21st Annual ITC Information Technology Competition

Digital Forensics Challenge

Written By: Cornelius Rogers

Case: DIB-3750G-28

OVERVIEW

For this competition, your team will be provided digital evidence images to forensically examine. Each team will be obligated to follow industry best practices in the handling and processing of this digital evidence. The tools and methodologies used to preserve and examine the evidence must also follow industry best practices as each team will be obligated to account for and defend the accuracy of their findings.

SCENARIO

Corporate Profile

Do IT Better is an Information Technology Services Provider who provides hosting and consultation services to start-ups in the Greater Los Angeles area. *Do IT Better* recently hired a new IT staff in the hopes of expanding their business to more start-ups and small to mid-size companies. The CEO of *Do IT Better*, Darren Lau, has requested the assistance of a team of consultants to investigate a potential security breach.

Security Incident Overview

On March 31, 2017, the information security team for *Do IT Better* led by Casey Kan detected suspicious traffic originating on their corporate network from a workstation belonging to Nathan Munoz, a web developer on the new IT staff who was in a meeting at the time of the incident. Shortly after, a man attempted to badge out using what we suspect to be a fake ID badge. The man was detained for trespassing on private property and potential corporate espionage. In his possession were a laptop and USB which were subsequently confiscated and imaged. The host on the corporate network and primary web server were also taken offline and imaged as a precaution.

Consultant Task:

The consultants have been tasked by the CEO to perform a forensic analysis on the files provided to determine any potential evidence which could be relevant to this case and any other potential cases.

Evidence Provided:

(1) Image of Corporate Workstation

(2) Image of Corporate Web Server

(3) Image of Suspect Laptop

DELIVERABLE: Examination and Reporting Phase

Teams will be expected to provide a narrative examination report documenting their methodologies, analysis, and findings. Any exhibits you have should be provided with the report. If the exhibits are too large to print, then they should be included in electronic copy. Teams will be provided the evidence prior to the challenge for examination and deliverables. Teams should use this time to draft their final examination report and create their presentation materials. The final examination report is due no later than 5:00PM Pacific, April 21, 2017. The final presentation materials are due no later than 5:00PM Pacific, April 28, 2017. If you do not turn in a report, you will not be allowed to move to the following Presentation Phase. Furthermore, you are not permitted to have anyone other than the members of your team actively play a role in examining the evidence, writing the examination report, or presenting your findings.

The following is some items your report should, at a minimum, include:

1) Introduction

    a. A quick description of the compelling event

    b. A description of the services requested

    c. Team Members and Roles they played

2) Summary

    a. Synopsis of findings

3) Methodologies

a. A description of the evidence you reviewed for the case.

b. Chain of Custody information.

c. Evidence Validation and Verification.

d. What tools were used to review the evidence during the course of the exam?

4) Analysis and Findings

a. Detailed Explanation of any probative or exculpatory findings and the analysis conducted to reach that finding

b. Include References to Exhibits

c. Include definitions of technical terminology

5) Conclusion

a. Mitigation and Remediation Actions

b. Were any exceptions noted during the exam?

c. Disposition of all evidence and case materials

d. Description of all exhibits

NOTE: Teams should be prepared to receive and analyze digital evidence from multiple sources. As with any Digital Forensics / Incident Response case, the provided evidence may hold malicious files. Teams should be careful handling possible malicious files and take steps to prevent infection of the examination machine or loss of data.

DELIVERABLE: Presentation Phase

Each team will be expected to present their findings during the ITC Event in front of the panel of Judges. Your team should be prepared to provide a verbal testimony as to your team's methodologies and findings. The ability of your team to present your findings and accurately represent the evidence will be scored. Each team will have no more than 20 minutes to present their findings, followed by 10 minutes of Question and Answer from the Judges Panel. During the Q & A portion of this phase, you and your team should be able to attest to the findings of your report, provide further meaning as asked, and be able to defend your methodologies.

SCORING

Judges will be scoring each team based upon four (4) categories: Ability to identify key Forensic Artifacts, Demonstration of Technical Skills, Final Report, and Final Presentation for a maximum score of 100 points. Teams will be ranked based on their cumulative score from the highest to the lowest.