27.2.14 Lab - Isolate Compromised Host Using 5-Tuple

This lab has been updated for use on NETLAB+.
www.netdevgroup.com

Objectives

In this lab, you will review logs that were gathered during the exploitation of a documented vulnerability to determine the compromised hosts and file.

Part 1: Review Alerts in Sguil

Part 2: Pivot to Wireshark

Part 3: Pivot to Kibana

Background / Scenario

The 5-tuple is used by IT administrators to identify requirements for creating an operational and secure network environment. The components of the 5-tuple include a source IP address and port number, destination IP address and port number, and the protocol in use in the data payload. This is the protocol field of the IP packet header.

In this lab, you will also review the logs to identify the compromised hosts and the content of the compromised file.

Instructions

After the attack, the users no longer have access to the file named **confidential.txt**. Now you will review the logs to determine how the file was compromised.

Note: If this was a production network, it is recommended that **analyst** and **root** users change their passwords and comply with the current security policy.

Part 1: Review Alerts in Sguil

a. Launch the **Security Onion** VM and log in with the user **`analyst`** and password **`cyberops.`**

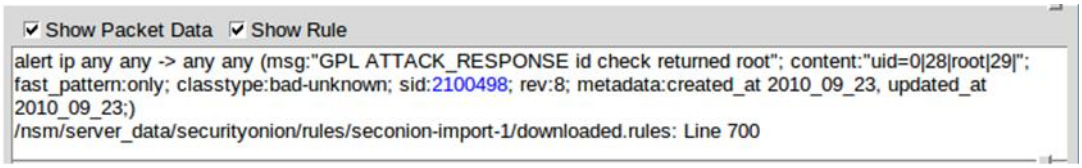
b. Double-click the **Sguil** icon on desktop and log in using username `analyst` and password `cyberops`. Click **Select All** to select the interfaces and then **Start SGUIL**.

c. Review the events listed in the Event Message column. One of these messages is **GPL ATTACK_RESPONSE id check returned root**. This message indicates that root access may have been gained during an attack. The host at 209.165.200.235 returned root access to 209.165.201.17. The alert ID **5.1** is used as an example in this lab.

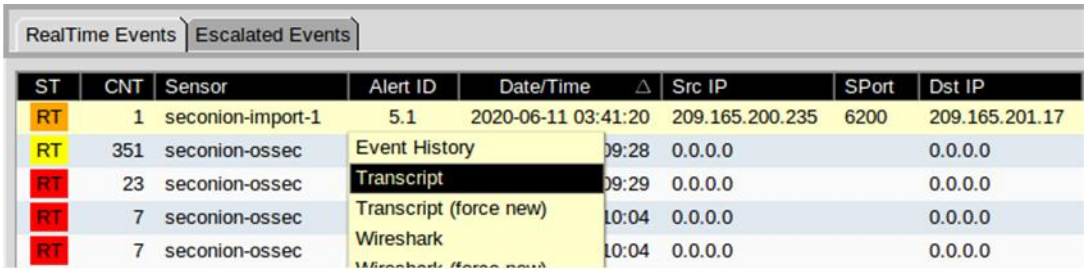
ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	seconion-import-1	5.1	2020-06-11 03:41:20	209.165.200.235	6200	209.165.201.17	45415	6	GPL ATTACK_RESPONSE id check returned root
RT	351	seconion-ossec	1.1	2020-06-19 18:09:28	0.0.0.0		0.0.0.0		0	[OSSEC] File added to the system.
RT	23	seconion-ossec	1.2	2020-06-19 18:09:29	0.0.0.0		0.0.0.0		0	[OSSEC] Integrity checksum changed.

