

BONUS 3 - Isolate Compromised Host Using 5-Tuple

Informazioni:

Questo report si pone come obiettivo quello di enunciare e spiegare le procedure seguite per identificare i contenuti di un file rubato, con aggiunta di dettagli in merito al trasferimento, andando a ritrovare sia l' IP di partenza sia quello di arrivo, più la data del trasferimento.

Trovare l' "attack response"

Iniziamo aprendo la "Onion Virtual Machine", ed eseguiamo il log in con le credenziali che seguono:

username = analyst

password = cyberops

una volta dentro apriamo SGUIL e ri-eseguiamo il log in con le stesse credenziali. Ci troveremo davanti al registro degli eventi, e quello che dobbiamo cercare è " **GPL ATTACK_RESPONSE id check returned root** ".

The screenshot displays the SGUIL-0.9.0 interface. The top bar shows 'Mon 10:23' and 'SGUIL-0.9.0 - Connected To localhost'. The main window is titled 'RealTime Events' and contains a table of events. The table has columns: ST, CNT, Sensor, Alert ID, Date/Time, Src IP, SPort, Dst IP, DPort, Pr, and Event Message. The event at CNT 1 is highlighted in yellow and matches the search criteria: 'GPL ATTACK_RESPONSE id check returned root'.

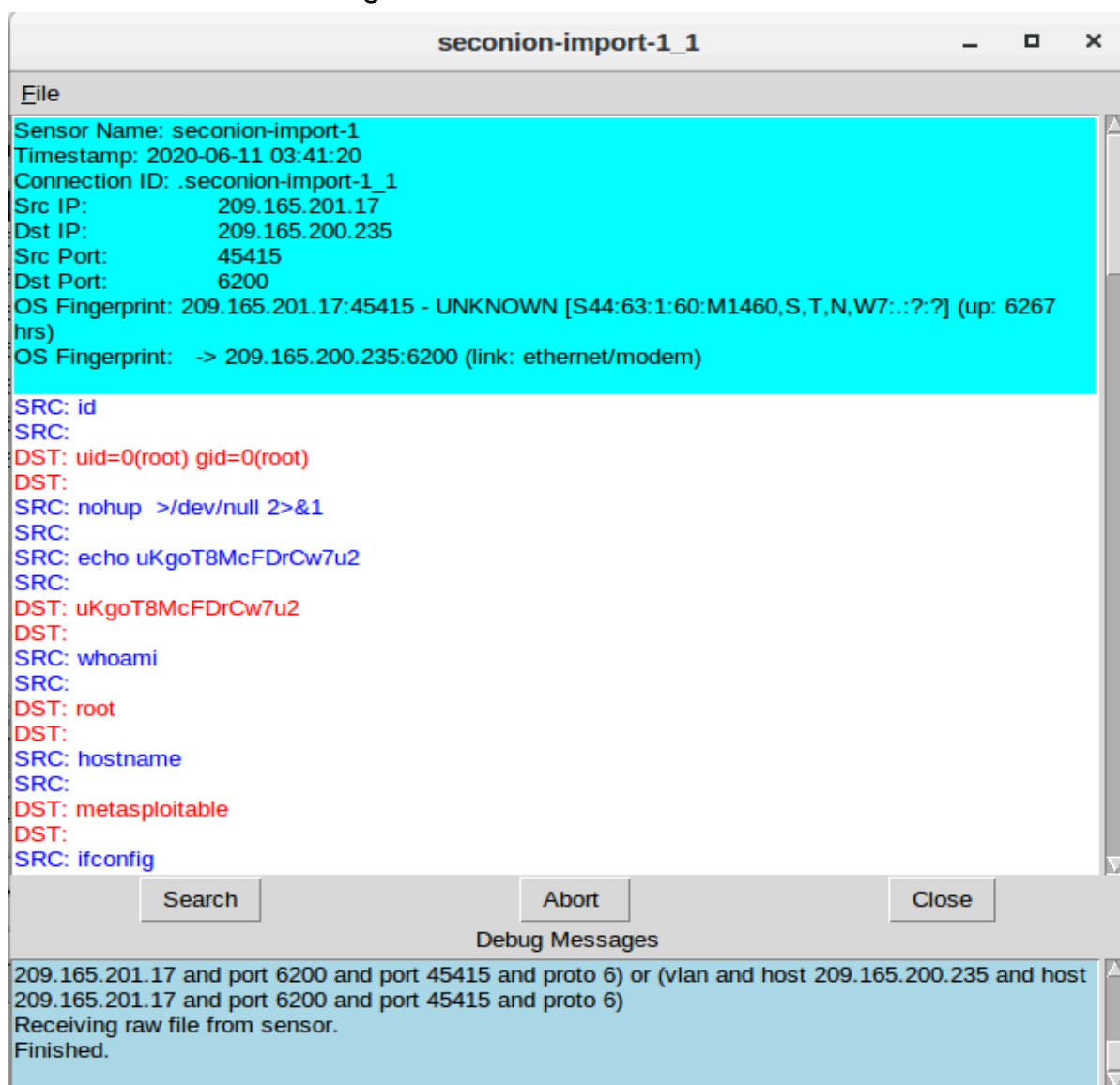
ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	17	seconion-...	5.234	2019-07-19 18:53:12	172.16.4.205	49249	185.243.115.84	80	6	ET POLICY Data POST to a...
RT	114	seconion-...	5.251	2019-07-19 18:57:23	172.16.4.205	49255	31.7.62.214	443	6	ET POLICY HTTP traffic on ...
RT	2	seconion-...	5.365	2020-02-21 00:53:55	172.17.8.174	62362	172.17.8.8	53	17	ET POLICY DNS Update Fro...
RT	13	seconion-...	5.366	2020-02-21 00:55:07	49.51.172.56	80	172.17.8.174	49731	6	ET CURRENT_EVENTS Lik...
RT	13	seconion-...	5.379	2020-02-21 00:55:07	49.51.172.56	80	172.17.8.174	49731	6	ET CURRENT_EVENTS Win...
