Blue Team Level 1 Certification

(Standard)

Introduction to BTL1

- - 4 Topics

SECURITY FUNDAMENTALS DOMAIN

- Introduction to Security Fundamentals
 - 1 Topic
- Soft-Skills
- 7 Topics
- Cacurity Control
- 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
- A PA3) Tactics and Techniques Used
 - 12 Topics | 2 Quizzes
- PA4) Investigating a Phishing Email
 - 8 Topics | 2 Quizzes
- PA5) Analysing URLs, Attachments, and
 - 8 Topics | 1 Quiz
- PA6) Taking Defensive Actions
 - 12 Topics | 1 Quiz
- O PA7) Report Writing
 - 7 Topics | 1 Quiz
- O 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

- O DF1) Introduction to Digital Forensics
 - 5 Topics
- O DF2) Forensics Fundamentals
 - 10 Topics | 5 Quizzes

Equipment

Blue Team Level 1 Certification (Standard) > DF3) Digital Evidence Collection > Equipment

IN PROGRESS

Digital Forensics Domain Digital Forensics Equipment



Collecting evidence in digital forensics investigations is something that takes careful planning and preparation and if the investigator doesn't have the proper toolkit, then the evidence may become compromised. Many law enforcement departments around the globe have dedicated forensic laboratories where they can analyze evidence in a manner that will prevent it from being tampered with. As an investigator, you will need to have the same kind of tools at your disposal, comparable to what you would find in a laboratory.

EQUIPMENT

Forensic Laptop or Workstation



Bringing a laptop specifically designated for digital evidence can be essential when gathering the evidence at the scene or capturing evidence that may be in memory. Popular Linux distributions such as CAINE or DEFT can often be found on these laptops, as well as commercialized systems for law enforcement.

Electro-Static Evidence Bags with Tamper-proof Stickers



Electro-Static Evidence Bags will help protect any sensitive digital components from Electro-Static Discharge (ESD) during the transport of the evidence from its initial location, to a secure lab environment. Labeling is often applied to these bags to let investigators know what is contained inside of them. Having bags or stickers that are sealed, and the seal must be physically broken to gain access to the evidence within is critical to ensure the chain of custody is maintained, and that evidence is not tampered with whilst in storage or transit.

0	DF3) Digital Evidence Collection
	8 Topics 1 Quiz
	O Section Introduction, Evidence Collection
	O Equipment
	O ACPO Principles of Digital Evidence Collection & Preservation
	O Chain of Custody
	O Disk Imaging: FTK Imager
	O Live Forensics
	O Live Acquisition: KAPE
	O Evidence Destruction
	Activity) End of Section Review, Evidence Collection
	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
	CURITY INFORMATION AND EVENT
0	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
IN	CIDENT 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
ВТ	L1 EXAM
	Exam Preparation
	Using RDP and SSH
	How to Start Your Exam

Labels

ш	CASE #	ITEM
<u>ပ</u>	DATE	TIME
M	DESCRIPTION	
E	LOCATION	

Labeling is essential when conducting any kind of evidence collection. Knowing what piece of hardware is, helps yourself and other people in the chain of custody determine what the evidence is, without having to go inside of it.

Photographs



Photographs, like in any kind of crime scene, can be helpful to show the investigator the bigger picture. This could include how the equipment was set-up at the crime scene, as well as providing clues later on, that might be helpful to the investigation.

Grounding Bracelets



 $Similar\ to\ Electro-Static\ Bags,\ grounding\ bracelets\ are\ important\ for\ investigators\ to\ use,\ to\ ensure\ that\ when\ handling\ evidence,\ they\ do\ not\ inadvertently\ compromise\ or\ damage\ the\ evidence.$

Hardware Write-Blockers



 $Hardware\ Write\ Blockers\ can\ be\ an\ essential\ piece\ of\ equipment\ that\ will\ ensure\ that\ your\ evidence\ has\ not\ been tampered\ with.\ It\ can\ either\ be\ software\ on\ your\ forensic\ laptop,\ or\ a\ hardware\ device\ that\ permits\ read-only\ access\ to\ data\ storage\ devices\ without\ compromising\ the\ integrity\ of\ any\ data\ that\ may\ be\ contained\ on\ them.$

Blank Hard Drives



In the event that you need to copy data on-site, having blank hard disks are an essential piece of hardware to have in your toolkit. These can be used in conjunction with write-blockers to copy the disk to another one without making $any \ write able \ changes \ to \ the \ media. \ Drives \ used \ for \ forensic \ work \ need \ to \ be \ extremely \ high \ capacity, \ especially \ if$ $bit-by-bit\ copies\ of\ suspect\ hard\ drives\ are\ being\ copied.\ The\ size\ of\ the\ receiving\ drive\ must\ always\ be\ higher\ than$ that of the original drive.

SPECIALIST EQUIPMENT

In some cases, specialized equipment/software is used on the scene to assess the digital evidence that was found. This can include:

- $\bullet \ \ Wireless \, Stronghold/Faraday \, Boxes \, \, to \, block \, any \, wireless \, signals \, from \, reaching \, the \, evidence, preventing \, block \, and \, blo$ remote access or wiping.
- Specialized Write-Blockers write-blockers that could also be used on cell phones, GPS devices, IoT devices, and other non-standard hard-drives.
- Phone Jammers acting the same as a faraday box or wireless stronghold.
- $\bullet \ \ \textbf{Dedicated Flash Drives} \ \ \text{containing tools like Encase, FTK, CSILinux and MacQuisiton.}$

< Previous Topic



Next Topic >

