Final Project Week

Cybersecurity

Final Project Week

Picking Up from Project 2

In the Red Team vs. Blue Team project, you attacked a vulnerable VM, analyzed data in Kibana, and suggested alerts.

- In this week's assignment, you will assess vulnerable VMs that expose vulnerable web servers rather than vulnerable network services.

- You will use Kibana to both analyze logs, and set and test alerts.

Project Week 3 Overview

This week, you will exploit a vulnerable WordPress installation.

- You will set up alerts in Kibana before performing your assessments.
- This will allow you to see dashboard alerts in real-time.
- After completing the alerting and penetration testing portions of the project, you will use Wireshark to capture and analyze live traffic on the virtual network.

Project Week 3

Throughout this week, you will:

01 Day 1: Configure and test alerts in Kibana and begin your assessment of the Target 1 VM.

02 Day 2: Continue your assessment of Target 1 and begin to use Wireshark to analyze live traffic on the wire.

03 Day 3: Complete your Wireshark analysis. You will also begin your individual reports and group presentations.

04 Day 4: Group presentations

This project requires knowledge of pen testing, SIEM, and system administration.

Gaining such broad knowledge of cybersecurity tools is a significant achievement.

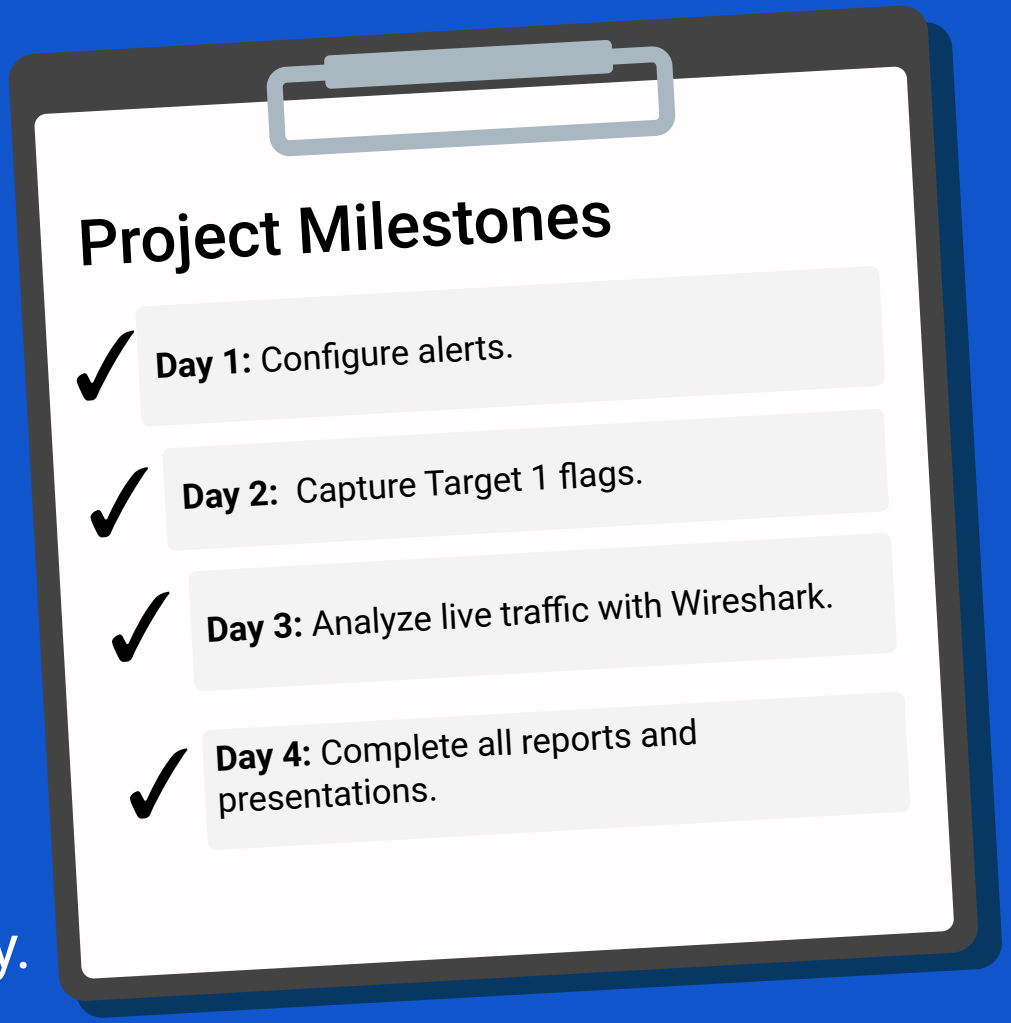
Congratulations on all you have accomplished and learned so far!

