Service-Side Attacks and Detection
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 **15 April 2020**, an adversary attacked a Windows server on the network between the times of **1700-1759 UTC**.

Note that commonly used ports for Windows servers include the following TCP ports: 135, 137, 139, and 445.

Use FireSIGHT alerts to begin your analysis.

Pivot within FireSIGHT's events to derive likely hypotheses. Correlate these possibilities with host intrusion prevention events in ePO and lab2.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): _____
- 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) _____

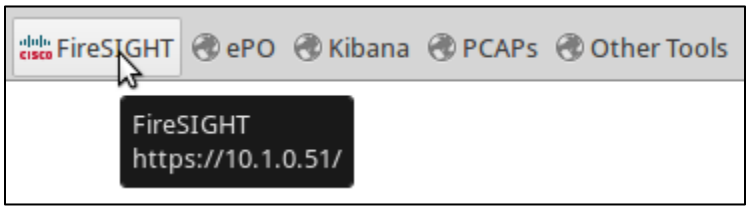
ANALYSIS PROCESS
Follow along with the video as it goes through the following steps of analysis.

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.

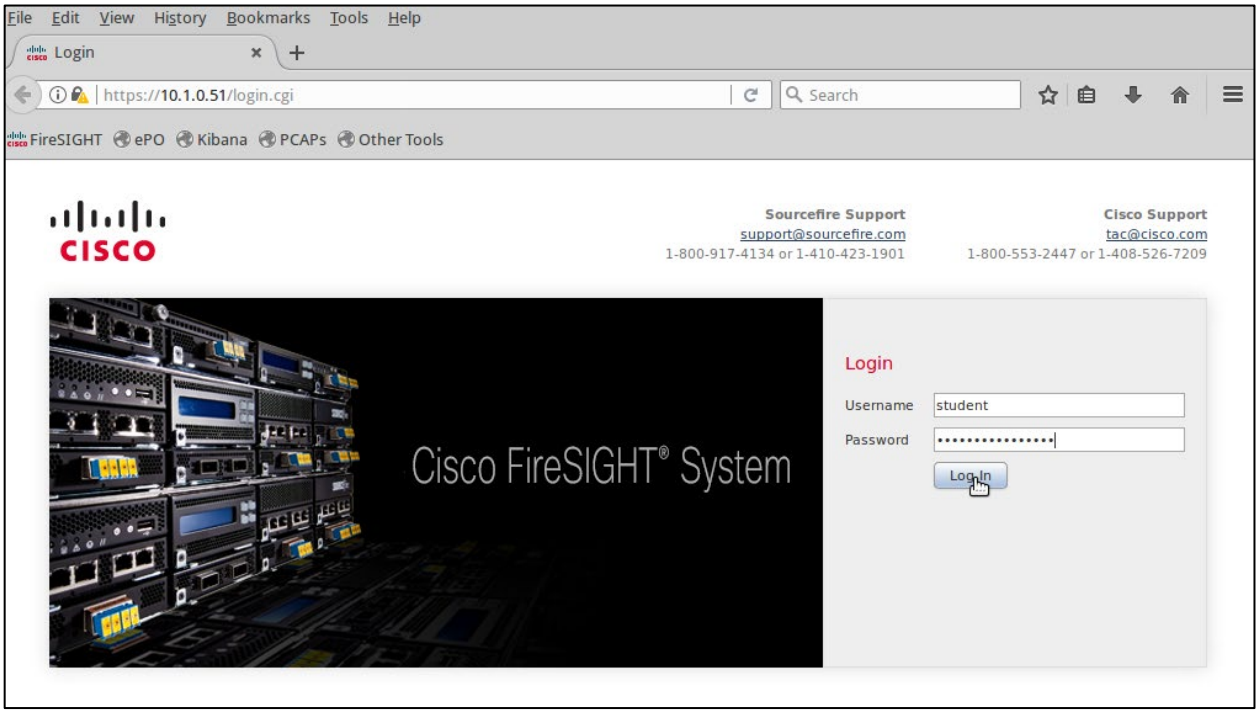
Note: Potential Indicators of Compromise (IoC), such as IP addresses and domain names, should be "de-fanged" as a best practice. De-fanging simply involves the insertion of a character into the IoC that is otherwise invalid in the IoC's context, so that copying/pasting/clicking the IoC won't inadvertently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

