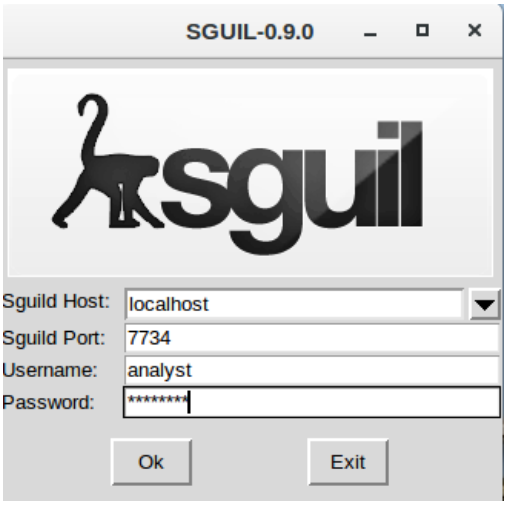
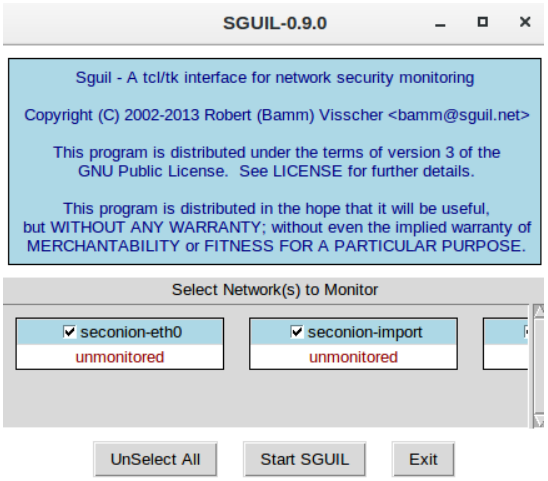
Bonus 2 Isolare un Host Compromesso Usando la 5-Tupla

PARTE 1: ESAMINARE GLI ALERT IN SGUIL

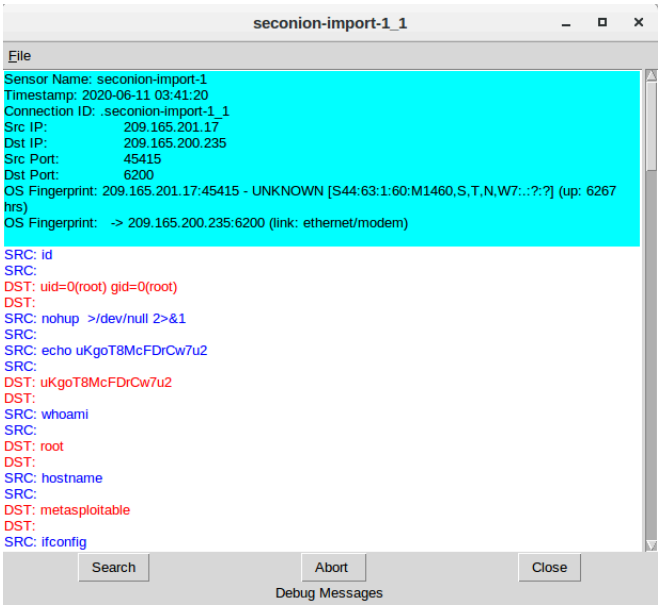
Dopo l'attacco, gli utenti non hanno più accesso al file chiamato confidential.txt, in questo laboratorio andremo ad analizzare i log per capire come il file sia stato compromesso.

Apriamo la VM CyberOps Security Onion ed eseguiamo il tool Sguil eseguendo l'accesso. Dovremo selezionare i Network disponibili, li selezioneremo tutti e avvieremo Sguil.





Il tool ci presenterà una schermata contenente un elenco di eventi registrati. Scorrendo tra questi, noteremo una voce denominata **"**GPL ATTACK_RESPONSE check returned root**"**, la quale indica che, in seguito a un attacco, l'accesso come utente root potrebbe essere stato ottenuto dall'attaccante.
Cliccando col tasto destro sulla voce "5.1" della colonna "Alert ID" selezioneremo la voce "Transcript" che ci porterà a una finestra che ci mostrerà vari dati tra cui gli IP dell'attaccante e del target, data e ora dell'evento in questione e i vari comandi scritti nel terminale.