Lab Environment

This week's lab environment is an extension of the lab from Project 2. It features the following VMs:

VM	IP Address	Description
Kali	`192.168.1.90`	A standard Kali install that will be used to attack other machines.
Capstone	`192.168.1.105`	The vulnerable target VM that students can use to test alerts. Filebeat and Metricbeat will forward logs to the ELK machine.
ELK	`192.168.1.100`	The same ELK setup that you created in Project 1. It holds the Kibana dashboards that you will use in Day 2.
Target 1	`192.168.1.110`	Exposes a vulnerable WordPress server. Sends logs to ELK.
Target 2	`192.168.1.115`	A more difficult WordPress target. Should be ignored unless all other portions of the project are completed. Sends logs to ELK.

The following milestones should be achieved at the end of each day.



You will have the opportunity to attack Target 2, a more complex web application.

Only start this task *if* you have found the Target 1 flags, completed the Wireshark analysis and wrote your reports.

End of Project Deliverables

At the end of this project, you will submit the following:

01 Red Team Report of Target 1 (Linked in Day 1 Activity File)

02 Blue Team Report of Target 1 (Linked in Day 1 Activity File)

03 Network Analysis of Wireshark Task (Linked in Day 3 Activity File)

04 Group Presentation

Group Work

Group work is a component of this project

01

You will be assigned groups on Day 1. Then you will on the daily tasks **individually**.
If needed, you can consult with their group members for help or collaboration.

02

Each student will complete and submit each of the three reports.

03

As groups, you will present your findings on one of the reports. You will convene and decide which of the three reports they want to present on. Then, you will use the presentation templates to create slides and present.

Day 1: Target Assessment

This Week’s Scenario

In this week's project, you will play the role of Security Engineer for X-CORP, supporting the SOC infrastructure.

- The SOC analysts have noticed some discrepancies with alerting in the Kibana system and the manager has asked the Security Engineering team to investigate and confirm that newly created alerts are working.

- If the alerts are working, the engineers need to monitor live traffic on the wire to detect any abnormalities that aren't reflected in the alerting system.

- They are to report back all their findings to the manager with appropriate analysis.

