

## Lab – Isolate Compromised Host Using 5-Tuple

### PAS1

La 5-tuple è un insieme di informazioni che viene utilizzato per identificare le connessioni di rete e include:

- IP di origine
- IP di destinazione
- Porta di origine
- Porta di destinazione
- Protocollo di rete

Con questi elementi possiamo isolare il traffico relativo all'host compromesso.

Avviamo la security onion e accediamo con utente analyst e password cyberops

Apriamo Sguil ed effettuiamo il login.

Esaminiamo gli eventi e selezioniamo il messaggio che ci dice che tramite un attacco è stato effettuato l'accesso come root : **GPL ATTACK\_RESPONSE id check turned root**.

Una volta selezionato facciamo clic col tasto destro del mouse e selezioniamo **transcript**

The screenshot shows the SGUIL-0.9.0 interface connected to localhost. The main window displays a table of RealTime Events, with one row highlighted for "Event History". A context menu is open over this row, with "Transcript" selected. The bottom right pane shows a detailed view of a selected network packet. The packet details tab shows the following information:

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
TCP	209.165.200.235	209.165.201.17	4	5	0	76	31846	2	0	64	3506
UAPRSF											
Source Dest R R R C S S Y I											
Port Port 1 0 G K H T N N Seq # Ack # Offset Res Window Urp ChkSum											
DATA	6200	45415	. . . X X . . .	2951186435	1436935650	8	0	181	0	29271	
	75	69	64	3D	30	28	72	6F	6F	74	29
	30	28	72	6F	6F	74	29	0A			

Below the packet details, there are buttons for "Search Packet Payload", "Hex", "Text", and "NoCase". The status bar at the bottom right shows "CTRL (DESTRA)".

Il transcript mostra le transazioni tra la sorgente della minaccia (SRC) e il target (DST) durante l'attacco. L'attore della minaccia sta eseguendo comandi Linux sul target.

The screenshot shows the SGUIL-0.9.0 interface connected to localhost. The transcript window displays the following details:

- Sensor Name:** seconion-import-1\_1
- Timestamp:** 2020-06-11 03:41:20
- Connection ID:** seconion-import-1\_1
- Src IP:** 209.165.201.17
- Dst IP:** 209.165.200.235
- Src Port:** 45415
- Dst Port:** 6200
- OS Fingerprint:** 209.165.201.17:45415 - UNKNOWN [S44:63:1:60:M1460,S,T,N,W?::?:?] (up: 6267 hrs)
- OS Fingerprint:** -> 209.165.200.235:6200 (link: ethernet/modem)
- SRC: id**
- SRC: whoami**
- DST: uid=0(root) gid=0(root)**
- DST: nohup >/dev/null 2>&1**
- SRC: echo uKgoT8McFDrCw7u2**
- SRC: ifconfig**
- DST: uKgoT8McFDrCw7u2**
- DST: whoami**
- SRC: hostname**
- SRC: metasploitable**
- DST: ifconfig**

The right pane shows a list of events and messages, including:

