Excessive User Rights
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

Unknown users in your organization have been known to install and use unauthorized peer-to-peer (P2P) file sharing and Internet chat applications on their computers. You received an anonymous tip mentioning several of these users were using these applications on **April 15th, 2020** between the times of **1900-1959 UTC**

Use FireSIGHT alerts to begin your analysis.

Pivot within FireSIGHT's events to derive likely hypotheses. Correlate these possibilities with lab4.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:

- P2P Policy Violator
  - IP Address: _____
  - P2P Client/Version Used: _____
- P2P Infrastructure
  - IP Address: _____
  - Ports Used (e.g., 80/TCP): _____
  - Protocol Used (e.g., HTTP): _____
- Chat Policy Violator
  - IP Address: _____
- Chat Infrastructure
  - IP Address: _____
  - Port Used (e.g., 80/TCP): _____
  - Protocol Used (e.g., HTTP): _____

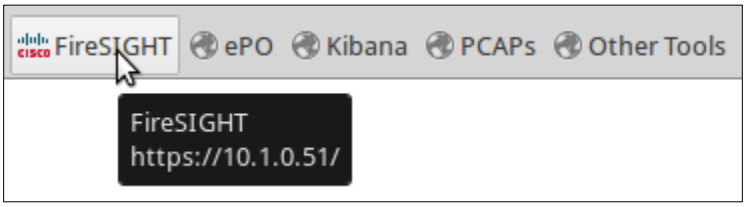
ANALYSIS PROCESS
Follow along with the video as it goes through the following steps of analysis.

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.

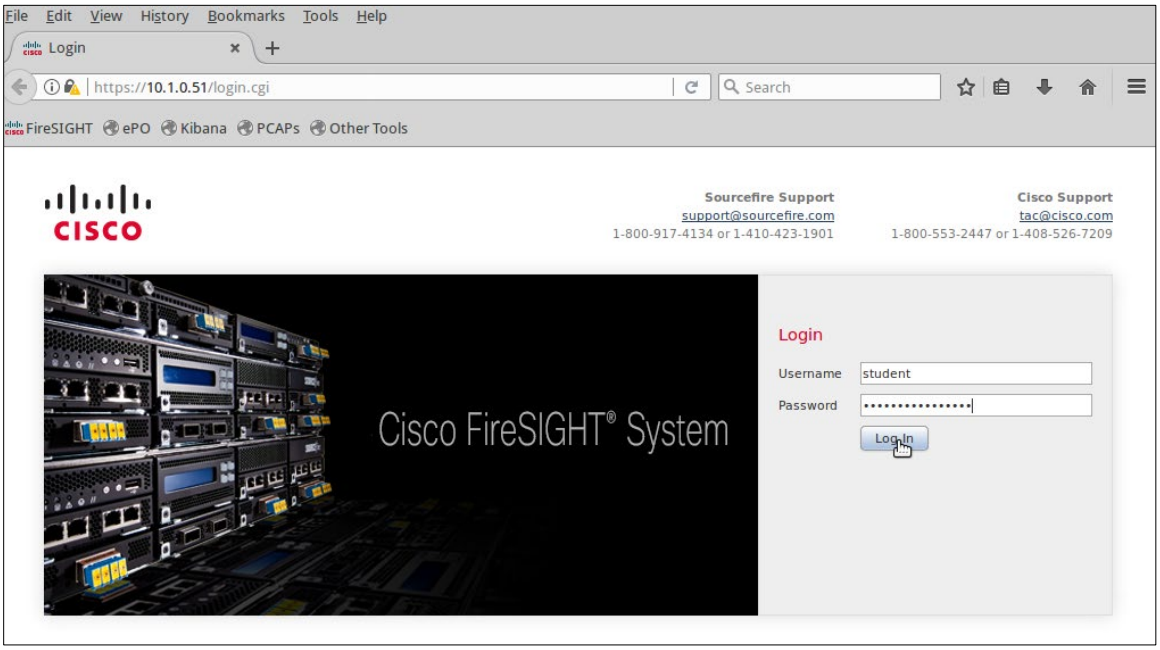
Note: Potential Indicators of Compromise (IoC), such as IP addresses and domain names, should be "de-fanged" as a best practice. De-fanging simply involves the insertion of a character into the IoC that is otherwise invalid in the IoC's context, so that copying/pasting/clicking the IoC won't inadvertently 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).

