

# Progetto Cyber Security & Ethical Hacking

**Team:** Secure Sentinels

**Modulo:** Cybersecurity & Ethical Hacking (Epicode)

**Data:** 24 Febbraio 2026

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

### Obiettivi

In questo laboratorio, si esamineranno 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)**

La 5-tupla viene utilizzata dagli amministratori IT per identificare i requisiti per la creazione di un ambiente di rete operativo e sicuro. I componenti della 5-tupla includono un indirizzo IP e un numero di porta di origine, un indirizzo IP e un numero di porta di destinazione, il protocollo in uso nel payload dei dati.

Verrà utilizzata la Macchina Virtuale CyberOps Security Onion, progettata per il monitoraggio della sicurezza di rete, il rilevamento delle intrusioni (IDS) e la gestione degli incidenti. Gli strumenti che saranno utilizzati saranno Sguil (piattaforma di Network Security Monitoring), Wireshark (analizzatore di pacchetti di rete) e Kibana (strumento di visualizzazione e analisi dei log)

### Parte 1: Esaminare gli Alert in Sguil

#### Istruzioni

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

- a. Viene avviata la **VM Security Onion** ed effettuato il login.
- b. Si apre **Sguil** e si effettua il login. Fare clic su **Select All** per selezionare le interfacce e poi su **Start SGUIL**.



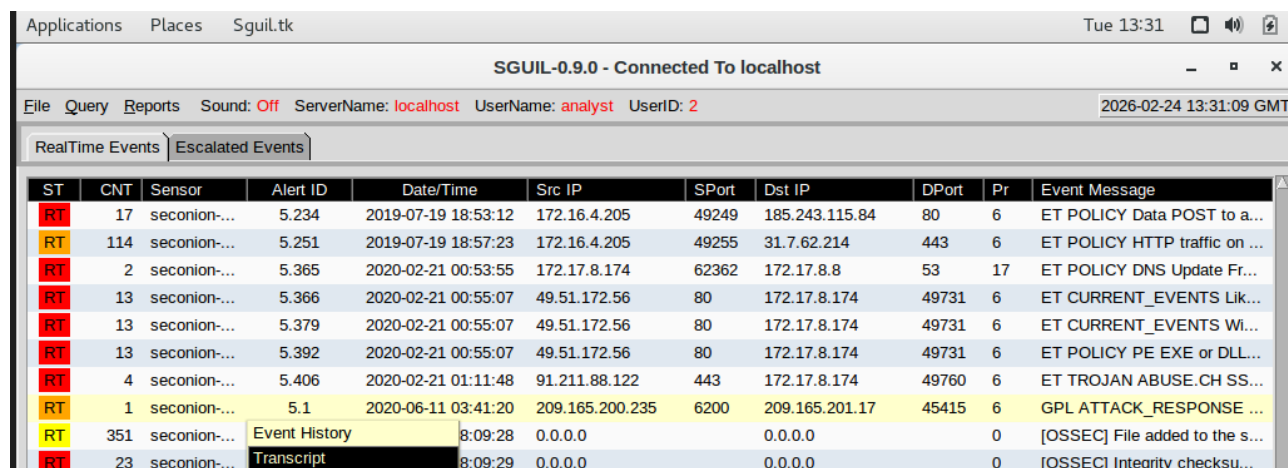
c. Si esaminano gli eventi elencati nella colonna **Event Message**. Uno di questi messaggi è **GPL ATTACK\_RESPONSE id check returned root**. Questo messaggio indica che potrebbe essere stato ottenuto l'accesso root durante un attacco. L'host **209.165.200.235** ha restituito l'accesso **root** a **209.165.201.17**.

