12.2 - Project Week (Day 2)

Class Preparation

1. Check into BCS
2. Update your git repository with ``git pull``
3. Launch/login to your **PERSONAL** Azure Portal

Homeworks Due

- Unit 11 (Cloud): due Sunday December 20
- Unit 12 (Project): due Sunday January 10

Upcoming Units

- Week 13: Cryptography (1/04 - 1/09)
- Weeks 14 & 15: Web Development, Vulnerabilities, and Hardening (1/11 - 1/23)

Schedule Notes

Winter Break - No Class

- Last class on Sat 12/19
- Off: Mon 12/21 - Sat 1/02
- Return on Monday 1/04

Schedule Change

- Crypto delayed until after Winter Break

Holidays (No Class)

- Mon 1/18 (MLK Day)
- Mon 2/15 (Presidents' Day)

Welcome to Project Week!

This week, you will set up an ELK stack server to monitor your cloud network.

Day 2: Filebeat

You completed installing the ELK server and will now install data collection tools called Beats.

If you have not completed all Day 1 activities, you can continue working on those tasks.

Beats

The ELK stack works by storing log data in Elasticsearch with the help of Logstash.

- While functional, this approach is not ideal because it requires administrators to collect all data reported by tools like `syslog`, even if they only need a small portion of it.

For example: Administrators often need to monitor changes to specific files, such as `/etc/passwd`, or track specific information, such as a machine's uptime.

In cases like this, it is wasteful to collect all of the machine's log data in order to only inspect a fraction of it.

Beats

Recently, ELK addressed this issue by adding an additional tool to its data collection suite, called **Beats**.

- Beats are special-purpose data collection modules. Rather than collecting all a machine's log data, Beats allow you to collect only the very specific pieces you’re interested in.
- ELK officially supports eight Beats. We will use two of them in this project:
  - **Filebeat** collects data about the file system.
  - **Metricbeat** collects machine metrics, such as uptime.

beats

elastic.co/beats/

Filebeat

Filebeat helps generate and organize log files to send to Logstash and Elasticsearch. Specifically, it logs information about the file system, including which files have changed and when.

FILEBEAT

- Filebeat is often used to collect log files from very specific files, such as those generated by Apache, Microsoft Azure tools, the Nginx web server, and MySQL databases.
- Since Filebeat is built to collect data about specific files on remote machines, it must be installed on the VMs you want to monitor.

(elastic.co)

Time's Up

By the end of this class, your ELK server should be receiving logs. You'll have:

- Installed and launched Docker containers to a host machine.
- Configured and deployed an ELK server.
- Installed Filebeat on a Linux server.

(Completing the Metricbeat installation was a similar process.)

Day 2 Activity: Filebeat

Today, you will install Filebeat and Metricbeat on the DVWA container you created during the cloud week.

This will provide a rich source of logs when you complete you deployment.

Bonus: install Metricbeat

Suggested Time:
Full Class Time