BONUS 3 - Isolate Compromised Host Using 5-Tuple

Informazioni:

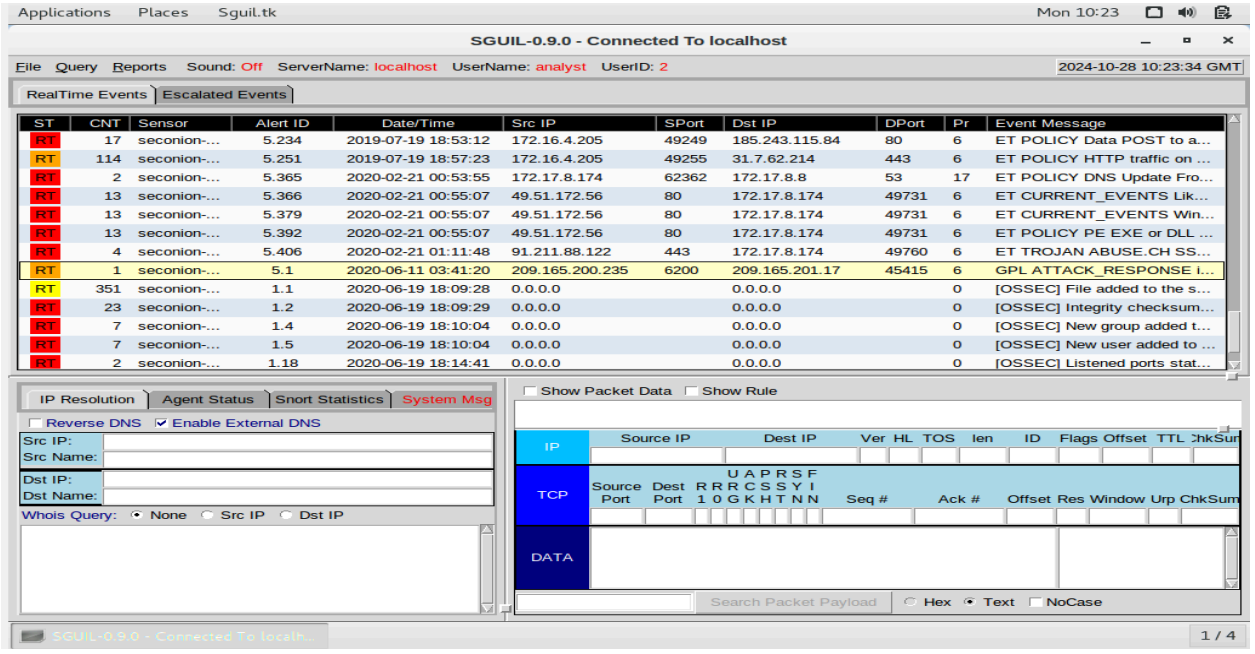
Questo report si pone come obiettivo quello di enunciare e spiegare le procedure seguite per identificare i contenuti di un file rubato, con aggiunta di dettagli in merito al trasferimento, andando a ritrovare sia l' IP di partenza sia quello di arrivo, più la data del trasferimento.

Trovare l' "attack response"