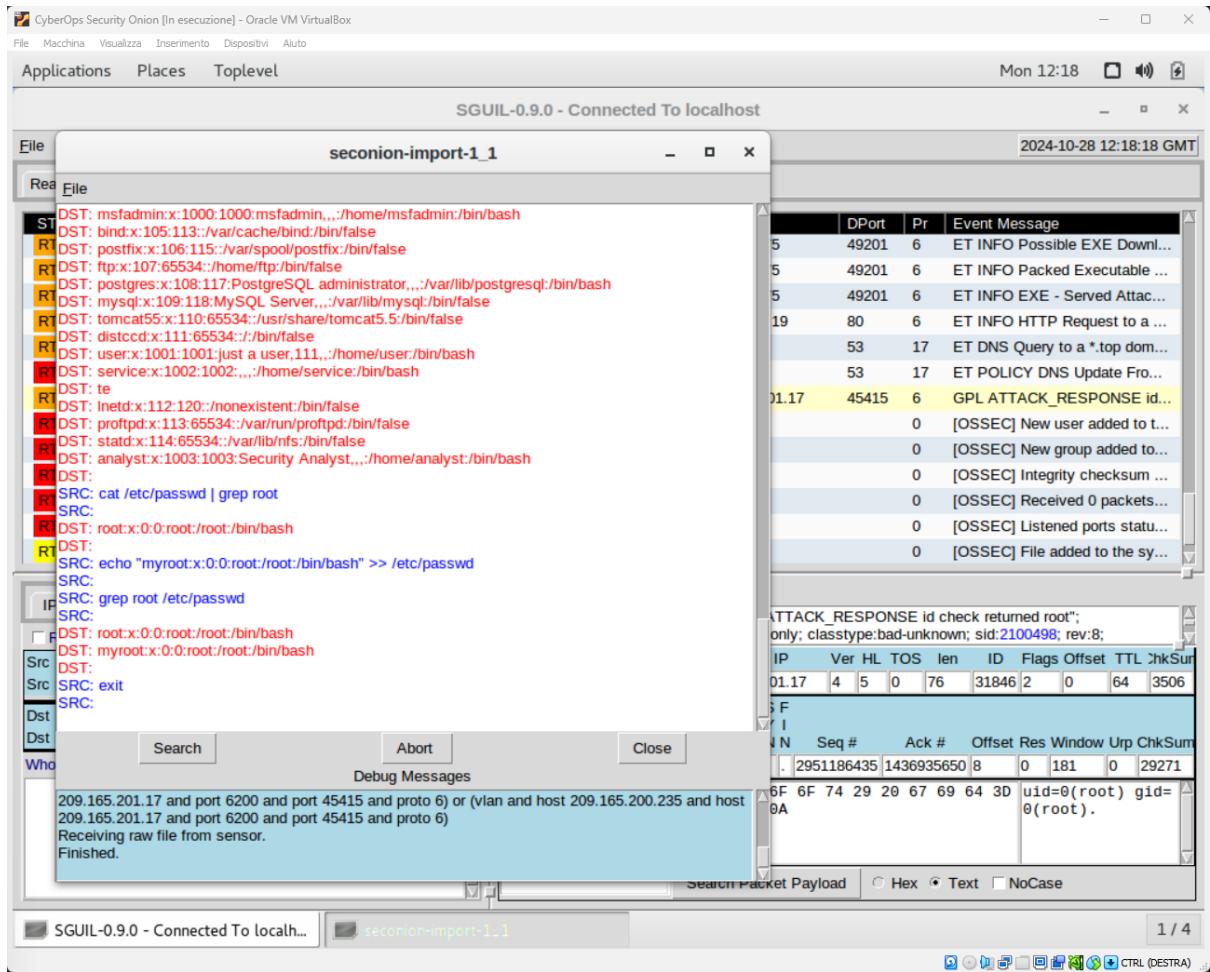
- ET INFO Possible EXE Download
- ET INFO Packed Executable ...
- ET INFO EXE - Served Attach...
- ET INFO HTTP Request to a ...
- ET DNS Query to a \*.top dom...
- ET POLICY DNS Update Fro...
- GPL ATTACK\_RESPONSE id...
- [OSSEC] New user added to t...
- [OSSEC] New group added to ...
- [OSSEC] Integrity checksum ...
- [OSSEC] Received 0 packets...
- [OSSEC] Listened ports statu...
- [OSSEC] File added to the sy...

The bottom pane shows a packet capture and analysis window with the following details:

IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	chksum
01.17	4	5	0	76	31846	2	0	64	3506
SF I N Seq # Ack # Offset Res Window Urp ChkSum									
2951186435 1436935650 8 0 181 0 29271									
6F 6F 74 29 20 67 69 64 3D uid=0(root) gid=0(root).									

Debug Messages:

```
209.165.201.17 and port 6200 and port 45415 and proto 6) or (vlan and host 209.165.200.235 and host 209.165.201.17 and port 6200 and port 45415 and proto 6)
Receiving raw file from sensor.
Finished.
```