© 2018 - 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

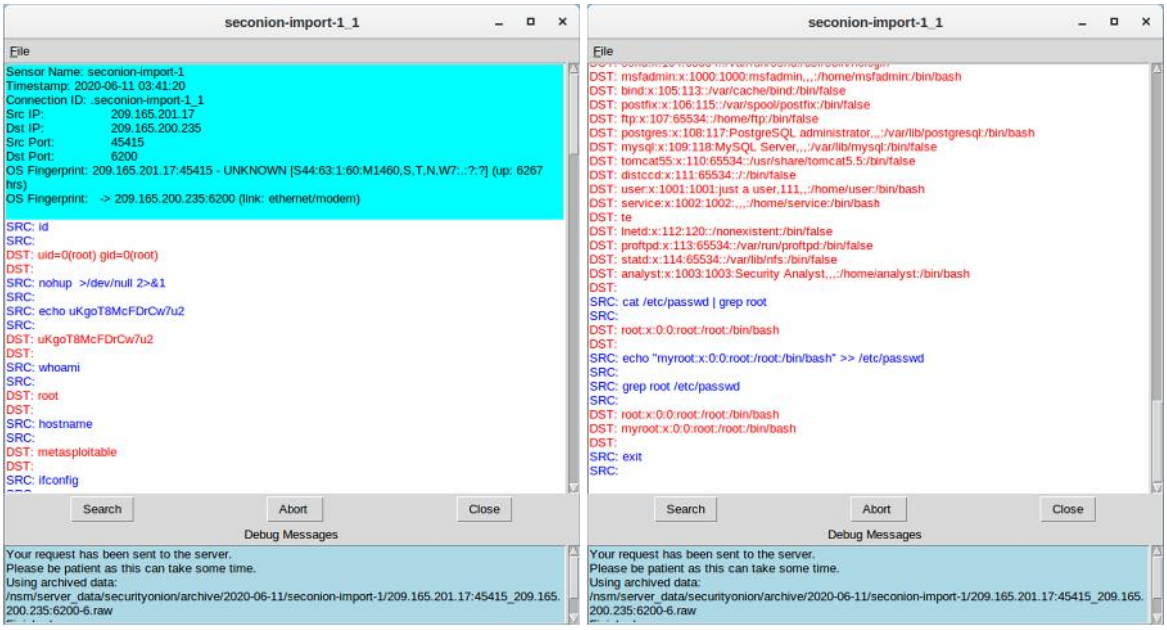
d. Select the **Show Packet Data** and **Show Rule** checkboxes to view each alert in more detail



e. Right-click the alert ID 5.1 and select **Transcript**.



f. Review the transcripts for the alert. The transcript displays the transactions between the threat actor source (SRC) and the target (DST) during the attack. The threat actor is executing Linux commands on the target.

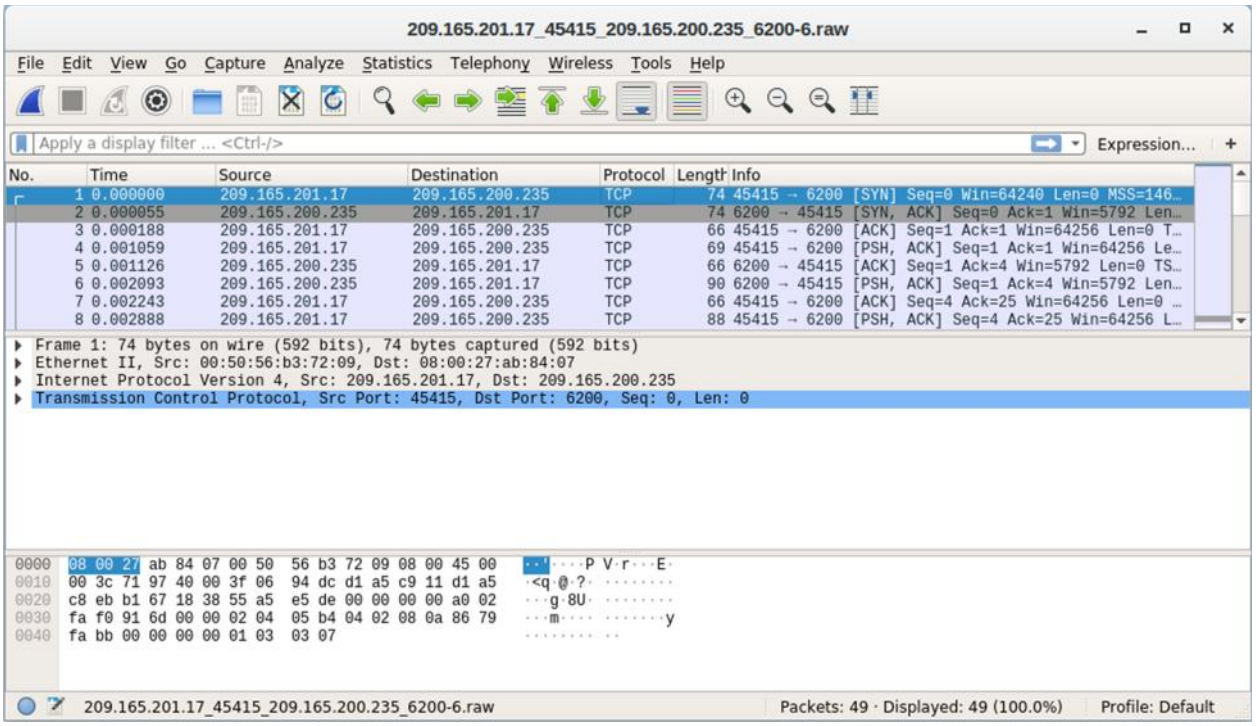


What kind of transactions occurred between the client and the server in this attack?