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

username = analyst
password = cyberops

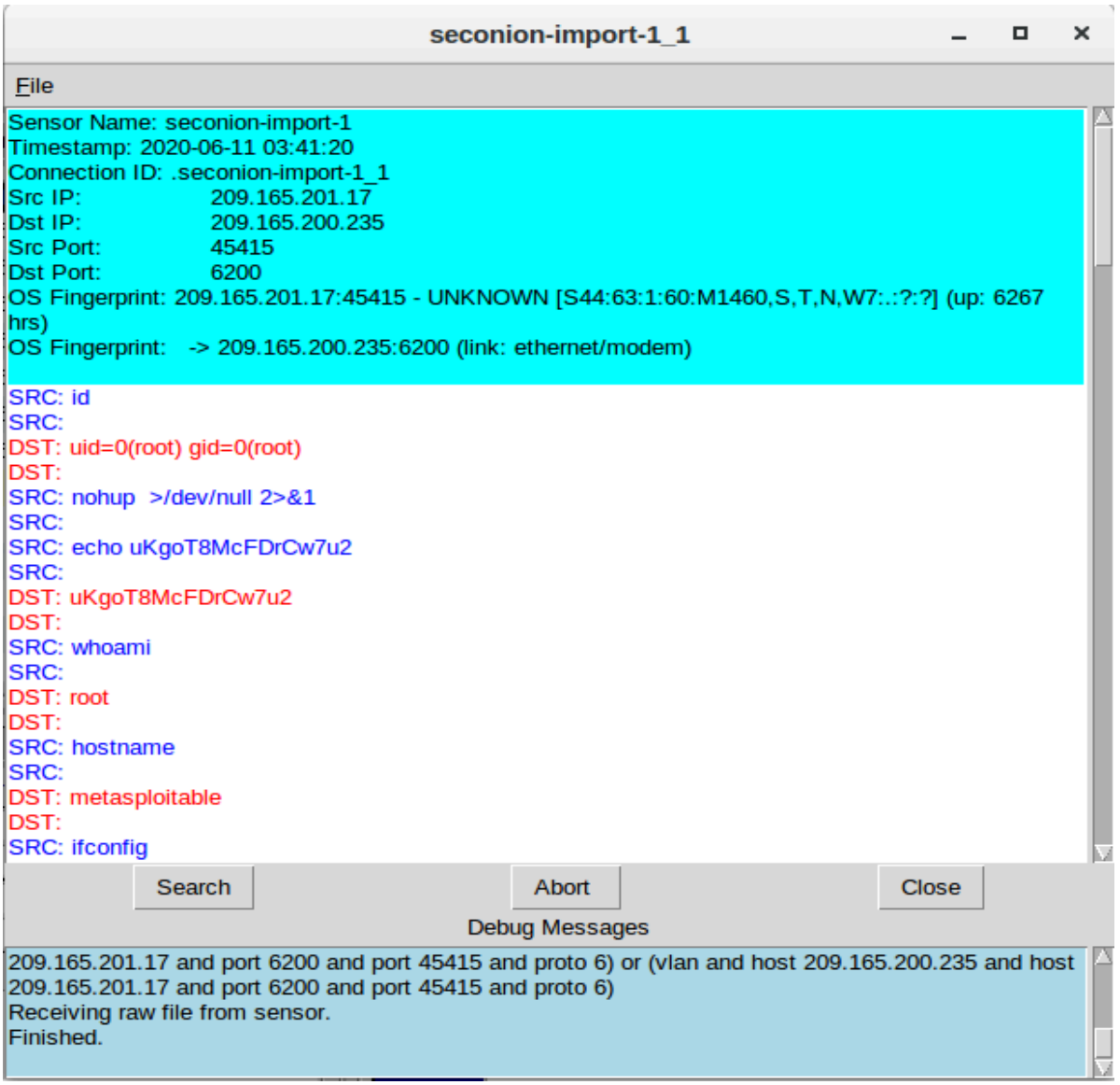
una volta dentro apriamo SGUIL e ri-eseguiamo il log in con le stesse credenziali. Ci troveremo davanti al registro degli eventi, e quello che dobbiamo cercare è " GPL ATTACK_RESPONSE id check returned root ".



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.