RT	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 ...
RT	351	seconion-...	1.1	2020-06-19 18:09:28	0.0.0.0		0.0.0.0		0	[OSSEC] File added to the s...

d. Si selezionano le caselle di controllo **Show Packet Data** e **Show Rule** per visualizzare ogni alert più in dettaglio

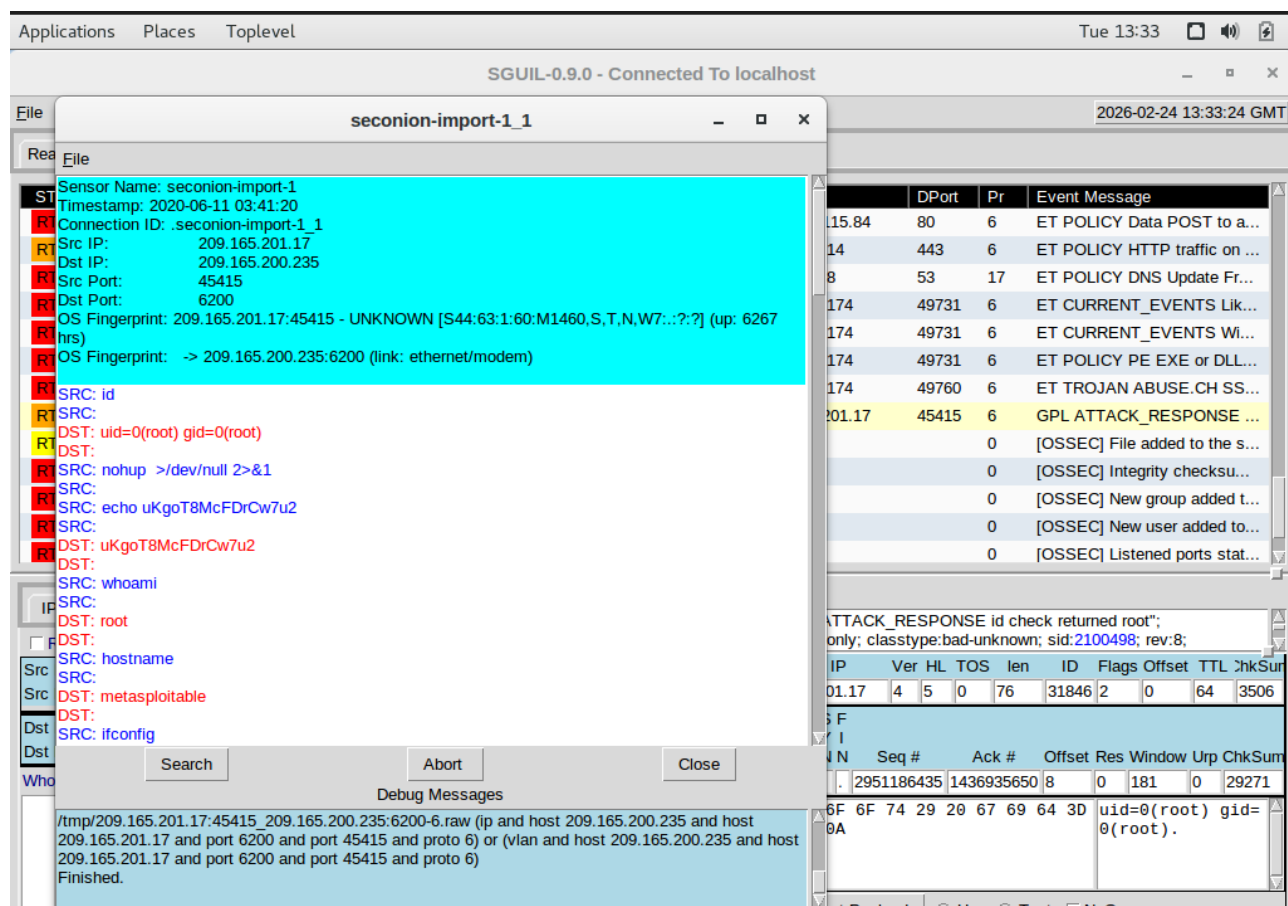
ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	17	seconion-...	5.234	2019-07-19 18:53:12	172.16.4.205	49249	185.243.115.84	80	6	ET POLICY Data POST to a...
RT	114	seconion-...	5.251	2019-07-19 18:57:23	172.16.4.205	49255	31.7.62.214	443	6	ET POLICY HTTP traffic on ...
RT	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 Fr...
RT	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...
RT	13	seconion-...	5.379	2020-02-21 00:55:07	49.51.172.56	80	172.17.8.174	49731	6	ET CURRENT_EVENTS Wl...
RT	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...
RT	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 ...
RT	351	seconion-...	1.1	2020-06-19 18:09:28	0.0.0.0		0.0.0.0		0	[OSSEC] File added to the s...
RT	23	seconion-...	1.2	2020-06-19 18:09:29	0.0.0.0		0.0.0.0		0	[OSSEC] Integrity checksu...
RT	7	seconion-...	1.4	2020-06-19 18:10:04	0.0.0.0		0.0.0.0		0	[OSSEC] New group added t...
RT	7	seconion-...	1.5	2020-06-19 18:10:04	0.0.0.0		0.0.0.0		0	[OSSEC] New user added to...
RT	2	seconion-...	1.18	2020-06-19 18:14:41	0.0.0.0		0.0.0.0		0	[OSSEC] Listened ports stat...