Step 1: Searching within FireSIGHT

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

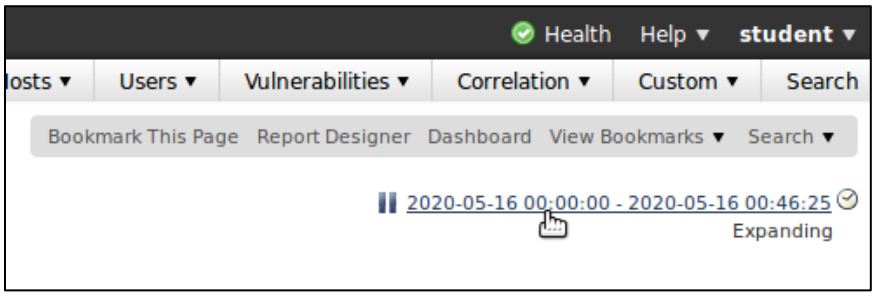


2. Enter username "**student**" and password "**12qwaszx!@QWASZX**" and select **Log In**.

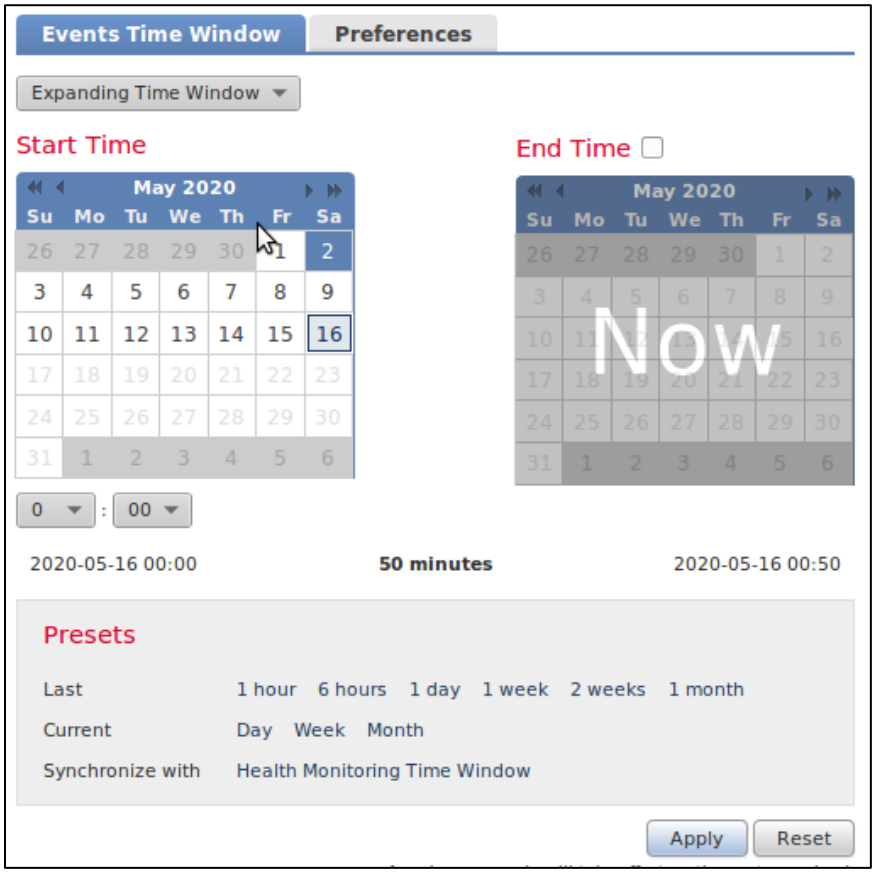


FireSIGHT displays the intrusion events screen by default. Notice no events are listed since the timeframe is not set correctly as discussed in the first exercise.

3. Configure the correct timeframe mentioned in the instructions. Start by selecting the date/time range near the top-right corner of the window.



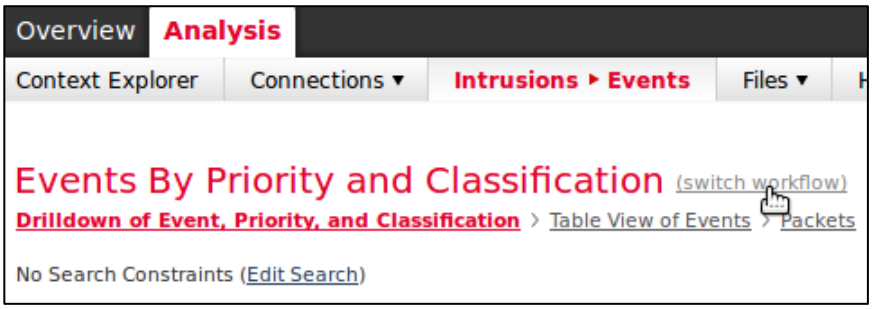
Ensure the **Events Time Window** tab is selected in the date picker pop-up. Using any of the date range selection steps from the first lab as a guide, configure the start and stop times to **April 15th, 2020 between 1700 and 1759 UTC**. Press **Apply** when finished.



Verify the start and stop times displayed directly above the **Presets** heading are correct. Press **Apply** when finished. FireSIGHT populates with events from the specified timeframe.

4. The solution to Exercise 1 narrowed in on the more important events of the attack at this point by searching on the IP address in news link. This lab is missing such an indicator so the previous filtering technique does not work. It does mention commonly used ports for Windows servers, though. This information may be useful in another one of FireSIGHT's workflows.

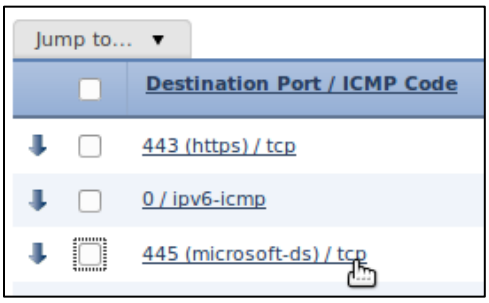
   Select the "(switch workflow)" link to get started.



   FireSIGHT displays its different workflows. Knowing a Windows server was attacked, NetBIOS TCP port 139 and SMB TCP port 445 are good places to start. Since server ports are usually connected to as a destination by other clients, a workflow suited for this information is **Destination Port**. Select this option to continue.

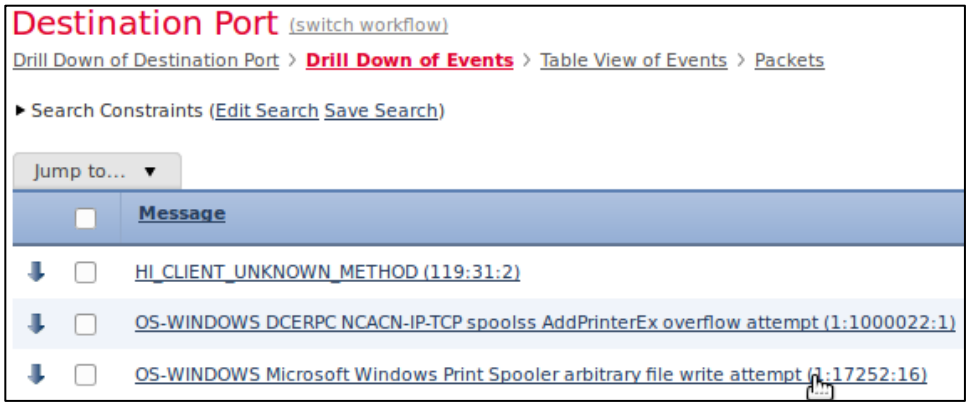
5. The Destination Port workflow displays a list of destination ports in descending order based on port event count.

