

[Creative Commons License](http://creativecommons.org/licenses/by/3.0/deed.en_US)

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.

**Network Security Syllabus**

|  |  |
| --- | --- |
| **Course Title: Network Security: Overview, Device Hardening, Remote Access, and Authentication** | **Course Number** (If applicable): **LAN253AA** |
| **COURSE DESCRIPTION:** LAN253AA is a Network Security Course that focuses on an overview of network security, device hardening, secure remote access, and Authentication Services.  **NOTE:** This is the first of a series of three courses (LAN253AA Network Security: Overview, Device Hardening, Remote Access, and Authentication, LAN253AB Network Security: Perimeter Security, Firewalls, and Intrusion Prevention, and LAN253AC Network Security: VPN, Securing LAN, and IPV6) which introduces core concepts and skills necessary to design, implement, and manage the security of network data and devices. Students will utilize critical thinking and problem solving skills to develop an in-depth theoretical and practical understanding of network security principles. After successfully completing the series of courses, students should be able to design, implement and maintain security policies in a network infrastructure. There is a “Final Exam” to assess student learning across the three courses (LAN253AA, LAN253AB, LAN253AC) occurs at the end of this course which is the summative assessment of the series of three 3 courses. | |
| **PREREQUISITES:** LAN153 | |
| **REQUIRED MATERIALS:**  None | |
| **ADDITIONAL RESOURCES** (if applicable): | |

|  |  |
| --- | --- |
| **LEARNING OUTCOMES/COMPETENCIES:** | |
|  | **Computer Network Defense** |
| 433 | Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources |
| 750 | Perform event correlation using information gathered from a variety of sources within the enterprise to gain situational awareness and determine the effectiveness of an observed attack |
| 26 | Knowledge of cross-domain guards |
| 27 | Knowledge of cryptology |
| 61 | Knowledge of incident response and handling methodologies |
| 66 | Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions via intrusion detection technologies |
| 85 | Knowledge of network security architecture, including the application of Defense-In-Depth principles |
| 229 | Skill in using incident handling methodologies |
| 895 | Skill in recognizing and categorizing types of vulnerabilities and associated attacks |
| 922 | Skill in using network analysis tools to identify vulnerabilities |
|  | **Data Administration** |
| 90 | Knowledge of operating systems |
| 98 | Knowledge of policy-based and risk adaptive access controls |
|  | **Digital Forensics** |
| 61 | Knowledge of incident response and handling methodologies |
|  | **Incident Response** |
| 438 | Collect and analyze intrusion artifacts (e.g., source code, malware, and trojans) and use discovered data to enable mitigation of potential Computer Network Defense incidents within the enterprise |
| 474 | Coordinate with intelligence analysts to correlate threat assessment data |
| 478 | Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation |
| 738 | Perform analysis of log files from a variety of sources (e.g., individual host logs, network traffic logs, firewall logs, and intrusion detection system logs) to identify possible threats to network security |
| 861 | Track and document Computer Network Defense incidents from initial detection through final resolution |
| 13 | Knowledge of basic system, network, and operating system hardening techniques |
| 49 | Knowledge of host/network access controls (e.g., access control list) |
| 50 | Knowledge of how network services and protocols interact to provide network communications |
| 893 | Skill in securing network communications |
| 896 | Skill in protecting a network against malware |
|  | **Network Services** |
| 736 | Patch network vulnerabilities to ensure information is safeguarded against outside parties. |
| 829 | Repair network connectivity problems |
| 857 | Test and maintain network infrastructure including software and hardware devices |
| 106 | Knowledge of remote access technology concepts |
| 127 | Knowledge of systems administration concepts |
| 893 | Skill in securing network communications |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **COURSE ASSESSMENT:**   |  |  | | --- | --- | | **Category** | **Weight** | | Quizzes | 30 | | Labs | 55 | | Final Exam | 15 | | **Final Grade** | **100%** |   **Grading Scale**   |  |  | | --- | --- | | **Percentage** | **Grade** | | 92 - 100 | A | | 85 -91 | B | | 77 - 94 | C | | 70 -76 | D | | 69 | F | |

**COURSE SCHEDULE:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Module** | **Module Title** | **Learning Outcomes** | **Assignment** |
| 1 | Overview of Network Security | 1. Identify the rationale for network security. 2. Identify the three principles of security. 3. Identify risks, threats, vulnerabilities and countermeasures. 4. Identify administrative, technical and physical security controls. 5. Identify network attacks that affect the confidentiality, integrity, or availability of network resources. 6. Identify the steps for compromising targets 7. Differentiate between security policies, standards and guidelines. | Quiz  Lab 1 – Configuring a Windows-Based Firewall to Allow Incoming Traffic |
| 2 | Device Hardening | 1. Identify common procedures to harden network devices. 2. Identify procedures to secure a router. 3. Identify the types of Rootkits. 4. Demonstrate the use of tools that identify system and device vulnerabilities. 5. Demonstrate the implementation of automated and one-step commands and tools. | Quiz  Lab 2 – Implementing Secure DHCP and DNS |
| 3 | Secure Remote Access | 1. Identify the characteristics of using Secure Shell (SSH) for remote access. 2. List the steps required to configure a router with SSH. 3. Identify the components involved in system logging. 4. Describe remote administration software. 5. Discuss security concerns with bring your own device (BYOD). | Quiz  Lab 3 – Configuring a Linux-Based Firewall to Allow Outgoing Traffic |
| 4 | Authentication Services | 1. Identify the purpose of authentication, authorization, and accounting (AAA) and the various implementation techniques. 2. Identify the purpose of RADIUS. 3. Configure RADIUS. 4. Configure a remote access policy to use Active Directory to authenticate VPN clients. 5. Differentiate the operation of local workstation authentication versus server-based authentication for both Windows and Linux. | Quiz  Lab 4 – Configuring RADIUS |