Project Week: Red vs. Blue

Cybersecurity

Project Week 2

Welcome to Project Week!

This week, you will embark upon your second project: A Red vs. Blue scenario in which you will play the role of both pentester and SOC analyst.

Project Week 2

Throughout this week you will:

Day 1

Work as a red team to apply everything you've learned in pen testing to access a vulnerable target.

The target will be capturing logs of the your activity as you attack it.

Day 2

Work as a Blue Team and use the ELK setup you created in Project 1 .

You will use this to extract hard data and visualizations for your report.

Day 3

Report and present your log data to suggest mitigation measures for each exploit you successfully performed.

This project requires knowledge of pen testing, SIEM, and system administration. Gaining such a broad knowledge of cybersecurity tools is a significant achievement.

Congratulations on all you have accomplished so far.

Lab Environment

This lab environment contains an attack VM, a target VM, and an ELK server.

Kali

This is a standard Kali Linux machine for use in the penetration test on Day 1.

Credentials:

- Username: `root`
- Password: `toor`

Capstone

This is the vulnerable target VM students will attack.

It has Filebeat and Metricbeat installed, and forwards logs to the ELK machine.

ELK

This is the same ELK setup that you created in Project 1.

It holds the Kibana dashboards you will use in Day 2.

Day 1: Red Team

ELK Stack Refresher

- Logs are collected on deployed machines.
- Logs are forwarded to the Elasticsearch database.
- Kibana is used to visualize data.

ELK Stack Refresher

Beats are small programs that run on the machines being monitored and forward logs to the database.

- **Filebeat** collects data about the file system, such as files changed, requested, and uploaded.
- **Metricbeat** collects data about the system, such as uptime and SSH logins.
- **Packetbeat** collects network data, such a incoming and outgoing packets.

Project Milestones

- ✓ **Day 1:** Find the flag on the Capstone VM.
- ✓ **Day 2:** Answer all provided questions about the logs captured in Kibana.
- ✓ **Day 3:** Complete a presentation summarizing your findings.

Day 1 Overview

Today’s activity will require the following high-level steps:

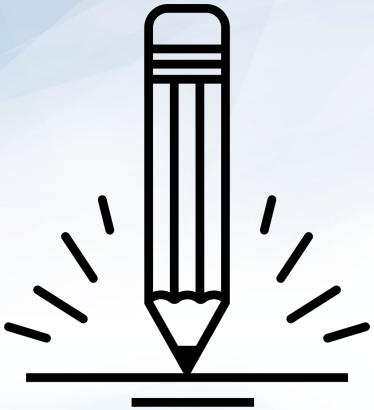
01 Identify the IP address and exposed services of the target VM.

02 Find hidden files on the target.

03 Brute-force and crack passwords to gain entry.

04 Upload a PHP reverse shell to an insecure web server.

05 Explore the target system and finding the flag.



Day 1 Activity: Attack!

You will act as an offensive red team and exploit a vulnerable VM.

Suggested Time:
Full Class Time

Time's Up

In today's class, you enumerated, exploited and escalated privileges on a vulnerable VM.

As you were working, the ELK server was recording your actions.

Next class, you will act as a blue team to analyze these logs and determine mitigation strategies.

Day 2: Blue Team

Blue Team Objectives

In Day 1, the red team:

- Identified the IP address and exposed services of the target VM.
- Found hidden files on the target.
- Brute-forced and cracked passwords to gain entry.
- Uploaded a PHP reverse shell to an insecure web server.
- Explored the target system and found the flag.