FireSIGHT displays both TCP port 139 and TCP port 445 near the top of the destination port list. Since TCP port 445 received the highest count of the two ports, select "445 (Microsoft-ds) / tcp" to drilldown further to view its associated events in Table View of Events.

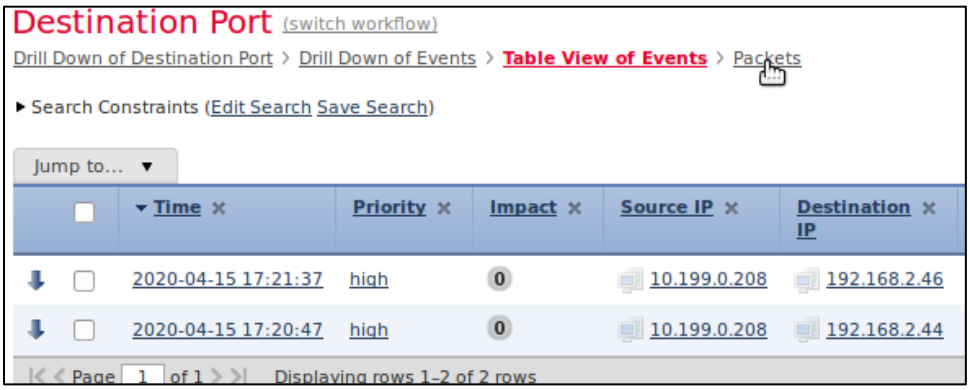


Step 2: Viewing Event Details

1. FireSIGHT displays several events related to TCP port 445. Notice the "OS-WINDOWS Microsoft Windows Print Spooler arbitrary file write attempt (1:17252:16)" alert. This event is of interest for this scenario since it is associated with a service-side remote code execution (RCE) vulnerability (i.e., MS10-061). Select it to drilldown further.

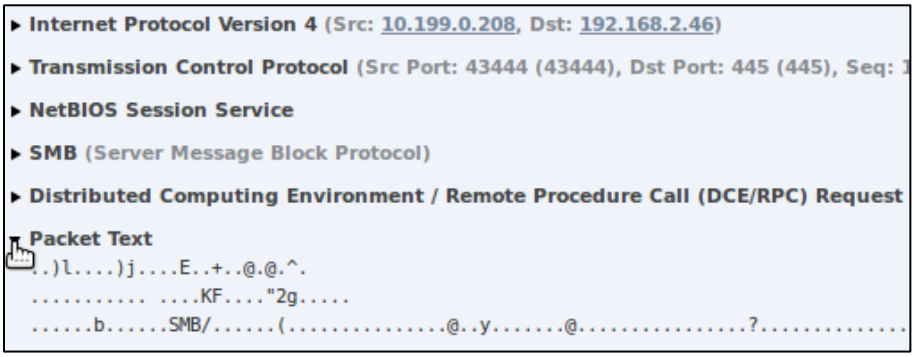


2. Two events are listed in the FireSIGHT console below. Note the source IP originates from 10.0.0.0/8 (i.e., the lab's untrusted fake Internet) and the destination IP is part of 192.168.2.0/24 (i.e., the lab's trusted Intranet).

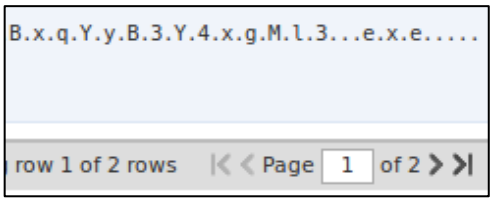


Printer-related traffic over SMB is not inherently malicious since it facilitates resource sharing and inter-node communication within networks. Such traffic occurring between untrusted and trusted networks is unusual though. A single external IP having RCE alerts to two internal IPs provides further evidence of potential malicious intentions.

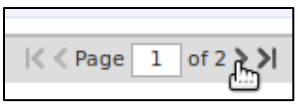
3. Select the **Packets** link above to inspect the details of these two events. FireSIGHT displays the contents of the first alert. Scroll down to **Packet Text** and expand its contents to investigate the payload sent to 192.168.2[.]46. Note the "SMB/" header.



Scrolling the browser window to the right reveals a reference to a transferred Windows executable file named "*BxqYyB3Y4xgMl3[.]exe*."



Select **Packet Text** again to collapse its contents. Choose ">" to the right of "Page 1 of 2" at the bottom-right of the window to investigate the second alert.

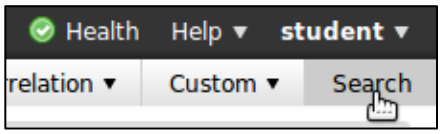


Scroll down to **Packet Text** again and expand its contents to investigate the payload sent to 192.168.2[.]44. Note an executable file named "*HFNQGTq3PLJSU[.]exe*" is found when scrolling to the right.

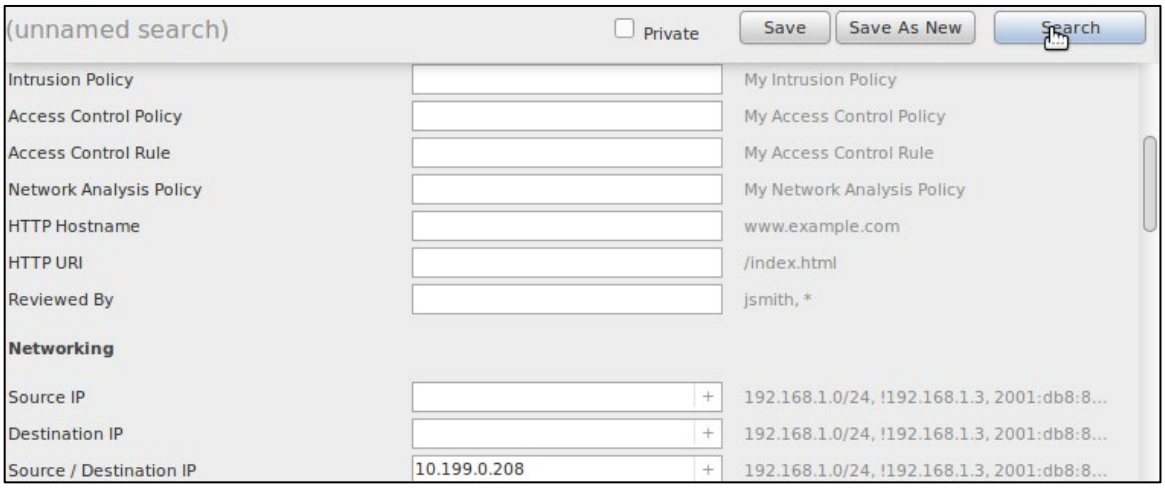
Coupled with the associated alerts, it appears an adversary at *10.199.0[.]208* attacked victims at *192.168.2[.]44* and *192.168.2[.]46* using the *SMB* protocol over *TCP port 445*. The files *BxqYyB3Y4xgMl3[.]exe* and *HFNQGTq3PLJSU[.]exe* appear to be Stage 2 payloads transferred directly from the adversary.