e. Si effettua il clic con il pulsante destro sull'ID dell'alert 5.1 e si seleziona **Transcript**



ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	17	seconion-...	5.234	2019-07-19 18:53:12	172.16.4.205	49249	185.243.115.84	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 ...
RT	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 Fr...
RT	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...
RT	13	seconion-...	5.379	2020-02-21 00:55:07	49.51.172.56	80	172.17.8.174	49731	6	ET CURRENT_EVENTS Wi...
RT	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...
RT	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 ...
RT	351	seconion-...	Event History	8:09:28	0.0.0.0		0.0.0.0		0	[OSSEC] File added to the s...
RT	23	seconion-...	Transcript	8:09:29	0.0.0.0		0.0.0.0		0	[OSSEC] Integrity checksu...

f. Esame delle trascrizioni per l'alert. La trascrizione mostra 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.



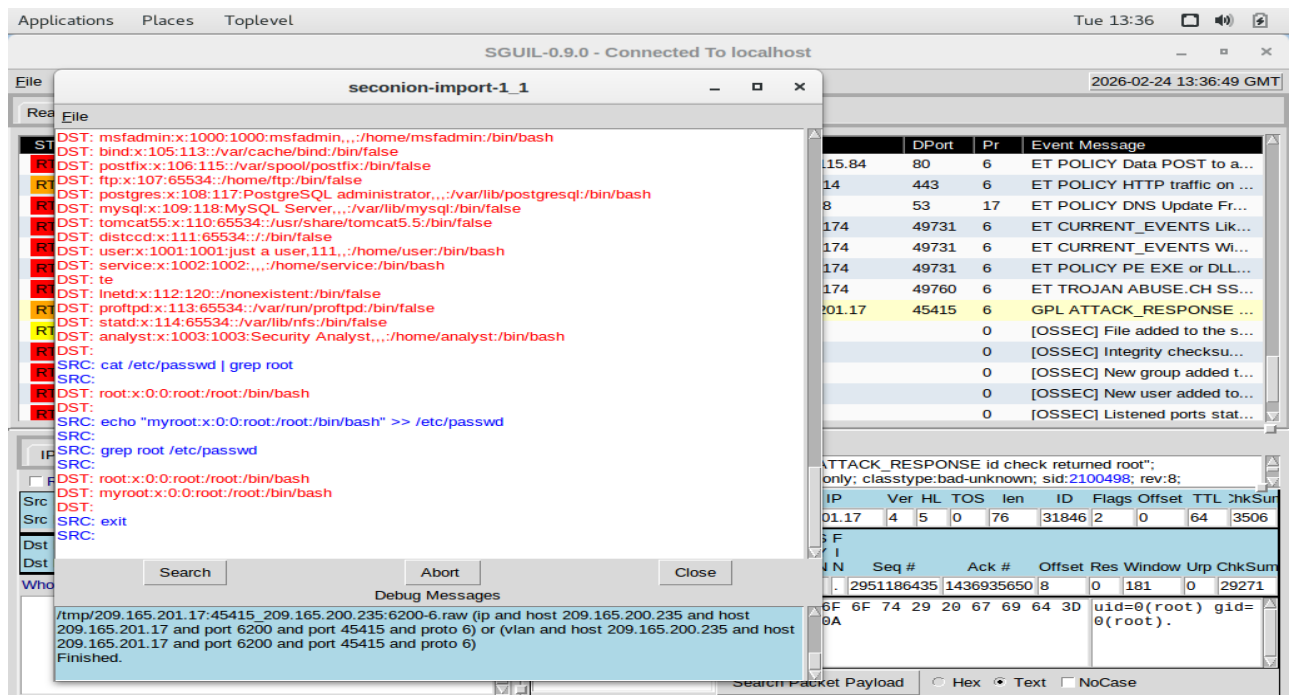
**seconion-import-1\_1**

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: 6200  
OS Fingerprint: 209.165.201.17:45415 - UNKNOWN [S44:63:1:60:M1460,S,T,N,W7:..?:?] (up: 6267 hrs)  
OS Fingerprint: -> 209.165.200.235:6200 (link: ethernet/modem)

SRC: id  
DST: uid=0(root) gid=0(root)  
DST:  
SRC: nohup >/dev/null 2>&1  
SRC:  
SRC: echo uKgoT8McFDrCw7u2  
DST: uKgoT8McFDrCw7u2  
DST:  
SRC: whoami  
SRC:  
DST: root  
DST:  
SRC: hostname  
SRC:  
DST: metasploitable  
DST:  
SRC: ifconfig

Debug Messages

/tmp/209.165.201.17:45415\_209.165.200.235:6200-6.raw (ip and host 209.165.200.235 and host 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)  
Finished.



