WST-2

Weapon System Training 2
Introduction

Instructor: Maj Michael "Catapult" Lester

USAF Weapons School • Nellis AFB

Lesson Classification

This lesson is classified

UNCLASSIFIED //
FOR OFFICIAL USE ONLY

Classified by: Capt Michael Lester

Derived from: USCYBERCOM SCG

Disclaimer

These lessons are not testable and are designed only for your benefit during mission planning and execution.

Motivation

- You will be working with ELK during this WST
- Anything you build today can be used during the mission tomorrow
- I will help you build anything you want so long as you can show me how it supports a hypothesis you have about some adversary activity

Overview

- Schedule
- Purpose
- Tools
- Environment
- Pipeline
- Time Windows
- ROEs

Schedule

- Guided (5 hours)
  - WST-2 Introduction
  - WST-2 Kibana User Interface and Components
  - WST-2 Dashboard Workflow
  - WST-2 Lab 2
  - WST-2 Lab 3
  - WST-2 Lab 4
- Unguided (1 hour)
  - You can work on building your own custom visualizations and analytics
  - Consider splitting out tasks/work
  - I will here to help answer questions

Purpose

- Give students baseline proficiency with tools that are commonly used throughout USAF DCO units.
- Demonstrate the implementation of generic threat hunting analysis techniques applicable outside of the tools we will use to implement them.

Tools

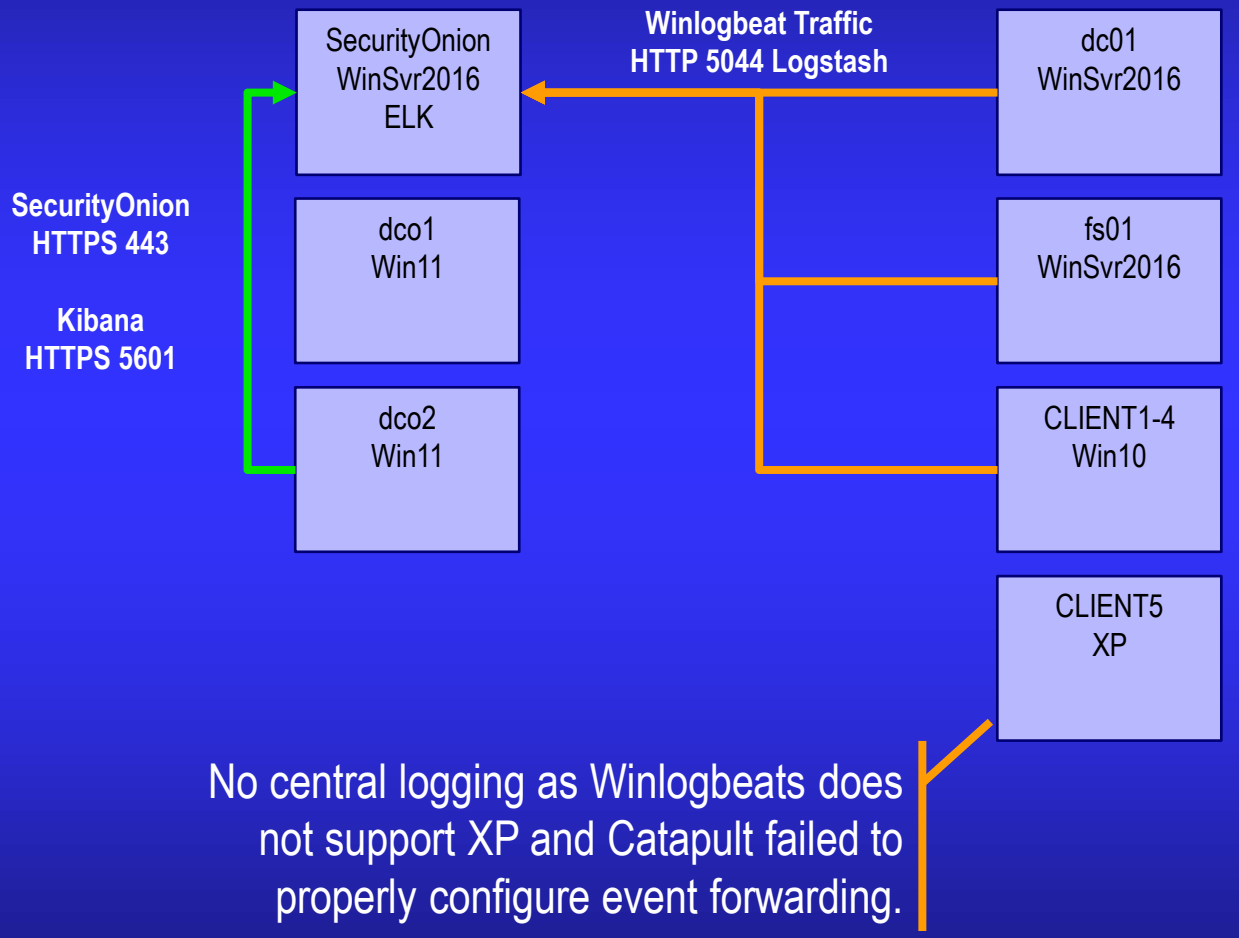
- SecurityOnion
  - A free, open source appliance (OS distribution with pre-packaged software) for threat hunting, network security monitoring, and log analysis.
- ElasticSearch, Logstash, and Kibana (ELK stack)
  - ElasticSearch: Search and analytics engine for both structured and unstructured data.
  - Logstash: Performs log aggregation, storage, and enrichment.
  - Kibana: Web interface for visualizations and analysis.
  - ELK is a component of SecurityOnion and is commonly used as a Security Information and Event Manager (SIEM).
- Winlogbeat
  - An agent that that collects, normalizes, enriches, and ships logs from Windows systems to an ELK server.