4. At this stage, further correlation within FireSIGHT is warranted to confirm the above hypothesis and determine if any other attacks were carried out. With a potential adversary IP address, use FireSIGHT's search capability to narrow in on the more important events.

   As performed in Exercise 1, select **Search** on the right side of the Analysis menu to begin.

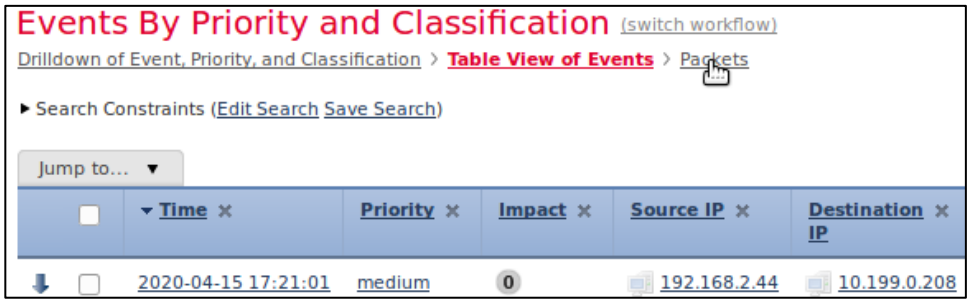


   Enter "10.199.0[.]208" in the **Source/Destination IP** field and press **Search**.

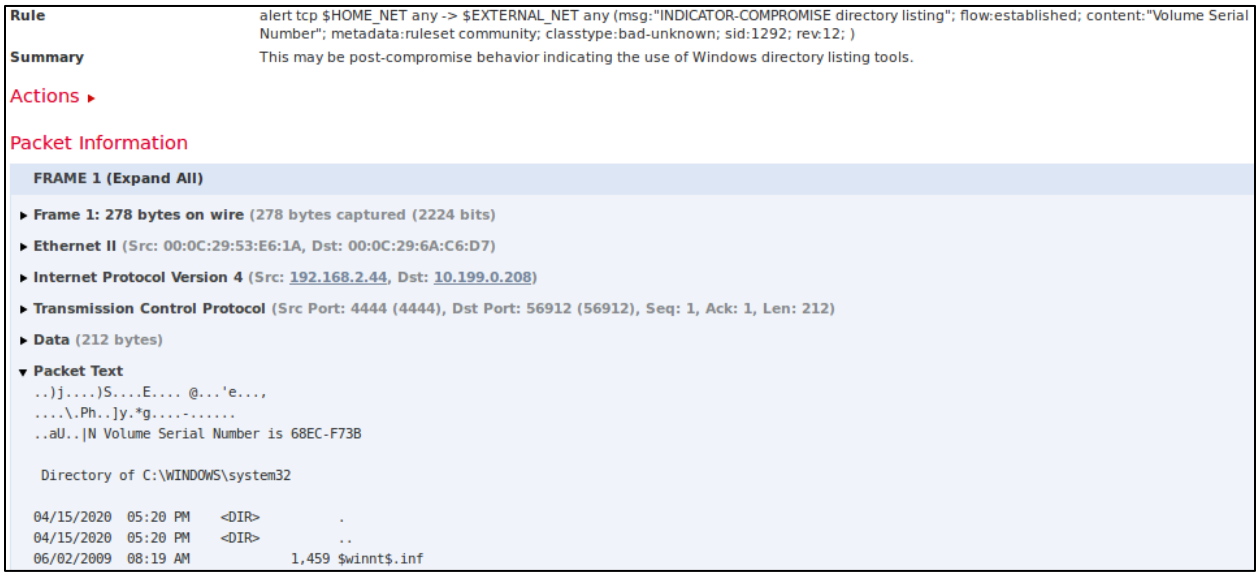


5. Notice the "INDICATOR-COMPROMISE directory listing (1:1292:12)" alert in the results. This event may indicate a potential IoC was detected. Select it to drilldown further.

FireSIGHT displays events associated with this alert. Note the 192.168.2[.]44 victim was the source of traffic and the 10.199.0[.]208 adversary was the destination. This communication may indicate C2 activity.

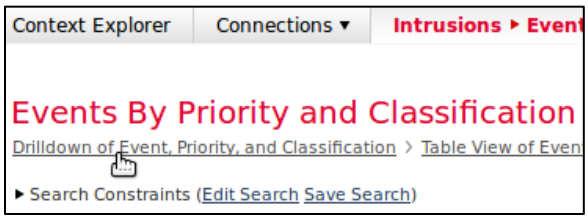


6. Select the **Packets** link above to inspect the details of this event. Scroll down to **Packet Text** and expand its contents to investigate what was sent to the adversary. Notice the payload shows a Windows command line header and a directory listing for "C:\Windows\System32."