RT	13	seconion-...	5.392	2020-02-21 00:55:07	49.51.172.56	80	172.17.8.174	49731	6	ET POLICY PE EXE or DLL ...
RT	4	seconion-...	5.406	2020-02-21 01:11:48	91.211.88.122	443	172.17.8.174	49760	6	ET TROJAN ABUSE.CH SS...
RT	1	seconion-...	5.1	2020-06-11 03:41:20	209.165.200.235	6200	209.165.201.17	45415	6	GPL ATTACK_RESPONSE I...
RT	351	seconion-...	1.1	2020-06-19 18:09:28	0.0.0.0		0.0.0.0		0	[OSSEC] File added to the s...
RT	23	seconion-...	1.2	2020-06-19 18:09:29	0.0.0.0		0.0.0.0		0	[OSSEC] Integrity checksum...
RT	7	seconion-...	1.4	2020-06-19 18:10:04	0.0.0.0		0.0.0.0		0	[OSSEC] New group added t...
RT	7	seconion-...	1.5	2020-06-19 18:10:04	0.0.0.0		0.0.0.0		0	[OSSEC] New user added to ...
RT	2	seconion-...	1.18	2020-06-19 18:14:41	0.0.0.0		0.0.0.0		0	[OSSEC] Listened ports stat...

Below the table, there is a 'System Msg' section with fields for 'Reverse DNS', 'Enable External DNS', 'Src IP', 'Src Name', 'Dst IP', 'Dst Name', and 'Whois Query'. To the right, there is a 'Show Packet Data' section with a table for packet analysis, including columns for IP, Source IP, Dest IP, Ver, HL, TOS, len, ID, Flags, Offset, TTL, and ChkSum. The packet analysis table shows a TCP packet with source IP 172.17.8.174 and destination IP 172.17.8.8.

Questo messaggio ci indica che qualcuno potrebbe aver ottenuto i permessi di root durante questo attacco.

Per vedere ogni allerta più nel dettaglio, bisogna cliccare sui due riquadri in basso “Show Packet Data” e “Show Rule”.

A questo punto, clicchiamo con il tasto destro sull’ “Alert ID” 5.1 e poi selezioniamo “Transcript”. Questo ci consentirà di ricevere una trascrizione testuale dell’allerta. In questo testo possiamo trovare la transazione dalla minaccia (denominata come “SRC”) al bersaglio (denominato “DST”) durante l’attacco. Come possiamo vedere, la minaccia sta eseguendo comandi Linux sulla macchina del bersaglio.