Il comando <whoami> e la risposta "root" indicano appunto l'ottenimento dei privilegi root dell'attaccante e la macchina target è la Metasploitable2. Continuando a scorrere vedremo l'attaccante vagare tra i vari file di sistema leggendo il file "shadow".

```
SRC: cat /etc/shadow
SRC:
DST: root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
DST: daemon:*:14684:0:99999:7:::
DST: bin:*:14684:0:99999:7:::
DST: sys:$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:14742:0:99999:7:::
DST: sync:*:14684:0:99999:7:::
DST: games:*:14684:0:99999:7:::
DST: man:*:14684:0:99999:7:::
DST: lp:*:14684:0:99999:7:::
DST: mail:*:14684:0:99999:7:::
DST: news:*:14684:0:99999:7:::
DST: uucp:*:14684:0:99999:7:::
DST: proxy:*:14684:0:99999:7:::
DST: www-data:*:14684:0:99999:7:::
DST: backup:*:14684:0:99999:7:::
DST: list:*:14684:0:99999:7:::
DST: irc:*:14684:0:99999:7:::
DST: gnats:*:14684:0:99999:7:::
DST: nobody:*:14684:0:99999:7:::
DST: libuuid:!:14684:0:99999:7:::
DST: dhcp:*:14684:0:99999:7:::
DST: syslog:*:14684:0:99999:7:::
DST: klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
DST: sshd:*:14684:0:99999:7:::
DST: msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:14684:0:99999:7:::
DST: bind:*:14685:0:99999:7:::
DST: postfix:*:14685:0:99999:7:::
DST: ftp:*:14685:0:99999:7:::
```

L'attaccante continua a leggere file e apre il file "password", filtrando i risultati aggiungendo <grep root> per poi passare alla creazione di un clone dell'utente root con gli stessi privilegi, chiamandolo "myroot".

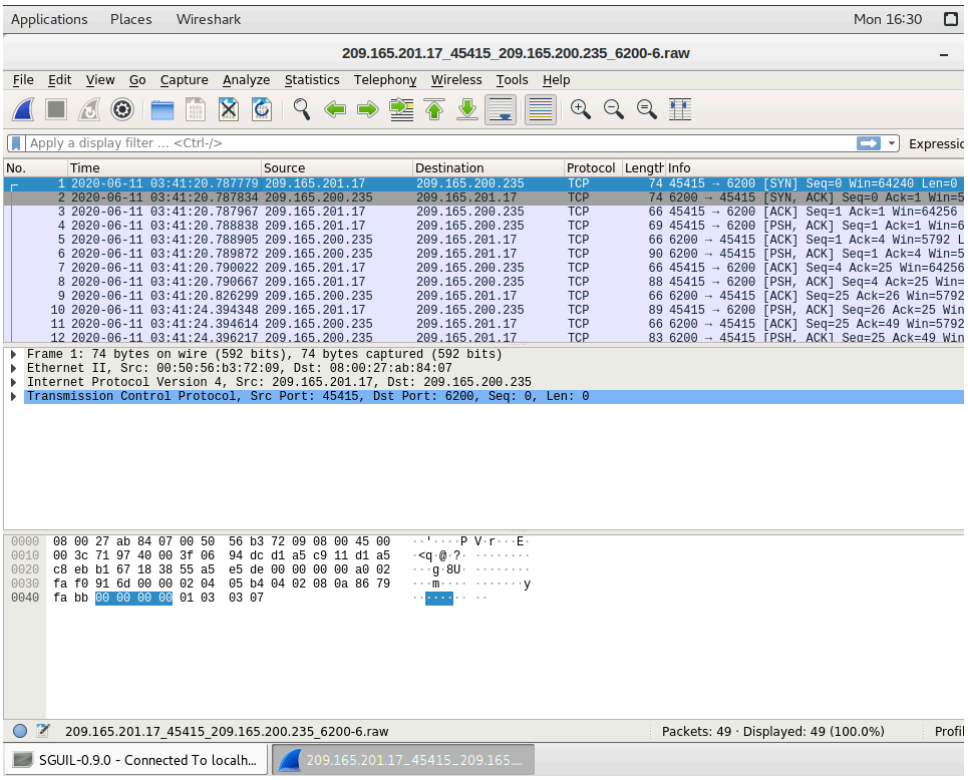
```
SRC: cat /etc/passwd | grep root
SRC:
DST: root:x:0:0:root:/root:/bin/bash
DST:
SRC: echo "myroot:x:0:0:root:/root:/bin/bash" >> /etc/passwd
SRC:
SRC: grep root /etc/passwd
SRC:
DST: root:x:0:0:root:/root:/bin/bash
DST: myroot:x:0:0:root:/root:/bin/bash
DST:
SRC: exit
SRC:
```