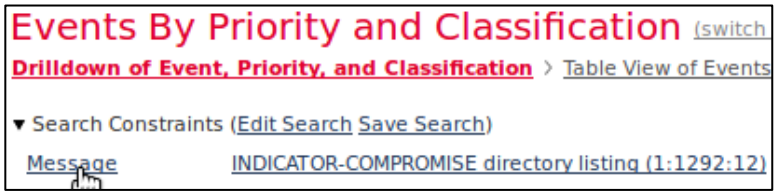


Analysis of the **Rule** field above indicates this alert was triggered by the "Volume Serial Number" content within the packet. It appears the **`dir`** command was executed and the results were returned to the adversary using *TCP port 4444* as a C2 channel.

7. Other alerts returned during the search for 10.199.0[.]208 need to be investigated as well. Return to the list of results by selecting **Drilldown of Event, Priority and Classification**.



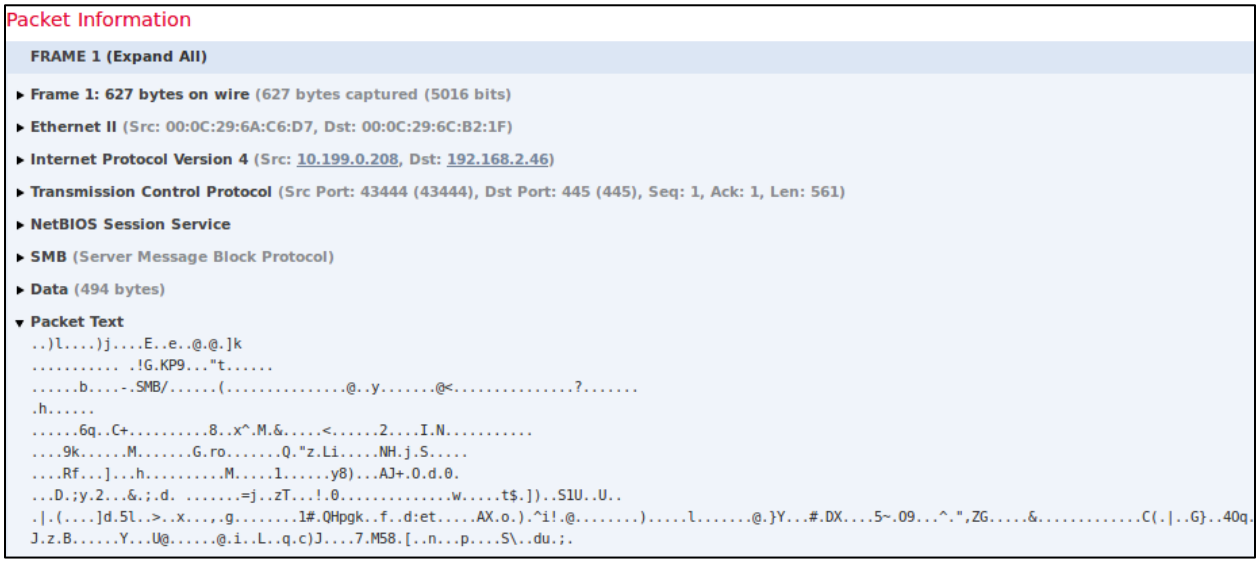
Notice only the alert previously investigated is visible. To bring all other alerts back, expand **Search Constraints** and select **Message** to remove this constraint.



Select **Search Constraints** again to collapse the list for more viewing space.

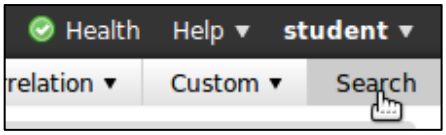
8. In the resulting list, notice the "SHELLCODE x86 NOOP" and "SHELLCODE Shikata Ga Nai x86 polymorphic shellcode decoder detected" alerts. These events may describe how the exploit used in the attack was encoded. Alerts like these may not always fire due to the use of random number generation within various types of malware.

   The following figure shows the **Packet Text** for the "SHELLCODE Shikata Ga Nai" alert associated with the adversary's attack on 192.168.2[.]46 over SMB (TCP port 445).

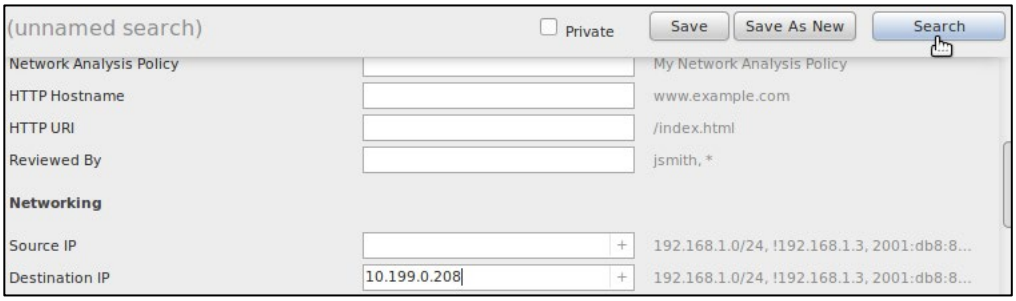


9. Knowing at least one of the victims communicated with the adversary's C2 system, it is time to determine if other victim-initiated communications to this host exist.

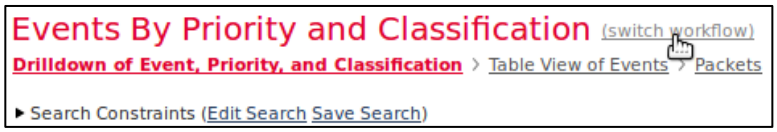
The easiest way to discover events to the C2 IP address is to use a search field that only matches destination IPs. Select **Search** in the Analysis menu again to begin.



Enter "10.199.0[.]208" in the **Destination IP** field and press **Search**.