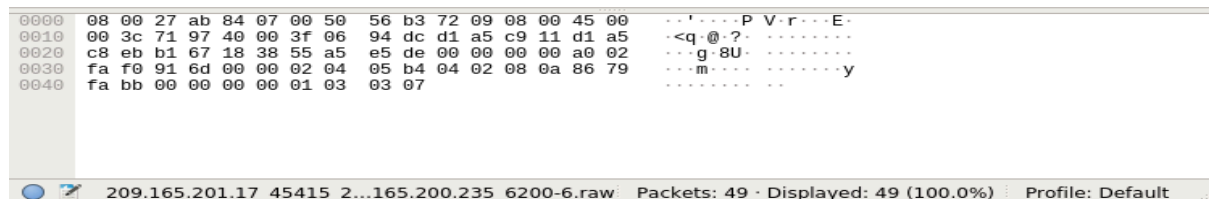
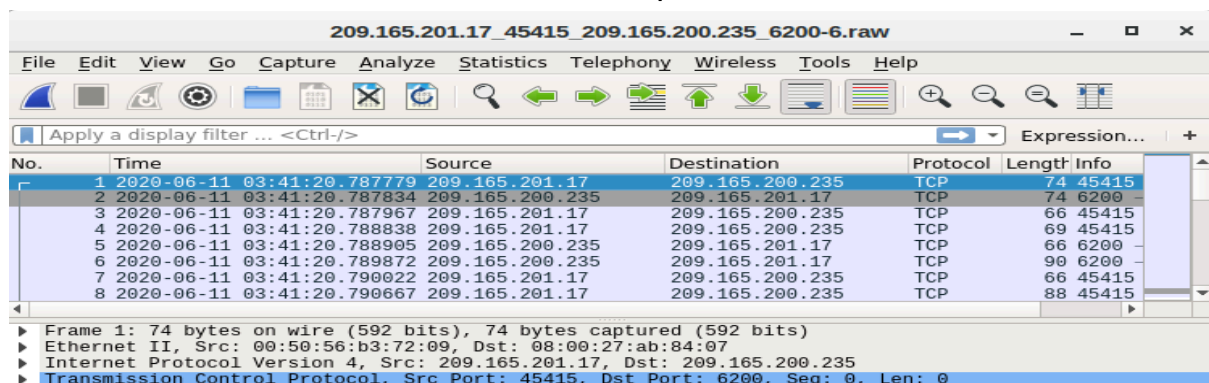


In questo screen possiamo vedere che l’attaccante, il cui IP è 209.165.201.17, ha ottenuto i permessi di root sulla macchina con IP “209.165.200.135”.

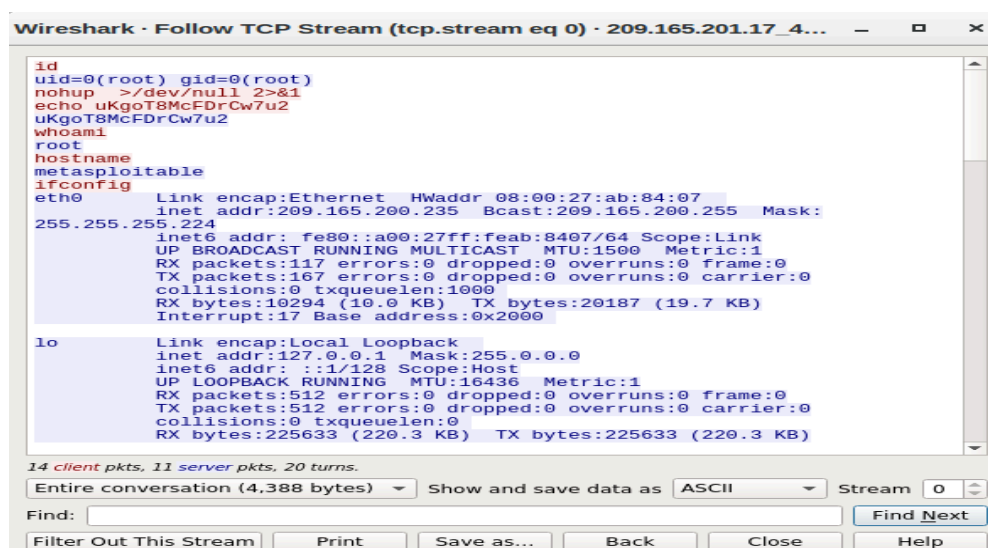
L'attaccante ha quindi navigato nei file di sistema, ha copiato il file "shadow" ed ha successivamente modificato i file al percorso /etc/shadow ed /etc/password.

