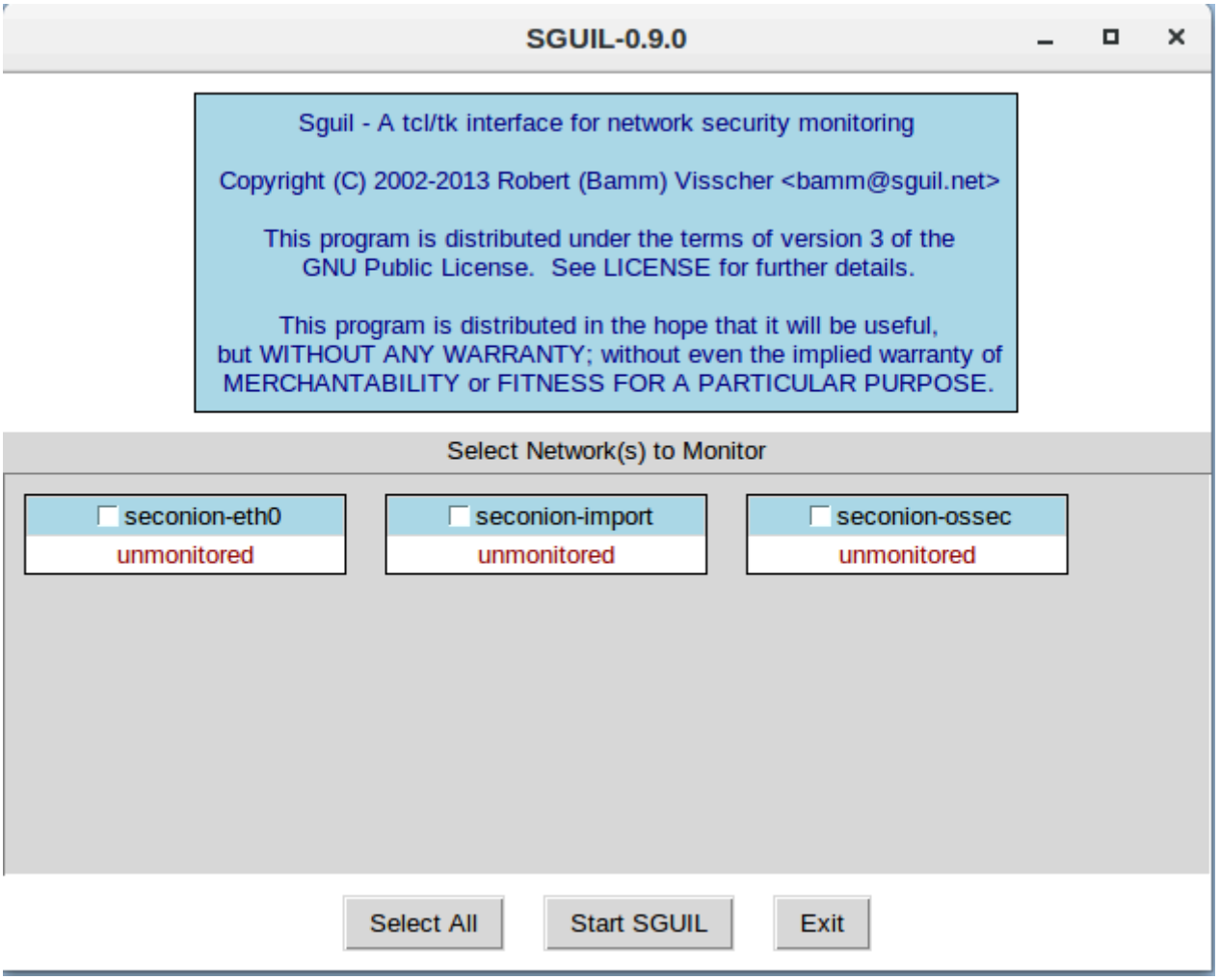
Isolamento di un Host Compromesso tramite 5-Tuple

Isolamento di un Host Compromesso tramite 5-Tuple

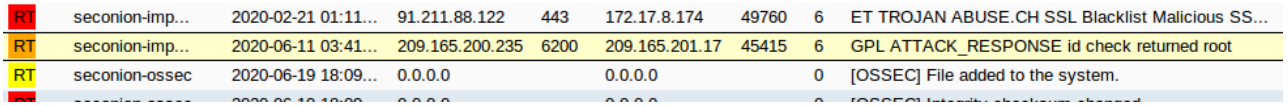
Parte 1: Revisione degli Avvisi in Sguil

1. **Avvio della VM Security Onion**
   - Ho avviato la macchina virtuale Security Onion.
   - Ho effettuato l'accesso con l'utente `analyst` e la password `cyberops`.
2. **Apertura di Sguil**
   - Ho aperto Sguil e ho effettuato il login.
   - Ho selezionato `Select All` per selezionare tutte le interfacce e ho avviato Sguil cliccando su `Start SGUIL`.



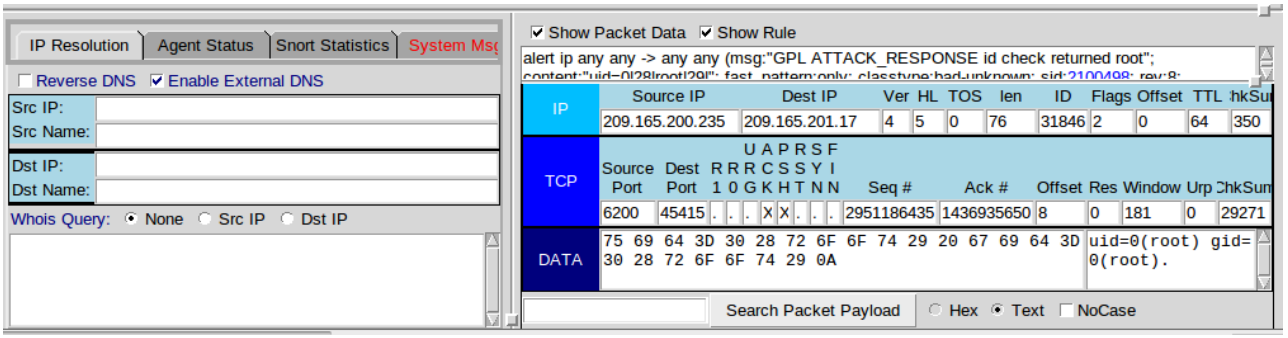
> Username: analyst
> Password: cyberops

3. **Revisione degli eventi in Sguil**
   - Ho esaminato gli eventi nella colonna `Event Message`.
   - Ho individuato l'evento `GPL ATTACK_RESPONSE id check returned root`, che indica che un attacco ha ottenuto accesso root.
   - L'host `209.165.200.235` ha restituito accesso root all'host `209.165.201.17`.