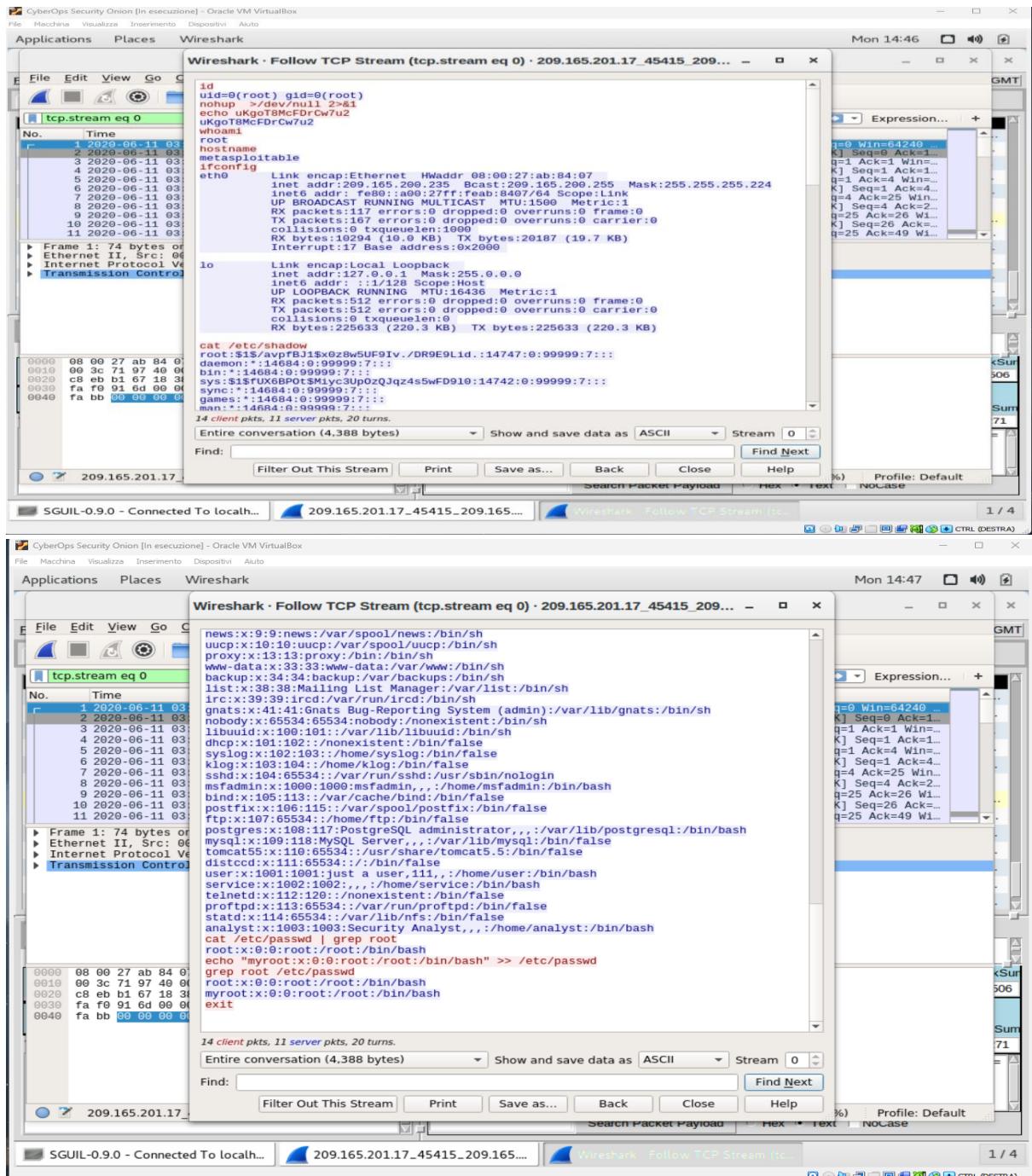
L'attaccante proveniente da 209.165.201.17 ha ottenuto l'accesso root a 209.165.200.235.  
L'attaccante ha esplorato il file system, ha copiato il file shadow e ha modificato /etc/shadow  
e /etc/passwd.