ELK Stack Refresher

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

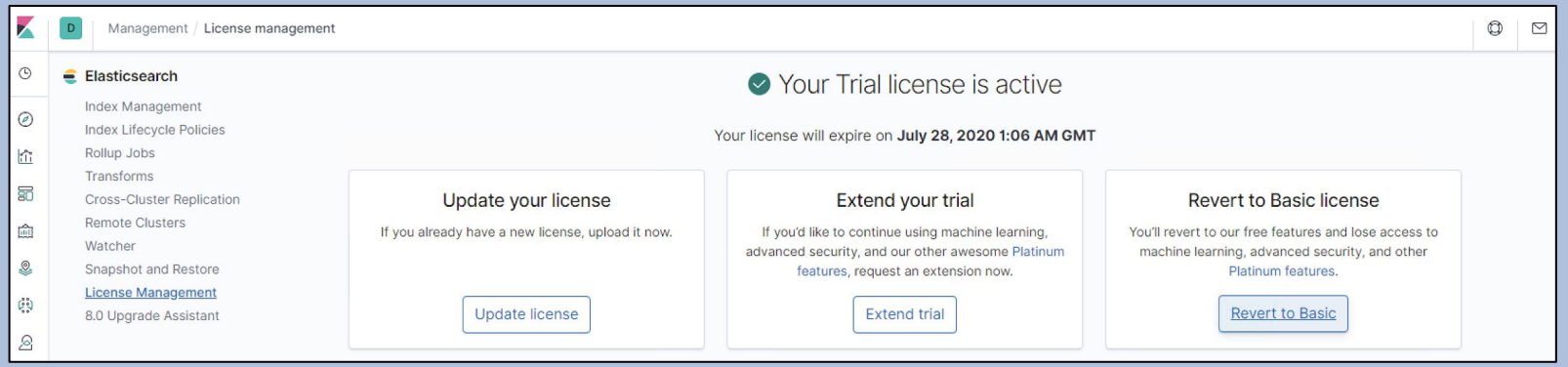
Beats Refresher

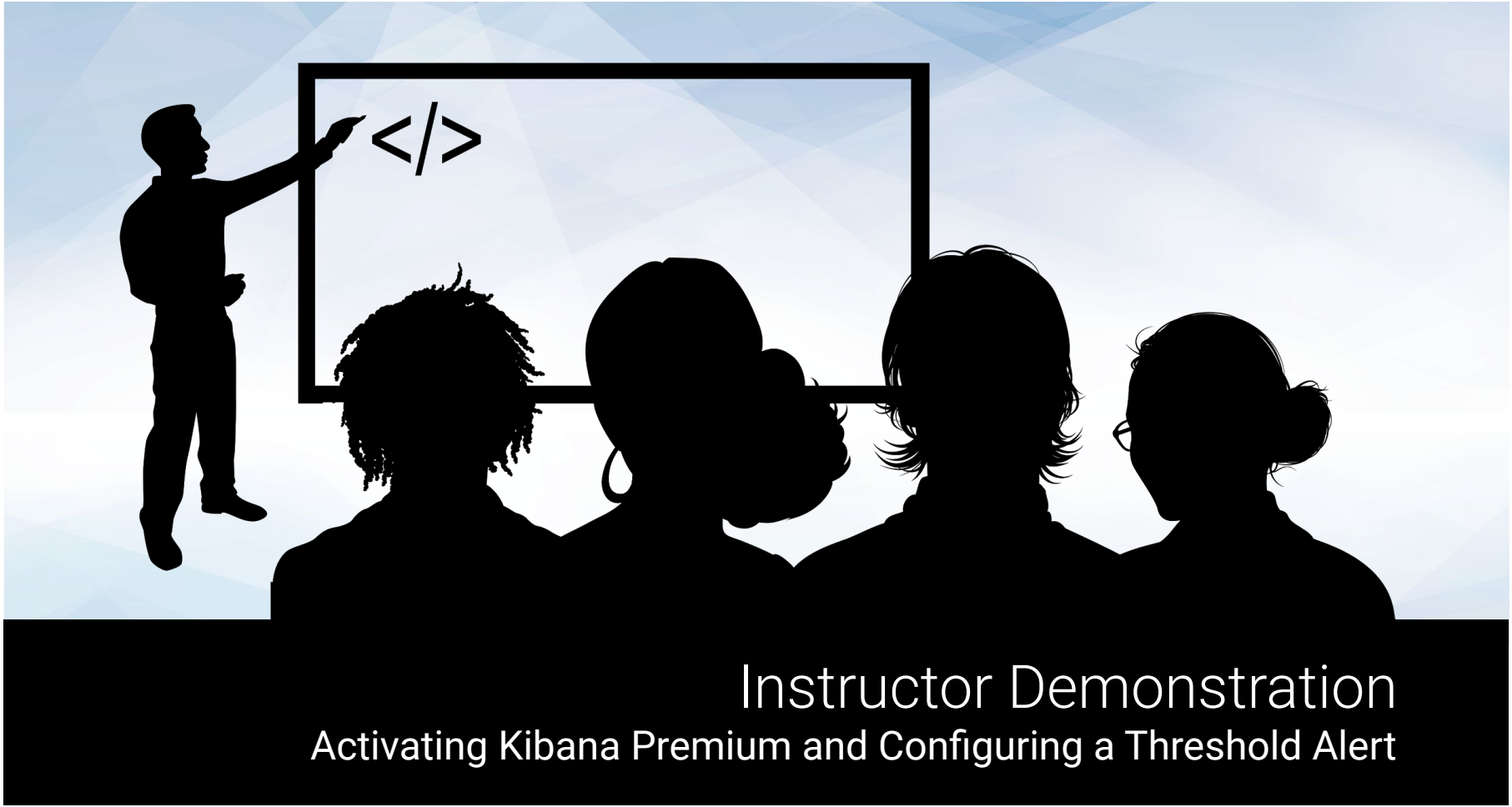
Beats are small programs that run on the machines being monitored and forward logs to the database.

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

Activating Kibana Premium

Since alerts are a Kibana Premium feature, we need to activate a free trial. This trial also enables the Watcher plugin, which you will use to configure alerts.





Instructor Demonstration

Activating Kibana Premium and Configuring a Threshold Alert

Assessing WordPress Targets

After setting up alerts, we'll use Kali to attack a web server running a vulnerable version of WordPress.