Utilizzo di Wireshark

Torniamo indietro all'ID 5.1, facciamo sempre clic con il tasto destro ma questa volta selezioniamo "Wireshark". Questo ci apre la finestra di Wireshark che ci consente di vedere tutti i pacchetti di rete.



Per vedere tutti quanti i pacchetti che utilizzano il protocollo TCP, clicchiamo con il tasto destro su un pacchetto qualsiasi, selezioniamo "Follow" e quindi "TCP Stream".



Questo ci apre la conversazione TCP, e le informazioni che ne possiamo dedurre corrispondono a quelle viste nella trascrizione. Il nome della macchina bersaglio è “metasploitable” e il suo indirizzo IP è 209.165.200.235.

whoami

Da ciò che possiamo notare, l'attaccante ha eseguito il comando “whoami” sulla macchina del bersaglio, e la risposta “root” ci mostra che il bersaglio è in possesso dei privilegi, appunto, di root in questa macchina.

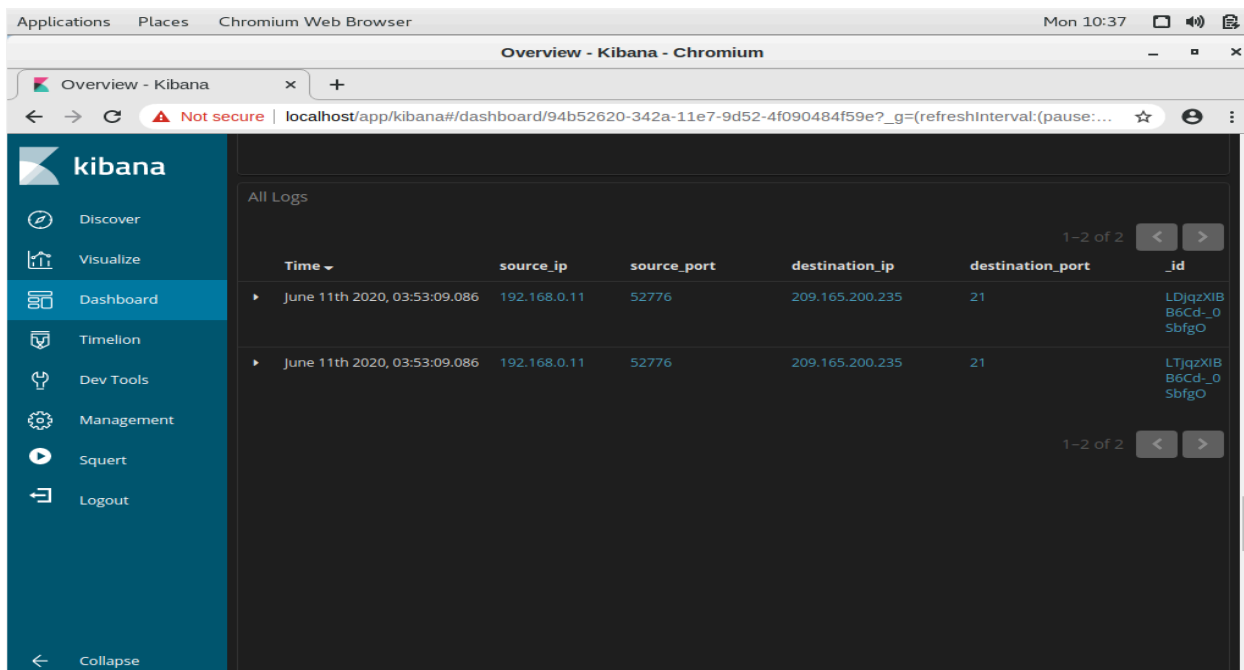
Utilizzo di Kibana

Torniamo all'interfaccia di Sguil. Facciamo clic con il tasto destro sull'IP dell'attaccante (o del bersaglio, indifferente) e selezioniamo “Kibana IP Lookup” e poi “SrcIP”. Facciamo il login con le solite credenziali (username: analyst, password: cyberops) ed una volta dentro andiamo a selezionare in alto a destra il range temporale dell'analisi. Nella tabella “Absolute”, impostare il mese (1-30) di Giugno 2020.

