

# Report Bonus 2: Isolare un Host Compromesso Usando la 5-Tupla

A cura di Iris Canole, Federico Giannini, Daniele Castello, Luca Pani, Rosario Papa, Yari Olmi, Alessandro Salerno

## Obiettivi

In questo laboratorio, esaminerai i log raccolti durante lo sfruttamento di una vulnerabilità documentata per determinare gli host e il file compromessi.

- PARTE 1: Esaminare gli Alert in Sguil.
- PARTE 2: Passare a Wireshark (Pivoting).
- PARTE 3: Passare a Kibana (Pivoting).

Dopo l'attacco, gli utenti non hanno più accesso al file chiamato `confidential.txt`.

Ora esamineremo i log per determinare come il file è stato compromesso.

## Parte 1: Esaminare gli Alert in Sguil

1. Abbiamo avviato la VM Security Onion ed effettuato il login.

Credenziali:

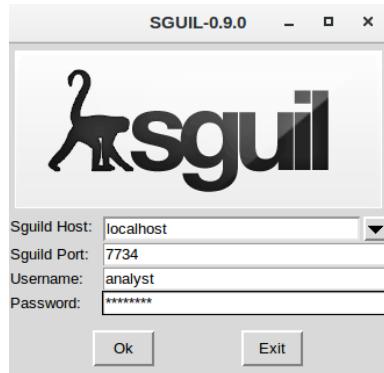
- UTENTE: `analyst`
- PASSWORD: `cyberops`



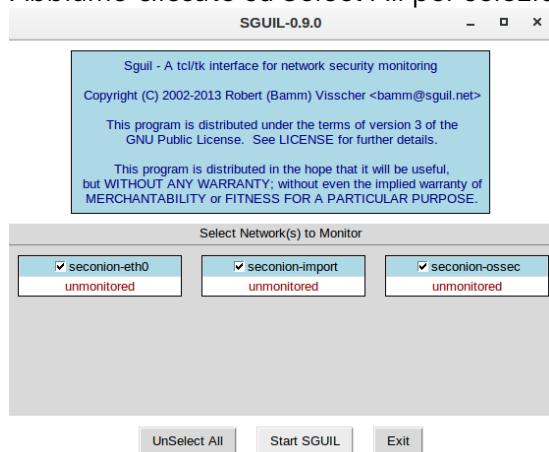
2. Abbiamo aperto Sguil e poi effettuato il login.

Credenziali:

- USERNAME: analyst
- PASSWORD: cyberops



Abbiamo cliccato su Select All per selezionare le interfacce e poi su Start SGUIL.



3. Abbiamo esaminato gli eventi elencati nella colonna Event Message.

Uno di questi messaggi è `GPL ATTACK_RESPONSE id check returned root`, ed indica che potrebbe essere stato ottenuto l'accesso root durante un attacco.

L'host 209.165.200.235 ha restituito l'accesso root a 209.165.201.17 .

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
ER	17	seconion...	5.234	2019-07-19 18:53:12	172.16.4.205	49249	188.243.115.84	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 ...
ER	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...
ER	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...
ER	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...
ER	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 ...
ER	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!...

4. Abbiamo selezionato le caselle di controllo Show Packet Data e Show Rule per visualizzare ogni alert più in dettaglio.

Show Packet Data	Show Rule
alert ip any any -> any any (msg:"GPL ATTACK_RESPONSE id check returned root"; content:"uid=0[28]root[29]"; fast_pattern:only; classtype:bad-unknown; sid:2100498; rev:8;	

5. Abbiamo cliccato con il pulsante destro sull'ID dell'alert 5.1 e selezionato Transcript.

RT	1	seconion...	5.1	2020-06-11 03:41:20
RT	351	seconion...	Event History	8:09:28
RT	23	seconion...	Transcript	8:09:29
RT	7	seconion...	Transcript (force new)	8:10:04
RT	7	seconion...	Wireshark	8:10:04
RT	2	seconion...	Wireshark (force new)	8:14:41
RT	1	seconion...	NetworkMiner	8:18:41
			Bro	
			Bro (force new)	
			IP Resolution	
			Agent Status	
			Log	
			Debug Messages	

## 6. Abbiamo esaminato le trascrizioni per l'alert.

Mostrano le transazioni tra l'attore della minaccia (SRC) e il bersaglio (DST) durante l'attacco.

