Live Worm Propagation 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

A user arrived at your office with a personal USB drive and plugged it into their work computer. Unbeknownst to the user, the drive was infected with a worm, which propagated throughout your network. These activities occurred on **16 April 2020** between the times of **1700-1759 UTC.**

Use FireSIGHT alerts to begin your analysis.

Pivot within FireSIGHT's events to derive likely hypotheses. Correlate these possibilities with lab5.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:

- Initial Victim
  - IP Address: _____
  - USB Insertion Timestamp (UTC): _____
  - Post-Compromise Activity: _____
    _____
- C2 Infrastructure
  - IP Address: _____
  - Port Used (e.g., 80/TCP): _____
  - Protocol Used (e.g., HTTP): _____
  - Domain Name Used (e.g., badsite[.]local): _____
- Subsequent Victims
  - IP Address(es): _____
    _____
    _____
    _____
  - Port Exploited (e.g., 80/TCP): _____
  - Protocol Exploited (e.g., HTTP): _____
  - Exploit Technique Used: _____
    _____
    _____

ANALYSIS PROCESS

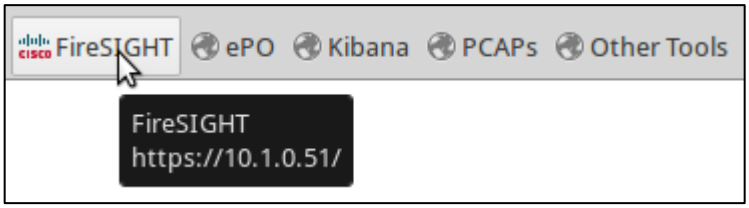
Follow along with the video as it goes through the following steps of analysis.

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.

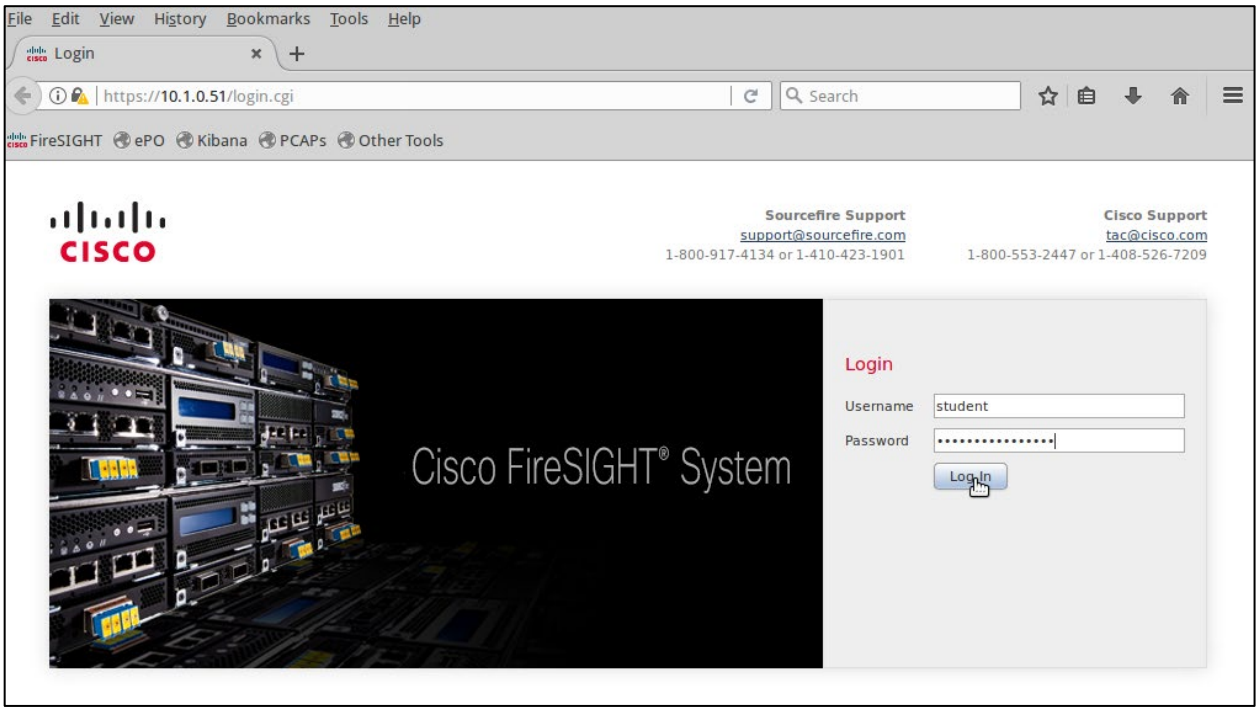
Note: Potential Indicators of Compromise (IoC), such as IP addresses and domain names, should be "de-fanged" as a best practice. De-fanging simply involves the insertion of a character into the IoC that is otherwise invalid in the IoC's context, so that copying/pasting/clicking the IoC won't inadvertently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