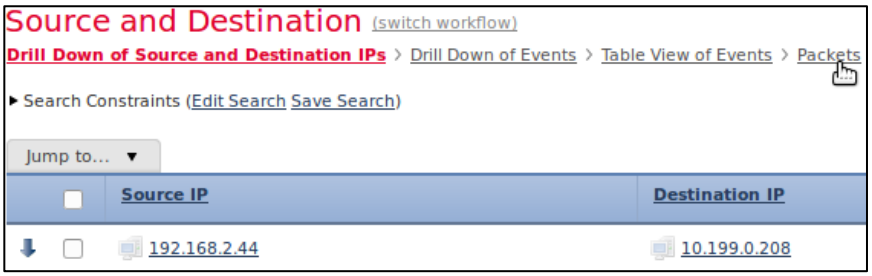
10. FireSIGHT returns a small list of events. To quickly determine the source IPs, start by selecting **(switch workflow)**.



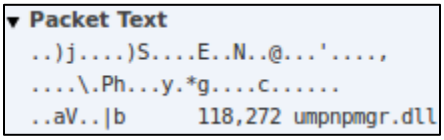
Choose **Source and Destination** from the **Events By Priority and Classification** dialog.

11. A short list of source/destination pairs appears, showing no other victims reaching out to the C2 infrastructure. This does not necessarily mean other hosts (e.g., 192.168.2[.]46) were not compromised. The malware may have just included a delay-mechanism.

Feel free to select **Packets** to view the data 192.168.2[.]44 sent to the attacker.



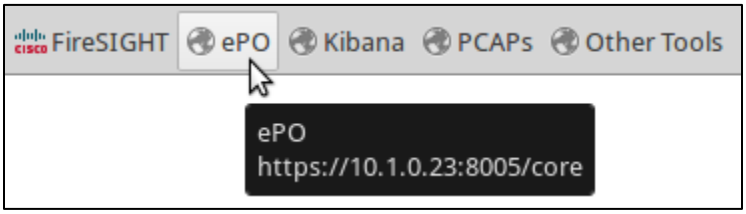
The first event contains a small amount of data. The content appears to be a filename within a folder listing. This may be a fragment of the previously executed **`dir`** command.



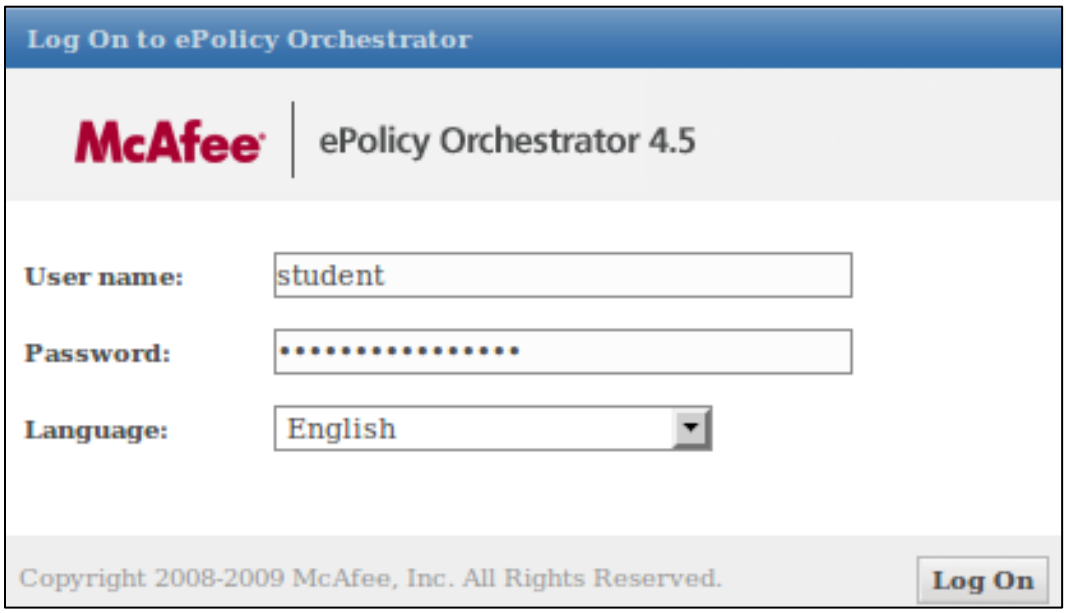
Step 3: ePO Event Correlation

Obtaining additional correlation data increases the likelihood of a hypothesis being correct. Analysis in FireSIGHT showed 192.168.2[.]44 called out to the adversary's C2 infrastructure. Even though it was attacked, 192.168.2[.]46 did not exhibit this behavior. The ePO console, which centralizes events from its Host-based Intrusion System (HIPS) agents installed on many of the network's hosts, may provide the data needed to determine if 192.168.2[.]46 was affected.