Domanda: <u>Che tipo di transazioni si sono verificate tra il client e il server in questo attacco?</u>

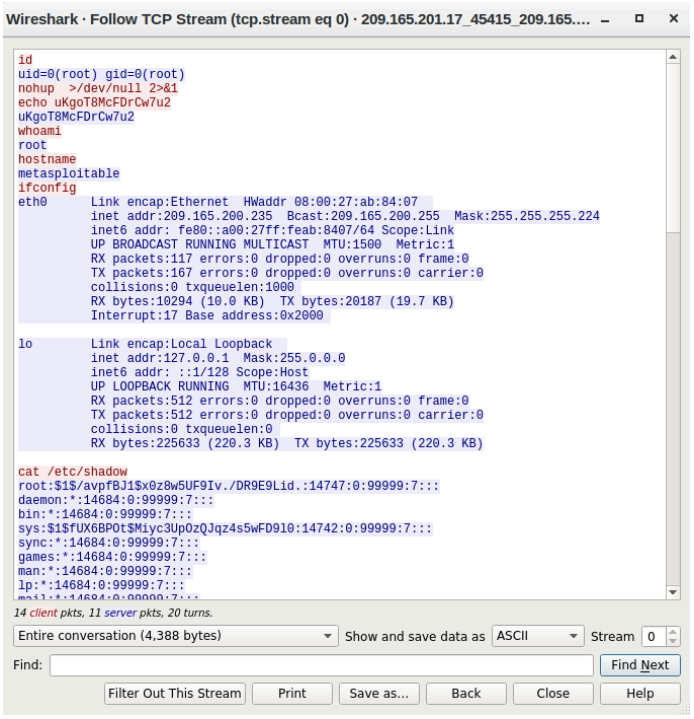
R: Dalle informazioni ottenute finora possiamo dire che le transazioni sono avvenute in locale in una sessione remota (tramite SSH) oppure semplicemente in un ambiente simulato.

PARTE 2: PASSARE A WIRESHARK

Cliccando di nuovo col tasto destro sulla stessa voce di prima andremo a selezionare wireshark per provare a fare un'analisi più approfondita.



Su un pacchetto qualsiasi clicchiamo col destro e si va su "Follow">>"TCP Stream".



La finestra popuppata mostrerà di nuovo l'interazione tra attaccante e target.

Domanda: <u>Cosa hai osservato? Cosa indicano i colori del testo rosso e blu?</u>

R: Il testo in rosso indicano i comandi mandati dall'attaccante mentre quelle blu sono le risposte del terminale di Metasploitable2

