

Blue Team Level 1 Certification  
(Standard)

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

Section Introduction, Linux  
Investigations

Linux Artifacts - Passwd and Shadow

Activity) Password Cracking

Linux Artifacts - /Var/Lib and /Var/Log

Linux Artifacts - User Files

Activity) End of Section Review, Linux  
Investigations

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

## Activity) Password Cracking

Blue Team Level 1 Certification (Standard) &gt; DF5) Linux Investigations &gt; Linux Artifacts - Passwd and Shadow &gt; ...

Digital Forensics Domain  
PASSWORD CRACKING

In this activity, you will be playing through a scenario as a digital forensics analyst investigating a compromised Linux system, and cracking passwords to gain access to other accounts on the system. You can retake this activity as many times as you like, but you'll need to score 70% or higher to pass. **Good luck!**

## CHALLENGE SCENARIO

Welcome investigator! We're currently working on a compromised Debian-based Linux system. We've been able to log in as the root user and we're doing a thorough investigation, but it appears there are some other accounts under the names:

- JohnC
- ServiceAccount
- Piper

We've retrieved both the **passwd** and **shadow** files for you, so you just need to use them to crack the passwords for the other three accounts. Once you've got the plain text passwords let us know, so we can continue our investigation. Download the two files below, and a wordlist we recommend using with John The Ripper.

Download "BTL1\_Password\_Cracking\_Activity.zip"

## CHALLENGE SUBMISSION

[1/3] What is the plain text password for the user JohnC?

[2/3] What is the plain text password for the user ServiceAccount?

[3/3] What is the plain text password for the user Piper?

Finish Quiz