To attack this web server, we will use a new tool called **`wpscan`**, which can:

- Find WordPress usernames and passwords.
- Enumerate URLs on a WordPress installation.
- Profile targets by detecting WP version and installing plugins.

Assessing WordPress Targets

We will use **wpscan** to profile the target site and enumerate usernames and passwords.

```
# Detect WP Version and General Scan
$ wpscan --url http://target.com

# Enumerate Vulnerable Plugins
$ wpscan --url http://target.com --enumerate vp

# Enumerate Usernames
$ wpscan --url http://target.com --enumerate u

# Enumerate Usernames and Write Output to File
$ wpscan --url http://target.com --enumerate u --log logfile

# Enumerate Vulnerable Plugins and Usernames, and Save Output to File
$ wpscan --url http://target.com --enumerate vp,u --log logfile
```

Setting Up Target 1

We need to run a few commands on Target 1in order to ensure it forwards logs to Kibana. Run the following on the VM:

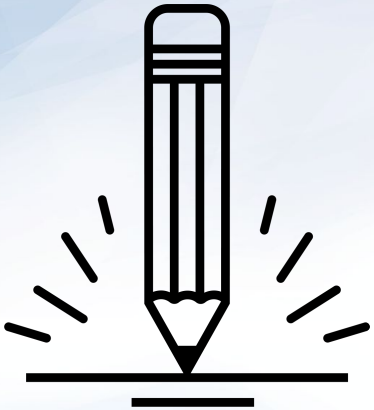
01 Open the Hyper-V Manager.

02 Connect to Target 1.

03 Login with username `vagrant` and password `tnargav`.

04 Escalate to root with `sudo -s`.

05 Run `/opt/setup`.



Day 1 Activity: Target No. 1

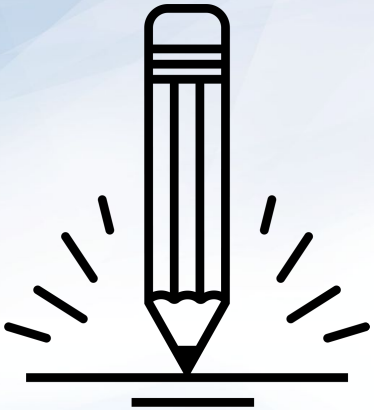
Today, you will configure Kibana based on Project 2 alert recommendations, test alerts by performing exploits against the Capstone VM, and capture flags on Target 1.

Suggested Time:
Full Class Time

Day 2: Target Assessment Cont’d.

Welcome back!

Today you will continue the finish assessing Target 1. Then you will begin the Wireshark traffic analysis.