**PAS2**

Apriamo wireshark dallo stesso avviso e visioniamo i pacchetti esfiltrati

The screenshot shows the SGUIL-0.9.0 interface connected to localhost. The main window displays a table of RealTime Events, with one row for 'WireShark' highlighted. A context menu is open over this row, showing options like 'Event History', 'Transcript', 'Transcript (force new)', 'WireShark', 'NetworkMiner', and 'NetworkMiner (force new)'. Below the table, there are sections for 'IP Resolution', 'Agent Status', and 'Bro (force new)'. The 'Bro' section is expanded, showing configuration for 'Reverse DNS' and 'Enable External DNS', and fields for 'Src IP', 'Src Name', 'Dst IP', and 'Dst Name'. The 'Whois Query' section has 'None' selected. On the right, a detailed packet analysis window is open for a TCP connection between 209.165.200.235:6200 and 209.165.201.17:45415. The window shows the IP header, TCP header, and the DATA payload. The payload contains a message in hex and ASCII: '75 69 64 3D 30 28 72 6F 6F 74 29 20 67 69 64 3D uid=0(root) gid=0(root).'. At the bottom, there are buttons for 'Search Packet Payload', 'Hex', 'Text', and 'NoCase'.

Per visualizzare tutti i pacchetti assemblati in una conversazione TCP, fare clic con il pulsante destro del mouse su un pacchetto qualsiasi e selezionare Segui > Flusso TCP



Possiamo capire che il flusso TCP mostra la discussione tra l'attaccante (scritta in rosso) e la macchina target (scritta in blu). Il nome del target è metasploitable e il suo indirizzo è 209.165.200.235.

Quando l'attaccante invia il comando whoami , ci mostra che l'attaccante ha ottenuto i privilegi di root sulla macchina target.

Quindi dopo aver avuto tutte le info sull'account utente, l'attaccante è uscito.

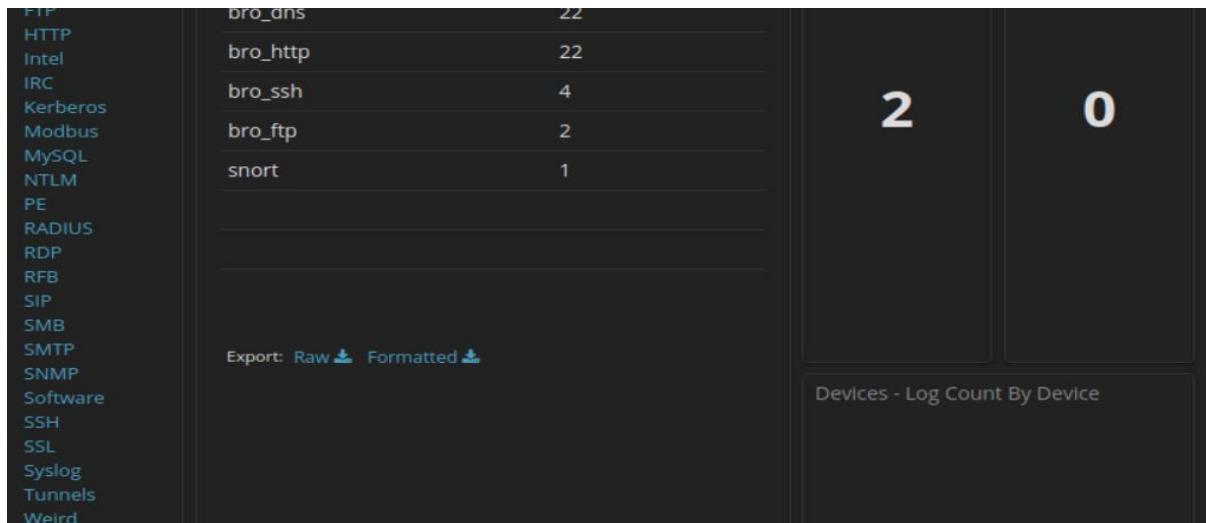
### PAS3

Selezioniamo il pacchetto indicato precedentemente e avviamo kibana IP lookup>SrcIp.

The screenshot shows the SGUIL-0.9.0 interface connected to localhost. The main window displays two tabs: 'RealTime Events' and 'Escalated Events'. The 'RealTime Events' tab is active, showing a table of log entries with columns: ST, CNT, Sensor, Alert ID, Date/Time, Src IP, Sport, Dst IP, DPort, Pr, and Event Message. Several entries are highlighted in yellow, indicating specific events of interest. Below the table is a 'System Msg' pane with various lookup options like 'Quick Query', 'Advanced Query', and several IP and domain lookups. A 'Whois Query' section is also present. On the right side, there is a detailed packet capture window showing a single packet with fields like SrcIP, DstIP, Ver, HL, TOS, len, ID, Flags, Offset, TTL, and ChkSum. The packet payload is shown in a large text area with the word 'DATA'.