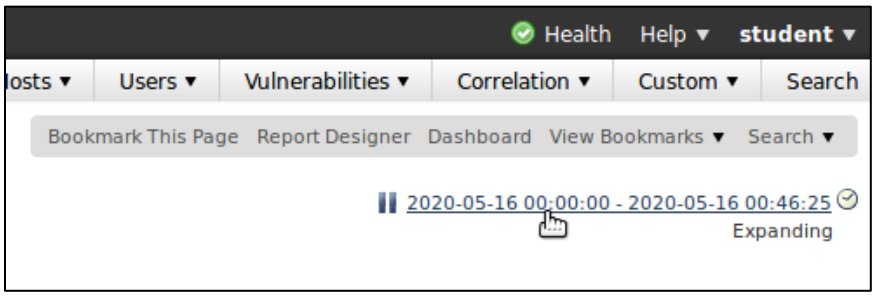
1. Select the **FireSIGHT** bookmark in the open Mozilla Firefox web browser.



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



3. Configure the timeframe to **16 April 2020 between 1700 and 1759 UTC** as mentioned the instructions. Use the steps described in the first lab as a guide. FireSIGHT populates with events from the specified timeframe.

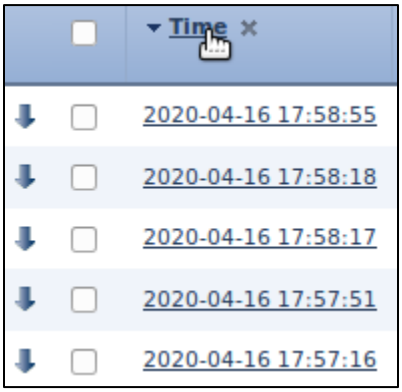


EXERCISE 2 – VIEWING EVENT DETAILS

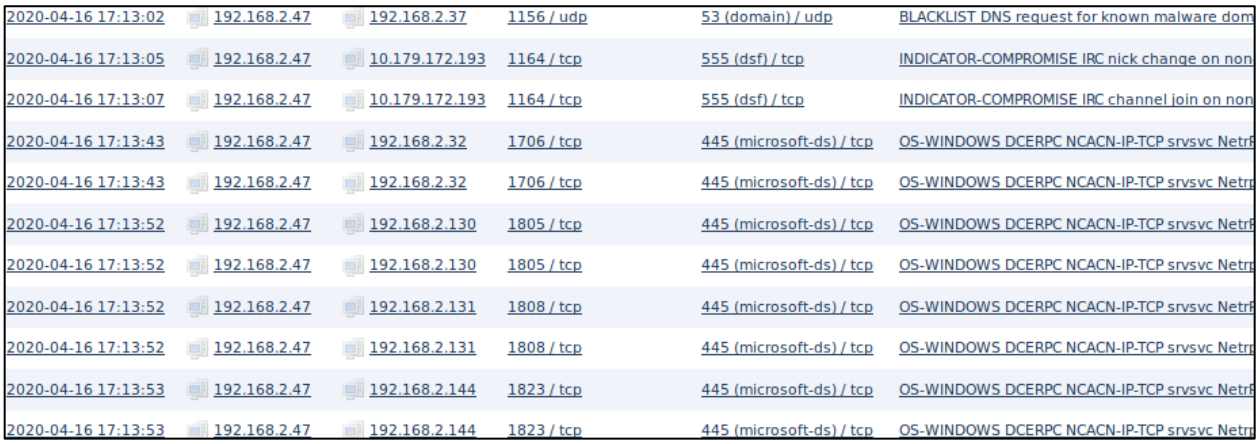
1. Review the alerts and note numerous potential malicious events are visible. Start your analysis by focusing on the high Priority events. Select the events labeled "high" and press **View**.