1. To access the ePO console, select the **ePO** bookmark within Mozilla Firefox.

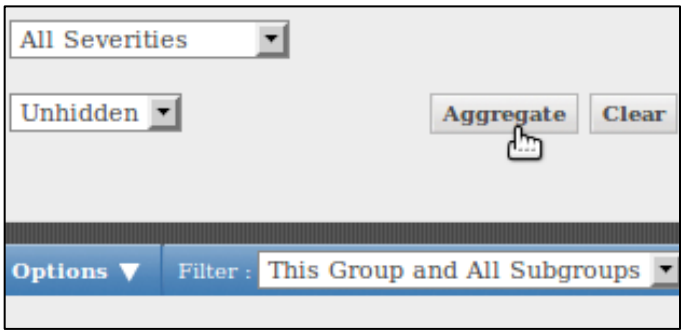


2. Enter username "**student**" and password "**12qwaszx!@QWASZX**" and press **Log On**.

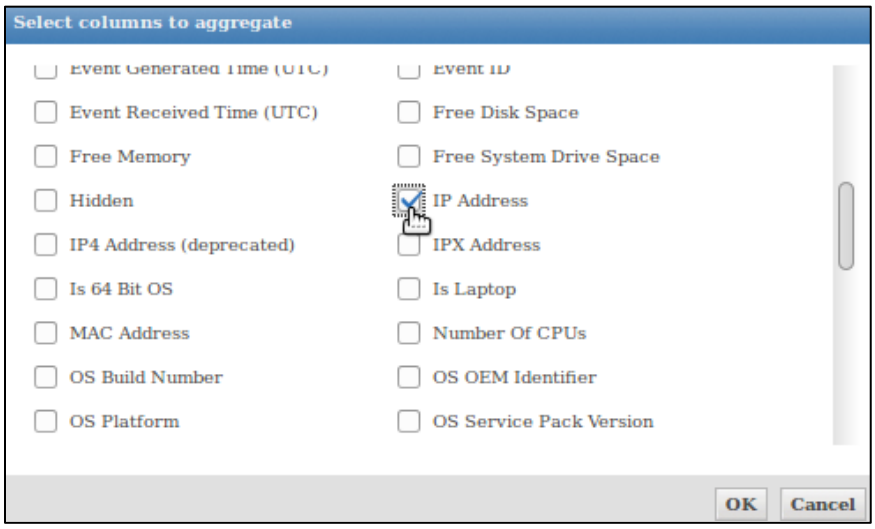


3. Access the HIPS reporting feature by selecting the **Host IPS** icon in the menu bar.

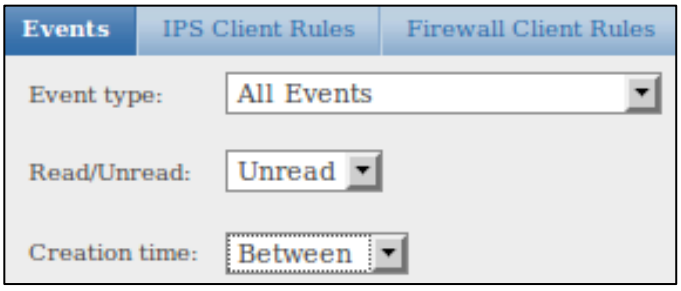
4. Organize Host IPS based on the IP addresses of the victims. Start by selecting "This Group and All Subgroups" within the **Filter** drop-down menu on the right-hand side of the window. Next, press the **Aggregate** button.



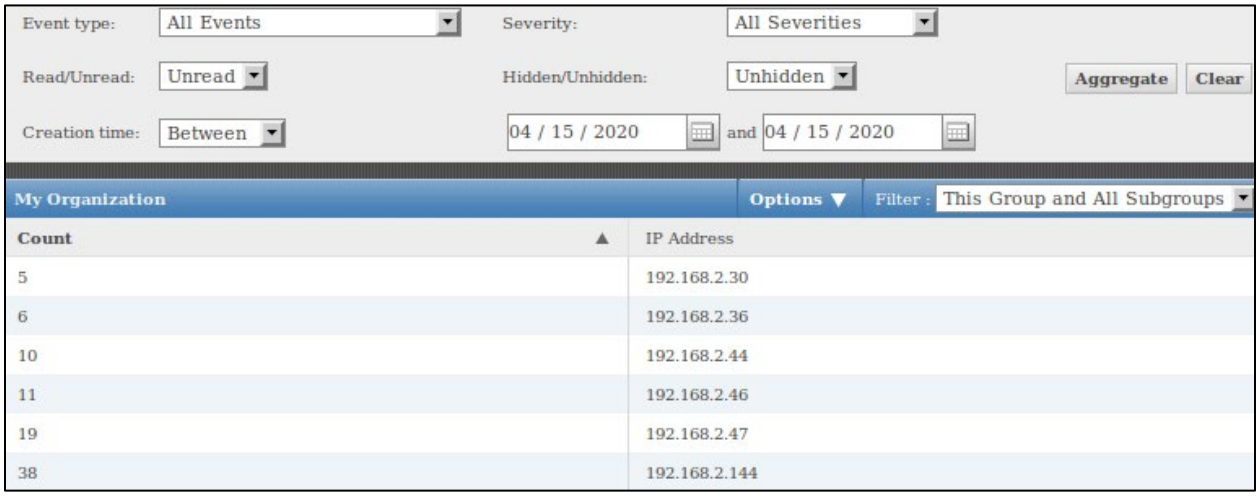
Select "IP Address" from the options and press **OK**.



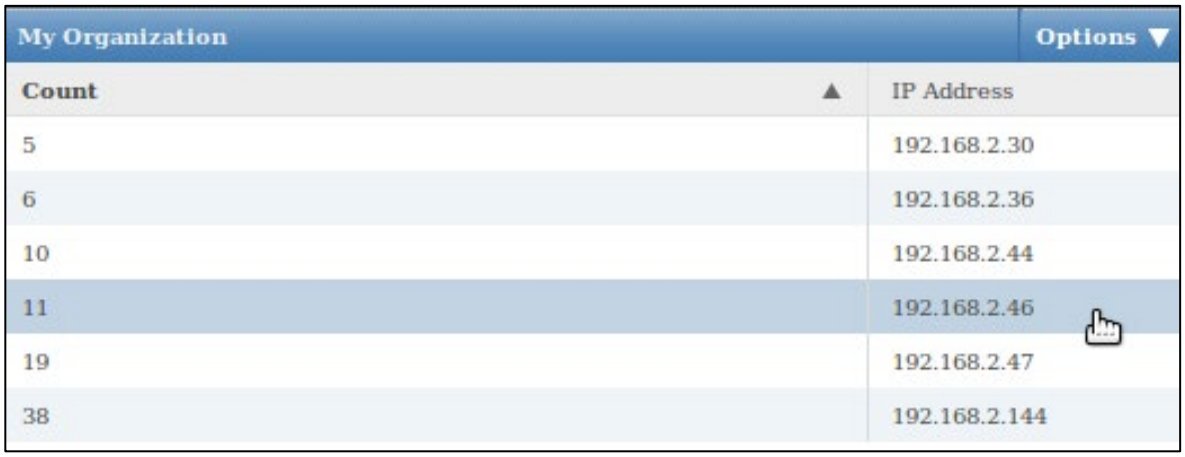
5. Narrow down the IP addresses and their aggregate event counts further by limiting events to the target timeframe. Select the **Creation Time** drop-down menu and choose the "Between" option.



ePO displays start and stop date pickers to the right of the **Creation Time** menu. Select the first one and set it to "April 15, 2020." Configure the second date picker to "April 15, 2020" as well. This timeframe represents April 15, 2020 0:00 UTC to April 15, 2020 23:59 UTC.



