Blue Team Level 1 Certification (Standard)

- ✓ ~~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
- ✓ ~~PA5) Analysing URLs, Attachments, and Artifacts~~
  - ● 8 Topics | 1 Quiz
  - ✓ Section Introduction, Analysing Artifacts
  - ✓ ~~Visualization Tools~~
  - ✓ ~~URL Reputation Tools~~
  - ✓ ~~File Reputation Tools~~
  - ✓ ~~Malware Sandboxing~~
  - ✓ ~~[Video] Manual Artifact Analysis~~
  - ✓ ~~Artifact Analysis With PhishTool~~
  - ✓ ~~[Video] Artifact Analysis with PhishTool~~
  - ⚠ ~~Activity) End of Section Review, Analysing Artifacts~~
- ◐ PA6) Taking Defensive Actions
  - ● 12 Topics | 1 Quiz
- ○ PA7) Report Writing
  - ● 7 Topics | 1 Quiz

Section Introduction, Analysing Artifacts

Blue Team Level 1 Certification (Standard) > PA5) Analysing URLs, Attachments, and Artifacts > Se...   **COMPLETE**

Phishing Analysis
SECTION INTRODUCTION

SBT
BLUE TEAM
LEVEL
1

Now that you understand how to collect email, web, and file-based artifacts, this section will teach you how to analyze them so we can determine if suspicious emails are truly malicious, and gather information which will be useful when it comes to taking defensive measures to protect the business.

LEARNING OBJECTIVES

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

- Perform analysis on URLs to determine their true destination, whether it is malicious, and what type of phishing attack is occurring.
- Perform analysis on attachments to determine if they are malicious, and gather further artifacts for defensive measures and threat intelligence sharing.
- Understand how to use a range of tools including online services and a virtual machine to perform both manual and automated analysis of artifacts.

‹ **Previous Lesson**   **Back to Lesson**   **Next Topic** ›

Privacy & Cookies Policy