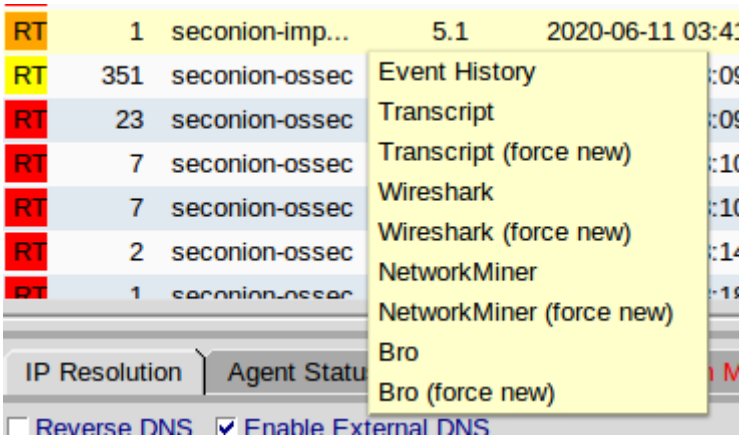


RT	seconion-imp...	2020-02-21 01:11...	91.211.88.122	443	172.17.8.174	49760	6	ET TROJAN ABUSE.CH SSL Blacklist Malicious SS...
RT	seconion-imp...	2020-06-11 03:41...	209.165.200.235	6200	209.165.201.17	45415	6	GPL ATTACK_RESPONSE id check returned root
RT	seconion-ossec	2020-06-19 18:09...	0.0.0.0		0.0.0.0		0	[OSSEC] File added to the system.

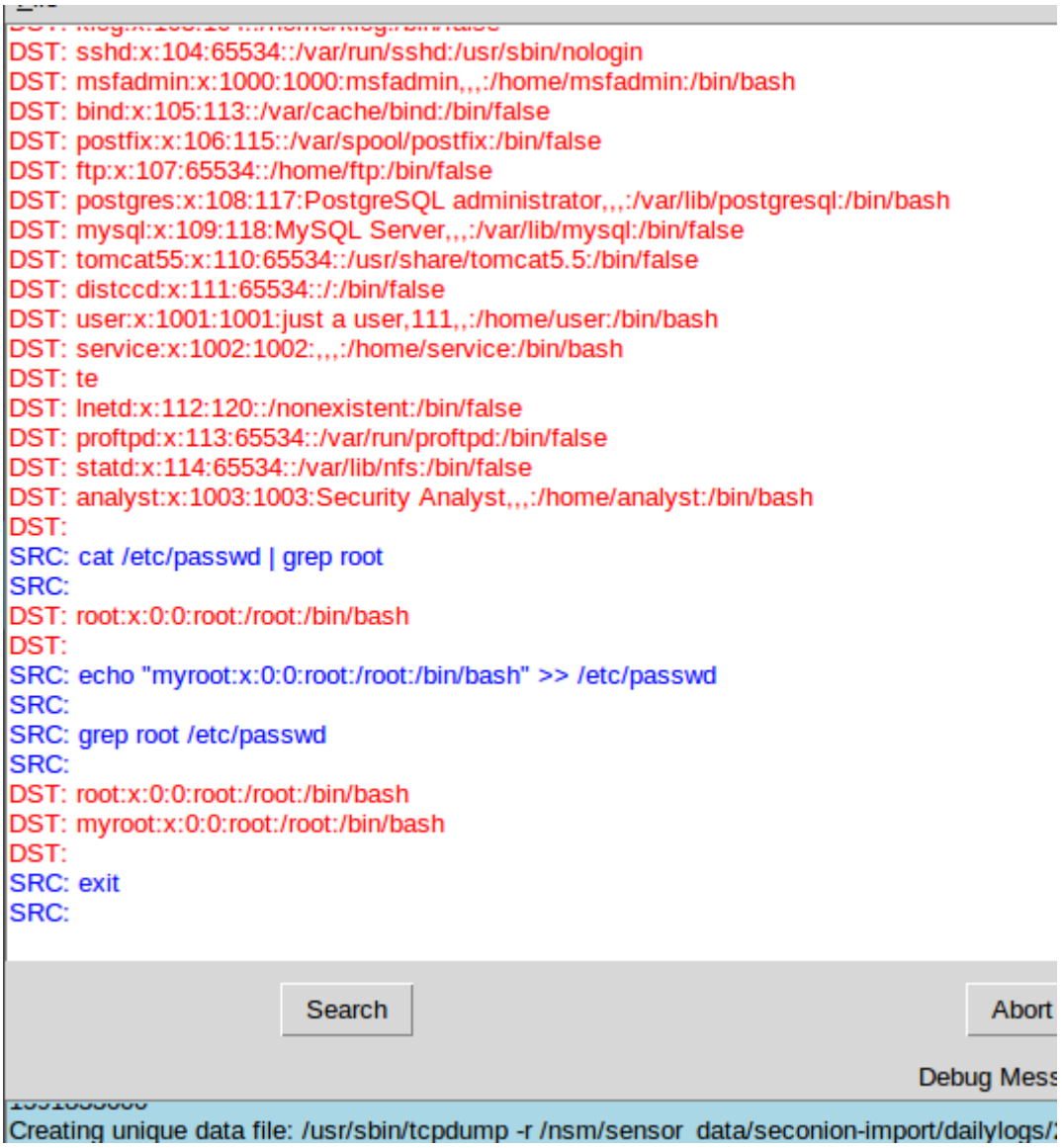
4. **Esame dettagliato degli avvisi**
   - Ho selezionato le opzioni `Show Packet Data` e `Show Rule` per visualizzare i dettagli dell'avviso.