L'attore della minaccia sta eseguendo comandi Linux sul bersaglio.

```

seconion-import-1_1 -> seconion-import-1_1
File
Sensor Name: seconion-import-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: 22
OS Fingerprint: 209.165.201.17:45415 - UNKNOWN [S44:63:1:60:M1460,S,T,N,W??:?]
OS Fingerprint: -> 209.165.200.235:6200 (link: ethernet/modem)

SRC: id
SRC: uid=0(root) gid=0(root)
DST: 
SRC: nohup >/dev/null 2>&1
SRC: 
SRC: echo uKgoT8McFDcWv7u2
SRC: 
DST: uKgoT8McFDcWv7u2
DST: 
SRC: whoami
SRC: 
DST: root
SRC: hostname
SRC: 
DST: metasploitable
DST: 
SRC: ifconfig

```

Debug Messages

Your request has been sent to the server.  
Please be patient as this can take some time.  
Using archived data: /nsm/server\_data/securityunion/archive/2020-06-11/seconion-import-1/209.165.201.17:45415\_209.165.200.235:6200-6.raw  
Finished.

**DOMANDA: Che tipo di transazioni si sono verificate tra il client e il server in questo attacco?**

In questo attacco, l'attaccante ha compromesso il server, ha confermato di essere root, ha rubato gli hash delle password e ha creato un account amministratore nascosto `myroot` per garantirsi l'accesso futuro.

## Cronologia delle transazioni

### Reconnaissance

- **Comando:** `id`  
**Risposta:** `uid=0(root) gid=0(root)`
- **Comando:** `whoami`  
**Risposta:** `root`

L'attaccante verifica i suoi privilegi.

La risposta conferma che ha accesso root sulla macchina.

- **Comando:** `hostname`

**Risposta:** metasploitable

L'attaccante identifica il nome della macchina.

- **Comando:** ifconfig

L'attaccante controlla la configurazione di rete.

## Information Gathering

- **Comando:** cat /etc/passwd

L'attaccante legge il file che contiene la lista degli utenti del sistema

- **Comando:** cat /etc/shadow

L'attaccante legge il file che contiene gli hash delle password degli utenti.

Con questi hash, l'attaccante può tentare di decifrare le password offline.

## Creating a Backdoor User

- **Comando:** echo "myroot:x:0:0:root:/root:/bin/bash" >> /etc/passwd
- **Comando:** echo "myroot::14747:0:99999:7:::" >> /etc/shadow

L'attaccante ha modificato il sistema per assicurarsi di poter rientrare anche se la vulnerabilità originale venisse corretta.

## Verifica della persistenza

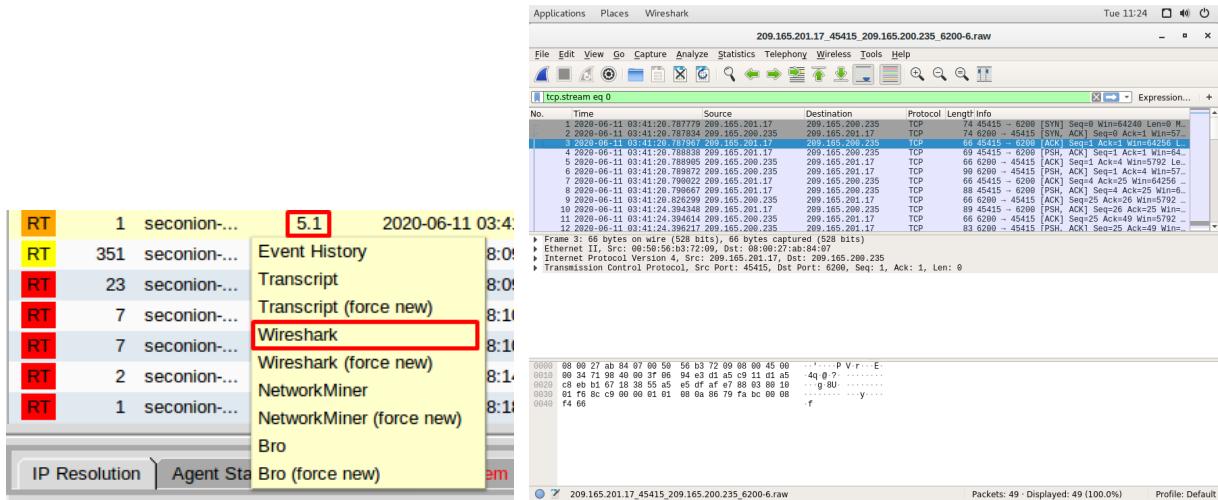
- **Comando:** grep root /etc/passwd
- **Risposta:** gli ha mostrato sia l'utente `root` originale sia il nuovo utente `myroot`.

