

Blue Team Level 1 Certification
(Standard)

✓ 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

○ PA6) Taking Defensive Actions

12 Topics 1 Quiz

○ PA7) Report Writing

7 Topics 1 Quiz

○ Section Introduction, Report Writing

○ Email Header, Artifacts, and Body Content

○ Analysis Process, Tools, and Results

○ Defensive Measures Taken

○ Artifact Sanitization

○ Activity) Report Writing Exercise Answers

□ Activity) End of Section Review, Report Writing

○ 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

○ 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

Artifact Sanitization

Blue Team Level 1 Certification (Standard) > PA7) Report Writing > Artifact Sanitization

IN PROGRESS

Phishing Analysis
SANITIZING ARTIFACTS

When writing your reports, it's of critical importance that you sanitize any URLs or IP Addresses in a process known as *defanging* ("make something harmless").

But why?

Imagine, that you've given a post incident report to a colleague which contains information about a recent compromise you've been investigating. One of the unsanitized URLs inside of this report was found within a PowerShell script, which downloads and automatically executes a malicious payload. If your colleague accidentally clicks on that link, then there's a chance that it will open up within their web browser, download, and potentially execute compromising a system within your organization.

To overcome this, we can perform defanging of URLs and IP addresses. The rules for doing this are simple:

- Surround the "." within URLs and IP addresses with a "[" to become "[.]".
- Change the "tt" to "xx" within the **http** of URLs to become "**hxxp**".

For example:

8.8.8.8 becomes 8[.]8[.]8[.]8

http://hello.example.com becomes hxxp[:]//hello[.]example[.]com

Doing this for a batch of URLs and IP addresses can be a little tedious. Luckily, this can be "automated" using CyberChef's *Defang IP Addresses* and *Defang URL* operations:

Recipe	Input
Defang IP Addresses	length: 139 lines: 10 127.71.107.49 88.71.177.52 120.26.248.245 121.62.255.149 159.23.223.75 10.156.27.190 151.33.5.255 168.240.52.181 244.0.112.140 64.9.152.104
	time: 3ms length: 199 lines: 10 127[.]71[.]107[.]49 88[.]71[.]177[.]52 120[.]26[.]248[.]245 121[.]62[.]255[.]149 159[.]23[.]223[.]75 10[.]156[.]27[.]190 151[.]33[.]5[.]255 168[.]240[.]52[.]181 244[.]0[.]112[.]140 64[.]9[.]152[.]104
STEP	BAKE! Auto Bake

Recipe	Input
Defang URL Escape dots Escape http Escape :// Process Valid domains and full ...	length: 323 lines: 10 http://example.org/activity https://www.example.com/bikes https://example.com/branch#book https://example.com/?ranger=anger http://www.example.com/ http://adjustment.example.com/bike https://bridge.example.com/ http://battle.example.net/ http://advertisement.example.com/#boot https://airport.example.com/aunt/authority.html
	time: 1ms length: 279 lines: 10 hxxp[:]//example[.]org/activity hxxps[:]//www[.]example[.]com/bikes hxxps[:]//example[.]com/branch#book hxxps[:]//example[.]com/?ranger=anger hxxp[:]//www[.]example[.]com/ hxxp[:]//adjustment[.]example[.]com/bike hxxp[:]//bridge[.]example[.]com/ hxxp[:]//battle[.]example[.]net/ hxxp[:]//advertisement[.]example[.]com/#boot hxxps[:]//airport[.]example[.]com/aunt/authority[.]html

4 Topics1 Quiz

SECURITY INFORMATION AND EVENT MANAGEMENT DOMAIN

SI1) Introduction to SIEM

7 Topics1 Quiz

SI2) Logging

6 Topics2 Quizzes

SI3) Aggregation

< Previous Topic

Mark Complete ✓

Back to Lesson

Next Topic >