Why these tools?

- ELK
  - ELK is a commonly used SIEM across several DCO units
  - It is free and open-source, therefore no cost to this unit
  - The concepts we teach you will be applicable to other SIEMs
  - Very flexible to the data you can ingest and analyze
  - Good for analyzing both host and network events
- Winlogbeat
  - Beats are a generic agent that are commonly deployed to collect events
  - EDRs such as Endgame are not authorized in every environment

Environment

- All of the labs will take place in the P&T-1/2 range.
- One student per range
- One SecurityOnion instance per range



Time Windows

- There are two timelines that you will narrow your search windows to:
  - 13 Jan 2022 1000 – 1300: Instructor SoM
  - 13 Jan 2022 0840 – 1000: P&T-1 Execution
- You can see what your attack in the last mission looked like from a DCO perspective
- Think about what queries and filters you might apply to detect your activity if you were a network defender

End State

- By the end of today, you will:
  - Be familiar with navigating Kibana
  - Create two dashboards for threat hunting and investigation
  - Create visualizations implementing frequency analysis to detect abnormal activity
  - Create visualizations to analyze process parent/child relationships
  - Create custom drill down events to pass filters and queries from one dashboard to another
  - Create filters and queries to identify specific adversary TTPs
  - Use what you've created to detect the two previously mentioned attacks
- Key analytic techniques:
  - Frequency Analysis / Long-tail Analysis
  - Timeline Analysis

ROEs

- Add your last name to your saved visualizations, dashboards, and queries
- Do not search past 18 July 2022 in your time filters
- Reference the implementation details of instructor created dashboards and visualizations only if you get stuck
- Instructor dashboards and visualizations have “(Instructor)” in the title

Mission Day ROEs

- During mission planning:
  - Start with your hypotheses
  - Determine what events you need to look at, what fields in those events matter
  - Determine how you are going to analyze those events
  - Build filters, queries, and dashboards during flight line by line (these will be made by yourself)

#FOOTSTOMP

ROEs

Note	Detailed information that is required to fully understanding the concept or to be able to execute a procedure but is not necessarily related to a key learning objective.
Learning Point	Information related to key learning objectives.
Warning	Important information related to safety and security.
Raise Hand	Raise your hand for instructor assistance. This is often used at critical points to validate your understanding of the material.

Overview

- Schedule
- Purpose
- Tools
- Environment
- Pipeline
- Time Windows
- ROEs

Questions?

- Instructor's name: Maj Michael "Catapult" Lester
- Instructor's address: USAF Weapons School
  4269 Tyndall Avenue
  Nellis AFB 89191-6062
- Instructor's phone: (702) 679-2200
- Instructor's e-mail: michael.lester.5@us.af.mil

WST-2

Weapon System Training 2
Introduction

Instructor: Maj Michael "Catapult" Lester

USAF Weapons School • Nellis AFB