Step 1: Searching within FireSIGHT

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

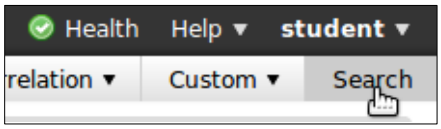


2. Enter the username "Student" and password "12qwaszx!@QWASZX" and press "Log In".

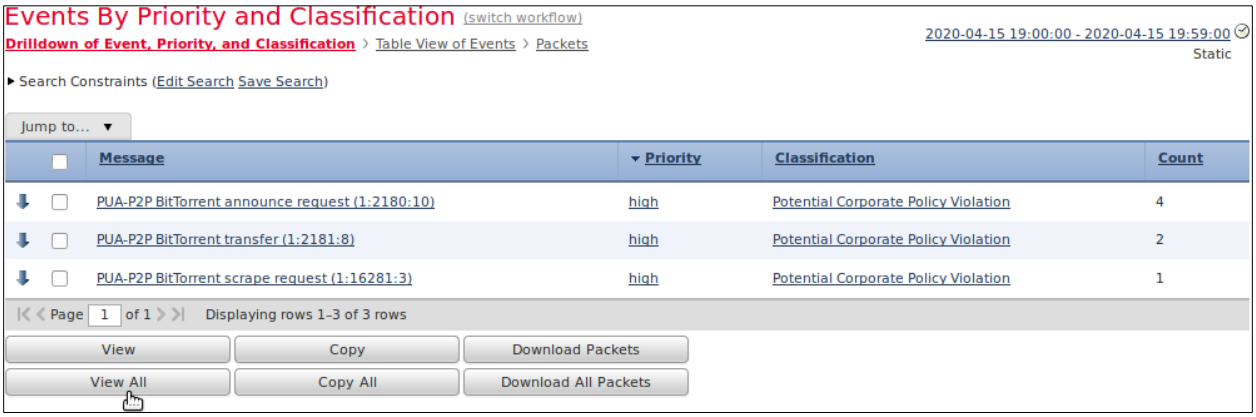


3. Configure the timeframe to **April 15th, 2020 between 1900 and 1959 UTC** as mentioned the instructions. Use the steps described in the first lab as a guide. FireSIGHT populates with events from the specified timeframe.

4. The lab instructions mentioned users abusing their permissions to install and use peer-to-peer (P2P) software. Search FireSIGHT for events associated with these applications. Looking for the term “P2P” in **Messages** might work. Enter “P2P” and press "Search".



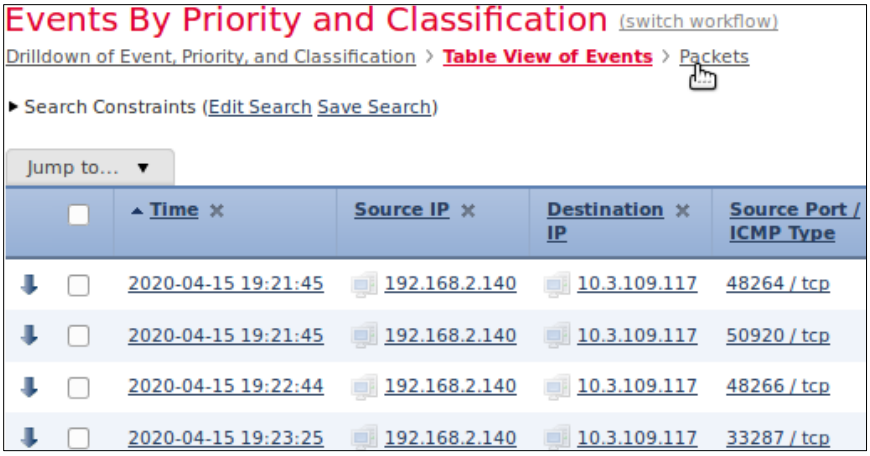
FireSIGHT returns a list of grouped events in a tabular format.



Step 2: Viewing Event Details (P2P)

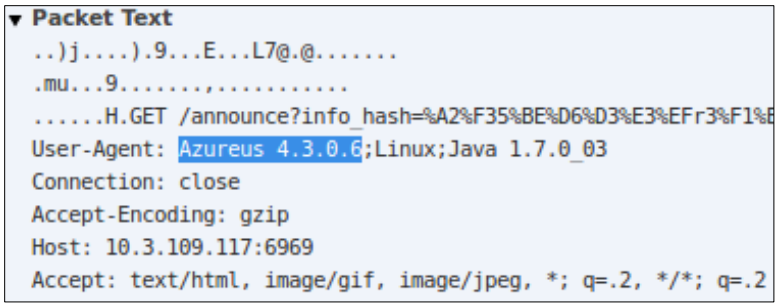
1. Review the search results and note several BitTorrent alerts. BitTorrent is a common P2P application client and protocol. Press "View All" since all alerts appear to be relevant. FireSIGHT displays several events for these alerts. Select the "Time" column header to sort the events from oldest to newest to create an easy-to-read, top-down timeline.

Note the Source IP originated from the 192.168.2.0/24 trusted network and the Destination IP was part of the 10.0.0.0/8 untrusted network. Select the "Packets" link to inspect the details of these events.