   - Ho cliccato con il tasto destro sull'`alert ID 5.1` e selezionato `Transcript`.

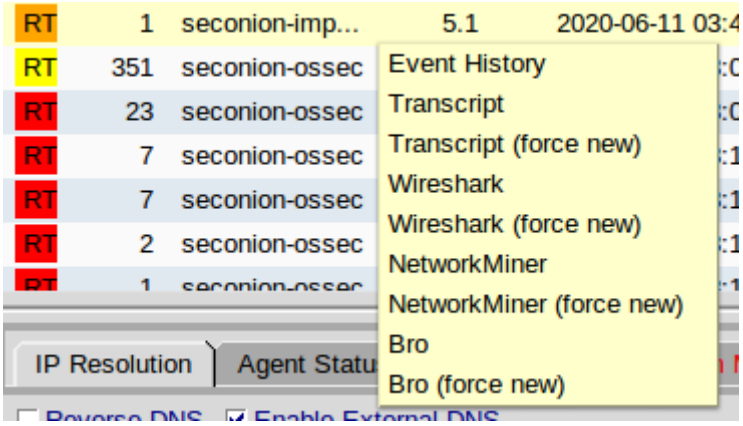


5. **Analisi dei transcript**
   - Ho analizzato i dati dei transcript per comprendere le interazioni tra il client (attaccante) e il server (target).
   - L'attaccante con IP `209.165.201.17` ha ottenuto accesso root al sistema con IP `209.165.200.235`.
   - L'attaccante ha esplorato il file system, copiato il file `shadow` e modificato i file `/etc/shadow` e `/etc/passwd`.

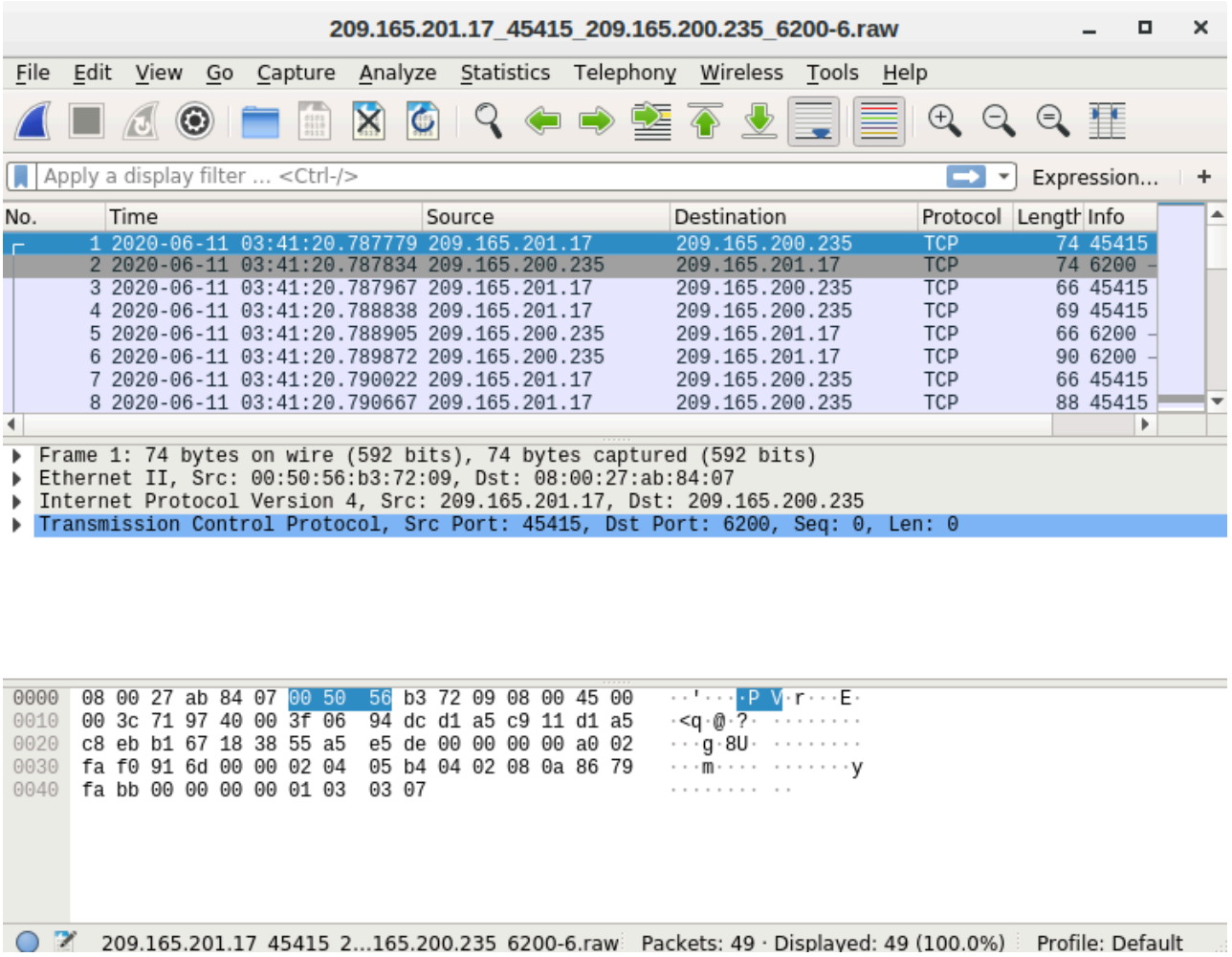


Parte 2: Pivot su Wireshark

1. **Apertura di Wireshark**
   - Ho cliccato con il tasto destro sull'`alert ID 5.1` e selezionato `Wireshark`.

