

Blue Team Level 1 Certification
(Standard)

Introduction to BTL1

✓ Welcome to Blue Team Level 1!

4 Topics

✓ Lab and Forum Access

SECURITY FUNDAMENTALS DOMAIN

✓ 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 Artifacts

✓ Manual Collection Techniques — Web Artifacts

✓ Manual 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

✓ PA5) Analysing URLs, Attachments, and Artifacts

8 Topics 1 Quiz

PA6) Taking Defensive Actions

12 Topics 1 Quiz

PA7) Report Writing

7 Topics 1 Quiz

PA8) Phishing Response Challenge

3 Topics 1 Quiz

THREAT INTELLIGENCE DOMAIN

TI1) Introduction to Threat Intelligence

7 Topics

TI2) Threat Actors & APTs

Automated Collection With PhishTool

Blue Team Level 1 Certification (Standard) > PA4) Investigating a Phishing Email > Automated Coll...

COMPLETE

Phishing Analysis ARTIFACT COLLECTION, PHISHTOOL



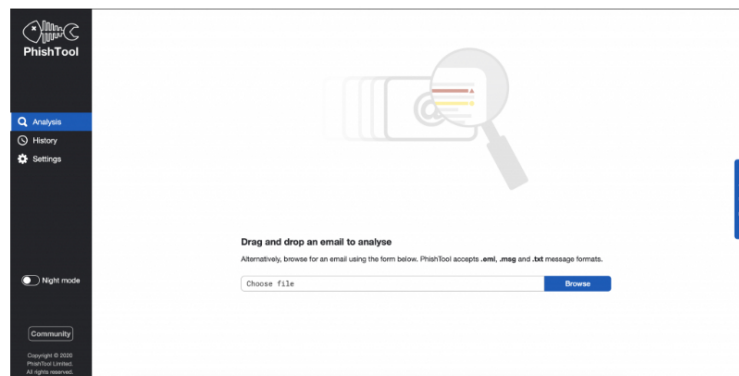
PhishTool provides a forensic analysis console, giving individuals the power to forensically analyze phishing emails, tag malicious artifacts, and generate investigation reports. This incredible platform can do all the heavy-lifting in terms of artifact retrieval and even artifact analysis. This lesson will walk you through how to use the platform to upload phishing emails and generate reports.

ACCOUNT REGISTRATION

You can register for a free Community Edition account over at <https://phishtool.com>. These accounts have a limit on the amount of emails that can be analyzed – but thanks to the great guys at PhishTool, all email FILES included in Blue Team Level 1 have been whitelisted, meaning they will not use up your monthly analysis allowance!

EXAMPLE ONE

On the analysis console homepage, you'll be presented with the view as shown in the below screenshot. This is where we can drag-and-drop a malicious email, or browse of file system and upload it.



In this case, we're going to click the Browse button and find the email we want to submit for analysis. In this case, we're going to upload this Amazon credential harvester!

RE: [Rappel] [New Summary] Request to reset connected password was submitted - Mise à jour et co...