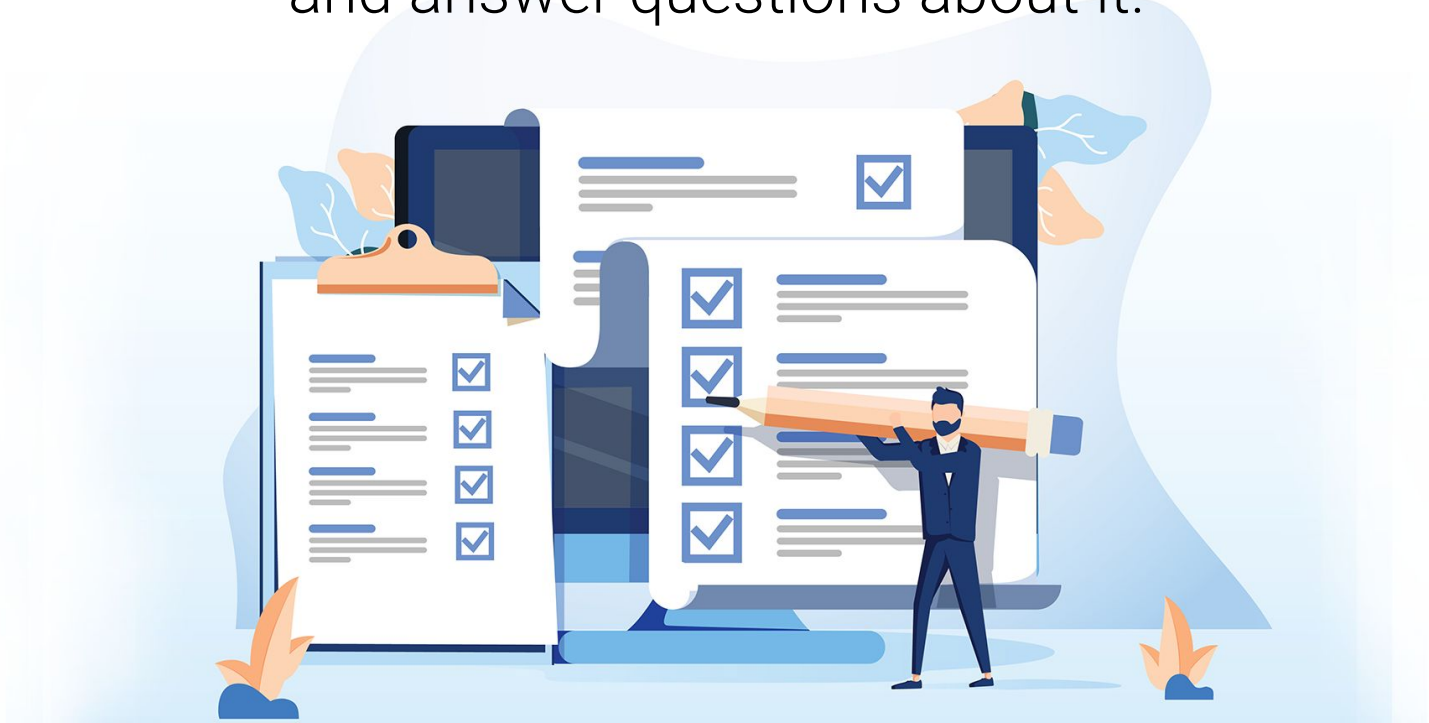
Day 2 Activity: Target No. 1

Today, you will complete the Target 1 assessment and begin analyzing traffic with Wireshark.

Suggested Time:
Full Class Time

Day 3: Network Analysis

On Days 1 and 2, you configured alerts in Kibana and attacked Target 1.Today, you will use **Wireshark** on the Kali VM to capture traffic from the virtual network. You will then analyze the traffic and answer questions about it.



Analyzing Traffic with Wireshark

To get started, you will need to:

01 Connect to the Kali VM.

02 Launch Wireshark and capture traffic on the **`eth0`** interface.

03 Save the capture to file.

04 Profile users' behavior from their packet data.

Analyzing Traffic with Wireshark

Specifically, you will be looking for information such as:

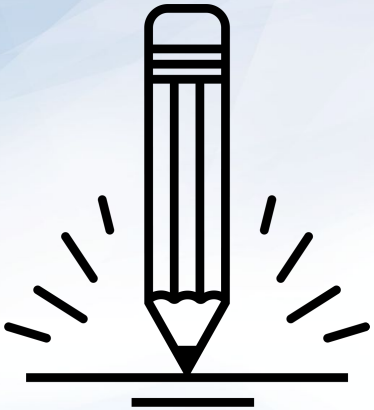
- Protocols in use.
- Network activity, such as web browsing, downloading files via FTP, torrenting, etc.
- Number of machines sending traffic.

Group Presentations

Once you have completed the Wireshark analysis, you will work in groups to develop a presentation of your three-day findings. You will present in the next class.

In groups of 3-6, you will work on a presentation that include a Red Team section, a Blue Team section and Network Analysis section.

One or two students should work on each section. Then as a group, you will combine the three sections to create a single cumulative presentation.

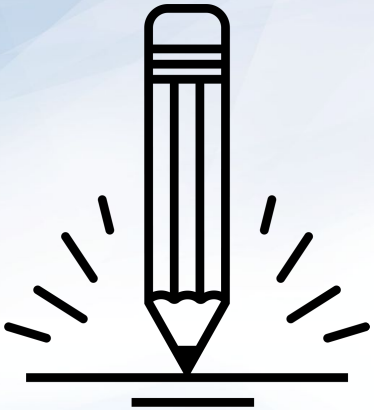


Day 3 Activity: Wireshark Strikes Back

Today, you will use the Kali VM to analyze live traffic and answer questions about various security incidents.

Suggested Time:
Full Class Time

Group Activity: Prepare Presentations



Once you have completed the three days' activities, Join your groups and begin working on your presentation. Templates for each section are available on Google Drive:

Red Team Presentation Template

Blue Team Presentation Template

Network Analysis Presentation Template

Suggested Time:
Remaining Class Time

Day 4:
Finalize Deliverables and Group Presentations

End of Project Deliverables

01 Red Team Report of Target 1

02 Blue Team Report of Target 1

03 Network Analysis of Wireshark Task

04 Group Presentation