Message	Priority
OS-WINDOWS SMB replay attempt via NTLMSSP - overlapping encryption keys detected (3:15453:16)	high
OS-WINDOWS DCERPC NCACN-IP-TCP srvsvc NetrPathCanonicalize overflow attempt (1:1000020:1)	high
OS-WINDOWS DCERPC NCACN-IP-TCP srvsvc NetrpPathCanonicalize path canonicalization stack overflow attempt (1:1000021:1)	high
BLACKLIST DNS request for known malware domain irc.zief.pl - virut (1:16302:6)	high
INDICATOR-COMPROMISE IRC nick change on non-standard port (1:1000004:2)	high
INDICATOR-COMPROMISE IRC channel join on non-standard port (1:1000003:10)	high

2. Determine when the events started. Click the **Time** column header twice to chronologically sort events from oldest to newest.



Notice how one specific internal host, 192.168.2[.]47, started communicating with numerous internal hosts within a short period of time and triggering DCE/RPC alerts. The host also communicated with an external host, 10.179.172[.]193, where an "INDICATOR-COMPROMISE" IRC alert was triggered. IRC is often used in C2 infrastructures, so this type of traffic is of high interest, especially when found with other alerts.



2020-04-16 17:13:02	192.168.2.47	192.168.2.37	1156 / udp	53 (domain) / udp	BLACKLIST DNS request for known malware dom
2020-04-16 17:13:05	192.168.2.47	10.179.172.193	1164 / tcp	555 (dsf) / tcp	INDICATOR-COMPROMISE IRC nick change on non
2020-04-16 17:13:07	192.168.2.47	10.179.172.193	1164 / tcp	555 (dsf) / tcp	INDICATOR-COMPROMISE IRC channel join on non
2020-04-16 17:13:43	192.168.2.47	192.168.2.32	1706 / tcp	445 (microsoft-ds) / tcp	OS-WINDOWS DCERPC NCACN-IP-TCP srvsvc NetrF
2020-04-16 17:13:43	192.168.2.47	192.168.2.32	1706 / tcp	445 (microsoft-ds) / tcp	OS-WINDOWS DCERPC NCACN-IP-TCP srvsvc Netrp
2020-04-16 17:13:52	192.168.2.47	192.168.2.130	1805 / tcp	445 (microsoft-ds) / tcp	OS-WINDOWS DCERPC NCACN-IP-TCP srvsvc NetrF
2020-04-16 17:13:52	192.168.2.47	192.168.2.130	1805 / tcp	445 (microsoft-ds) / tcp	OS-WINDOWS DCERPC NCACN-IP-TCP srvsvc Netrp
2020-04-16 17:13:52	192.168.2.47	192.168.2.131	1808 / tcp	445 (microsoft-ds) / tcp	OS-WINDOWS DCERPC NCACN-IP-TCP srvsvc NetrF
2020-04-16 17:13:52	192.168.2.47	192.168.2.131	1808 / tcp	445 (microsoft-ds) / tcp	OS-WINDOWS DCERPC NCACN-IP-TCP srvsvc Netrp
2020-04-16 17:13:53	192.168.2.47	192.168.2.144	1823 / tcp	445 (microsoft-ds) / tcp	OS-WINDOWS DCERPC NCACN-IP-TCP srvsvc NetrF
2020-04-16 17:13:53	192.168.2.47	192.168.2.144	1823 / tcp	445 (microsoft-ds) / tcp	OS-WINDOWS DCERPC NCACN-IP-TCP srvsvc Netrp

It appears the Initial Victim is *192.168.2[.]47* (i.e., where the USB drive was inserted) since it is the first internal host to attack other internal hosts. We can see parts of the attack process based on the Initial Victim's subsequent activities. First, it makes a DNS request for a malware domain, then communicates to the resolved IP using IRC, and finally *scans for and attempts to compromise* any open DCE/RPC ports.

Based on the DCE/RPC alerts, it also appears subsequent internal victims may include 192.168.2[.]32, 192.168.2[.]130, 192.168.2[.]131, and 192.168.2[.]144. Since attempted compromise is not necessarily an indication of a successful compromise, further analysis into these hosts is required.

3. Analyze the Initial Victim's activities in more detail to better understand how the malware is spreading. Select the packets with a Source IP of 192.168.2[.]47 on the first page of events, and press **View**.