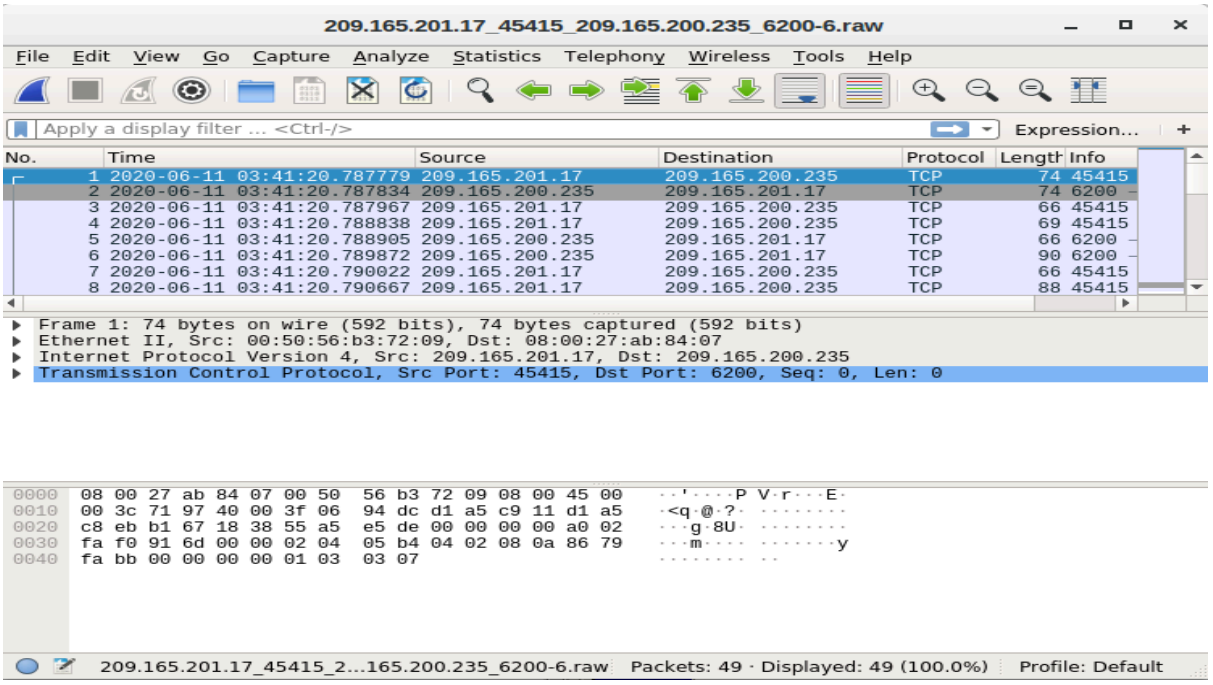


In questo screen possiamo vedere che l’attaccante, il cui IP è 209.165.201.17, ha ottenuto i permessi di root sulla macchina con IP “209.165.200.135”.

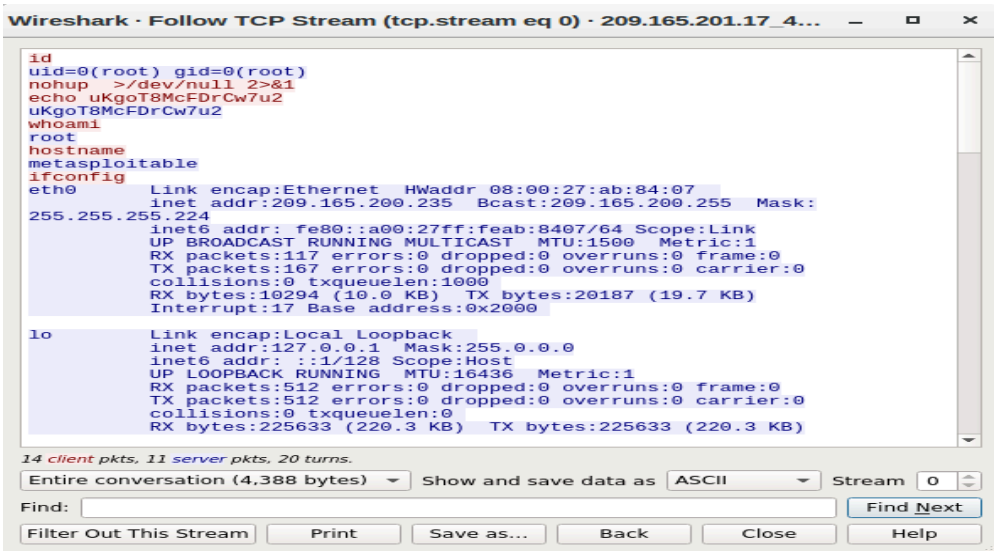
L’attaccante ha quindi navigato nei file di sistema, ha copiato il file “shadow” ed ha successivamente modificato i file al percorso /etc/shadow ed /etc/password.