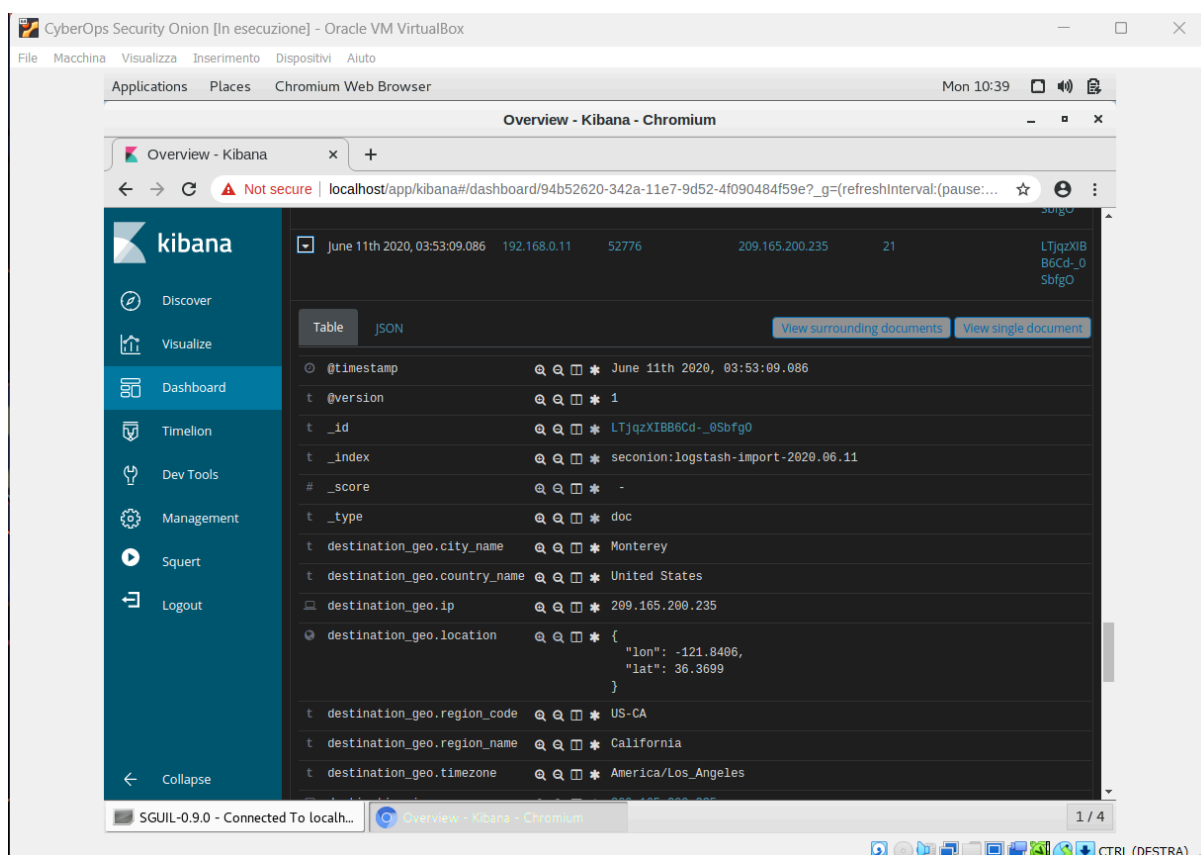
Si aprirà così una lista di diversi tipi di dati, e sappiamo che il file “confidentials.txt” non è più accessibile. Utilizzando il grafico a torta però saremo in grado di capire se per rubare il file è stato utilizzato il protocollo FTP.

Per fare questo, andiamo con il cursore nello spazio vuoto accanto al numero presente nella riga “bro_ftp”. Compariranno due lenti di ingrandimento con un + ed un - al loro interno, e cliccando su quella con il +, e quindi su “Filter for value” effettueremo la filtrazione che ci serve.