L'attaccante ha confermato che la modifica al file è andata a buon fine.

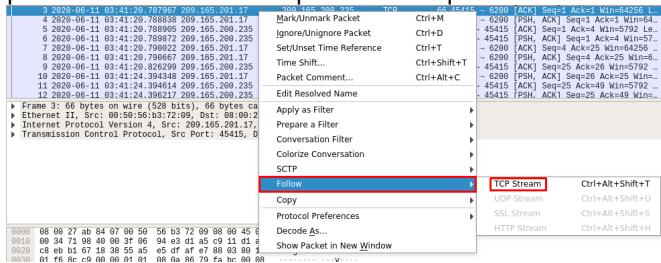
---

## Parte 2: Passare a Wireshark

1. Abbiamo selezionato l'alert che ci ha fornito la trascrizione nel passo precedente. Abbiamo cliccato con il pulsante destro sull'ID dell'alert 5.1 e selezionato **Wireshark**.



2. Per visualizzare tutti i pacchetti assemblati in una conversazione TCP, Abbiamo cliccato con il pulsante destro su un pacchetto qualsiasi e abbiamo selezionato Follow > TCP Stream.



```
id
uid=0(root) gid=0(root)
nohup ./dev/null 2>&1
echo ukgoT8McFDrcw7u2
ukgoT8McFDrcw7u2
whoami
root
host.name
metasploitable
ifconfig
eth0    Link encap:Ethernet HWaddr 00:00:27:ab:84:07
        inet addr:209.165.200.235 Bcast:209.165.200.255 Mask:255.255.255.224
        inet6 addr: fe80::a00:27ff:fe84:07%eth0 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:10294 (10.9 KB) TX bytes:20187 (19.7 KB)
          Interrupt:17 Base address:0x2090

lo      Link encap:Local Loopback
        inet addr:127.0.0.1 Bcast:127.255.255.255 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)

cat /etc/shadow
root:$1$uKg0T8McFDrcw7u2$DR9E9L1d.:14747:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:**:14684:0:99999:7:::
sys:**:14684:0:99999:7:::
sync:**:14684:0:99999:7:::
games:**:14684:0:99999:7:::
man:**:14684:0:99999:7:::
lp:**:14684:0:99999:7:::
mail:**:14684:0:99999:7:::
```

**DOMANDA:** Cosa hai osservato? Cosa indicano i colori del testo rosso e blu?

**RISPOSTA:** Si è aperta una finestra che mostra l'interazione tra l'attaccante e il server Target. In **rosso** vediamo ciò che scrive l'attaccante, quindi i comandi, mentre in **blu** è ciò che il server nella console risponde.

**DOMANDA:** L'attaccante esegue il comando whoami sul bersaglio. Cosa rivela questo sul ruolo dell'attaccante sul computer bersaglio?

