. Knowledge of what constitutes a "threat" to a network. (CND150
11. Knowledge of common network tools (e.g., ping, traceroute, nslookup, etc.). (CND271)
12. Skill in recognizing and categorizing types of vulnerabilities and associated attacks. (CND895)
13. Skill in using network analysis tools to identify vulnerabilities. (CND922)
14. Risk
15. Knowledge of Computer Network Defense tools, including open source tools, and their capabilities. (CND19)
16. Knowledge of cryptology. (CND27)
17. Knowledge of system administration concepts for Unix/Linux and/or Windows operating systems. (CND122)
18. Skill in performing packet-level analysis (e.g., Wireshark, tcpdump, etc.). (CND214)
19. Skill in using protocol analyzers. (CND233)
20. Knowledge of unix command line (e.g., mkdir, mv, ls, passwd, grep, etc.). (CND342)
21. Knowledge of windows command line (e.g., ipconfig, netstat, dir, nbstat, etc.). (CND347)

**Data Administration**1. Knowledge of data administration and data standardization policies and standards. (DA28)
2. Knowledge of network access and authorization (e.g., public key infrastructure). (DA79)
3. Knowledge of operating systems. (DA90)
4. Knowledge of the characteristics of physical and virtual data storage media. (DA137)
5. Perform backup and recovery of databases to ensure data integrity. (DA740)
6. Knowledge of data backup, types of backups (e.g., full, incremental), and recovery concepts and tools. (DA29)

**Digital Forensics**1. Knowledge of critical protocols (e.g., IPSEC, AES, GRE, IKE. MD5, SHA, 3DES). (DR25)
2. Knowledge of data backup, types of backups (e.g., full, incremental), and recovery concepts and tools. (DF29)
3. Knowledge of network architecture concepts including topology, protocols, and components. (DF80)
4. Skill in analyzing malware. (DF153)
5. Knowledge of Laws that affect cybersecurity (e.g., Wiretap Act, Pen/Trap and Trace Statue, Stored Electronic Communication Act). (DF305)
6. Knowledge of system administration concepts for Unix/Linux and/or Windows operating systems. (DF122)

**Incident Response**1. Knowledge of network architecture concepts including topology, protocols, and components. (IR80)
2. Knowledge of packet-level analysis. (IR93)
3. Knowledge of what constitutes a "threat" to a network. (IR150)
4. Skill in analyzing malware. (IR153)
5. Knowledge of basic system, network, and operating system hardening techniques. (IR13)
6. Knowledge of data backup, types of backups (e.g., full, incremental), and recovery concepts and tools. (IR29)

**Network Services**1. Develop and implement network backup and recovery procedures. (NS522)
2. Knowledge of remote access technology concepts. (NS106)
3. Skill in implementing, maintaining, and improving established security practices. (NS205)
4. Skill in configuring and utilizing software-based computer protection tools (e.g. software firewalls, anti-virus software, anti-spyware). (NS892)
5. Knowledge of IA principles. (NS55)
6. Knowledge of IT security principles and methods, such as firewalls, demilitarized zones, and encryption. (NS70)
7. Knowledge of systems administration concepts. (NS127)
8. Skill in protecting a network against malware. (NS896)
9. Knowledge of wireless fidelity (WIFI). (NS903)
 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **COURSE ASSESSMENT:** **Grading Scale**

|  |  |
| --- | --- |
| **Category** | **Weight** |
| Labs | 50 |
| Quizzes | 35 |
| Final Exam | 15 |
|  |  |
| **Final Grade** | **100%** |

|  |  |  |
| --- | --- | --- |
| **Total Points** | **Percentage** | **Grade** |
| 368-400 | 92-100 | A |
| 340-367 | 85-91 | B |
| 308-339 | 77-84 | C |
| 276-307 | 69-76 | D |
| 0-275 | 0-68 | F |