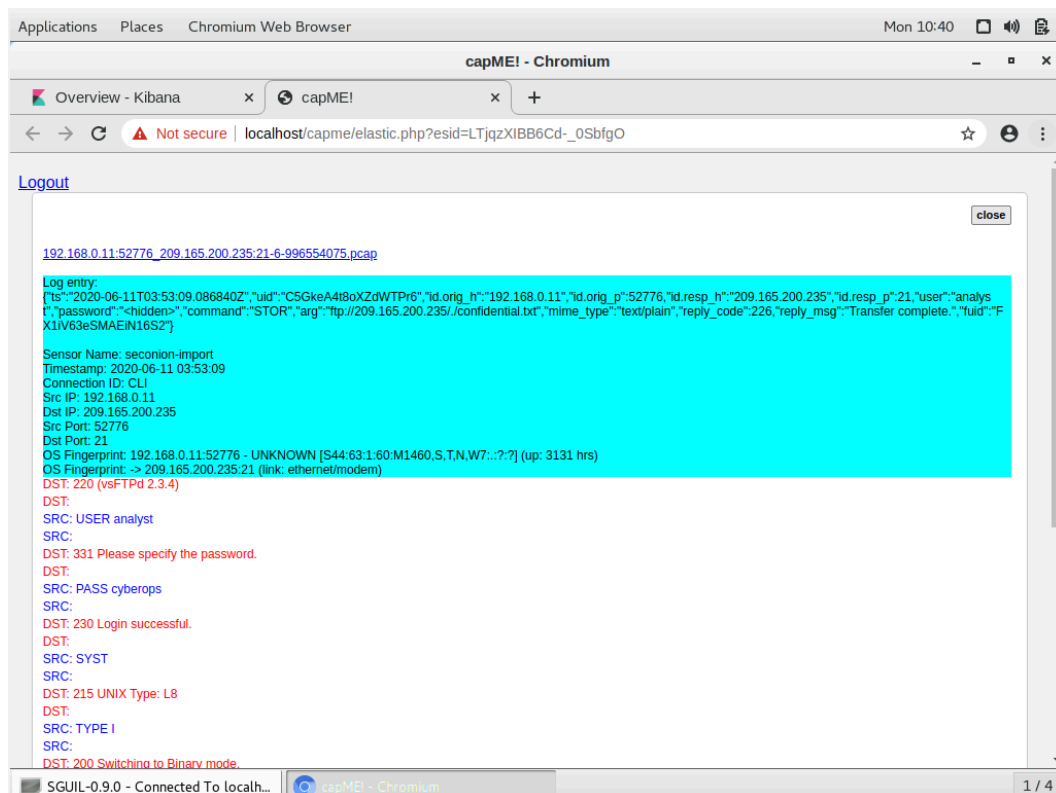
Scendiamo fino alla sezione “All logs” e troveremo due liste.



Cercando un pochino in entrambe, troveremo che in una delle due, alla voce “ftp_argument” è presente “ftp://209.165.200.235/./confidential.txt”. Questa è la lista che stavamo cercando, quindi torniamo su fino al campo “_id” e clicchiamo sul link.