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”.



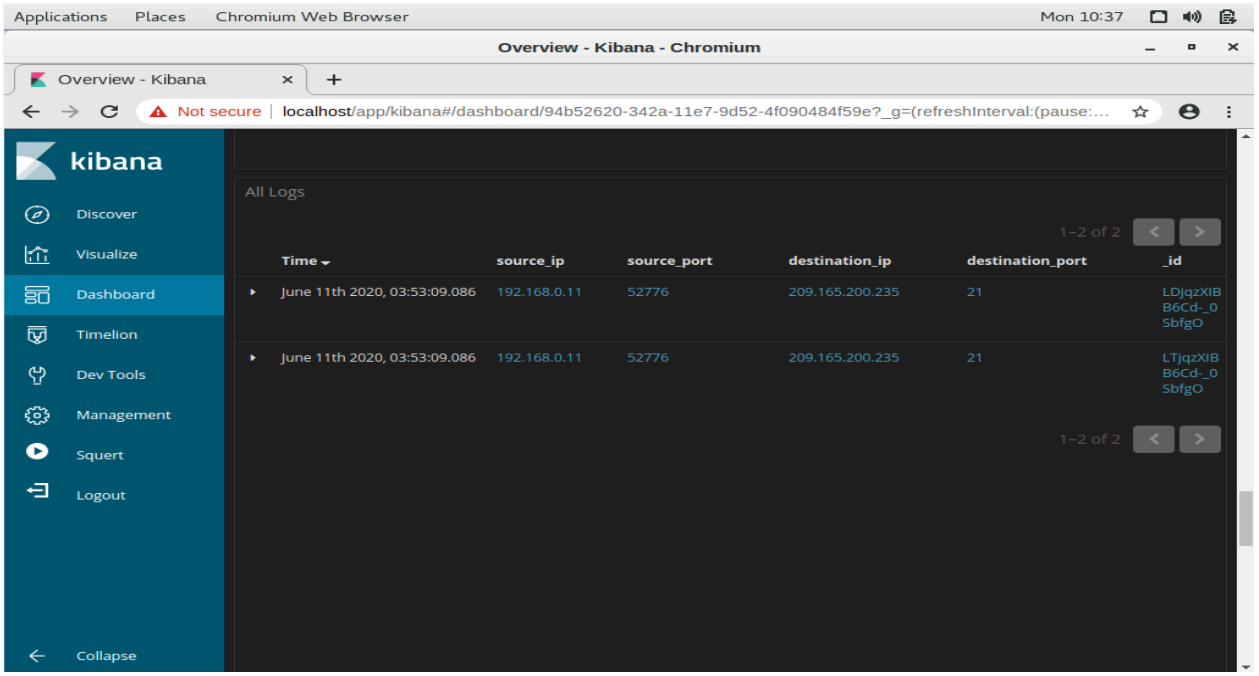
Questo ci apre la conversazione TCP, e le informazioni che ne possiamo dedurre corrispondono a quelle viste nella trascrizione. Il nome della macchina bersaglio è “metasploitable” e il suo indirizzo IP è 209.165.200.235.