As the blue team, you will find evidence of each of these steps by:

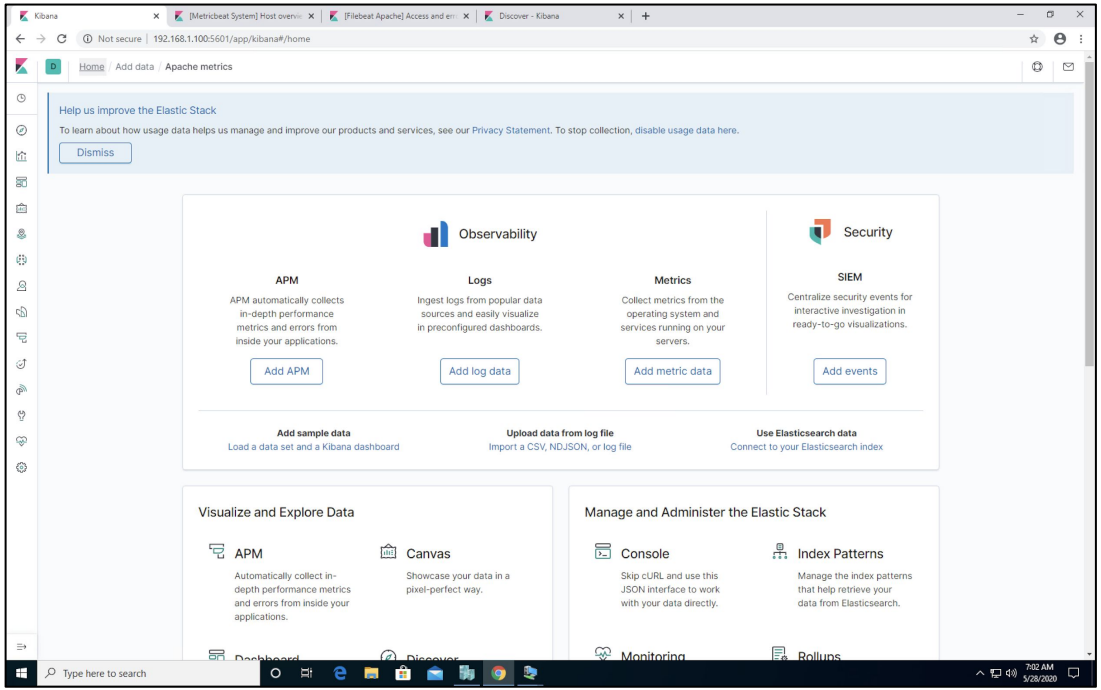
- Finding data depicting each step of the attack.
- Using this data to propose possible alarm metrics and thresholds.
- Using this data to propose hardening and mitigation techniques.

Kibana

The ELK server is configured on your VMs and ready to use. You just need to launch Google Chrome on the Windows host to access it.

Chrome is configured to load the following pages by default:

- Kibana homepage
- Filebeat system metrics
- Filebeat Apache metrics
- Packetbeat metrics



Searching Logs in Kibana

We will use the following beats in Kibana:

01

Filebeat monitors files on disk for changes and watches system events, such as user logins.

02

Metricbeat monitors system health metrics, such as uptime.

It also generates metrics based on Apache access logs.

03

Packetbeat captures network data, allowing users to explore packets as they come in.

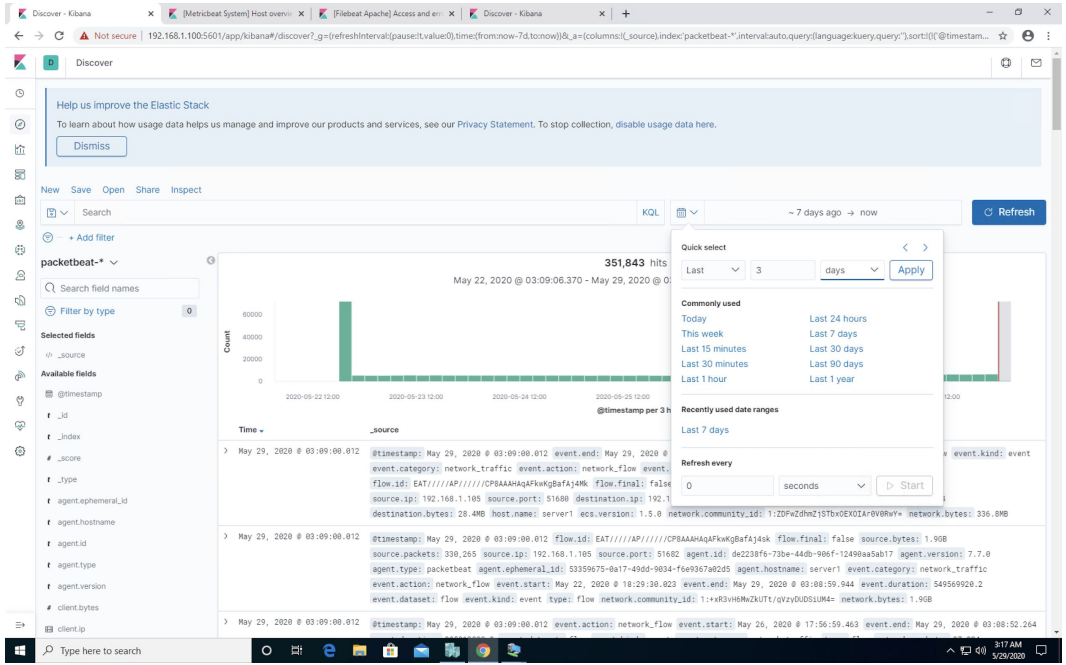
Packetbeat is like Wireshark for ELK.