☑	2020-04-16 17:13:02	192.168.2.47	192.168.2.37	1156 / udp	53 (domain) / udp	BLACKLIST DNS request for known malware dom
☑	2020-04-16 17:13:05	192.168.2.47	10.179.172.193	1164 / tcp	555 (dsf) / tcp	INDICATOR-COMPROMISE IRC nick change on non
☑	2020-04-16 17:13:07	192.168.2.47	10.179.172.193	1164 / tcp	555 (dsf) / tcp	INDICATOR-COMPROMISE IRC channel join on non
☑	2020-04-16 17:13:43	192.168.2.47	192.168.2.32	1706 / tcp	445 (microsoft-ds) / tcp	OS-WINDOWS DCERPC NCACN-IP-TCP srvsvc NetrF
☑	2020-04-16 17:13:43	192.168.2.47	192.168.2.32	1706 / tcp	445 (microsoft-ds) / tcp	OS-WINDOWS DCERPC NCACN-IP-TCP srvsvc Netrp
☑	2020-04-16 17:13:52	192.168.2.47	192.168.2.130	1805 / tcp	445 (microsoft-ds) / tcp	OS-WINDOWS DCERPC NCACN-IP-TCP srvsvc Netrp
☑	2020-04-16 17:13:52	192.168.2.47	192.168.2.130	1805 / tcp	445 (microsoft-ds) / tcp	OS-WINDOWS DCERPC NCACN-IP-TCP srvsvc NetrF
☑	2020-04-16 17:13:52	192.168.2.47	192.168.2.131	1808 / tcp	445 (microsoft-ds) / tcp	OS-WINDOWS DCERPC NCACN-IP-TCP srvsvc NetrF
☑	2020-04-16 17:13:52	192.168.2.47	192.168.2.131	1808 / tcp	445 (microsoft-ds) / tcp	OS-WINDOWS DCERPC NCACN-IP-TCP srvsvc Netrp
☑	2020-04-16 17:13:53	192.168.2.47	192.168.2.144	1823 / tcp	445 (microsoft-ds) / tcp	OS-WINDOWS DCERPC NCACN-IP-TCP srvsvc NetrF
☑	2020-04-16 17:13:53	192.168.2.47	192.168.2.144	1823 / tcp	445 (microsoft-ds) / tcp	OS-WINDOWS DCERPC NCACN-IP-TCP srvsvc Netrp

Note the first event is flagged as a blacklisted DNS request for a known malware domain at *irc.zief[.]pl*.

Event Information

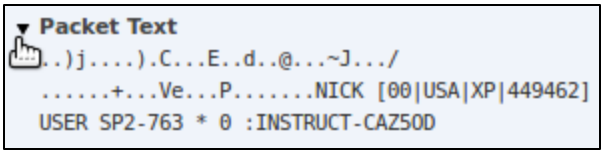
Event	BLACKLIST DNS request for known malware domain irc.zief.pl - virut (1:16302:6)
Timestamp	2020-04-16 17:13:02
Classification	A Network Trojan was Detected
Priority	high
Ingress Security Zone	Passive
Device	192.168.1.52
Ingress Interface	eth1
Source IP	**192.168.2.47**
Source Port / ICMP Type	1156 / udp
Destination IP	**192.168.2.37**
Destination Port / ICMP Code	53 (domain) / udp

4. Proceed to the next event by pressing ">" at the bottom-right of the window.

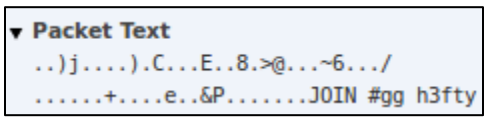
This alert indicates an *IRC* protocol indicator was detected. Review the Event Information section. Note the traffic was sent to *10.179.172[.]193* on *TCP port 555*. This activity may indicate communication to C2 Infrastructure.

Event	INDICATOR-COMPROMISE IRC channel join on non-standard port (1:1000003:10)
Timestamp	2020-04-16 17:13:07
Classification	A Network Trojan was Detected
Priority	high
Ingress Security Zone	Passive
Device	192.168.1.52
Ingress Interface	eth1
Source IP	**192.168.2.47**
Source Port / ICMP Type	1164 / tcp
Destination IP	**10.179.172.193**
Destination Port / ICMP Code	555 (dsf) / tcp

Expand **Packet Text** to view the payload. Note the host sent an IRC nickname command that appears to contain system-related parameters indicative of C2 traffic (e.g. "XP" as the victim's operating system, "SP2" as its service pack level, and "INSTRUCT-CAZ500" as its hostname). Along with the blacklisted DNS request alert, this type of activity is likely the C2 Infrastructure for this malware.