whoami

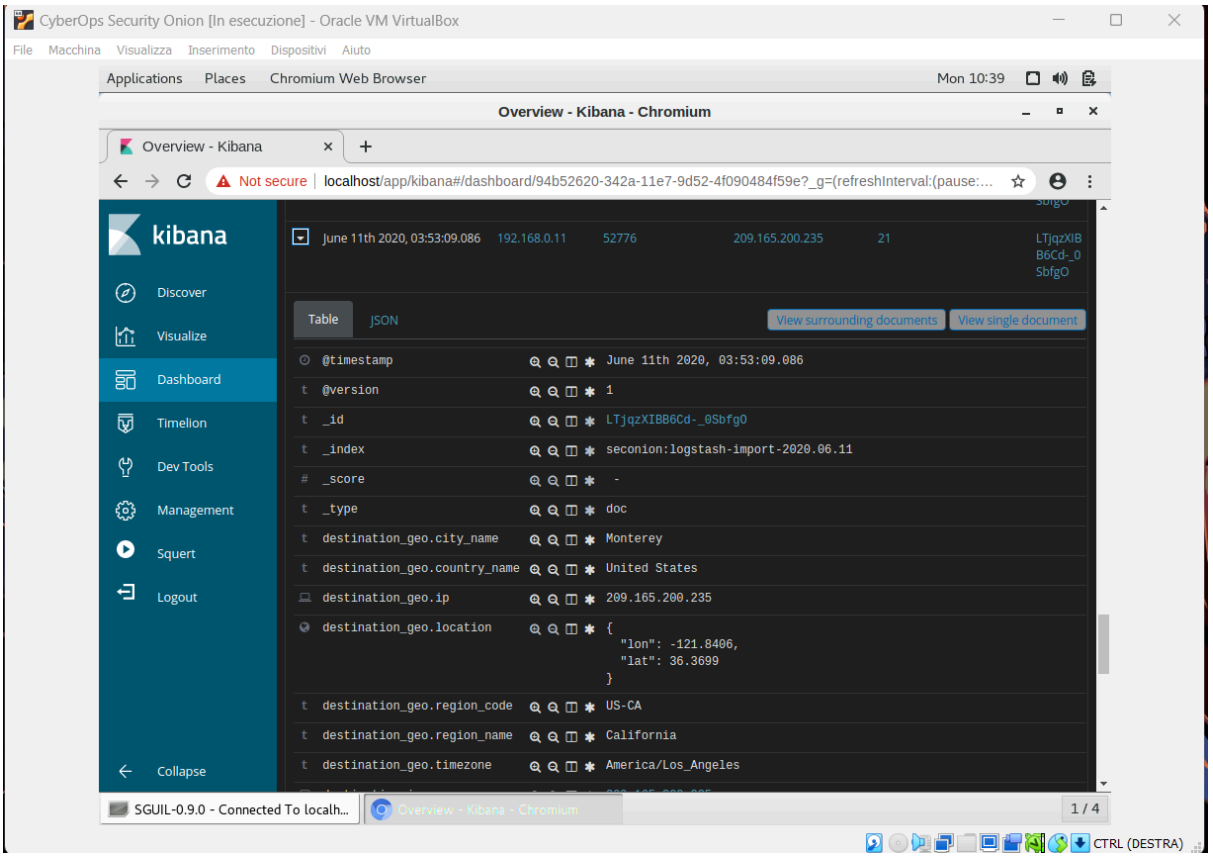
Da ciò che possiamo notare, l’attaccante ha eseguito il comando “whoami” sulla macchina del bersaglio, e la risposta “root” ci mostra che il bersaglio è in possesso dei privilegi, appunto, di root in questa macchina.

