

Blue Team Level 1 Certification
(Standard)

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

Section Introduction, Detection &
Analysis

Common Events & Incidents

Using Baselines & Behavior Profiles

Introduction to Wireshark (GUI)

Introduction to Wireshark (Analysis)

Lab) Network Traffic Analysis

YARA Rules For Detection

Legacy Activity) Threat Hunting With
YARACMD and PowerShell For Incident
Response

Lab) CMD and PowerShell

Activity) End of Section Review,
Detection & AnalysisIR4) 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

Legacy Activity) Threat Hunting With
YARA

Blue Team Level 1 Certification (Standard) > IR3) Detection and Analysis Phase > YARA Rules For Detection > Le...



In this activity you'll use YarGen and YARA to perform a basic threat hunt, identifying the presence of any malicious artifacts after an incident occurred and a system was compromised. Below is a brief and the files you'll need to complete the exercise. You can complete this activity as many times as you want, but you'll need to score 70% or higher to pass.

CHALLENGE SCENARIO

An employee clicked a link in a phishing email and downloaded malware to their system, which wasn't detected by the anti-virus or endpoint detection and response solution. We need to check if the malware made copies of itself to ensure the attacker's have persistence and can continue working to complete their objectives. We've collected a copy of the initial file that was downloaded from a packet capture. Use yarGen.py to create a detection rule for this binary, and then use YARA to audit the copy of the user's files we've provided you. Report on your findings, and let us know if this malware is hiding anywhere else.

Download the file below and transfer it to your Kali virtual machine, then read the "READ ME.txt" file inside. Good luck hunter.

Download "BTL1_Hunting_With_YARA.zip"

CHALLENGE SUBMISSION

[YARA General Questions 1/4] We want to generate a YARA rule using yarGen.py. The terminal is open in the location of yarGen.py and the malicious file is inside a directory named 'MALICIOUS' on the Desktop of the root user and we want to name the rule "YARARule.yara", saving it in the same location as the terminal. What is the command we want to use ?

Hint

Check