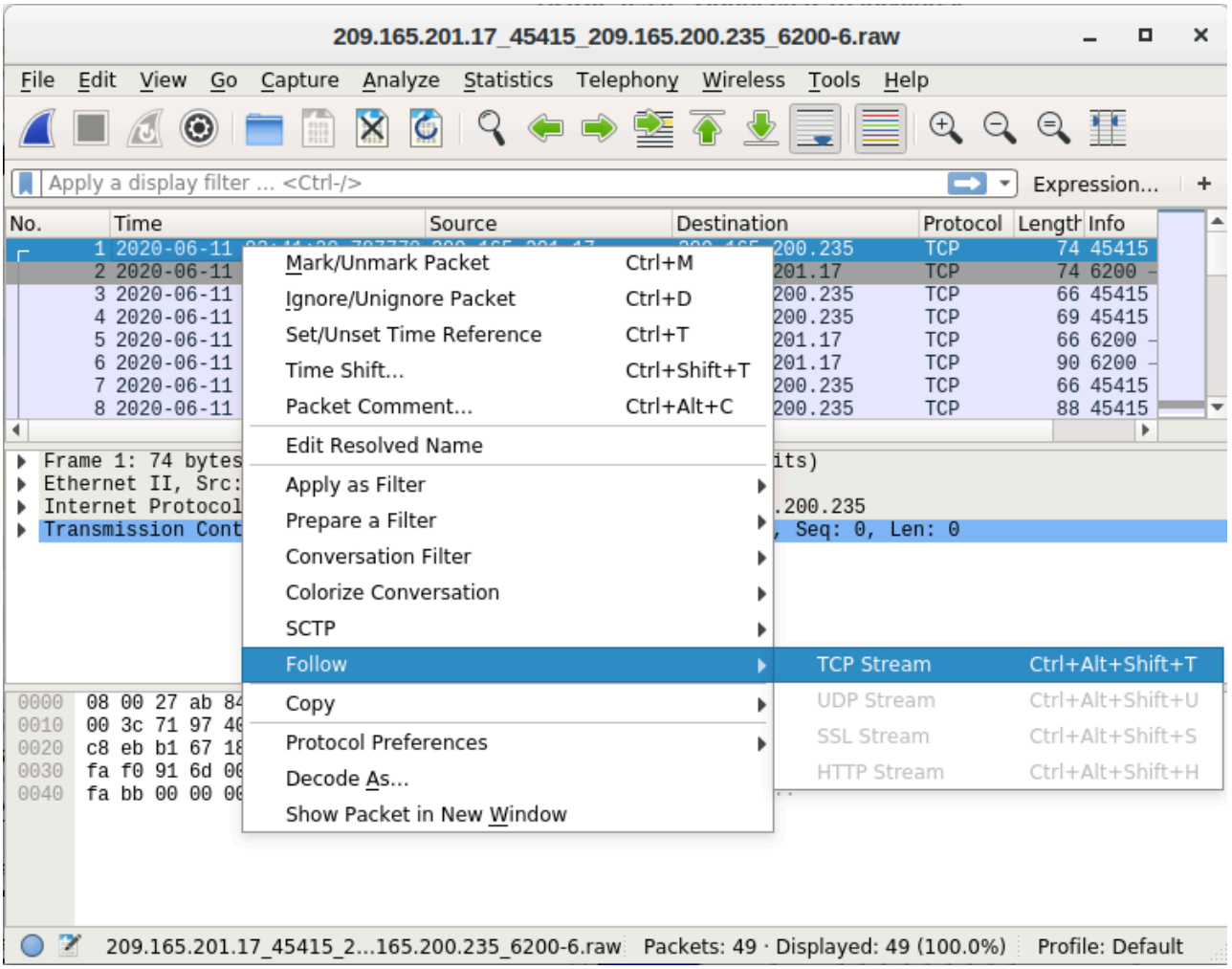


- Ho esaminato la visualizzazione principale di Wireshark.



2. **Analisi del flusso TCP**

- Ho cliccato con il tasto destro su un pacchetto e selezionato `Follow > TCP Stream`.