**RISPOSTA:** Questo comando rivela all'attaccante che ha accesso root sul Target.

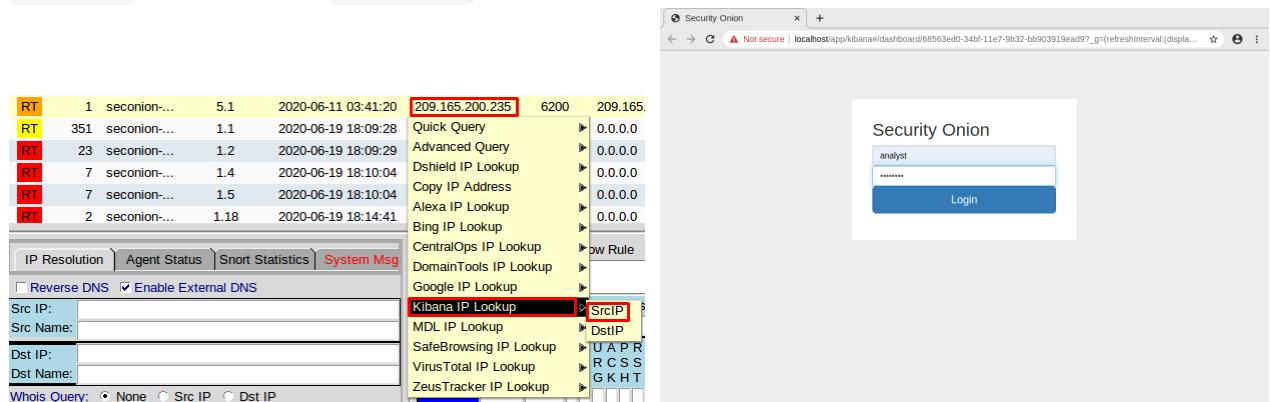
**DOMANDA:** Scorri il flusso TCP. Che tipo di dati ha letto l'attore della minaccia?

**RISPOSTA:** L'attaccante ha letto dati come, la configurazione di rete, la lista degli utenti del sistema e il file che contiene gli hash delle password degli utenti

3. Siamo usciti dalla finestra del flusso TCP. E infine abbiamo chiuso Wireshark quando abbiamo finito di esaminare le informazioni fornite.

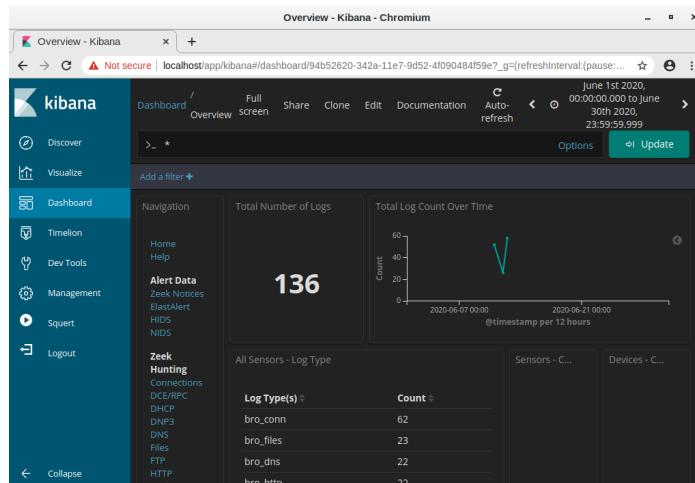
## Parte 3: Passare a Kibana

1. Su Sguil abbiamo fatto click con il pulsante destro sull'indirizzo IP di origine per l'ID dell'alert 5.1 e abbiamo selezionato Kibana IP Lookup > SrcIP. Abbiamo poi inserito il nome utente analyst e la password cyberops in quanto richiesto da Kibana.



The screenshot shows the Security Onion interface. A context menu is open over a table row containing an RT entry. The 'Kibana IP Lookup' option is highlighted with a red box. A submenu for 'SrcIP' is also highlighted with a red box. The 'Security Onion' dashboard is visible in the background.

2. Ci siamo ritrovati nella Dashboard di Kibana.



The screenshot shows the Kibana Overview dashboard. It displays a total of 136 logs. A chart titled "Total Log Count Over Time" shows the count of logs over time from June 1st to June 30th, 2020. Below the chart is a table showing the distribution of log types and their counts.

Log Type(s)	Count
bro_conn	62
bro_files	23
bro_dns	22
bro_http	22

E abbiamo cambiato l'intervallo di tempo in modo tale che l'11 giugno fosse incluso nell'intervallo.

