



Prepared by:

*[Learner first and last name]*

[Manual Overview 4](#_Toc488063812)

[Manual Layout 4](#_Toc488063813)

[Executive Summary and Purpose 5](#_Toc488063814)

[0.1 Executive Summary 5](#_Toc488063815)

[0.2 Purpose of This Manual 5](#_Toc488063816)

[Section One: Traffic Analysis 6](#_Toc488063817)

[1.1 Significance of Traffic Analysis 6](#_Toc488063818)

[1.2 Traffic Analysis Tools and Methodology 6](#_Toc488063819)

[Section Two: Firewalls 7](#_Toc488063820)

[2.1 Significance of Firewalls 7](#_Toc488063821)

[2.2 Firewall Tools and Methodology 7](#_Toc488063822)

[Section Three: Intrusion Detection and Prevention 8](#_Toc488063823)

[3.1 Significance of Intrusion Detection and Prevention Systems (IDPS) 8](#_Toc488063824)

[3.2 IDPS Tools and Methodology 8](#_Toc488063825)

[Section Four: Vulnerability Assessment 9](#_Toc488063826)

[4.1 Significance of Vulnerability Assessment 9](#_Toc488063827)

[4.2 Vulnerability Assessment Tools and Methodology 9](#_Toc488063828)

[Section Five: Network Scanning and Assessment 10](#_Toc488063829)

[5.1 Significance of Network Scanning and Assessment 10](#_Toc488063830)

[5.2 Network Scanning and Assessment Tools and Methodology 10](#_Toc488063831)

[Section Six: Auditing and Log Collection 11](#_Toc488063832)

[6.1 Significance of Auditing and Log Collection 11](#_Toc488063833)

[6.2 Auditing and Log Collection Tools and Methodology 11](#_Toc488063834)

[Section Seven: Tools Used 12](#_Toc488063835)

[7.1 A Brief Overview of Tools Used in This Manual 12](#_Toc488063836)

[Section Eight: References 13](#_Toc488063837)

# Manual Overview

You work for Strategic Security Consulting Group (SSCG). Recently, one of your clients in Los Angeles, North Star Software Developers (NSSD), called with a big problem. Some of its network servers were compromised, resulting in the possible loss of personal information and credit card numbers of purchasers of the company’s software products. It is not presently known whether this attack came from inside or outside of the company. NSSD is currently dealing with this problem as best as it can, but it needs your company to help prevent this from happening again in the future.

You have been assigned to create a training manual for NSSD’s IT personnel in which you test, describe, and recommend a variety of network security tools that, when used properly, will mitigate both the risk of future breaches and the effects of a breach when it takes place.

# Manual Layout

There are seven sections of the manual that cover all the components of a training manual designed to teach employees how to lessen the risk of a security breach and mitigate the effects of a breach should one happen. As the training manager, you must complete each section using information you learned in this course. Refer to the background information on North Star Software Developers (NSSD) and apply the appropriate tools and methods that will help the company defend its network against attacks and detect intrusions, anomalies, and vulnerabilities. Apply best practices of network defense and countermeasures from your research and hands-on lab activities. The following are the main sections of the manual you are responsible for completing:

1. Executive Summary and Purpose
2. Traffic Analysis
3. Firewalls
4. Intrusion Detection and Prevention
5. Vulnerability Assessment
6. Network Scanning and Assessment
7. Auditing and Log Collection
8. Summary of Tools
9. References

Delete all prompts containing the following language prior to submitting this section:

Delete this prompt language when you are finished writing your response.

# Executive Summary and Purpose

|  |
| --- |
| 0.1 Executive Summary Provide an overview of the company (North Star Software Developers), its current issues and concerns, and your role in helping with these problems. Delete this prompt language when you are finished writing your response. |

|  |
| --- |
| 0.2 Purpose of This Manual Explain the **purpose** **of this manual**. Why is it important that information technology employees at NSSD apply the principles and practices described in this manual? What is at stake if they do not appropriately apply their training and provide high-quality defense and mitigation strategies to the NSSD network? Delete this prompt language when you are finished writing your response. |

Delete all prompts containing the following language prior to submitting this section:

Delete this prompt language when you are finished writing your response.

# Section One: Traffic Analysis

|  |
| --- |
| 1.1 Significance of Traffic Analysis Explain the significance of **traffic analysis** as a core activity of network defense and cybersecurity. Be sure to define the term and use specific details and examples to illustrate its meaning in a business context. Discuss some best practices in the area of traffic analysis based on your research and lab activities. Delete this prompt language when you are finished writing your response. |

|  |
| --- |
| 1.2 Traffic Analysis Tools and Methodology  1. Provide a brief summary of the key company-approved tools, represented by those used in the lab exercises. In your summary, identify the importance of and rationale for selecting these tools. 2. Discuss how the tools work to analyze traffic on the network. Offer some examples. 3. Provide screenshots from the labs illustrating tool configuration and outputs.   Delete this prompt language when you are finished writing your response. |

Delete all prompts containing the following language prior to submitting this section:

Delete this prompt language when you are finished writing your response.