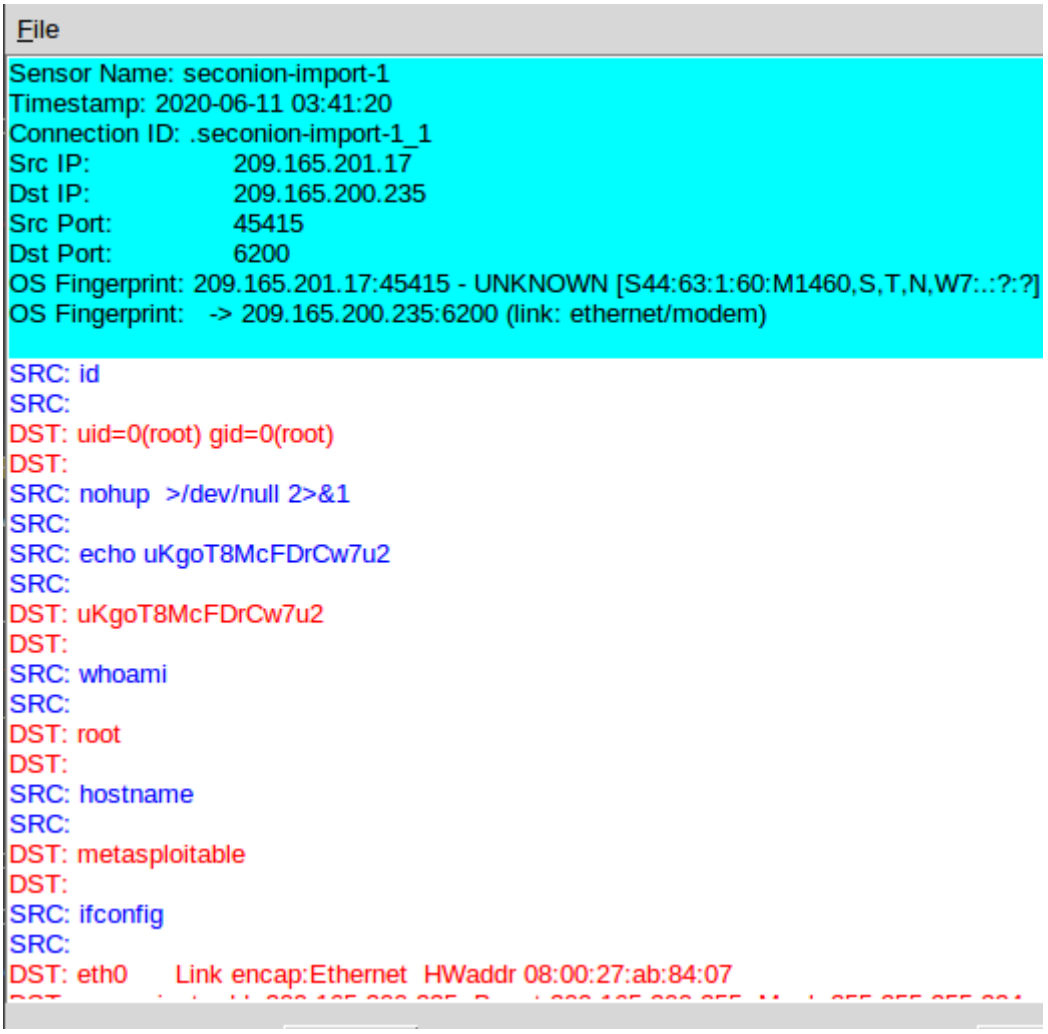


- Il flusso TCP ha mostrato la transazione tra l'attaccante (testo rosso) e il target (testo blu).
- L'hostname del target è `metasploitable`, con IP `209.165.200.235`.

```
id
uid=0(root) gid=0(root)
nohup  >/dev/null 2>&1
echo uKgoT8McFDrCw7u2
uKgoT8McFDrCw7u2
whoami
root
hostname
metasploitable
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:ab:84:07
          inet addr:209.165.200.235  Bcast:209.165.200.255  Mask:
255.255.255.224
          inet6 addr: fe80::a00:27ff:feab:8407/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:117 errors:0 dropped:0 overruns:0 frame:0
          TX packets:167 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:10294 (10.0 KB)  TX bytes:20187 (19.7 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:512 errors:0 dropped:0 overruns:0 frame:0
          TX packets:512 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:225633 (220.3 KB)  TX bytes:225633 (220.3 KB)
```

3. Comando whoami dell'attaccante
    - L'attaccante ha eseguito `whoami`, ottenendo la risposta root, confermando il controllo del sistema.



4. **Dati analizzati nel flusso TCP**
    - Ho scansionato il flusso TCP alla ricerca dei dati letti dall'attaccante.

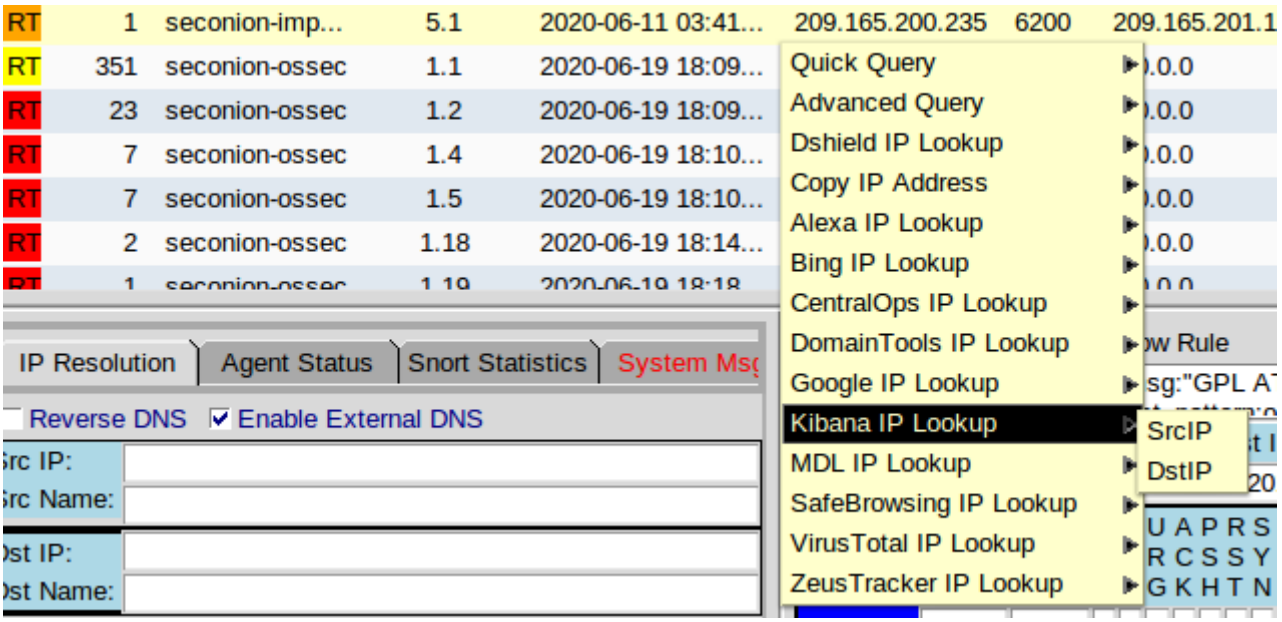
- L'attaccante ha consultato informazioni sugli account utente.

```
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002:,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
```

