SAT1: 013: Final Lab – Capstone Project

**Overview**

This lab is designed to allow you to use all of the tools and skills that you have learned this week. You will be asked to analyze provided artifacts, and develop a timeline of events, propose countermeasures and remediation's, and provide a 10-15 minute executive briefing on your results.

***Time: 6 Hours***

**Learning Objectives**

Upon completion of this lab, you should be able to:

1. Use the tools and techniques we have learned to document a cybersecurity incident using the Cyber Kill Chain©.

## Scenario

You are an employee for a cybersecurity contractor that has a contract with Norse Systems, Inc. They have been notified that one of their workstations is suspected of being compromised. You are the onsite team, and you have been given a set of artifacts from the compromised machine to analyze.

## Expectations

You and your team of 5 will work together to use the tools installed on your workstation to analyze the artifacts and develop a timeline for any events that may have occured, and build out a cyber kill chain to document the attack.

The only information you have available is provided as a part of the artifacts you have been given. Your instructor will provide guidance during the exercise, but do not rely on him for information, he will not provide information on the lab results.

You are expected, to provide a Executive briefing for your organizational C-Suite on your findings, including: indicators that you discovered, and what they mean; what systems or information could have been compromised, and your recommendations on how to mitigate the impacts. You should also make recommendations on how to prevent a future incident. It is recommended, but not required that you use a visual display such as powerpoint.

You have until 3pm to complete your lab, and each group will deliver their findings.

# Good Luck!