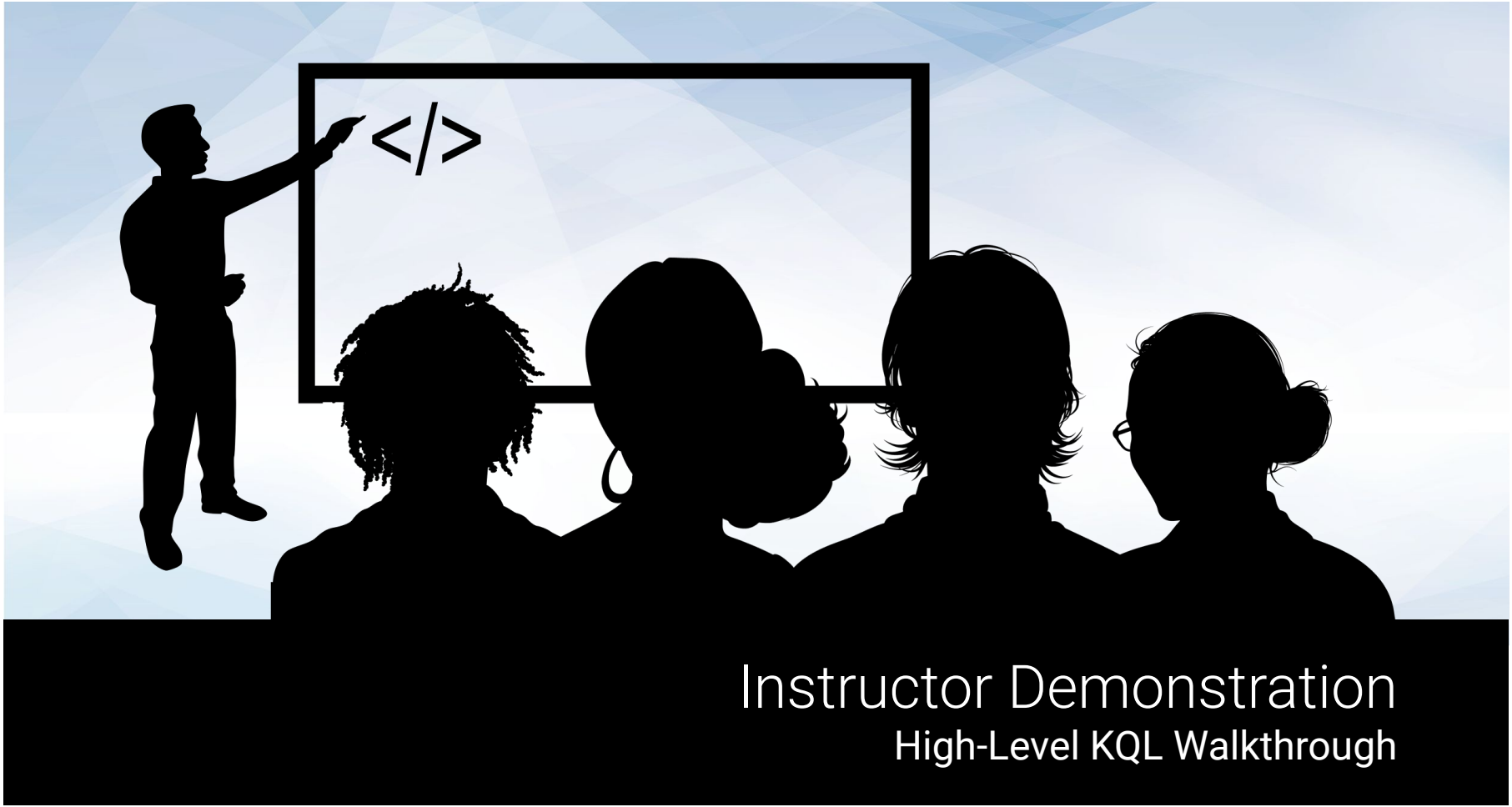
Searching Logs in Kibana

Kibana can provide an overwhelming amount of tools to work with. We will focus on the visualizations and dashboards and Kibana Query Language (KQL).

We can filter for properties such as:

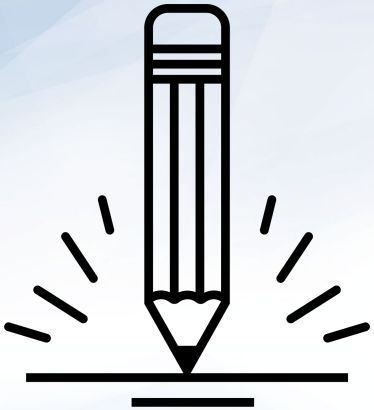
- Timestamps
- Source and destination IPs and ports
- Protocols
- URLs





Instructor Demonstration

High-Level KQL Walkthrough



Day 2 Activity: Incident Analysis with Kibana

You will use Kibana to analyze logs taken during the red team's attack. As you analyze, you will use the data to develop ideas for new alerts that could improve your monitoring.

Suggested Time:
Full Class Time

Time's Up

In today's class, you used Kibana to analyze the logs that were captured while you performed your penetration test.

Now that you know how much defenders can observe of what you do, you should have clearer insight into how and why attackers and defenders use certain tactics.

You used data to develop ideas for new alarms and ways to harden the vulnerable VM. These can be implemented to improve the monitoring setup and configuration security of the target machine.

Next you will summarize your findings in a Google Slides presentation that you can use in future interviews and feature on sites like LinkedIn.