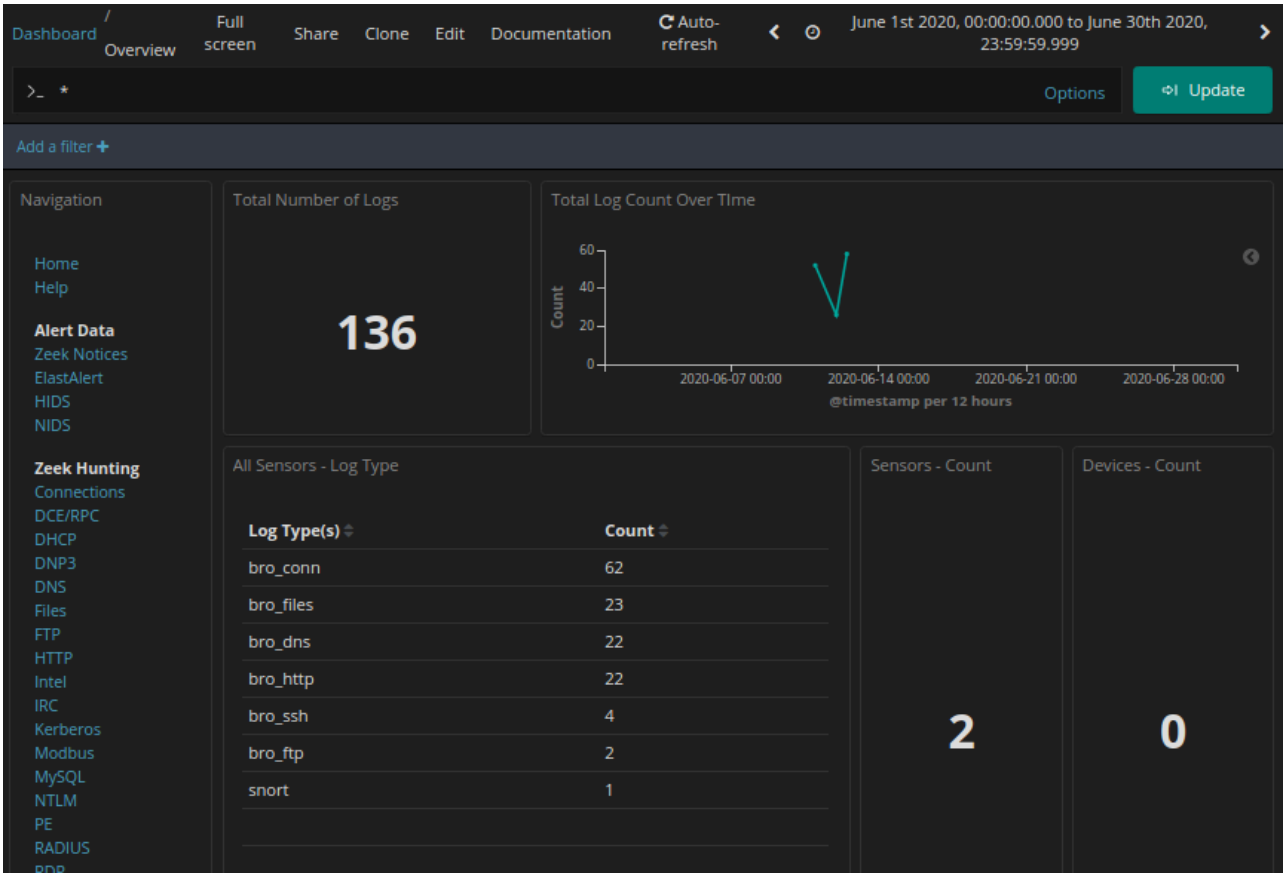
5. **Chiusura di Wireshark**
   - Ho chiuso la finestra del flusso TCP e poi Wireshark.

Parte 3: Pivot su Kibana

1. **Accesso a Kibana**
   - Sono tornata su Sguil, ho cliccato con il tasto destro sull'IP `209.165.200.235` e selezionato `Kibana IP Lookup > SrcIP`.



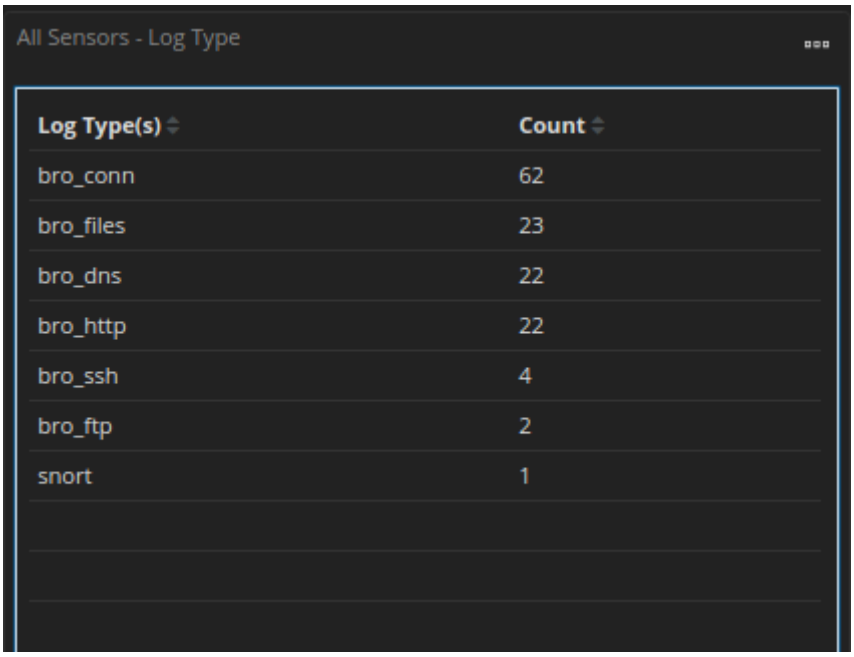
- Ho effettuato il login con l'utente `analyst` e la password `cyberops`.
- Ho cambiato l'intervallo temporale su `Giugno 2020` per includere l'11 giugno.

