

**Blue Team Level 1 Certification
(Standard)**

Introduction to Security Fundamentals

1 Topic

Soft Skills

7 Topics

Security Controls

5 Topics 1 Quiz

Networking 101

6 Topics 1 Quiz

Management Principles

4 Topics 1 Quiz

PHISHING ANALYSIS DOMAIN

PA1) Introduction to Emails and Phishing

7 Topics 1 Quiz

PA2) Types of Phishing Emails

10 Topics 2 Quizzes

PA3) Tactics and Techniques Used

12 Topics 2 Quizzes

PA4) Investigating a Phishing Email

8 Topics 2 Quizzes

Section Introduction: Investigating Emails

Artifacts We Need to Collect

Manual Collection Techniques—Email
ArtifactsManual Collection Techniques—Web
ArtifactsManual Collection Techniques—File
Artifacts[Video] Collecting Artifacts—Manual
Methods

Automated Collection With PhishTool

[Video] Collecting Artifacts—Automated
Methods

Lab) Manual Artifact Extraction

Activity) End of Section Review:
Investigating Emails

PA4) Analysis: URLs, Attachments, and

Section Introduction, Investigating Emails

Blue Team Level 1 Certification (Standard) > PA4) Investigating a Phishing Email > Section Introdu...

COMPLETE

Phishing Analysis SECTION INTRODUCTION



This section of the Phishing Analysis domain will cover how phishing investigations take place once an email has been reported as suspicious by the security team or the recipient. This includes retrieving email, web, and file-based artifacts using manual and automated methods so that they can be analyzed at the next stage of the investigation.

LEARNING OBJECTIVES

By the end of this section you will have achieved the following objectives:

- Explain the key email artifacts we need to retrieve from suspect emails, and why we need to record them.
- Retrieve key email artifacts from a reported phishing email using manual techniques via an email client and a text editor.
- Retrieve key artifacts from a reported phishing email using automated techniques using the PhishTool analysis workbench.
- Retrieve and understand why web-based and file-based artifacts are important during investigations where they are present in a phishing email.

[< Previous Lesson](#)[Back to Lesson](#)[Next Topic >](#)