no-reply@amazon <no-reply@email.lanhtaotaiba.com>

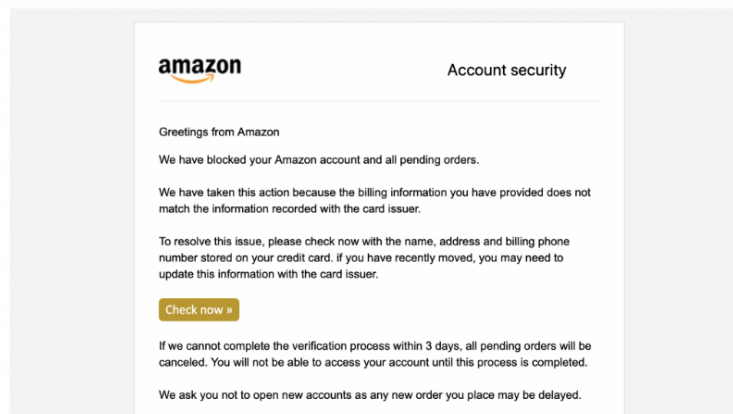
Friday, 24 April 2020 at 17:17

jshgo@hotmail.co.uk

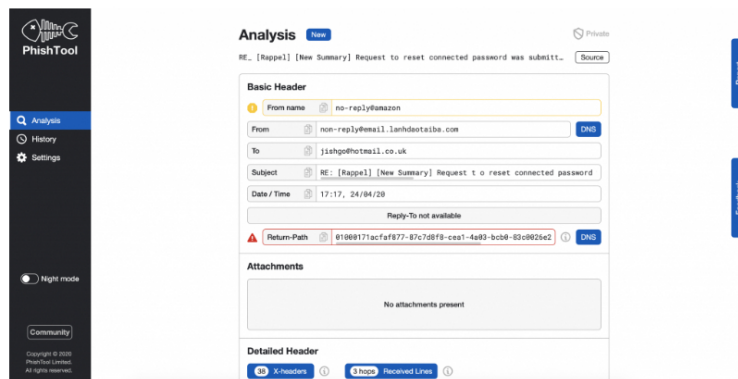
Show Details

You forwarded this message on 29/04/2020, 14:12.

6 Topics 2 Quizzes
TI3) Operational Threat Intelligence
7 Topics 1 Quiz
TI4) Tactical Threat Intelligence
7 Topics 1 Quiz
TI5) Strategic Threat Intelligence
5 Topics 1 Quiz
TI6) Malware and Global Campaigns
6 Topics 1 Quiz
DIGITAL FORENSICS DOMAIN
DF1) Introduction to Digital Forensics
5 Topics
DF2) Forensics Fundamentals
10 Topics 5 Quizzes
DF3) Digital Evidence Collection
8 Topics 1 Quiz
DF4) Windows Investigations
3 Topics 3 Quizzes
DF5) Linux Investigations
4 Topics 2 Quizzes
DF6) Volatility
3 Topics 1 Quiz
DF7) Autopsy
4 Topics 1 Quiz
SECURITY INFORMATION AND EVENT MANAGEMENT DOMAIN
SI1) Introduction to SIEM
7 Topics 1 Quiz
SI2) Logging
6 Topics 2 Quizzes
SI3) Aggregation
2 Topics 1 Quiz
SI4) Correlation
6 Topics 1 Quiz
SI5) Using Splunk
5 Topics 2 Quizzes
INCIDENT RESPONSE DOMAIN
IR1) Introduction to Incident Response
8 Topics 1 Quiz
IR2) Preparation Phase
10 Topics 2 Quizzes
IR3) Detection and Analysis Phase
7 Topics 4 Quizzes
IR4) Containment, Eradication, and Recovery Phase
5 Topics 1 Quiz
IR5) Lessons Learned and Reporting
7 Topics
IR6) MITRE ATT&CK
13 Topics 2 Quizzes
BTL1 EXAM
Exam Preparation
Using RDP and SSH
How to Start Your Exam



Once the analysis has completed, you will see a screen that looks similar to the following screenshot. This page holds all of the results from artifact extraction and analysis procedures. Whilst there is a ton of useful information we can retrieve and fun things we can do, for the scope of this lesson, we are only interested in retrieving artifacts from the email (don't worry, you'll be using PhishTool later for analysis tasks!). You can click the clipboard icon next to artifact names to copy them.



The artifacts we're interested in are:

1. Sending Address
2. Subject Line
3. Recipients
4. Date + Time
5. Sending Server IP
6. Reverse DNS
7. URLs (if applicable)
8. File Name (not applicable)
9. File Hash (not applicable)

So let's gather these from the PhishTool analysis console! In this **Basic Header** section, we will be able to retrieve artifacts **1, 2, 3, and 4**.