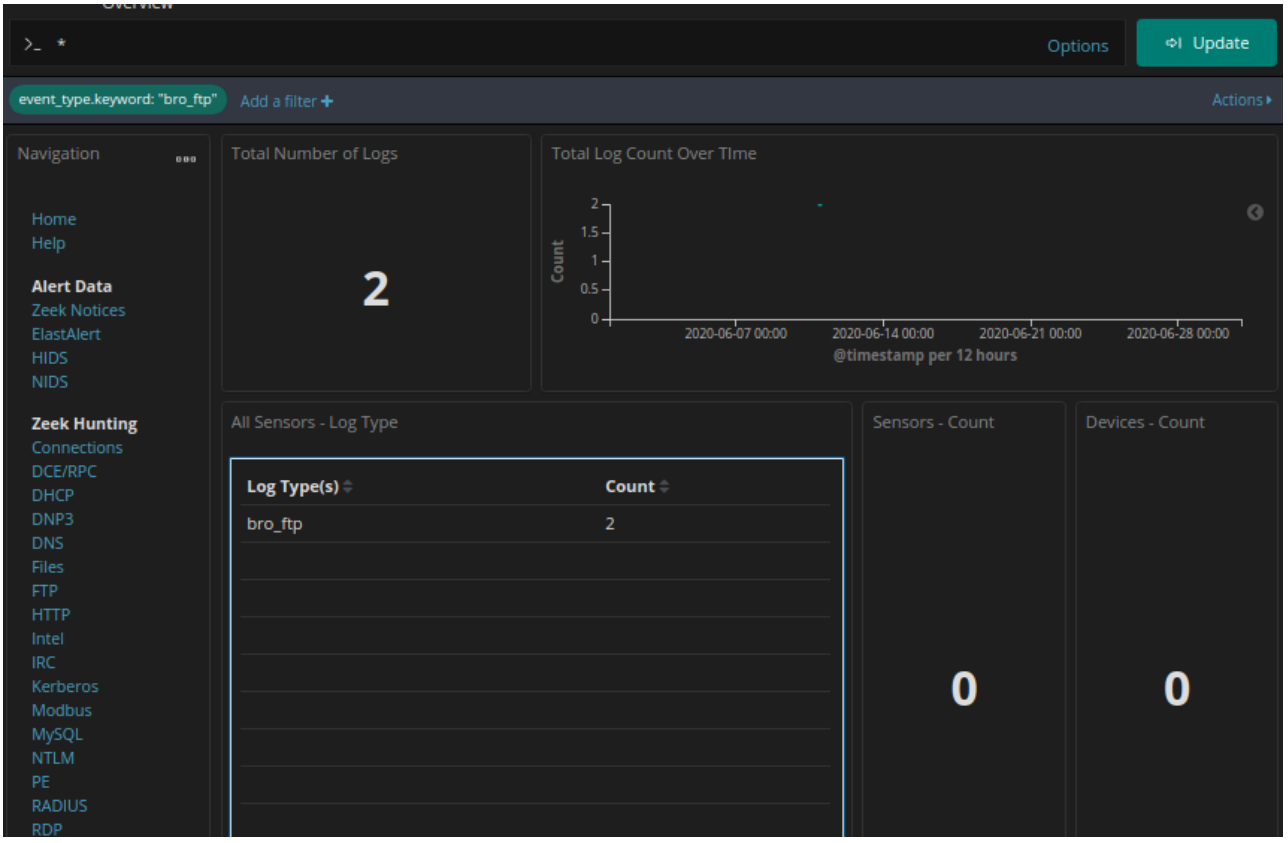


2. **Identificazione del protocollo FTP**

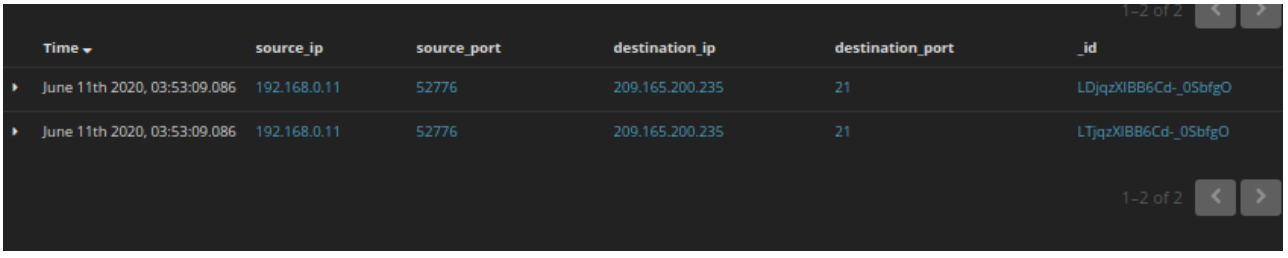
- Nella sezione `Sensors - Sensors and Services (Pie Chart)`, ho notato la presenza di `ftp`.

- Ho filtrato per `bro_ftp` cliccando su `+` accanto al conteggio.