Day 3: Reporting

In the final day of the project, you will summarize your Day 1 and Day 2 findings in a report.

You will prepare the report of your findings as a professional presentation. This will be a valuable deliverable to show potential employers, proving knowledge and experience.

Reporting

In the report, you will document the following:

Red Team

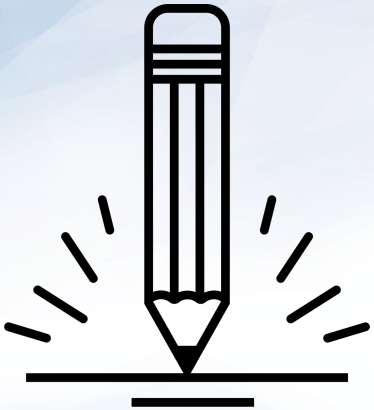
- Network topology
- Engagement overview and outcome
- Critical vulnerabilities

Blue Team

- Summary of attack
- For each phase of the exploitation:
  - Log evidence of attack
  - Key findings from evidence

Mitigations

- Mitigation techniques for each critical vulnerability.
- Suggested alarms and thresholds



Day 3 Activity: Reporting

Today, you will fill out a Google Slides template to create a report of your assessment and log analysis.

- Report Template

  You will need to make your own copy of the template.

Suggested Time:
Full Class Time

Don’t forget to complete this report for homework if you don’t finish during class.

Try to make it as presentable and professional as possible. This document can be very valuable for networking with cyber professionals and having a discussion with hiring managers.