  |

**COURSE SCHEDULE:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lesson** | **Module/Lesson Title & description** (if applicable) | **Learning Objectives** | **Assignment (w/category & point value)** |
|  | General Concepts | * Identify the concepts of confidentiality, integrity and availability.
* Perform packet level analysis.
 | General Security Concepts Quiz (5 pts.)Lab 1 – Capturing Network Traffic |
|  | Network FundamentalsInfrastructure Security | * Explain the security function and purpose of network devices and technologies.
* Implement secure network administration principles.
* Differentiate network design elements and compounds.
* Use common protocols to employ infrastructure security.
* Identify commonly used default network ports.
 | Network Fundamentals and Infrastructure Sec Quiz (15 pts.)Lab 2 – Log AnalysisLab 3 – Transferring Data Using TCP/IP |
|  | IDS Wireless Security  | * Explain the security function and purpose of network devices and technologies.
* Apply secure network administration principles.
* Implement a wireless network in a secure manner.
 | IDS and Network Security Quiz (5 pts.)Wireless Security Quiz (5pts)Lab 4 – Connecting to a Remote SystemLab 5 – Secure Implementation of Wireless Networking |
|  | Role of People in Security Operational and Organizational Security  | * Explain the importance of security related awareness and training.
 | Role of People/Operation Security Quiz (10 pts.)Lab 6 – Incident Response Procedure |
|  | Risk Management  | * Explain risk related concepts.
* Apply appropriate risk mitigation strategies.
 | Risk Management Quiz (10 pts.)Lab 7 – Vulnerability and Risk Assessment |
|  | Change Management DR, BC, and Organizational Policies  | * Compare aspects of business continuity.
* Execute disaster recovery plans and procedures.
 | DR/Change Mgmt. Quiz (10 pts.)Lab 8 – Information Storage and Backup |
|  | Physical Security   | * Explain the impact of physical security on computer and network security.
* Explain the impact and proper use of environmental controls.
 | Physical Security Quiz (5 pts.) Legal, Ethics and Privacy Quiz (15 pts.) |
|  | Forensics Legal Issues Privacy | * Apply appropriate incident response procedures.
* Identify the various laws that affect cybersecurity.
 | Forensics Quiz (5 pts.) Legal, Ethics and Privacy Quiz (15 pts.)Lab 9 – Anti-Forensic |
|  | Attacks  | * Identify the different types of malware that exist.
* Describe computer attacks.
 | Attacks Quiz (5 pts.)Lab 10 – Analyze and Differentiate Types of Malware Lab 11 – Using Windows Commands |
|  | Network Attacks  | * Identify different types of network attacks.
* Use assessment tools to discover security threats and vulnerabilities
 | Network Attacks Quiz (5 pts.)Lab 12 – Discovering Security Threats and Vulnerabilities |
|  | Baselines Secure Software Development  | * Explain the importance of application security.
* Carry out appropriate procedures to establish host security.
* Explain the importance of data security.
 | Secure Software Development Baselining Quiz (10 pts.)Lab 13 – Data TheftLab 14 – Securing Data Using Encryption Software |
|  | Email and IM Web Components  | * Describe security issues associated with Email and Instant Messaging.
* Explain web applications, plug-ins, and related security issues.
* Explain web-based application security issues.
 | Email/Web Components Quiz (10 pts.)Lab 15 – Analyze and Differentiate Types of Application Attacks |
|  | Authentication and Remote Access  | * Explain the function and purpose of authentication services.
* Explain the fundamental concepts and best practices related to authentication.
* Identify the methods and protocols used for remote access to networks.
 | Remote Access Quiz (10 pts.)Lab 16 – Password Cracking Lab 17 – Authentication, Authorization and Access Control |
|  | Access Control Privilege Management  | * Explain the fundamental concepts and best practices related to authorization and access control.
* Implement appropriate security controls when performing account management.
 | Access Control Quiz (5 pts.)Lab 18 – Access Control/Audit |
|  | Cryptography  | * Summarize general cryptography concepts.
* Apply appropriate cryptographic tools and products.
 | Cryptography Quiz (5 pts.)Lab 19 – General Cryptography Concepts |
|  | Public Key Infrastructure  | * Explain the core concepts of public key infrastructure.
* Implement Public Key Infrastructure (PKI), certificate management and associated components.
 | PKI Quiz (5 pts.)Lab 20 – Cryptography in Information Assurance |
|  | Final Exam |  | Final Exam (60 pts.) |