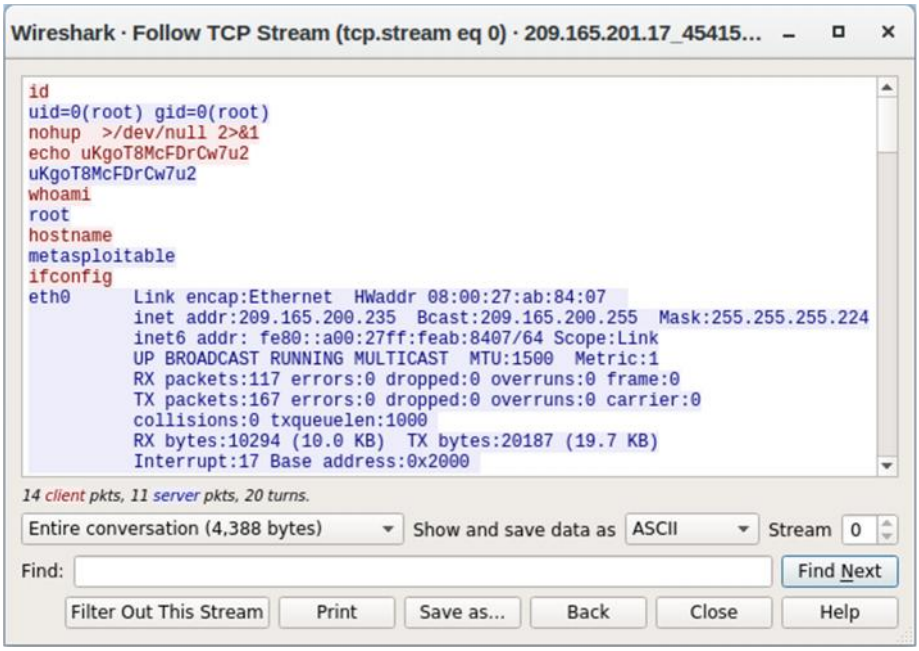
© 2018 - 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Part 2: Pivot to Wireshark

a. Select the alert that provided you with the transcript from the previous step. Right-click the alert ID 5.1 and select **Wireshark**. The Wireshark main window displays three views of a packet.



b. To view all packets that are assembled in a TCP conversation, right-click any packet and select **Follow** > **TCP Stream**.



What did you observe? What do the text colors red and blue indicate?

© 2018 - 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

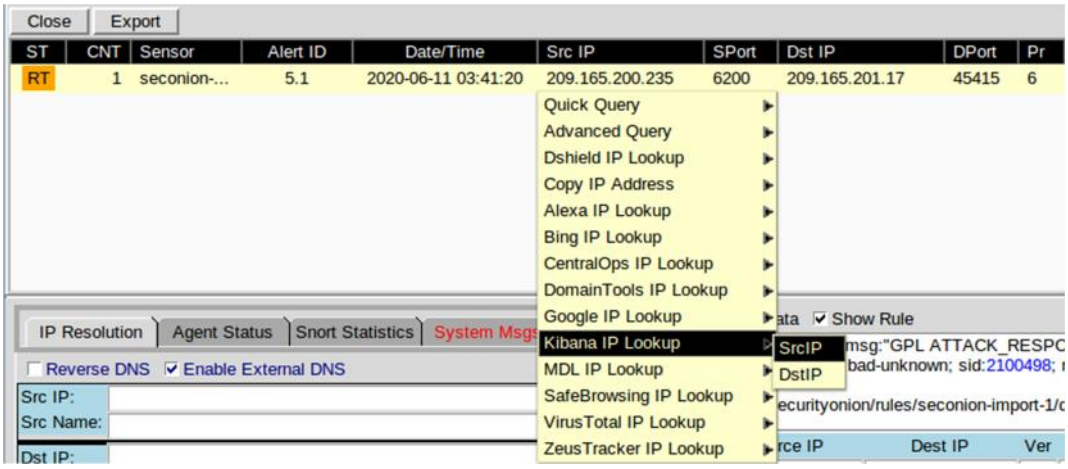
The attacker issues the **whoami** command on the target. What does this show about the attacker role on the target computer?