# Section Two: Firewalls

|  |
| --- |
| 2.1 Significance of Firewalls Explain the significance of **firewalls** as a core tenet of network defense and cybersecurity. Be sure to define the term and use specific details and examples to illustrate its meaning in a business context. Based on your research and lab activities, discuss some best practices in the area of usage and configuration. Delete this prompt language when you are finished writing your response. |

|  |
| --- |
| 2.2 Firewall Tools and Methodology  1. Provide a brief summary of the key company-approved tools, represented by those used in the lab exercises. In your summary, identify the importance of and rationale for selecting these tools. 2. Discuss how the tools work to protect the network. Offer some examples. 3. Provide screenshots from the labs illustrating tool configuration and outputs.   Delete this prompt language when you are finished writing your response. |

Delete all prompts containing the following language prior to submitting this section:

Delete this prompt language when you are finished writing your response.

# Section Three: Intrusion Detection and Prevention

|  |
| --- |
| 3.1 Significance of Intrusion Detection and Prevention Systems (IDPS) Explain the significance of **intrusion detection and prevention** as a core activity of network defense and cybersecurity. Be sure to define the term and use specific details and examples to illustrate its meaning in a business context. Discuss the key functions of IDPS technologies. Discuss some best practices in the area of intrusion detection and prevention based on your research and lab activities. Delete this prompt language when you are finished writing your response. |

|  |
| --- |
| 3.2 IDPS Tools and Methodology  1. Provide a brief summary of the key company-approved tools, represented by those used in the lab exercises. In your summary, identify the importance of and rationale for selecting these tools. 2. Discuss how the tools work to detect intrusions on the network. Offer some examples. 3. Provide screenshots from the labs illustrating tool configuration and outputs.   Delete this prompt language when you are finished writing your response. |

Delete all prompts containing the following language prior to submitting this section:

Delete this prompt language when you are finished writing your response.

# Section Four: Vulnerability Assessment

|  |
| --- |
| 4.1 Significance of Vulnerability Assessment Explain the significance of a **vulnerability assessment** as a core activity of network defense and cybersecurity. Be sure to define the term and use specific details and examples to illustrate its meaning in a business context. Discuss the key functions of vulnerability scanning technologies. Discuss some best practices in the area of vulnerability scanning and assessment based on your research and lab activities. Delete this prompt language when you are finished writing your response. |

|  |
| --- |
| 4.2 Vulnerability Assessment Tools and Methodology  1. Provide a brief summary of the key company-approved tools, represented by those used in the lab exercises. In your summary, identify the importance of and rationale for selecting these tools. 2. Discuss how the tools work to assess vulnerabilities the network. Offer some examples. 3. Provide screenshots from the labs illustrating tool configuration and outputs.   Delete this prompt language when you are finished writing your response. |

Delete all prompts containing the following language prior to submitting this section:

Delete this prompt language when you are finished writing your response.

# Section Five: Network Scanning and Assessment

|  |
| --- |
| 5.1 Significance of Network Scanning and Assessment Explain the significance of **network scanning and assessment** as a core activity of network defense and cybersecurity. Be sure to define the term and use specific details and examples to illustrate its meaning in a business context. Discuss the key functions of network scanning technologies. Discuss some best practices in the area of network scanning and assessment based on your research and lab activities. Delete this prompt language when you are finished writing your response. |

|  |
| --- |
| 5.2 Network Scanning and Assessment Tools and Methodology  1. Provide a brief summary of the key company-approved tools, represented by those used in the lab exercises. In your summary, identify the importance and rationale for selecting these tools. 2. Discuss how the tools work to detect rogue devices and malicious connections on the network. Offer some examples. 3. Provide screenshots from the labs illustrating tool configuration and outputs.   Delete this prompt language when you are finished writing your response. |

Delete all prompts containing the following language prior to submitting this section:

Delete this prompt language when you are finished writing your response.

# Section Six: Auditing and Log Collection

|  |
| --- |
| 6.1 Significance of Auditing and Log Collection Explain the significance of **auditing and log collection** as a core activity of network defense and cybersecurity. Be sure to define the terms and use specific details and examples to illustrate its meaning in a business context. Discuss the key activities of auditing and log collection. Discuss some best practices in the areas of auditing and log collection based on your research and lab activities. Delete this prompt language when you are finished writing your response. |

|  |
| --- |
| 6.2 Auditing and Log Collection Tools and Methodology  * 1. Provide a brief summary of the key company-approved tools, represented by those used in the lab exercises. In your summary, identify the importance of and rationale for selecting these tools.   2. Discuss how the tools work to audit the network and generate reports. Offer some examples.   3. Provide screenshots from the labs illustrating tool configuration and outputs.   Delete this prompt language when you are finished writing your response. |

Delete all prompts containing the following language prior to submitting this section:

Delete this prompt language when you are finished writing your response.

# Section Seven: Tools Used

|  |
| --- |
| 7.1 A Brief Overview of Tools Used in This Manual List all the tools used in this manual with a brief description of each. Delete this prompt language when you are finished writing your response. |

Delete all prompts containing the following language prior to submitting this section:

Delete this prompt language when you are finished writing your response.

# Section Eight: References

|  |
| --- |
| List all references used in the creation of this document here (if applicable). References must be in APA format. Delete this prompt language when you are finished writing your response. |