Blue Team Level 1 Certification (Standard)

DIGITAL FORENSICS DOMAIN

SECURITY INFORMATION AND EVENT MANAGEMENT DOMAIN

INCIDENT RESPONSE DOMAIN

Activity) Password Cracking

Blue Team Level 1 Certification (Standard) > DF5) Linux Investigations > Linux Artifacts – Passwd and Shadow > ...

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