Scroll through the TCP stream. What kind of data has the threat actor been reading?

c. Exit the TCP stream window. Close **Wireshark** when you are done reviewing the information provided.

Part 3: Pivot to Kibana

a. Return to Sguil. Right-click either the source or destination IP for the alert ID 5.1 and select **Kibana IP Lookup** > **SrcIP**. Enter username `analyst` and password `cyberops` if prompted by Kibana.



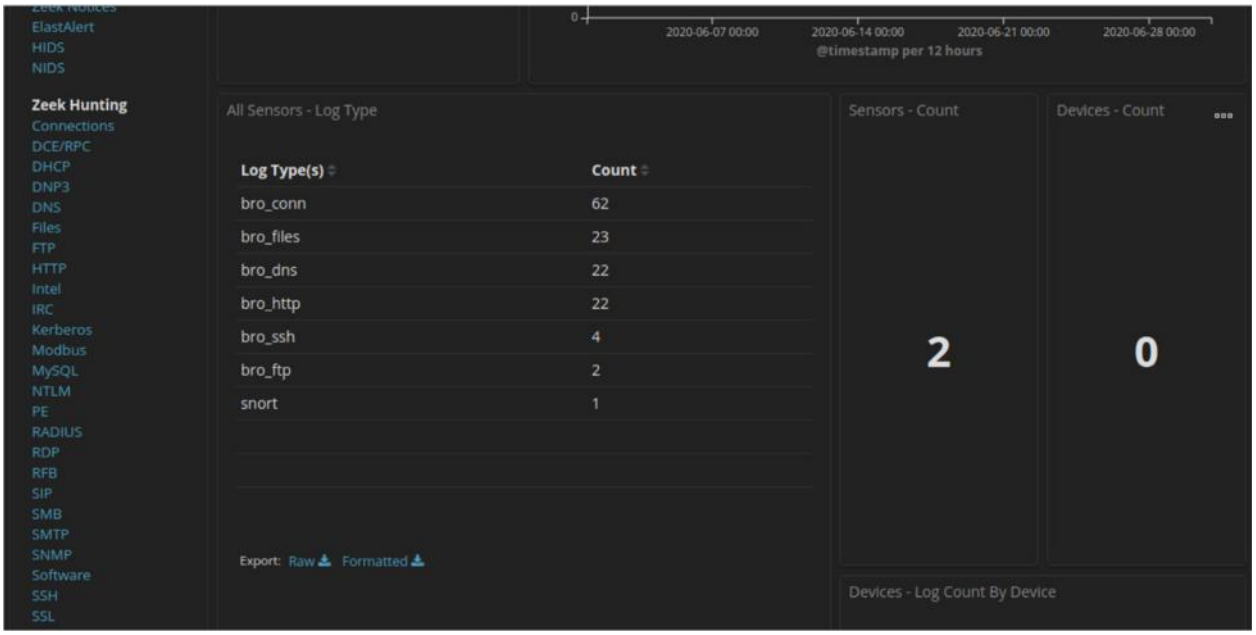
Note: If you received the message "Your connection is not private", click **ADVANCED > Proceed to localhost (unsafe)** to continue.

b. If the time range is the last 24 hours, change it to June 2020 so June 11 is included in the time range. Use the **Absolute** tab to change the time range.

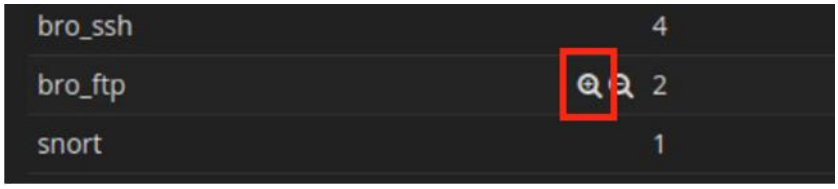
© 2018 - 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

www.netacad.com

c. In the displayed results, there is a list of different log types. You were told that the file **confidential.txt** is no longer accessible. We will determine if FTP was used to steal the file.



d. Let's filter for **bro_ftp**. Hover over the empty space next to the count of bro_ftp data types. Select **+** to filter for only FTP related traffic as shown in the figure.



e. Scroll down to the **All Logs** section. There are two entries listed.

What are the source and destination IP addresses and port numbers for the FTP traffic?

_____

f. Expand and review both log entries. In one of these entries, the *ftp_argument* has an entry of *ftp://209.165.200.235/./confidential.txt*. Also review the message in the log entry to learn more about this event.

g. Within the same log entry, scroll up back to the alert **_id** field and click the link.

h. Review the transcript for the transactions between the attacker and the target. If desired, you can download the pcap and review the traffic using Wireshark.

