Using Kibana to analyze logs taken during the Red Team attack, use the data to develop ideas for new alerts that can improve your monitoring.

After creating your dashboard and becoming familiar with the search syntax, use these tools to answer the questions below:

1. Identify the offensive traffic.

    - Identify the traffic between your machine and the web machine:
        - When did the interaction occur?
          May 1, 2021 from 6pm to 9pm
        - What responses did the victim send back?
          404, 200, 400
        - What data is concerning from the Blue Team perspective?
          All the request queries.
2. Find the request for the hidden directory.

    - In your attack, you found a secret folder. Let's look at that interaction between these two machines.
        - How many requests were made to this directory? At what time and from which IP address(es)?
          9919 requests. May 2 at 2pm from
        - Which files were requested? What information did they contain?
          2 files, the passwd.dav and shell.php. They contained hash's, encrypted passwords.
        - What kind of alarm would you set to detect this behavior in the future?
          Set an alarm for
        - Identify at least one way to harden the vulnerable machine that would mitigate this attack.
          Remove the folder from public view. Take it off the server.

3. Identify the brute force attack. (We have hydra, we have 10k hits, & password protected secret folder)

    - After identifying the hidden directory, you used Hydra to brute-force the target server. Answer the following questions:
        - Can you identify packets specifically from Hydra?
          Packets from user_agent: Mozilla/4.0 (Hydra).
        - How many requests were made in the brute-force attack?
          Over 10,000 hits.
        - How many requests had the attacker made before discovering the correct password in this one?
          2
        - What kind of alarm would you set to detect this behavior in the future and at what threshold(s)?
          User agent Hydra or HTTP Response code of 401. Limit bad attempts over 75.
        - Identify at least one way to harden the vulnerable machine that would mitigate this attack.
          Block Hydra, increase lockout attempts,

4. Find the WebDav connection.

    - Use your dashboard to answer the following questions:
        - How many requests were made to this directory?
          38 hits (Packetbeat)
        - Which file(s) were requested?
          Shell.php and passwd.dav
        - What kind of alarm would you set to detect such access in the future?
          Checking file extensions for .php files types. Monitor when files are created on a server.
        - Identify at least one way to harden the vulnerable machine that would mitigate this attack.
          Limit the devices/machines that have access to the server. Using IP Whitelisting as a technique or strict rules with in the network.

5. Identify the reverse shell and meterpreter traffic.

    - To finish off the attack, you uploaded a PHP reverse shell and started a meterpreter shell session. Answer the following questions:
        - Can you identify traffic from the meterpreter session?
          Yes, from port 4444 you are able to see shell.php was PUT and GET requests. But details are not clear when it was executed.
        - What kinds of alarms would you set to detect this behavior in the future?
          Create a log for traffic on 4444. Anything being uploaded as a php, block it.
        - Identify at least one way to harden the vulnerable machine that would mitigate this attack.
          IDS to pick up on when there is a connection. 444 was seen with traffic.

Day 3 Activity File: Reporting

Congratulations, you've made it! You've worn two hats this week, playing the roles of both attacker and defender. Don't underestimate the magnitude of this achievement: Learning enough to infiltrate a machine and analyze data collected during the attack is a milestone that takes many professionals a long time to achieve.

Today, you'll take a break from flexing your technical skills and focus on communicating what you've learned in the past two days. In a real engagement, your client pays you not to break into their network, but to teach them how to protect it. This is why communication skills are vital in the cybersecurity field.

To that end, you will summarize your work in a presentation containing the following sections:

- **Network Topology**
    - What are the addresses and relationships of the machines involved?
    - All of the VMs in the attack should be described. Optionally, you can also include the hypervisor machine itself.
- **Red Team**
    - What were the three most critical vulnerabilities you discovered?
        - Choose the three vulnerabilities that *you* consider to be most critical.
- **Blue Team**
    - What evidence did you find in the logs of the attack?
    - What data should you be monitoring to detect these attacks next time?
- **Mitigation**
    - What alarms should you set to detect this behavior next time?
    - What controls should you put in place on the target to prevent the attack from happening?

Instructions

Open the template on Google Slides: Project 2 Report Template

- Make a copy by clicking **File** > **Make a Copy**.
- Fill out the prompts on the slides as indicated. Make sure to remove all instructional text and prompts.
- Some examples of vulnerabilities to look for are:
    - Sensitive Data Exposure
    - Unauthorized File Upload
    - Remote Code Execution
    - Brute Force Vulnerability

- Local File Inclusion
- Cross Site Scripting
- Code Injection
- SQL Injection
- Security Misconfiguration

This presentation is due as homework. You must complete and submit it on BCS for credit. And remember, this document can be used to display your knowledge to interviewers and the larger cybersecurity network, so make it professional and presentable!