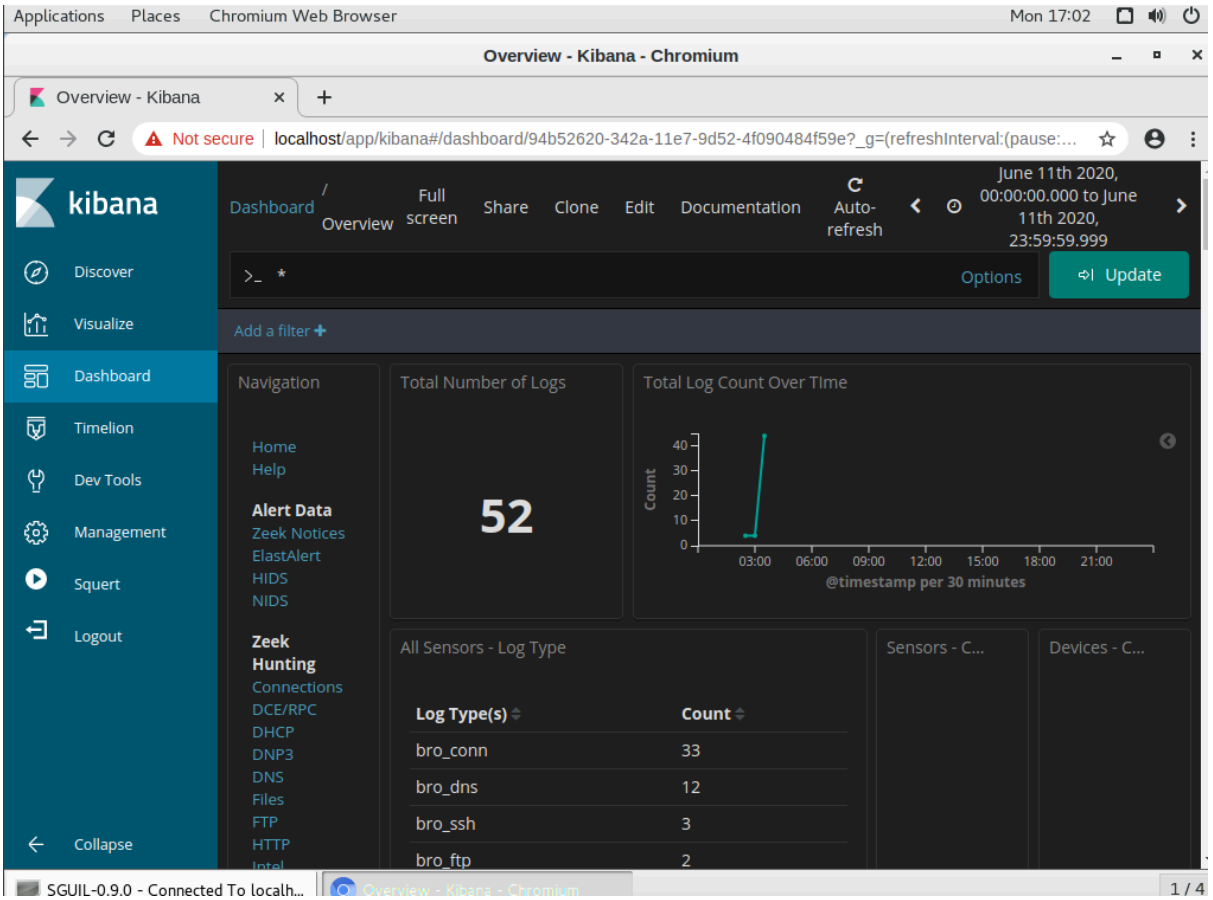
Domanda: <u>Cosa rivela questo sul ruolo dell'attaccante sul computer bersaglio?</u>