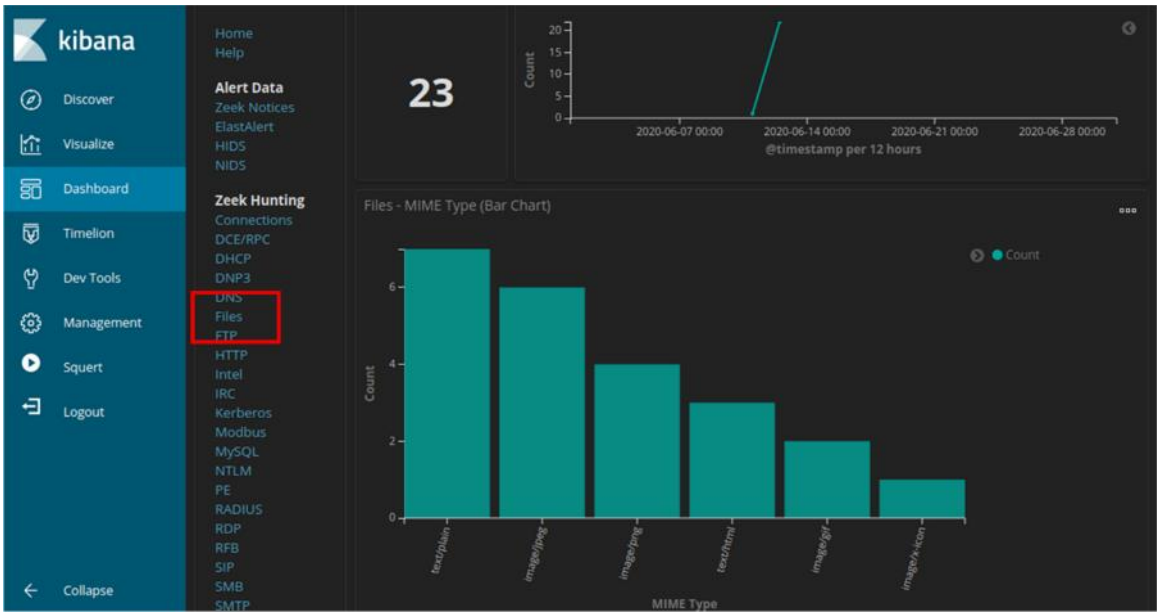
© 2018 - 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

What are the user credentials to access the FTP site?

---

i. Now that you have verified that the attacker has used FTP to copy the content of the file confidential.txt and then deleted it from the target, what is the content of the file? Remember one of the services listed in the pie chart is *ftp_data*.

j. Navigate to the top of the dashboard. Select **Files** under the Zeek Hunting heading in the left panel, as shown in the figure. This will allow you to review the types of the files that were logged.

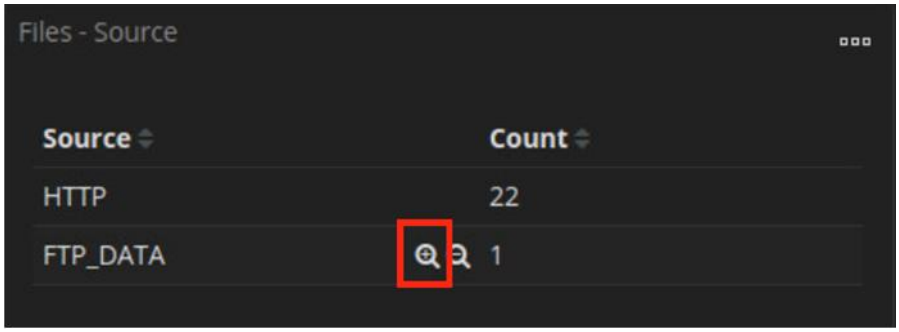


What are the different types of files? Look at the MIME Type section of the screen.

Scroll to the **Files - Source** heading. What are the file sources listed?

---

k. Filter for **FTP_DATA** by hovering over the empty space next to the Count for FTP_DATA and click **+**.



l. Scroll down to review the filtered results.

What is the MIME type, source and destination IP address associated with the transfer of the FTP data? When did this transfer occur?

© 2018 - 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

m. In the File logs, expand the entry associated with FTP data. Click the link associated with alert **_id**.

What is the text content of the file that was transferred using FTP?

With all the information has gathered so far, what is your recommendation for stopping further unauthorized access?

© 2018 - 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public