June 1st 2020,  
00:00:00.000 to June  
30th 2020,  
23:59:59.999

3. Nella schermata è presente un elenco di diverso tipo di dati.

All Sensors - Log Type	
Log Type(s) ▾	Count ▾
bro_conn	62
bro_files	23
bro_dns	22
bro_http	22
bro_ssh	4
bro_ftp	2
snort	1

4. Abbiamo filtrato per bro\_ftp selezionando il + nel Filter for value.



5. Siamo andati fino in fondo alla Dashboard e abbiamo trovato All Logs, le voci elencate erano quelle nello Screenshot sotto:

All Logs					
Time ▾	source_ip	source_port	destination_ip	destination_port	_id
June 11th 2020, 03:53:09.086	192.168.0.11	52776	209.165.200.235	21	LDJqzXIB B6Cd_0 SbfqO
June 11th 2020, 03:53:09.086	192.168.0.11	52776	209.165.200.235	21	LTJqzXIB B6Cd_0 SbfqO

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

**RISPOSTA:** L'indirizzo IP e la porta di origine è 192.168.0.11 e 52776, mentre quello di destinazione è 209.165.200.235 e 21.

6. Espandendo la seconda voce di Log, nel campo ftp\_argument abbiamo trovato la voce `ftp://209.165.200.235/.confidential.txt`



7. Abbiamo aperto poi il campo \_id schiacciando sul link e abbiamo trovato le transazioni tra l'attaccante e il server Target.

**DOMANDA:** Quali sono le credenziali utente per accedere al sito FTP?

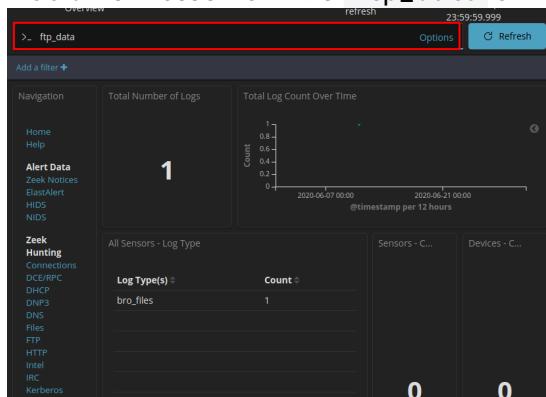
**RISPOSTA:** Le credenziali utente per accedere al sito FTP sono:

- **USER:** analyst
  - **PASS:** cyberops

8. Ora che sappiamo che l'attaccante ha usato FTP per copiare il contenuto del file confidential.txt e poi cancellarlo dal bersaglio.

**DOMANDA:** Qual è il contenuto del file? Ricorda che uno dei servizi elencati nel grafico a torta è `ftp_data`.

Abbiamo messo nel filtro `ftp_data` e il risultato è stato 1.



**RISPOSTA:** Il contenuto del file è stato il seguente:

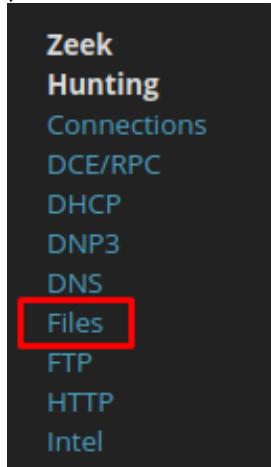
```
192.168.0.11:49817_209.165.200.235-20-6-2105080620.pcap

Log entry:
Time: 2020-06-11 03:53:09
Source: "192.168.0.11" (host)
Type: "PCAP"
Data: "SELECT * FROM sensor WHERE hostname='seconion-import' AND agent.type='pcap' LIMIT 1"
CapLEN: 0
CapDLEN: 0
CapRaw: "CAPME: Processed messages in 0.26 seconds. 0.08 MB / 0.08 MB

SRC: DEBUG: Using archived data from file: /data/seconion/archiver/2020-06-11/seconion-import[192.168.0.11:49817_209.165.200.235:20-6].raw
SRC: QUERY: SELECT * FROM sensor WHERE hostname='seconion-import' AND agent.type='pcap' LIMIT 1
SRC: CAPME: Processed messages in 0.26 seconds. 0.08 MB / 0.08 MB

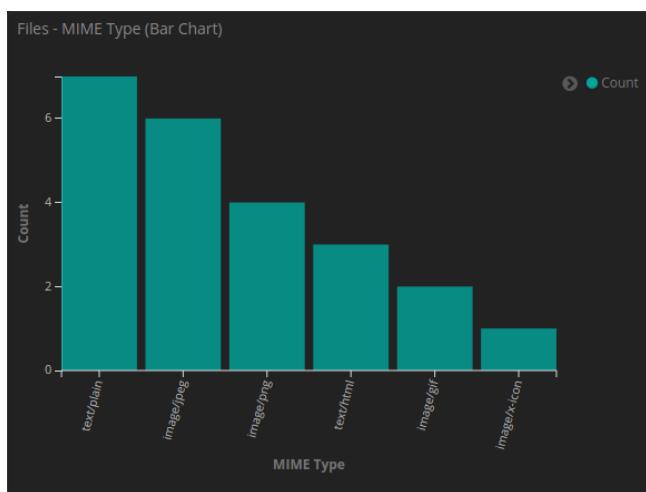
192.168.0.11:49817_209.165.200.235-20-6-2105080620.pcap
```