Below this there is a section for Detailed Header that includes the X-Originating-IP and the reverse DNS results.

Below this there is a section for **Detailed Header** that includes the A-Originating-IP and the reverse DNS results, which gives us artifacts 5 and 6.

Detailed Header

38 X-headers

3 hops Received Lines

1

Originating IP

54.240.48.44 (Hop 1)

1

IPWHOIS

Reverse DNS

a48-44.smtp-out.amazonses.com

1

And finally down at the bottom we have a section for **URLs**, where we can retrieve all hyperlinks that were included in the email.

URLs

7 URLs

1

'Return-Path' domain: http://amazonses.com

Web capture

WHOIS

http://i.groovehq.com/174a01b3-dc5b-4e36-9573-65f682fdedd2.comment228238286@groovehq.com.gif

http://c.groovehq.com/5379555938.gif

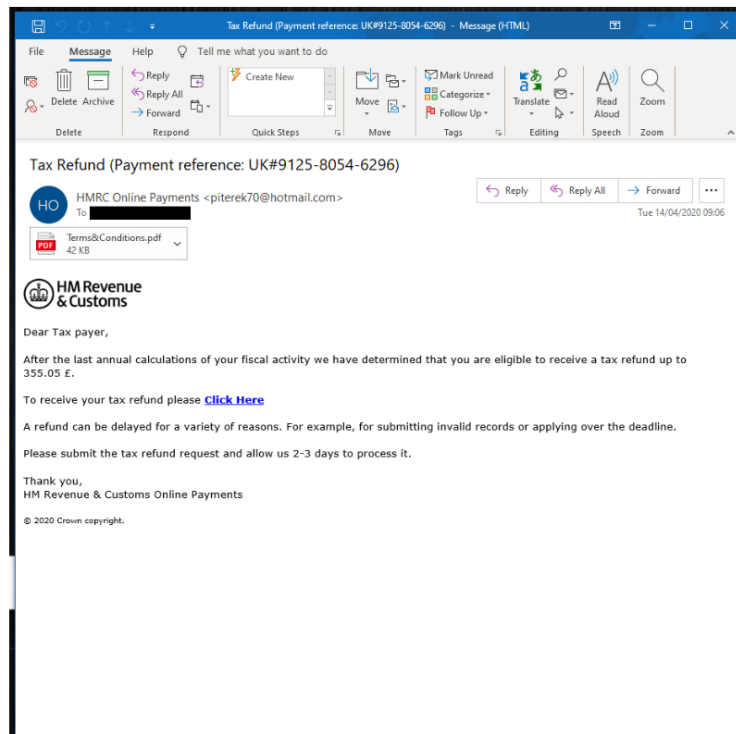
http://d36cz9buwru1tt.cloudfront.net/blank.gif

https://c16.googleusercontent.com/proxy/Xydgq1YSTzY76EJChb1PLYYuu2INTIUaQc_Dh54c96FcmJhA85JLGoaNNHajgIw0ZA...

https://lpsmu.wanguk01.com/7vsFUPQ

EXAMPLE TWO

In this second example we're going to submit an email that has a potentially malicious attachment, so we can show you how to retrieve file-based artifacts using PhishTool. Below is a screenshot of the phishing email we're going to analyze.



After submitting the email to PhishTool, under the Basic Header section there is a section titled **Attachments**. This provides us with the MD5 hash of the file, and the file name! We can also click on the VirusTotal link to automatically submit the hash for analysis and retrieve a community reputation score.

Attachments

CONCLUSION

This lesson has shown that it is able to retrieve email, web, and file-based artifacts all from within the PhishTool Analysis Workbench, making it a faster alternative to manual collection. It is still extremely important to know how to collect indicators manually using a client and text editor, in case you don't have access to PhishTool, such as when investigating analysts do not have an internet connection.

< Previous Topic

Back to Lesson

Next Topic >