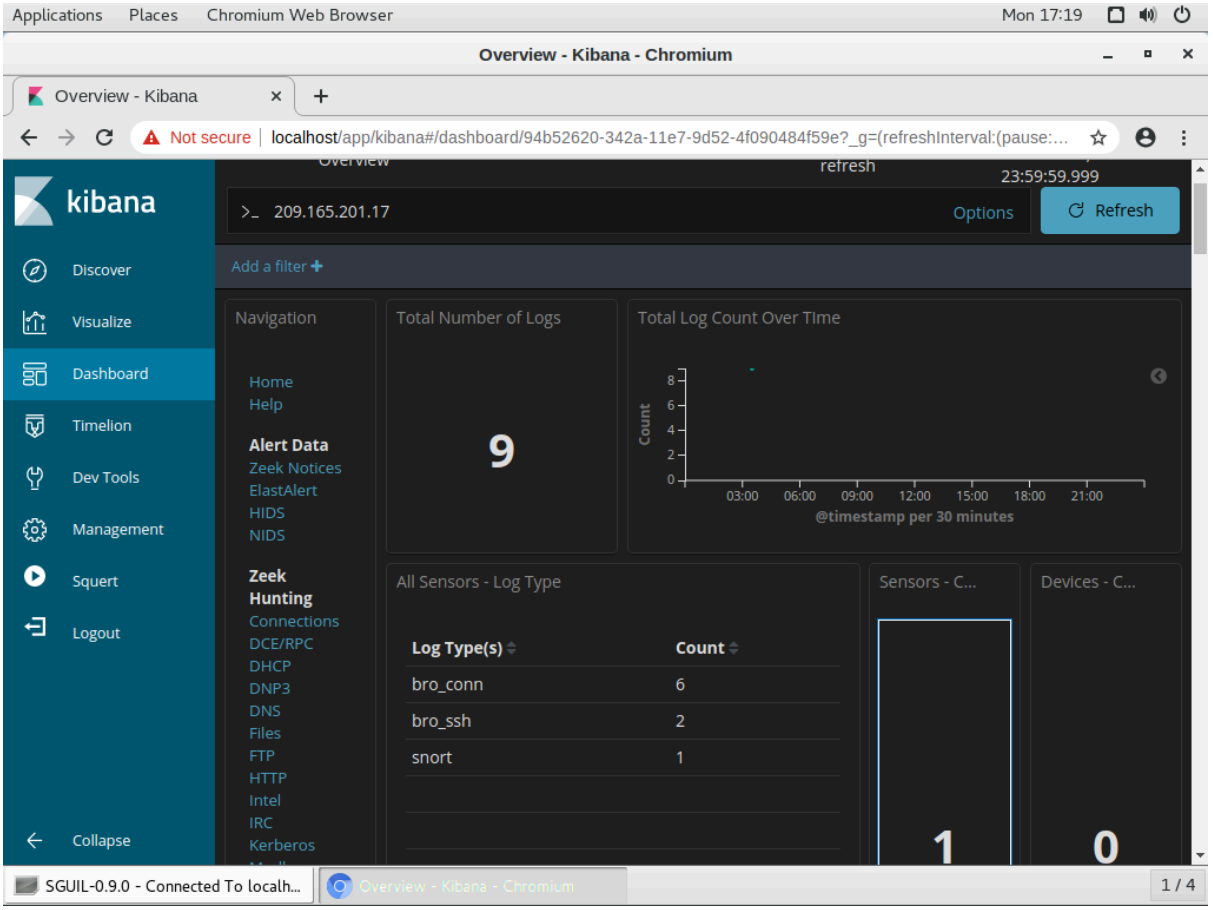
R: Ottenere i privilegi di root.

Domanda: **Scorri il flusso TCP. Che tipo di dati ha letto l'attore della minaccia?**
R: Il contenuto del file “passwd” focalizzandosi sull’utente root.

Kibana

Premendo col destro su l'IP della macchina target, andiamo a selezionare “Kibana IP Lookup” ed effettuiamo l’accesso. Impostiamo la data al 11 giugno 2020.





Il tool ci dice che sono stati effettuati 9 logs con quell'ip e, sapendo dalla task che il file confidential.txt non è più accessibile andiamo quindi a filtrare il log "bro_ftp" per vedere il traffico FTP.

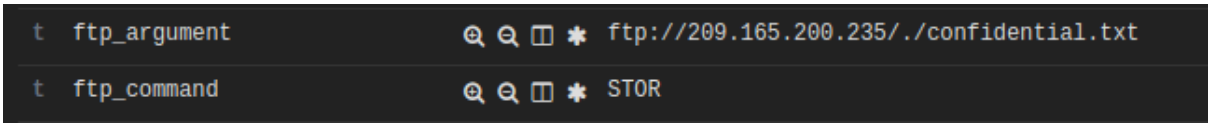
Log Type(s)	Count
bro_conn	6
bro_ssh	2
snort	1

Scorrendo in basso vedremo 2 log

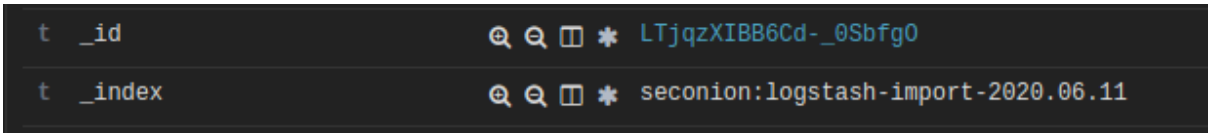
Time	source_ip	source_port	destination_ip	destination_port	_id
June 11th 2020, 03:54:54.173	209.165.201.17	46450	209.165.200.235	22	KzjqzXIBB6Cd-_0SZvhc
June 11th 2020, 03:47:30.968	209.165.201.17	46448	209.165.200.235	22	KTjqzXIBB6Cd-_0SZvhc

Domanda: **Quali sono gli indirizzi IP e i numeri di porta di origine e destinazione per il traffico FTP?**

R: Gli indirizzi IP di origine e destinazione sono rispettivamente 209.165.201.17 e 209.165.200.235, le porte invece sono la 46450 per quella d'origine e la 22 per la destinazione.
Aprendo il secondo vedremo il campo "ftp_arguments" è citato il file mancante.