Utilizzo di Kibana

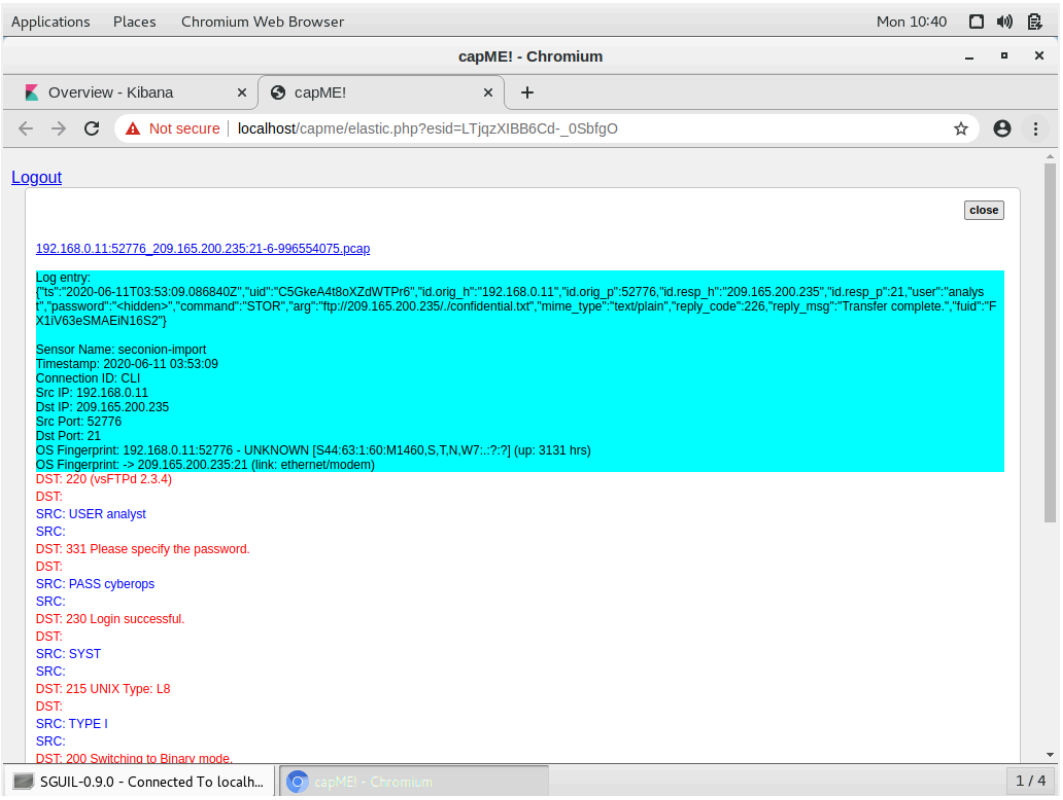
Torniamo all’interfaccia di Sguil. Facciamo clic con il tasto destro sull’IP dell’attaccante (o del bersaglio, indifferente) e selezioniamo “Kibana IP Lookup” e poi “SrcIP”. Facciamo il login con le solite credenziali (username: analyst, password: cyberops) ed una volta dentro andiamo a selezionare in 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.



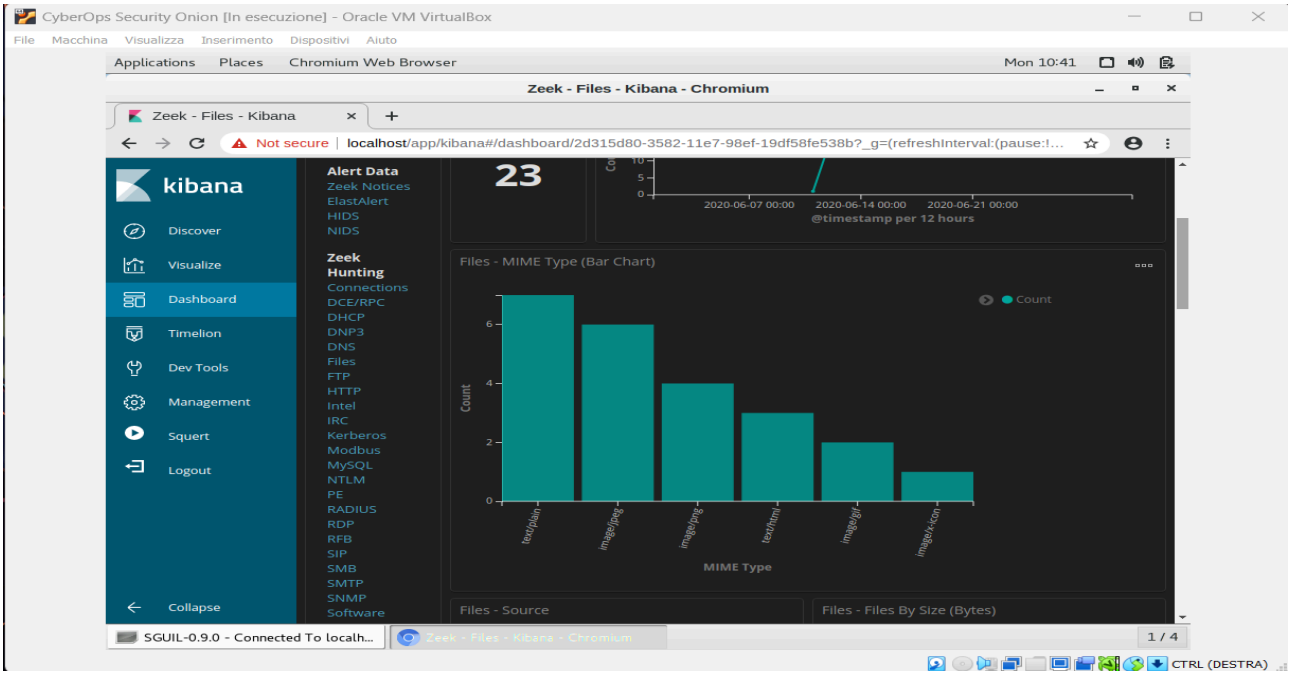
Cercando un pochino in entrambe, troveremo che in una delle due, alla voce “ftp_argument” è presente “ftp://209.165.200.235/./confidential.txt”. Questa è la lista che stavamo cercando, quindi torniamo su fino al campo “_id” e clicchiamo sul link.