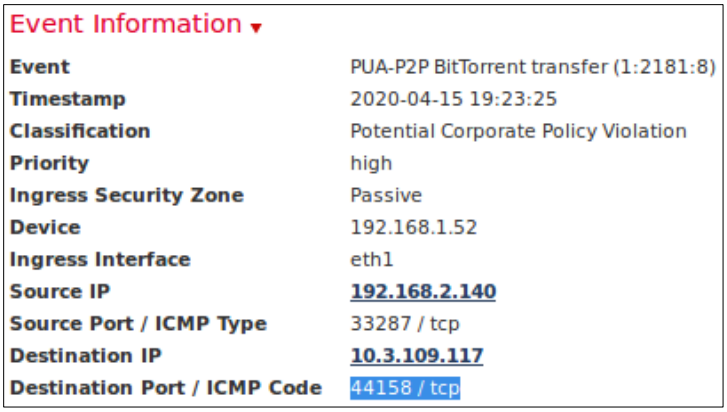
2. On the resulting page notice the first packet contained a BitTorrent announcement in the "Event" field. The source of the announcement using the unauthorized software is the host at *192.168.2[.]140* and the destination is the P2P infrastructure server at *10.3.109[.]117* on *TCP port 6969* using the *BitTorrent* protocol.

Expand "Packet Text" to investigate the payload. Notice the name of the BitTorrent P2P client was *Azureus* and its version was *4.3.0.6*.

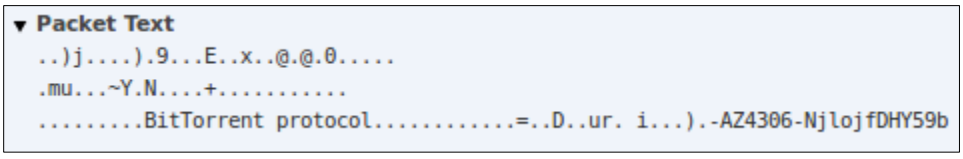


Once you have finished analyzing the current event, scroll down and press the ">" button to move on to the next event.

3. Skim through the second and third events following the same process as above. Once you get to the fourth event, notice the "BitTorrent Transfer" event. Here, the destination is the P2P infrastructure server at 10.3.109[.]117 again but it uses *TCP port 44158* instead.

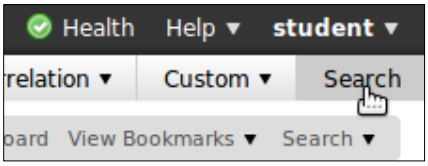


Expand "Packet Text" to investigate the payload of the "BitTorrent Transfer" events. Notice the "BitTorrent protocol" text in the payload, further confirming a P2P application was used.

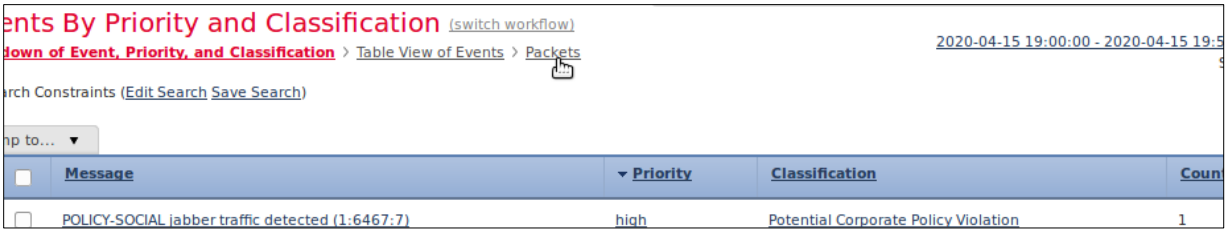


Step 3: Searching & Viewing Event Details (Internet Chat)

1. The lab instructions mentioned users abusing their permissions to install and use Internet chat software. Search FireSIGHT for events associated with these applications. Since chat events are often triggered by "Policy" rules, looking for this term in **Messages** might work. Enter "Policy" in this field and press "Search".



2. Review the search results and note the Jabber alert. Jabber is a common chat application. Since there is only one event for this alert, skip the Table View of Events view by selecting the "Packets" link directly to inspect its details.



3. On the resulting page in the Packet Information section, note the traffic originates from the internal policy violator at **Src** *192.168.2[.]30* to the external Internet chat server at **Dst** *10.45.90[.]123* on *TCP port 5222*.

This section also includes a reference to the *XMPP* chat protocol supported by the Jabber client. Expand "Packet Text" to investigate the payload. Notice it correlates the use the Jabber client with this protocol.

ANSWERS

- P2P Policy Violator
  - IP Address: **192.168.2[.]140**
  - P2P Client/Version Used: **Azureus/4.3.0.6**
- P2P Infrastructure
  - IP Address: **10.3.109[.]117**
  - Ports Used (e.g., 80/TCP): **6969/TCP & 44158/TCP**
  - Protocol Used (e.g., HTTP): **BitTorrent**
- Chat Policy Violator
  - IP Address: **192.168.2[.]30**
- Chat Infrastructure
  - IP Address: **10.45.90[.]123**
  - Port Used (e.g., 80/TCP): **5222/TCP**
  - Protocol Used (e.g., HTTP): **XMPP**