9. Abbiamo selezionato Files sotto l'intestazione Zeek Hunting nel pannello di sinistra. Questo permette di esaminare i tipi di file che sono stati registrati.



**DOMANDA:** Quali sono i diversi tipi di file? Guarda la sezione `MIME Type` dello schermo.

**RISPOSTA:** Sono presenti diversi tipi di file tra cui `text/plain`, `image/jpeg`, etc.

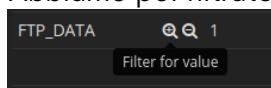


**DOMANDA:** Scorri fino all'intestazione Files - Source. Quali sono le sorgenti dei file elencate?

**RISPOSTA:** Le sorgenti dei file elencate sono `HTTP` e `FTP_DATA`.

Files - Source	
Source	Count
HTTP	22
FTP_DATA	1

10. Abbiamo poi filtrato per `FTP_DATA` cliccando sul + di `Filter for value`.



11. Abbiamo esaminato i risultati filtrati in fondo alla pagina.

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	C2jv8MW6X g4bb51	FX1IV63eSMA EIN1652	KDjqzXIBB6Cd -_0SVfiy

**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?

**RISPOSTA:**

- Il MIME type è `FTP_DATA`
- L'indirizzo IP di origine e di destinazione sono `192.168.0.11` e `209.165.200.235`
- Il trasferimento si è verificato l' `11th June 2020 alle ore 03:53:09`

12. Nei Log dei file abbiamo poi cliccato sul link associato a `_id`.

t	_id	🔍	🔍	☰	*	KDjqzXIBB6Cd-_0SVfiy
---	-----	---	---	---	---	----------------------

**DOMANDA:** Qual è il contenuto testuale del file trasferito tramite FTP?

**RISPOSTA:** Il contenuto del file è riportato nello Screenshot seguente:

`192.168.0.11:49817_209.165.200.235:20-6-1922484408.pcap`

Log entry:  
{"ts": "2020-06-11T03:53:09.088773Z", "fuid": "FX1IV63eSMAEIN1652", "tx\_hosts": ["192.168.0.11"], "rx\_hosts": ["209.165.200.235"], "conn\_uids": ["C2jv8MW6Xg4bb51"], "source": "FTP\_DATA", "depth": 0, "analyzers": [{"name": "SHA1", "MD5": "e7bc9c20bd5663635379c91294d5369", "sha1": "f7f54acee0342f61618e63a10824ee11b330725"}]}  
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 0.24 seconds: 0.08 0.09 0.00 0.07 0.00

`192.168.0.11:49817_209.165.200.235:20-6-1922484408.pcap`

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

**RISPOSTA:** È fondamentale scollegare dalla rete il sistema `192.168.0.11` per consentire l'indagine forense. È necessario effettuare un audit delle regole FTP restringendo l'invio di dati verso l'esterno e verificare l'eventuale presenza di attività di esfiltrazione analoghe. Applicare subito una regola di blocco sul firewall per l'IP `209.165.200.235`.

## Conclusioni

Grazie a strumenti come Sguil, Wireshark e Kibana, siamo riusciti a ricostruire completamente l'evento di sicurezza.

L'analisi ha confermato che l'attaccante è riuscito a diventare `root` su una macchina non sicura, utilizzandola poi per trasferire all'esterno il documento `confidential.txt` mediante una connessione FTP.