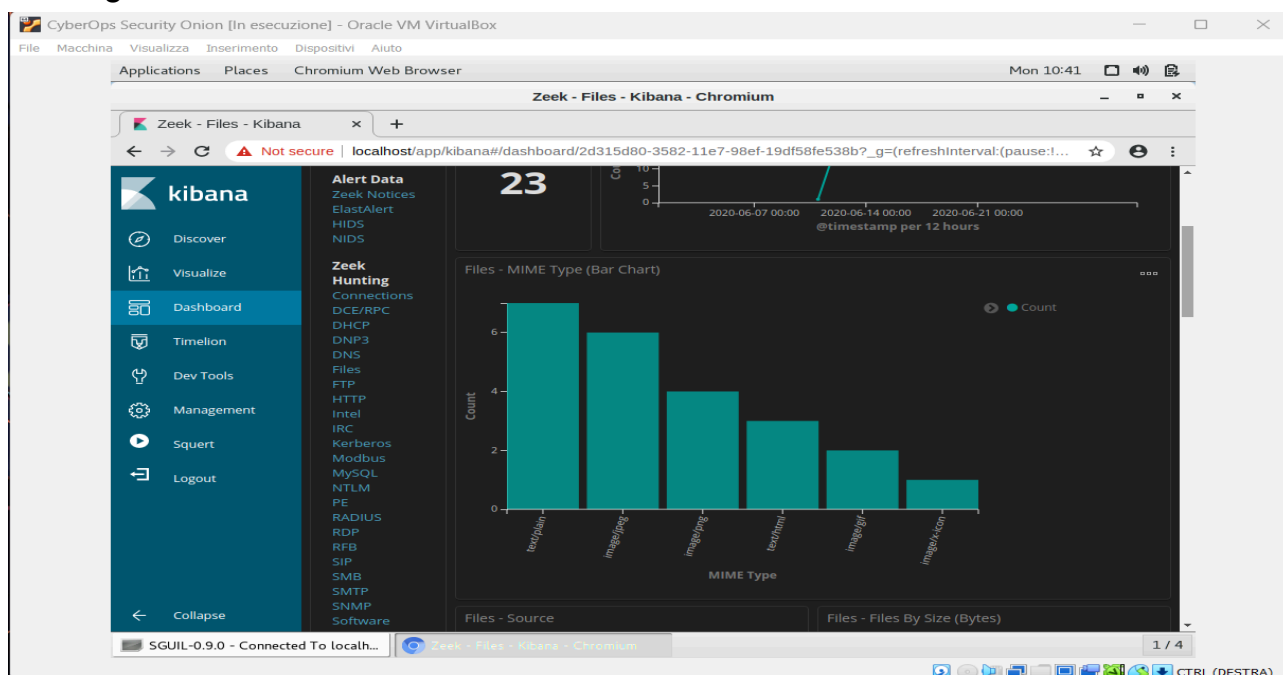


Questo ci apre la trascrizione della transazione tra l'attaccante ed il bersaglio.



Da ciò possiamo verificare che l'attaccante ha utilizzato FTP per copiare il contenuto del file "confidential.txt" e lo ha successivamente eliminato dalla macchina del bersaglio. Ma come facciamo a sapere quale sia il contenuto del file? Ci basti ricordare che uno dei servizi elencati nel grafico a torta di prima è proprio "ftp_data".

Torniamo su con il cursore e nel menù sulla sinistra, sotto la voce "Zeek Hunting", cerchiamo "Files".



Scendiamo fino alla voce “Source”, e facciamo la stessa procedura delle lenti di ingrandimento con il + che abbiamo fatto sopra, ma alla voce “FTP_DATA”.

The screenshot shows the Kibana dashboard in a Chromium browser window. The left sidebar contains the Kibana logo and navigation links: Discover, Visualize, Dashboard (selected), Timelion, Dev Tools, Management, Squert, and Logout. The main content area is divided into two panels. The left panel, titled 'Files - Source', shows a table with two columns: 'Source' and 'Count'. The right panel, titled 'Files - Files By Size (Bytes)', shows a table with two columns: 'Bytes Seen' and 'Count'. Both tables have a 'MIME Type' header above them. The 'Files - Source' table has two rows: 'HTTP' with a count of 22, and 'FTP_DATA' with a count of 1. The 'Files - Files By Size (Bytes)' table has eight rows, each with a file size and a count of 1. The bottom status bar shows 'SGUIL-0.9.0 - Connected To localh...' and 'Zeek - Files - Kibana - Chromium'.

Source	Count
HTTP	22
FTP_DATA	1

Bytes Seen	Count
99.685KB	1
70.19KB	1
55.912KB	1
50.438KB	1
38.326KB	1
23.687KB	1
23.11KB	1
22.569KB	1
12.137KB	1
10.032KB	1

A questo punto possiamo scorrere i risultati filtrati.

The screenshot shows the Kibana dashboard in a Chromium browser window. The left sidebar is the same as in the previous screenshot. The main content area is titled 'Files - Logs' and shows a table with columns: 'Time', 'file_ip', 'destination_ip', 'source', 'uid', 'fuid', and '_id'. The table has one row of data. The bottom status bar shows 'SGUIL-0.9.0 - Connected To localh...' and 'Zeek - Files - Kibana - Chromium'.

Time	file_ip	destination_ip	source	uid	fuid	_id
June 11th 2020, 03:53:09.088	192.168.0.1	209.165.200.235	FTP_DATA	C2jy8MWW6Xg4lbb51	FX1IV63eSMAEIN16S2	KDjazzXIBB8Cd_DSVfly

In questo modo possiamo vedere come il contenuto del documento “confidential.txt” fosse:

“CONFIDENTIAL DOCUMENT
DO NOT SHARE

This document contains information about the last security breach”.