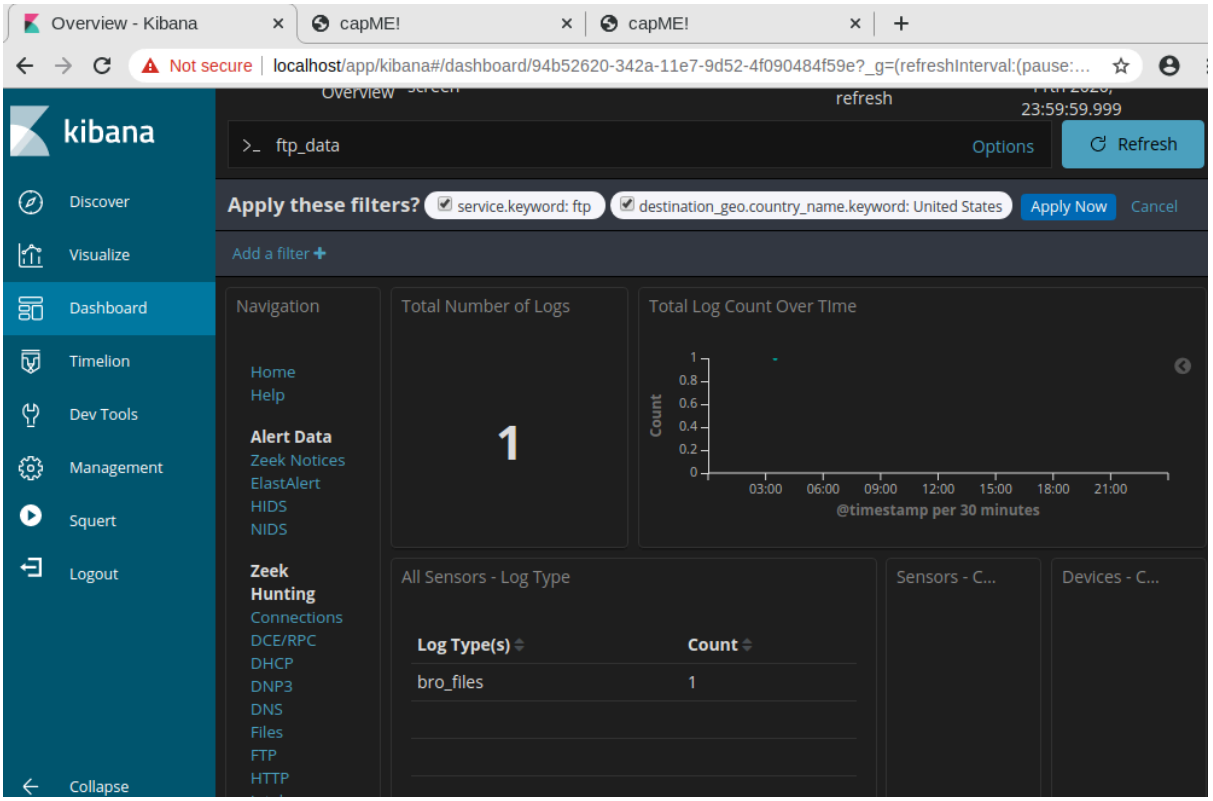
Tornando più su apriamo l'id di questo log