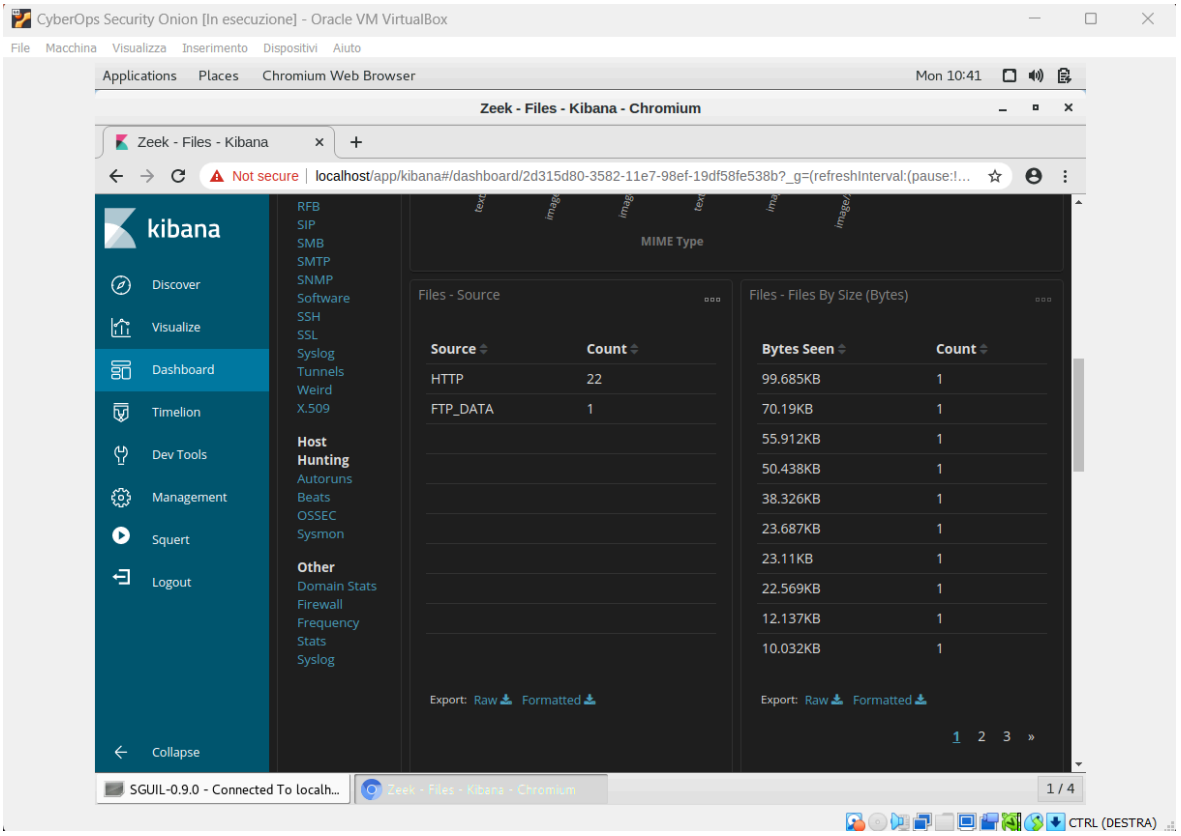
Questo ci apre la trascrizione della transazione tra l'attaccante ed il bersaglio.