Nei risultati che otterremo ci sono diversi tipi di dati, in questo caso FTP è presente e andremo a vedere se è stato utilizzato per rubare i file.

The screenshot shows the Kibana Overview dashboard titled 'Overview - Kibana - Chromium'. The left sidebar has a dark theme with navigation links: Discover, Visualize, Dashboard, Timelion, Dev Tools, Management, Squert, and Logout. The main area shows a summary card with the number '134' and a chart titled 'Total Log Count Over Time' showing data from June 1st, 2020, to June 30th, 2020. Below this are three cards: 'All Sensors - Log Type', 'Sensors - C...', and 'Devices - C...'. The 'All Sensors - Log Type' card lists log types and their counts: bro\_conn (60), bro\_files (23), bro\_dns (22), and bro\_http (22). The bottom status bar indicates 'SGUIL-0.9.0 - Connected To localh...' and 'Overview - Kibana - Chromium'.



filtriamo "bro\_ftp", dove vedremo l'indirizzo ip di origine con il relativo numero di porta e altrettanto per il l'ip di destinazione:

Overview - Kibana - Chromium

All Logs

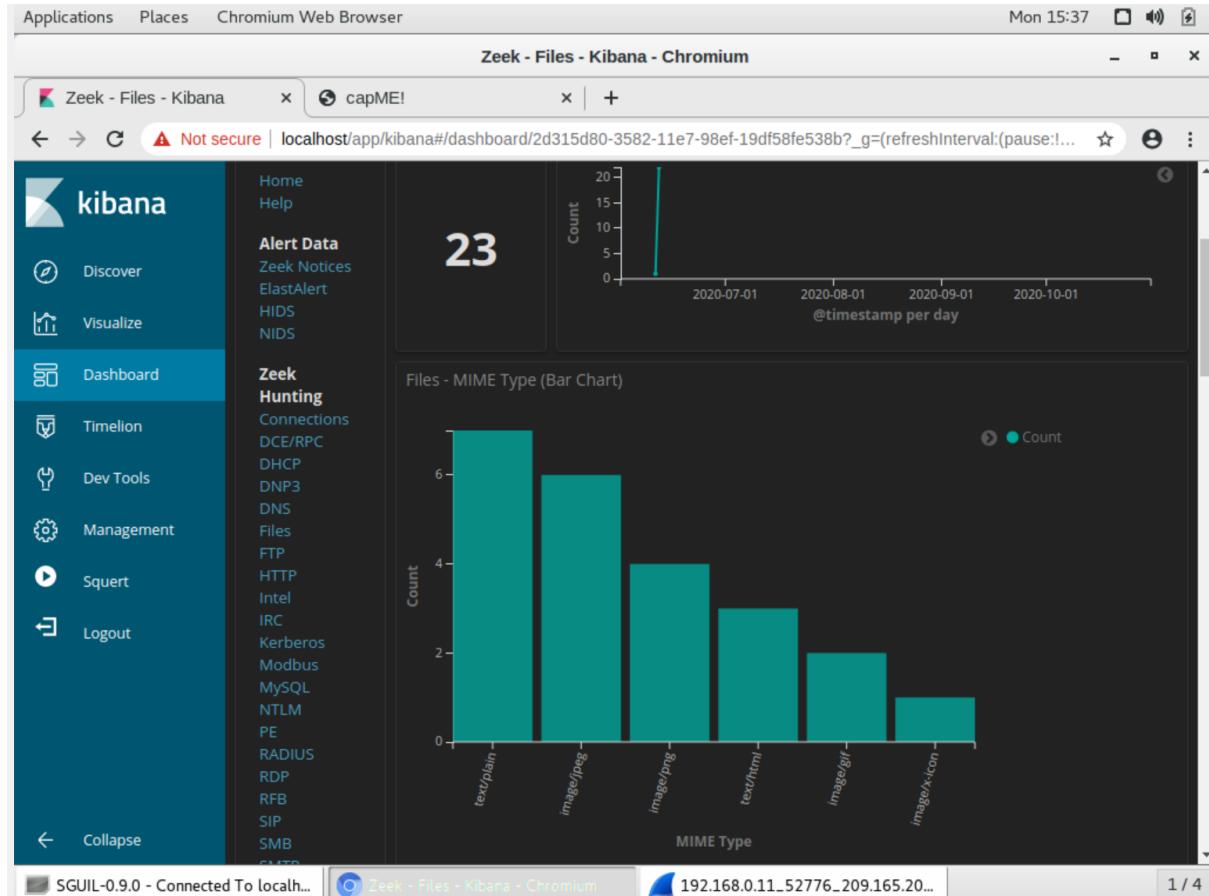
Time	source_ip	source_port	destination_ip
June 11th 2020, 03:53:09.086	192.168.0.11	52776	209.165.200.235
June 11th 2020, 03:53:09.086	192.168.0.11	52776	209.165.200.235