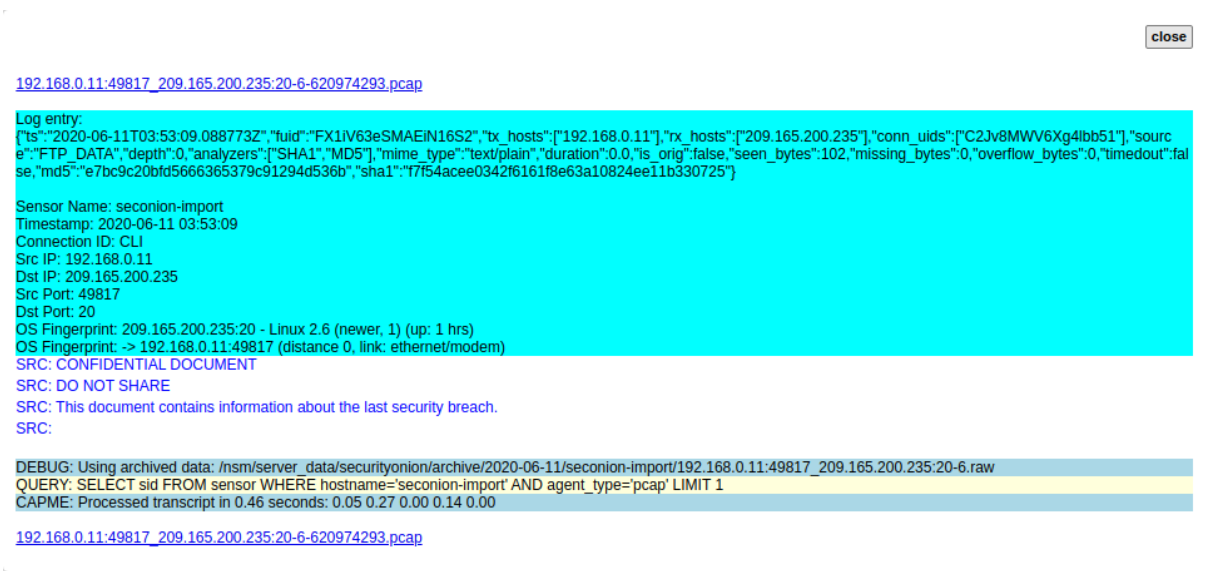
DST: 220 (vsFTPd 2.3.4)
DST:
SRC: USER analyst
SRC:
DST: 331 Please specify the password.
DST:
SRC: PASS cyberops
SRC:
DST: 230 Login successful.

Domanda: **<u>Quali sono le credenziali utente per accedere al sito FTP?</u>**
R: User "analyst", password "cyberops"

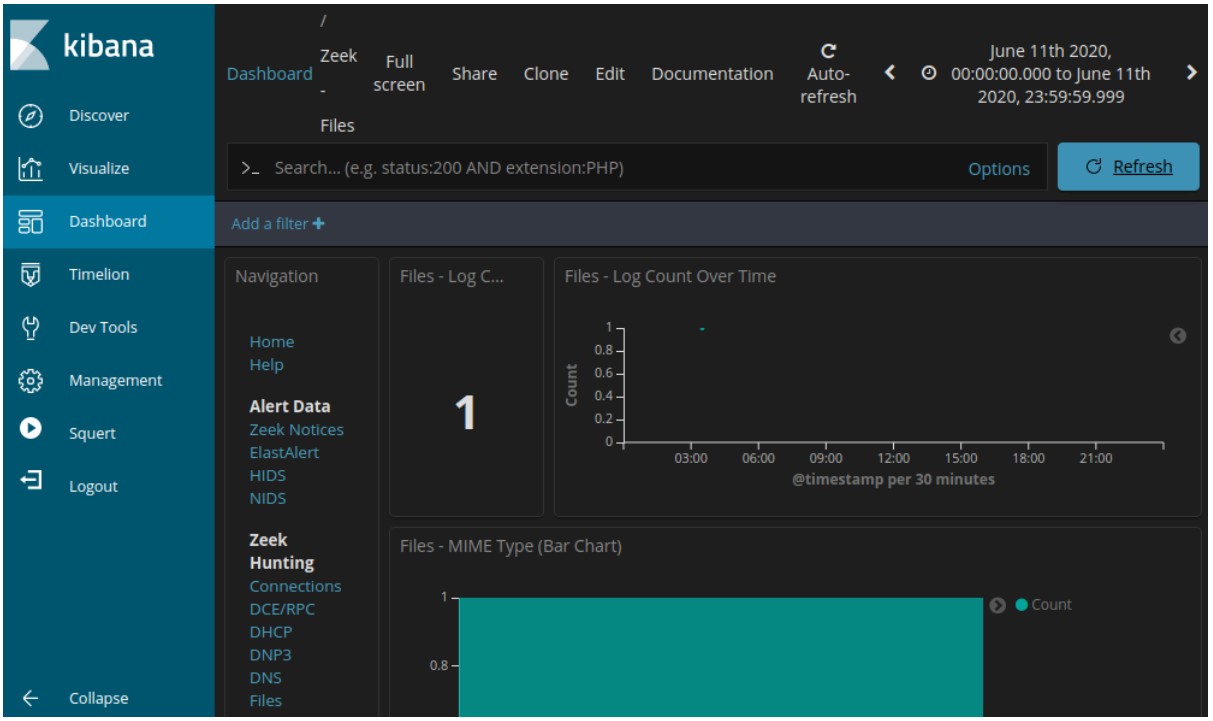
Tornando nella barra di ricerca filtriamo i risultati con "ftp_data", ci mostrerà un solo risultato



