

Blue Team Level 1 Certification

Introduction to BTL1

- ✓ Welcome to Blue Team Level 1:
 - 4 Topics

SECURITY FUNDAMENTALS DOMAIN

- - 1 Topic
- Soft Skills
- 7 Topics
- 5 Topics | 1 Quiz
- Networking 101
 - 6 Topics | 1 Ouiz
- 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
- A PA3) Tactics and Techniques Used
 - 12 Topics | 2 Quizzes
- PA4) Investigating a Phishing Email
 - 8 Topics | 2 Quizzes
- Analysing URLs, Attachments, and
 - 8 Topics | 1 Quiz
- C PA6) Taking Defensive Actions
 - 12 Topics | 1 Quiz
- O PA7) Report Writing
 - 7 Topics | 1 Ouiz
 - O Section Introduction, Report Writing
 - O Email Header, Artifacts, and Body Content
 - O Analysis Process, Tools, and Results
 - O Defensive Measures Taken
 - O Artifact Sanitization
 - O Activity) Report Writing Exercise
 - O Activity Cont.) Report Writing Exercise
 - Activity) End of Section Review, Report
- PA8) Phishing Response Challenge
- 3 Topics | 1 Quiz

THREAT INTELLIGENCE DOMAIN

- TI1) Introduction to Threat Intelligence
 - 7 Topics
- TI2) Threat Actors & APTs
 - 6 Topics | 2 Quizzes
- TI3) Operational Threat Intelligence
 - 7 Topics | 1 Quiz
- TI4) Tactical Threat Intelligence
 - 7 Topics | 1 Quiz

Email Header, Artifacts, and Body Content

Blue Team Level 1 Certification (Standard) > PA7) Report Writing > Email Header, Artifacts, and ... IN PROGRESS

Phishing Analysis HEADER, ARTIFACTS, CONTENT



The first things we gather from a malicious or suspect email are artifacts (also referred to as IOCs). We use this $information \ to \ try \ to \ link \ attacks \ together \ into \ campaigns, identify \ malicious \ actors \ behind \ the \ attacks, generate \ actors \ behind \ the \ attacks, generate \ actors \ behind \ the \ attacks, generate \ actors \ behind \ the \ attacks, generate \ actors \ behind \ the \ attacks, generate \ actors \ behind \ the \ attacks, generate \ actors \ behind \ the \ attacks, generate \ actors \ behind \ the \ attacks, generate \ actors \ behind \ the \ actors \ behind \ the \ actors \ behind \ actors \ behind \ the \ actors \ the \ actors \ behind \ the \ actors \ the \ actors \ the \ actors \ actors \ the \ act$ $metrics, and perform \, trend \, analysis, \, allowing \, us \, to \, predict \, what \, will \, happen \, in \, the \, near \, future.$

We need to include these in our report in a clear and concise way, so they can be found quickly, and other analysts can copy and paste them into different tools or services if needed (such as IOC reputation lookups, internal tools for

EMAIL HEADER AND ARTEFACTS

From the analysis section of this domain, you should feel confident retrieving the following artifacts from reported emails:

Email Header:

- Sending Email Address (Ex: JOhnSm1th@gmail.com)
- Reply-to Address (Ex: F4keaccOunt2421@gmail.com)
- Date Sent (Ex: 20th October 2019, 9:34 AM)
- Sending Server IP (Ex: 40.92.10.10)
- Reverse DNS of Sending Server IP (Ex: mail-oln040092010100.outbound.protection.outlook.com)
- Recipient(s) (Ex: jason.s@domain.com, kirsty.p@domain.com, brian.b@domain.com)
- Subject Line (Ex: Payroll Update URGENT!)

Email with URLs:

Any relevant URLs (Sanitised) (Fx: hxxps://Healthcare-United[.]com/wp/index/2020/PAYPAI /lure.php?)

Emails with Attachments:

- File Name(s) + Extension (Ex: PayrollDecember_UK.exe)
- MD5 Hash(es)

BODY CONTENT

In whatever platform you're using to store investigation notes, we would attach the email file directly to our case (in either .eml or .msg format, provided if it allows it) so that we have a copy of it for as long as needed. It's good practice to include a brief description of the email and a screenshot in your case notes, saving other analysts the important when it comes to taking defensive measures, it is still important as it can be used to identify trends or targeted attacks, and generate metrics about the type of malicious emails received.

You should aim to write approximately 1-2 sentences describing what the email looks like, and what it's trying to get the recipient to do. We cover two examples below that'll give you some guidance on how this information, as well as

) 314) Correlation

6 Topics | 1 Quiz

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

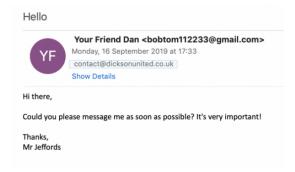
Exam Preparation

Using RDP and SSH

How to Start Your Exam

tne artifacts, snouid be presented in a clear and concise manner.

EXAMPLE ONE



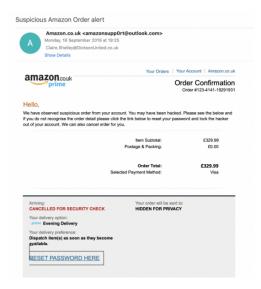
Artifacts Retrieved

- Sender: bobtom112233@gmail.com
- Reply-to: None
- Date: Monday 16th September 2019 17:33
- Sending Server IP: 209.85.167.42
- Reverse DNS: mail-lf1-f42.google.com
- · Recipients: contact@dicksonunited.co.uk
- Subject: Hello
- URL: None
- Attachments: None

Email Description

This email contains no malicious URLs or attachments and is attempting to get the recipient to respond, either
to engage in a social engineering attack, or to see if the recipient mailbox is in use so it can be targeted in
future attacks. Email classed as Recon.

EXAMPLE TWO



Artifacts Retrieved

- Sender: amazonsuppOrt@outlook.com
- Reply-to: no-reply@amazon.co.uk
- Date: Monday 16th September 2019 19:25
- Sending Server IP: 209.85.167.91

- Reverse DNS: mail-lf1-f91.google.com
- Recipients: claire.shelley@dicksonunited.co.uk
- Subject: Suspicious Amazon Order Alert
- URL: hxxp://maliciousdomainexample[.]com/
- Attachments: None

Email Description

This email from an Outlook mailbox is posing as Amazon using effective styling, and asks the user to click a link to reset their password claiming that the user's account has been hacked and used to purchase an order of £329.99. Using a sense of urgency is a common social engineer tactic, used to make the user rush and not think about what's actually happening. The email contains a malicious URL, as it is not pointing to an Amazonowned domain. Email classed as malicious / credential harvester.



Privacy & Cookies Policy

