

[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: Perimeter Security, Firewalls, and Intrusion Prevention** | **Course Number** (If applicable): LAN253AB |
| **COURSE DESCRIPTION:** LAN253AB is a Network Security Course that focuses on perimeter security access control lists (ACLs), firewalls, and intrusion prevention.  **NOTE**: This is the second 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:** LAN253AA | |
| **REQUIRED MATERIALS:**  None | |
| **ADDITIONAL RESOURCES** (if applicable): | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **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 | |

|  |  |
| --- | --- |
| **LEARNING OUTCOMES/COMPETENCIES:** | |
|  | **Computer Network Defense** |
| 427 | Assist in the construction of signatures which can be implemented on Computer Network Defense network tools in response to new or observed threats within the enterprise. |
| 433 | Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources |
| 472 | Coordinate with enterprise-wide Computer Network Defense staff to validate network alerts |
| 716 | Monitor external data sources (e.g., Computer Network Defense vendor sites, Computer Emergency Response Teams, SANS, Security Focus) to maintain currency of Computer Network Defense threat condition and determine which security issues may have an impact on the enterprise |
| 723 | Notify Computer Network Defense managers, Computer Network Defense incident responders, and other Computer Network Defense Service Provider team members of suspected Computer Network Defense incidents and articulate the event’s history, status, and potential impact for further action |
| 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 |
| 823 | Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts |
| 26 | Knowledge of cross-domain guards |
| 49 | Knowledge of host/network access controls (e.g., access control list) |
| 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 |
| 115 | Knowledge of signature development |
| 175 | Skill in developing / deploying signatures |
| 229 | Skill in using incident handling methodologies |
| 895 | Skill in recognizing and categorizing types of vulnerabilities and associated attacks |
|  | **Data Administration** |
| 98 | Knowledge of policy-based and risk adaptive access controls |
|  | **Digital Forensics** |
| 61 | Knowledge of incident response and handling methodologies |
|  | **Incident Response** |
| 470 | Coordinate with and provide expert technical support to enterprise-wide Computer Network Defense technicians to resolve Computer Network Defense incidents |
| 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 |
| 686 | Maintain deployable Computer Network Defense toolkit (e.g., specialized Computer Network Defense software/hardware) to support incident response team mission |
| 716 | Monitor external data sources (e.g., Computer Network Defense vendor sites, Computer Emergency Response Teams, SANS, Security Focus) to maintain currency of Computer Network Defense threat condition and determine which security issues may have an impact on the enterprise |
| 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 |
| 823 | Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts |
| 861 | Track and document Computer Network Defense incidents from initial detection through final resolution |
| 49 | Knowledge of host/network access controls (e.g., access control list) |
| 229 | Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions via intrusion detection technologies (IR 66) Skill in using incident handling methodologies |
| 893 | Skill in securing network communications |
| 896 | Skill in protecting a network against malware |
|  | **Network Services** |
| 891 | Skill in configuring and utilizing hardware-based computer protection tools (e.g., hardware firewalls, servers, routers) |

**COURSE SCHEDULE:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Module** | **Module Title** | **Learning Outcomes** | **Assignment** |
| 1 | Perimeter Security Access Control Lists (ACL’s) | 1. Identify the various types of Access Control Lists (ACLs). 2. Identify ACL configuration guidelines. 3. Configure ACLs. 4. Identify the attacks that ACLs are used to mitigate. | Quiz  Lab - Configuring Access Control Lists on a Linux-Based Firewall |
| 2 | Firewalls | 1. Define firewalls. 2. Identify the need for firewalls. 3. Identify the types of firewalls. 4. Determine the best placement for a firewall. 5. Construct examples of common firewall rules. 6. Configure firewall rules using iptables. | Quiz  Lab - Configuring a Linux-Based Firewall to Allow Incoming and Outgoing Traffic |
| 3 | Intrusion Prevention | 1. Describe the purpose and operation of network-based and host-based Intrusion Prevention Systems (IPS). 2. Detect malicious network traffic with IDS and IPS signatures. 3. Use Snort to analyze network traffic. 4. Write custom rules to detect certain network traffic. | Quiz  Lab – Intrusion Detection Using Snort  Lab - Writing Custom Rules |