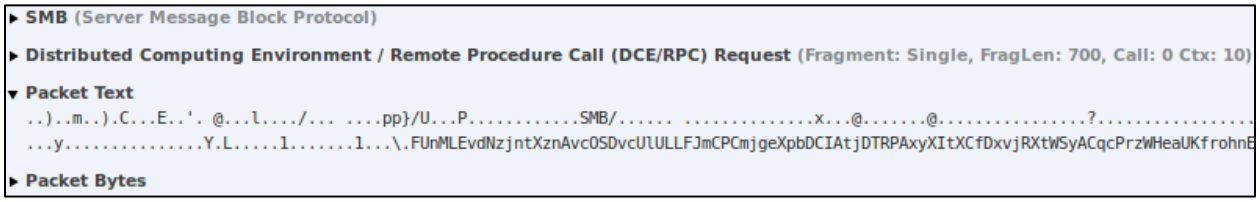
5. Proceed to the next event and review its payload. The victim appears to have joined an IRC channel named "#gg" that required the password "h3fty".



6. Proceed to the next event and review its event information. The initial victim appears to be attempting a DCE/RPC *buffer "srvsvc NetrPathCanonicalize overflow"* attack against internal host *192.168.2[.]32* on *TCP port 445* using the *SMB* protocol.

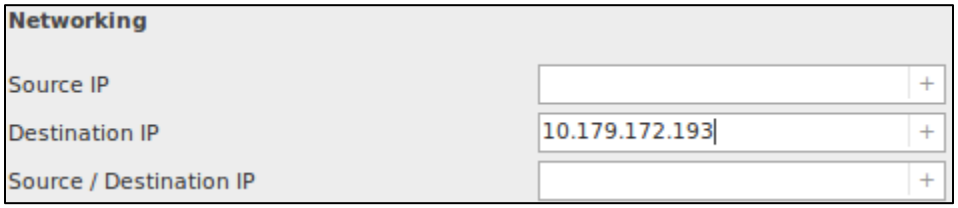
Event	OS-WINDOWS DCERPC NCACN-IP-TCP srvsvc NetrPathCanonicalize overflow attempt (1:1000020:1)
Timestamp	2020-04-16 17:13:43
Classification	Attempted Administrator Privilege Gain
Priority	high
Ingress Security Zone	Passive
Device	192.168.1.52
Ingress Interface	eth1
Source IP	**192.168.2.47**
Source Port / ICMP Type	1706 / tcp
Destination IP	**192.168.2.32**
Destination Port / ICMP Code	445 (microsoft-ds) / tcp
HTTP Hostname	Not Available
HTTP URI	uÀ
Intrusion Policy	RaD-X-1
Access Control Policy	Default Access Control
Access Control Rule	RaD-X
Rule	alert tcp any any -> $HOME_NET [135,139,445,593,1024:] (sid:1000020; gid:1; flow:established,to_ rev:1;)

Expand **Packet Text** to view its payload. It seems to contain the contents of the buffer overflow attempt.

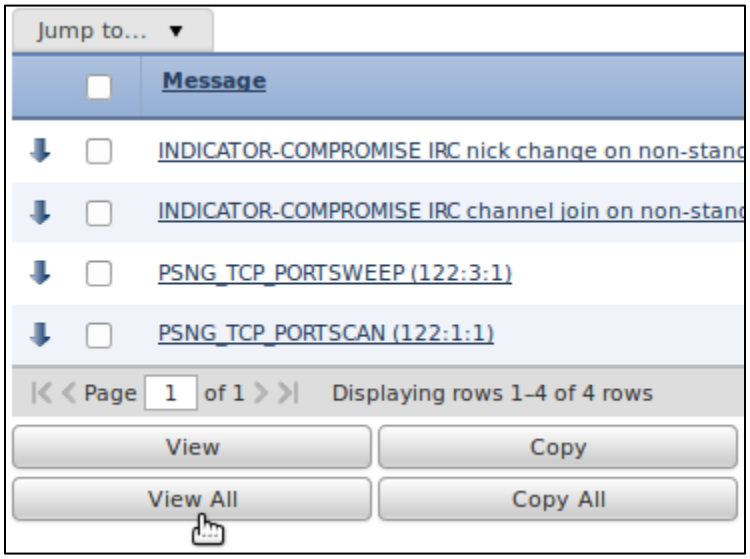


7. Proceed through the remaining events and notice the same type of attack carried out against *192.168.2[.]130*, *192.168.2[.]131*, and *192.168.2[.]144*.