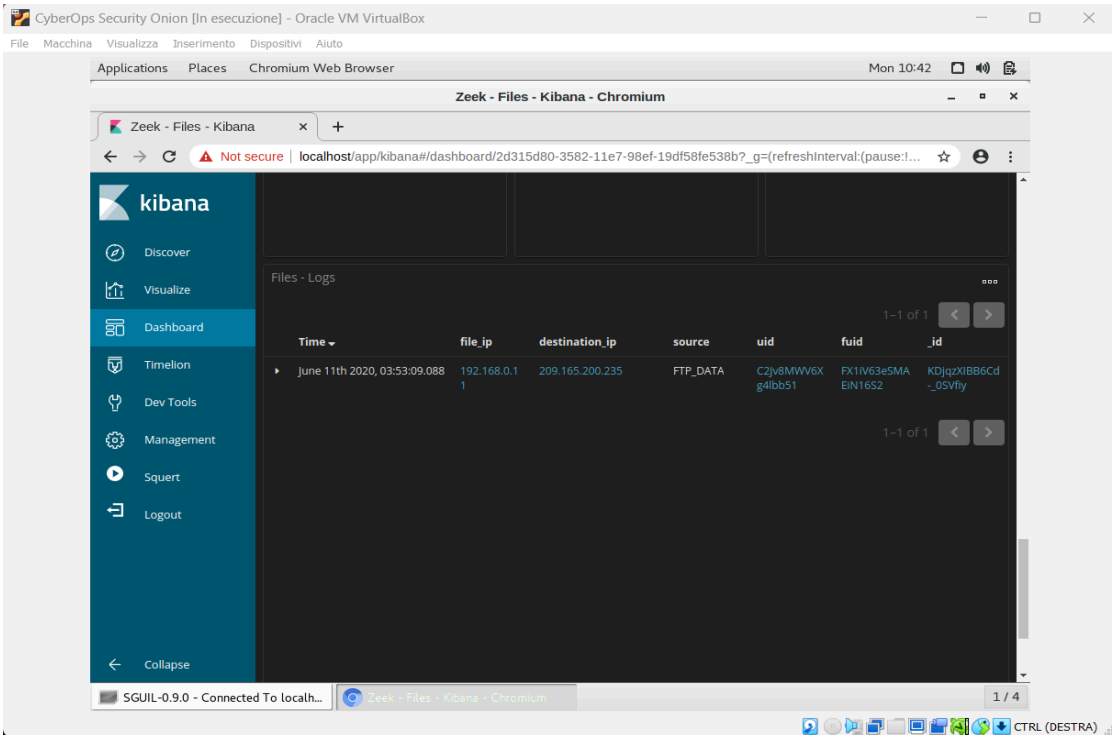
Da ciò possiamo verificare che l'attaccante ha utilizzato FTP per copiare il contenuto del file "confidential.txt" e lo ha successivamente eliminato dalla macchina del bersaglio. Ma come facciamo a sapere quale sia il contenuto del file? Ci basti ricordare che uno dei servizi elencati nel grafico a torta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



A questo punto possiamo scorrere i risultati filtrati.



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”.