Scorriamo in basso e analizziamo quest'unico log, abbiamo trovato il contenuto del file confidential.txt

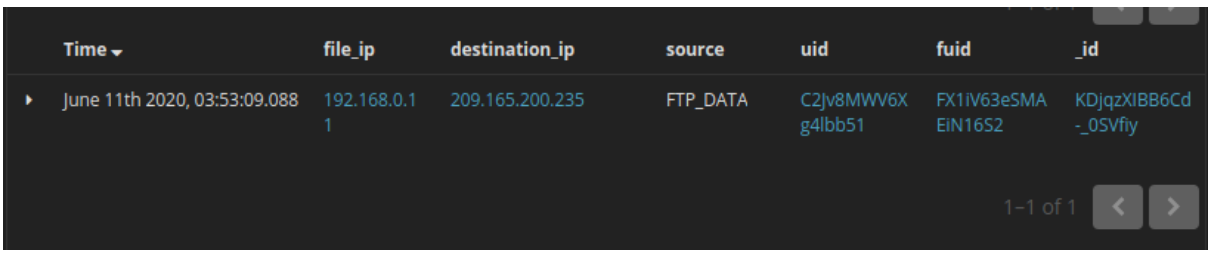


Torniamo nella dashboard d Kibana e clicchiamo su "Files" nell'elenco, la pagina si aggiornerà e ci mostrerà un unico file chiamato "ftp_data" di 102B



Domanda: **Quali sono i diversi tipi di file?**
R: Il file visualizzato sarà di tipo “text/plain”
Domanda: **Quali sono le sorgenti dei file elencate?**
R: FTP_DATA

Scorriamo in basso e torniamo sul file di log, apriamolo e vediamo i dettagli.



Domanda: **Qual è il tipo MIME, l'indirizzo IP di origine e di destinazione associato al trasferimento dei dati FTP? Quando si è verificato questo trasferimento?**
R: MIME Type: text/plain
IP origine: 192.168.0.11
IP dest: 208.165.200.235
Timestamp: 11 giugno 2020, ore 18:49:46

Premendo su “_id” visualizziamo il contenuto del file:

SRC: CONFIDENTIAL DOCUMENT
SRC: DO NOT SHARE
SRC: This document contains information about the last security breach.
SRC:

Domanda: Con tutte le informazioni raccolte finora, qual è la tua raccomandazione per fermare ulteriori accessi non autorizzati?

R: Isolare il sistema 192.168.0.11 per analisi forensi, Rivedere le policy di accesso FTP e limitare i trasferimenti esterni, Investigare se ci sono stati altri trasferimenti simili, Bloccare immediatamente l'IP 209.165.200.235 nel firewall,

---

Conclusione

L'analisi condotta ha evidenziato che un attaccante ha ottenuto l'accesso root a una macchina vulnerabile e ha sottratto il file *confidential.txt* tramite FTP.

Grazie all'uso combinato di Sguil, Wireshark e Kibana, è stato possibile ricostruire l'attacco e identificare sia l'origine che le modalità del compromesso.

Per prevenire ulteriori accessi non autorizzati, è essenziale isolare l'host compromesso, rafforzare i controlli sugli accessi e monitorare costantemente il traffico FTP e gli eventi di rete sospetti.