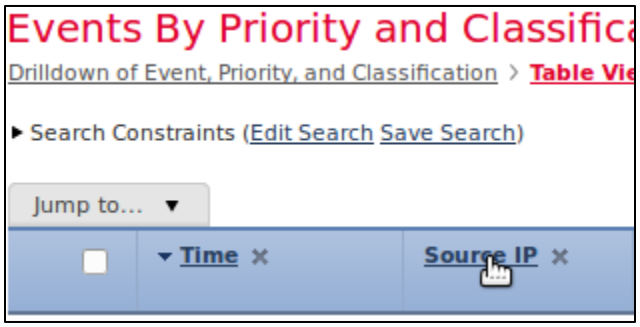
8. Since we know traffic to the C2 Infrastructure is indicative of successfully compromised hosts, we can determine which internal hosts communicated with it using FireSIGHT's search tool. Enter this IP address in the **Destination IP** field and press **Search**.



9. Review the search results and press **View All** since all alerts appear to be relevant.



10. Select the **Source IP** column header to sort the events by source IP address.



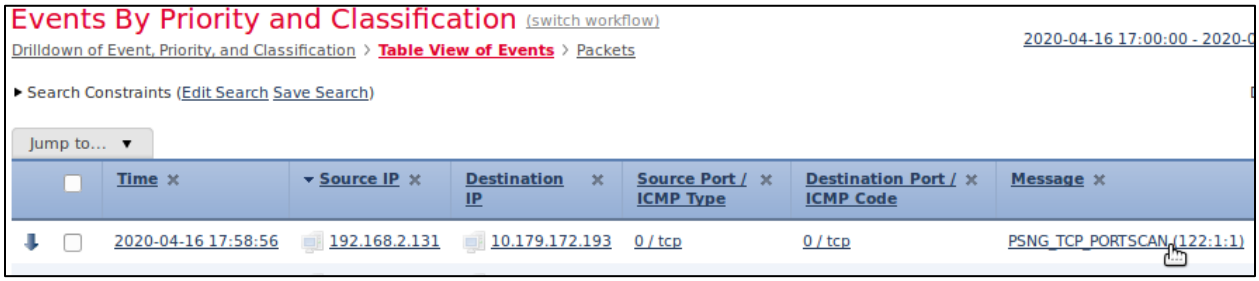
View the events and note the unique source IP addresses, i.e., 192.168.2[.]32, 192.168.2[.]130, 192.168.2[.]131, and 192.168.2[.]144 match the ones previously determined. These hosts are directly communicating with the C2 Infrastructure IP address and are likely compromised.

192.168.2.131	10.179.172.193	0 / tcp	0 / tcp	PSNG_TCP_PORTSWEEP (122:3:1)
192.168.2.131	10.179.172.193	4089 / tcp	555 (dsf) / tcp	INDICATOR-COMPROMISE IRC nick change on non-star

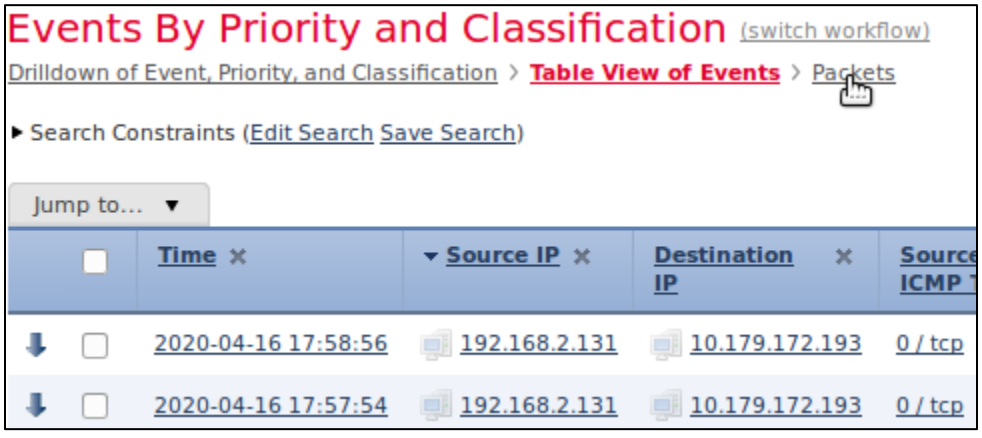
192.168.2.130	10.179.172.193	0 / tcp	0 / tcp	PSNG_TCP_PORTSCAN (122:1:1)
192.168.2.47	10.179.172.193	0 / tcp	0 / tcp	PSNG_TCP_PORTSWEEP (122:3:1)

192.168.2.47	10.179.172.193	1164 / tcp	555 (dsf) / tcp	INDICATOR-COMPROMISE IRC nick
192.168.2.32	10.179.172.193	0 / tcp	0 / tcp	PSNG_TCP_PORTSWEEP (122:3:1)

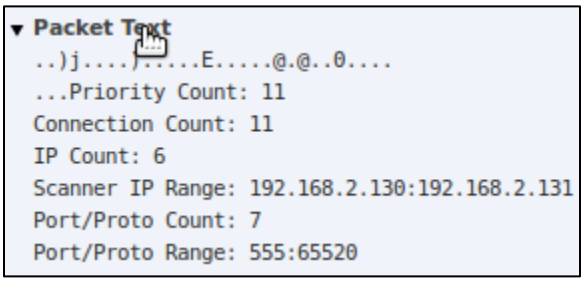
11. Return to the **Table View of Events** page and select the first "PSNG_TCP_PORTSCAN" message.