6. View the eleven (11) events associated with the **192.168.2[.]46** by selecting on this victim IP address.



A table of events for this IP address is displayed. ePO allows column customization to provide more useful data in this view. At the top-right of the table, click **Options** and select **Choose Columns**.

The default view provides the necessary details for this scenario. At the bottom of the window, press **Use Default** to set these columns and to return to the previous list of events.

7. In the list of results, two alerts in particular stand out: "Access Protection – Prevent creation of new executable files in the Windows folder" and "CMD tool access by a network-aware application." These alerts describe the Stage 2 executable files installed on the victims.

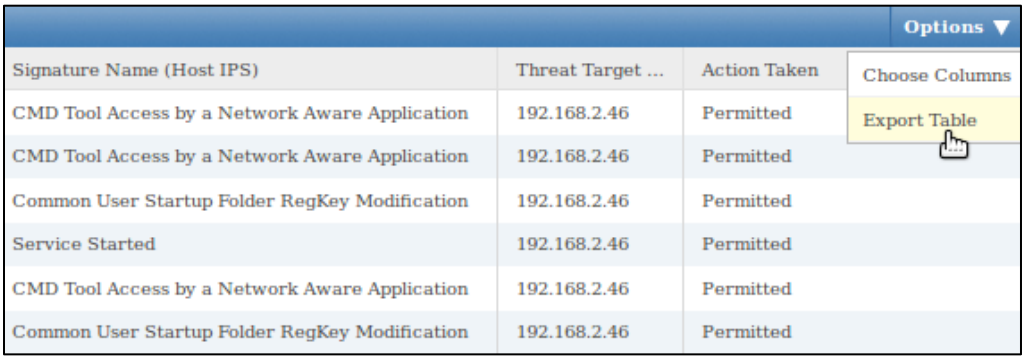
Event Generate... ▲	Threat Severity	System Name	Event Category	Signature Name (Hos...	Threat Targe
4/15/20 4:40:35 PM	Notice	INSTRUCT-169C3B	Host intrusion (hip.Files)	CMD Tool Access by a ...	192.168.2.46
4/15/20 4:40:35 PM	Notice	INSTRUCT-169C3B	Host intrusion (hip.Files)	CMD Tool Access by a ...	192.168.2.46
4/15/20 4:40:35 PM	Warning	INSTRUCT-169C3B	Host intrusion (hip.Regi...	Common User Startup ...	192.168.2.46
4/15/20 4:40:55 PM	Information	INSTRUCT-169C3B	Host intrusion (hip.Ser...	Service Started	192.168.2.46
4/15/20 4:41:11 PM	Notice	INSTRUCT-169C3B	Host intrusion (hip.Files)	CMD Tool Access by a ...	192.168.2.46
4/15/20 4:55:07 PM	Warning	INSTRUCT-169C3B	Host intrusion (hip.Regi...	Common User Startup ...	192.168.2.46
4/15/20 5:21:39 PM	Warning	INSTRUCT-169C3B	Host intrusion (hip.Files)	System File Modification	192.168.2.46
4/15/20 5:21:39 PM	Warning	INSTRUCT-169C3B	Host intrusion (hip.Files)	Access Protection - Pre...	192.168.2.46
4/15/20 5:21:43 PM	Notice	INSTRUCT-169C3B	Host intrusion (hip.Files)	CMD Tool Access by a ...	192.168.2.46
4/15/20 5:21:51 PM	Notice	INSTRUCT-169C3B	Host intrusion (hip.Files)	CMD Tool Access by a ...	192.168.2.46
4/15/20 5:21:55 PM	Warning	INSTRUCT-169C3B	Host intrusion (hip.Files)	System File Modification	192.168.2.46

Select “Access Protection – Prevent creation of new executable files in the Windows folder” above and scroll down to **files**. This field shows **BxqYyB3Y4xgMl3[.]exe**, the "Stage 2" file seen earlier in FireSIGHT. It appears this victim was exploited since an attempt to write the executable was made and permitted.

Event Description:	Host intrusion detected and handled
Host IPS Event Information	
View Host IPS Event Description	
files	C:\WINDOWS\system32\BxqYyB3Y4xgMl3.exe

Similar sets of HIPS event can be found on the 192.168.2[.]44 victim as well.

8. Optional: The ePO console also allows exports of event list results in several formats (e.g., CSV and XML) by selecting **Options >> Export Table**. These exports are useful when more advanced analysis is needed.



Signature Name (Host IPS)	Threat Target ...	Action Taken
CMD Tool Access by a Network Aware Application	192.168.2.46	Permitted
CMD Tool Access by a Network Aware Application	192.168.2.46	Permitted
Common User Startup Folder RegKey Modification	192.168.2.46	Permitted
Service Started	192.168.2.46	Permitted
CMD Tool Access by a Network Aware Application	192.168.2.46	Permitted
Common User Startup Folder RegKey Modification	192.168.2.46	Permitted

ANSWERS

- Adversary
  - IP Address: **10.199.0[.]208**
- Victim
  - IP Address(es): **192.168.2[.]44, 192.169.2[.]46**
  - Port Exploited (e.g., 80/TCP): **445/TCP**
  - Protocol Exploited (e.g., HTTP): **SMB**
- Stage 2 Infrastructure
  - IP Address: **10.199.0[.]208**
  - Port Used (e.g., 80/TCP): **445/TCP**
  - Protocol Used (e.g., HTTP): **SMB**
  - Files Provided (e.g., malware.7z): **BxqYyB3Y4xgMl3[.]exe, HFNQGTq3PLJSU[.]exe**
- C2 Infrastructure
  - IP Address: **10.199.0[.]208**
  - Port (e.g., 80/TCP): **4444/TCP**