Cliccando sul collegamento del campo alert \_id , faremo il transcript e scaricheremo il pcap e analizzeremo il traffico tramite wireshark:



Qui possiamo vedere che sono state rubate le credenziali di accesso dell'utente analyst, dove vediamo username e password.

Avendo verificato che l'attaccante ha utilizzato FTP per copiare il contenuto del file andremo nella sezione FILES e vedremo i file che sono stati registrati:



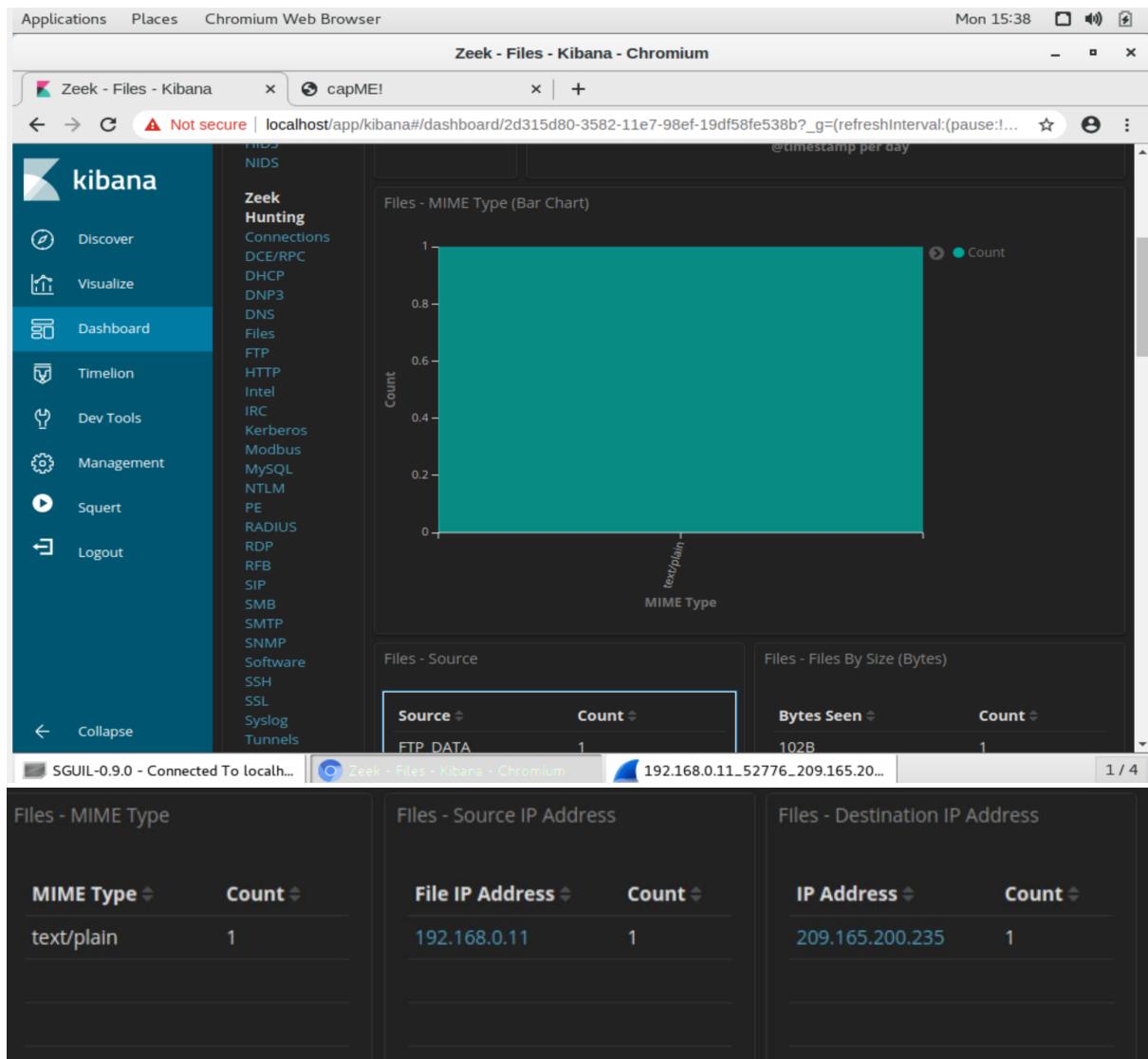
Qui notiamo che sono presenti file di testo e diverse tipologie di formati immagine.