Select the **Packets** view to view its associated packets.

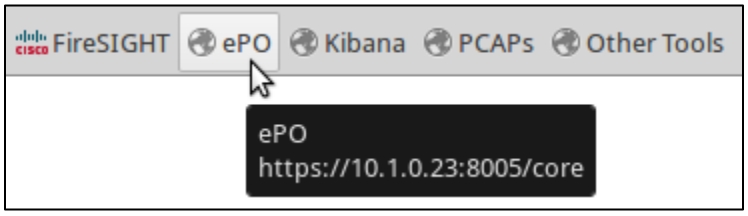


Expand the **Packet Text** of the first event to view the payload. Note the payload shows several of the victim IP addresses scanned.

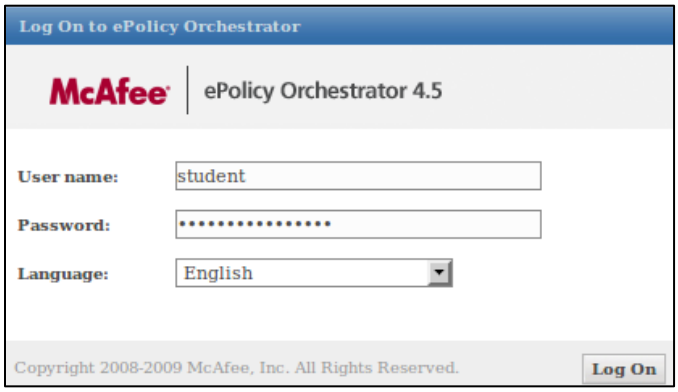


EXERCISE 3 – ePO CORRELATION

1. Determining the USB drive insertion timestamp can be performed in ePO. To access the ePO console, select the "ePO" bookmark within Mozilla Firefox.