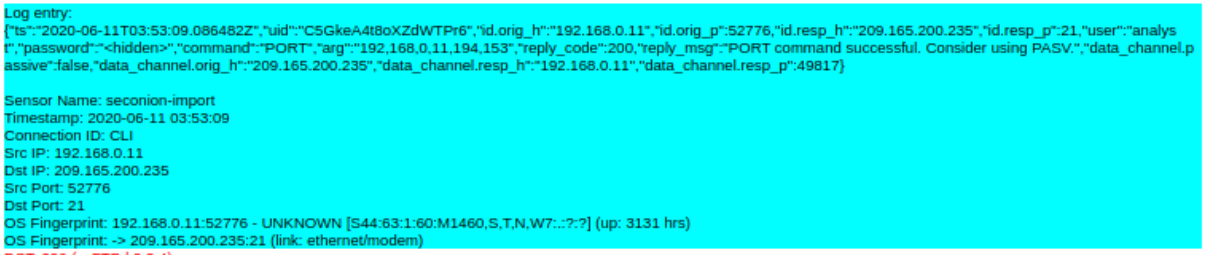


3. **Analisi del traffico FTP**
   - Ho trovato due voci di log relative al traffico FTP.
   - **IP sorgente:** `192.168.0.11:52776`
   - **IP destinazione:** `209.165.200.235:21`



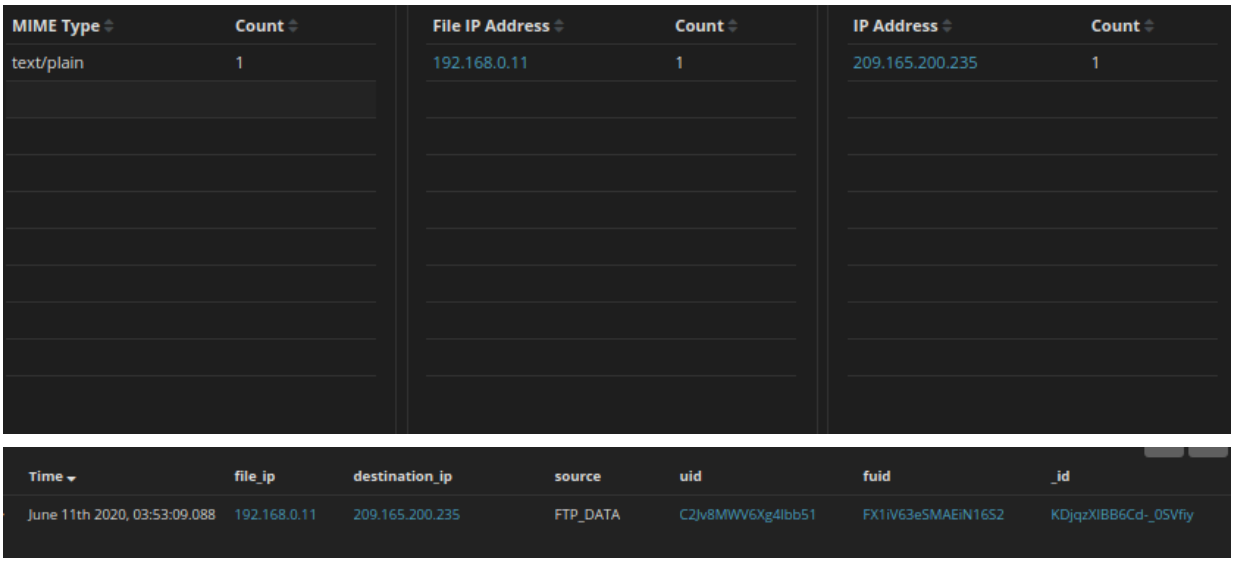
4. **Esame degli argomenti FTP**
   - Tramite capMe! ho trovato il traferimento del file `confidential.txt`.

5. **Credenziali FTP utilizzate**
   - L'attaccante ha usato le credenziali:
     - **Username:** `analyst`
     - **Password:** `cyberops`



6. **Analisi dei dati FTP**
   - Ho filtrato per `FTP_DATA` nella dashboard di Kibana.
   - Ho analizzato il tipo di file e la fonte del trasferimento:
     - **MIME Type:** `text/plain`
     - **IP sorgente:** `192.168.0.11`
     - **IP destinazione:** `209.165.200.235`

- **Data del trasferimento:** `11 giugno 2020, 3:53 AM`



MIME Type	Count
text/plain	1

File IP Address	Count
192.168.0.11	1

IP Address	Count
209.165.200.235	1

Time	file_ip	destination_ip	source	uid	fuid	_id
June 11th 2020, 03:53:09.088	192.168.0.11	209.165.200.235	FTP_DATA	C2Jv8MWV6Xg4lbb51	FX1iV63eSMAEiN16S2	KDjqzXIBB6Cd-_0SVfiy

7. **Contenuto del file** `confidential.txt`
   - Ho espanso i log relativi al trasferimento FTP e aperto l'`alert _id`.
   - Il contenuto del file trasferito era:

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

192.168.0.11:49817_209.165.200.235:20-6-1938136318.pcap

Log entry:
{"ts":"2020-06-11T03:53:09.088773Z","fuid":"FX1iV63eSMAEiN16S2","tx_hosts":["192.168.0.11"],"rx_hosts":["209.165.200.235"],"conn_uids":["C2Jv8MWV6Xg4lbb51"],"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 0.55 seconds: 0.18 0.21 0.00 0.15 0.00

192.168.0.11:49817_209.165.200.235:20-6-1938136318.pcap

Raccomandazioni per la Sicurezza

Con le informazioni raccolte, ho identificato una violazione di sicurezza. Per prevenire ulteriori accessi non autorizzati, consiglio:

1. **Cambio password immediato**
   - La password dell'utente `analyst` deve essere cambiata su tutti i sistemi coinvolti (`209.165.200.235` e `192.168.0.11`).
2. **Restrizioni sull'accesso FTP**

- Limitare l'uso di FTP o implementare SFTP per la protezione dei dati.

3. **Monitoraggio dei log di sistema**
   - Attivare un sistema di monitoraggio attivo per rilevare accessi sospetti.
4. **Implementazione di autenticazione a più fattori (MFA)**
   - Proteggere gli account critici con autenticazione a più fattori.
5. **Verifica dell'integrità dei file di sistema**
   - Controllare `/etc/shadow` e `/etc/passwd` per modifiche non autorizzate.

Conclusione

L'analisi ha rivelato che l'attaccante ha ottenuto accesso root a un sistema compromesso e ha trasferito dati sensibili tramite FTP. Le contromisure suggerite aiuteranno a mitigare il rischio di futuri attacchi simili.