## Files - Source

Source ◀ Count ◀

HTTP 22

FTP\_DATA 1



Da queste immagini vediamo HTTP e FTP\_DATA come fonti utilizzate.

Il file di trasferito è un file di testo inviato dall'ip 192.168.0.11 a 209.165.200.235 il giorno 11 giugno 2020 alle 3:53.

[Logout](#)

[close](#)

[192.168.0.11:49817\\_209.165.200.235:20-6-379169035.pcap](#)

Log entry:  
{"ts": "2020-06-11T03:53:09.088773Z", "tuid": "FX1jV63eSMAEIN16S2", "tx\_hosts": ["192.168.0.11"], "rx\_hosts": ["209.165.200.235"], "conn\_uids": ["C2Jv8MWV6Xg4bb51"], "source": "FTP\_DATA", "depth": 0, "analyzers": ["SHA1", "MD5"], "mime\_type": "text/plain", "duration": 0.0, "is\_orig": false, "seen\_bytes": 102, "missing\_bytes": 0, "overflow\_bytes": 0, "timedout": false, "md5": "e7bc9c20bfd5666365379c91294d536b", "sha1": "f7f54acee0342f6161f8e63a10824ee11b330725"}  
Sensor Name: seconion-import  
Timestamp: 2020-06-11 03:53:09  
Connection ID: CLI  
Src IP: 192.168.0.11  
Dst IP: 209.165.200.235  
Src Port: 49817  
Dst Port: 20  
OS Fingerprint: 209.165.200.235:20 - Linux 2.6 (newer, 1) (up: 1 hrs)  
OS Fingerprint: -> 192.168.0.11:49817 (distance 0, link: ethernet/modem)  
SRC: CONFIDENTIAL DOCUMENT  
SRC: DO NOT SHARE  
SRC: This document contains information about the last security breach.  
SRC:  
  
DEBUG: Using archived data: /nsm/server\_data/securityonion/archive/2020-06-11/seconion-import/192.168.0.11:49817\_209.165.200.235:20-6.raw  
QUERY: SELECT sid FROM sensor WHERE hostname='seconion-import' AND agent\_type='pcap' LIMIT 1  
CAPME: Processed transcript in 0.87 seconds: 0.43 0.34 0.00 0.10 0.00

[192.168.0.11:49817\\_209.165.200.235:20-6-379169035.pcap](#)

In questa schermata possiamo vedere che il contenuto è un documento riservato da non condividere.

Per raccomandarci di fermare ulteriori accessi non autorizzati , possiamo prendere molte precauzioni e OVVIALEMENTE, il cambio della password dell'utente Analyst deve essere modificata in tutta la rete come prassi basica, dopo di che possiamo:

- Disabilitare il protocollo FTP e passare a quello SFTP poichè cifra sia le credenziali sia i dati in transito , proteggendoli da intercettazioni.
- Stessa idea per HTTP, passando ad HTTPS avremo maggiore garanzia che i dati scambiati siano cifrati.
- Autenticazione a due fattori.
- Configurare accesso SSH utilizzando chiavi pubbliche e private, in questo modo solo chi ha la chiave privata può accedere.
- Monitoraggio e Logging avanzato per rilevare comportamenti sospetti e intervenire prima che ci siano danni.
- Configurare firewall e filtri d'accesso per limitare il traffico solo alle fonti autorizzate e bloccare IP sospetti.