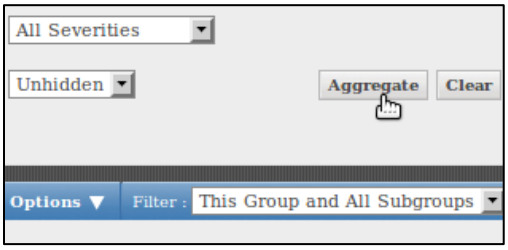


2. Enter the username "**student**" and password "**12qwaszx!@QWASZX**" and press **Log On**.

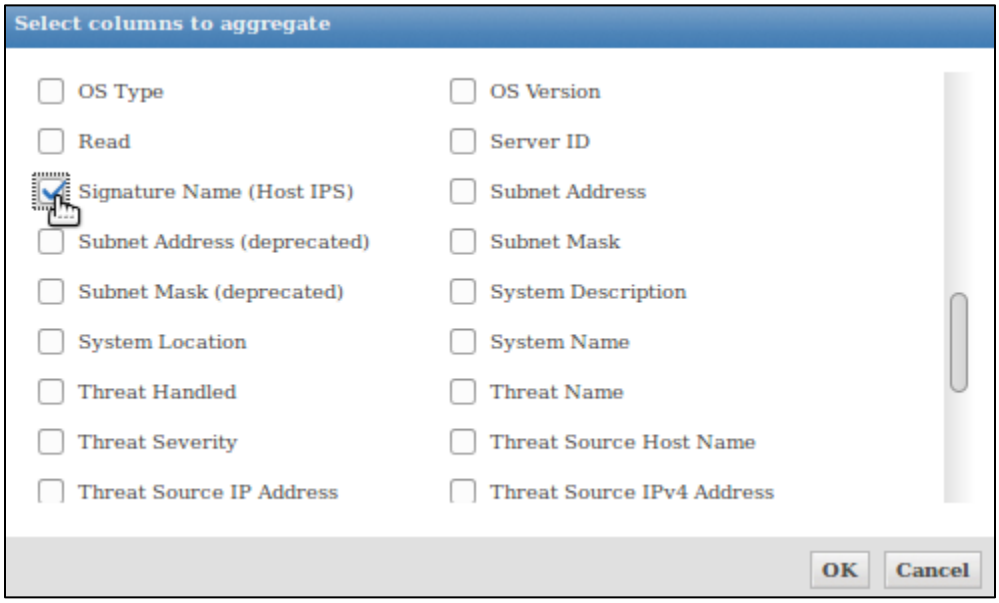


3. Access the HIPS reporting feature by selecting the **Host IPS** icon in the menu bar.

4. We need to organize HIPS events based upon our target timeframe and the victim IP addresses. Start by selecting "This Group and All Subgroups" within the **Filter** dropdown menu on the right-hand side of the window. Press the **Aggregate** button next.



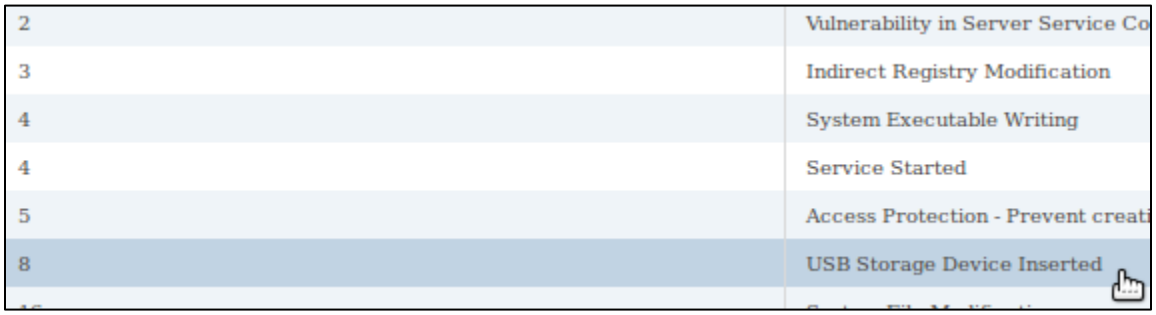
5. Select "Signature Name (Host IPS)" from the options presented and press **OK** to aggregate hosts by the event type.



6. The aggregate counts (and events) can be narrowed in scope by selecting the appropriate time frame. Click the **Creation Time** dropdown menu and select "Between", which will display date pickers for the start and stop of the timeframe.

7. Select the first date picker to the right of the **Creation Time** menu and select "April 16, 2020." On the second date picker, select "April 16, 2020" as well. This timeframe is representative of April 16, 2020 0:00 UTC through April 16, 2020 23:59 UTC.

8. Filter for the "USB Storage Device Inserted" event by selecting it.



9. A table of events appears. Note only one IP address, 192.168.2[.]47, is visible, further indicating this was the internal host the malicious USB drive was plugged into. Based on the events, the USB drive was first inserted on *04/16/2020 4:55:19PM UTC*.

Event Generated Time (U... ▲	Threat Target IPv4 Address	Threat Source Process Name	Action Taken
4/16/20 4:55:19 PM	192.168.2.47	System	Permitted
4/16/20 5:01:31 PM	192.168.2.47	System	Permitted
4/16/20 5:04:59 PM	192.168.2.47	System	Permitted
4/16/20 5:07:07 PM	192.168.2.47	System	Permitted
4/16/20 5:07:47 PM	192.168.2.47	System	Permitted
4/16/20 5:09:47 PM	192.168.2.47	System	Permitted
4/16/20 5:10:43 PM	192.168.2.47	System	Permitted
4/16/20 5:11:19 PM	192.168.2.47	System	Permitted

ANSWERS

- Initial Victim
  - IP Address: _____

- Initial Victim
  - IP Address: **192.168.2[.]47**
  - USB Insertion Timestamp (UTC): **04/16/2020 4:55:19PM**
  - Post-Compromise Activity: **Scanned Network, Attempted Compromises**
- C2 Infrastructure
  - IP Address: **10.179.172[.]193**
  - Port Used (e.g., 80/TCP): **555/TCP**
  - Protocol Used (e.g., HTTP): **IRC**
  - Domain Name Used (e.g., badsite[.]local): **irc.zief[.]pl**
- Subsequent Victims
  - IP Address(es): **192.168.2[.]32, 192.168.2[.]130, 192.168.2[.]131, 192.168.2[.144**
  - Port Exploited (e.g., 80/TCP): **445/TCP**
  - Protocol Exploited (e.g., HTTP): **SMB**
  - Exploit Technique Used: **buffer srvsvc NetrPathCanonicalize buffer overflow**