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

Le transazioni avvenute tra il **Client** (Attaccante: **209.165.201.17**) e il **Server** (Vittima: **209.165.200.235**) sulla porta **6200/TCP** sono:

### 1. Fase di Esplorazione e Conferma Privilegi

l'attaccante invia comandi per capire chi è e dove si trova all'interno del sistema compromesso.

**Comando id:** Il server risponde con **uid=0(root) gid=0(root)**, confermando che l'attaccante ha già ottenuto i massimi privilegi (**root**).

**Comando whoami:** Il server conferma nuovamente l'identità dell'utente come **root**.

**Comando hostname:** Il server risponde **metasploitable**, indicando il nome della macchina vittima.

**Comando ifconfig:** L'attaccante richiede i dettagli di rete per mappare meglio l'infrastruttura.

### 2. Esfiltrazione di Informazioni Critiche

L'attaccante passa all'analisi degli utenti presenti sul sistema.

**Comando cat /etc/passwd:** Il server invia l'intero contenuto del file degli utenti (si vedono utenti come **msfadmin**, **postgres**, **service**, ecc.).

**Filtraggio:** L'attaccante usa **grep root** per isolare le informazioni relative all'utente amministratore.

### 3. Fase di Persistenza (Creazione Backdoor)

L'attaccante decide di non usare l'utente **root** esistente, ma di crearne uno nuovo

**Comando:** **echo "myroot:x:0:0:root:/root:/bin/bash" >> /etc/passwd**

L'attaccante ha aggiunto un nuovo utente chiamato **myroot** con **UID 0** (identico a **root**). Questo gli permetterà di rientrare nel sistema in futuro con privilegi totali, anche se la password dell'utente **root** originale venisse cambiata.

### 4. Verifica e Chiusura

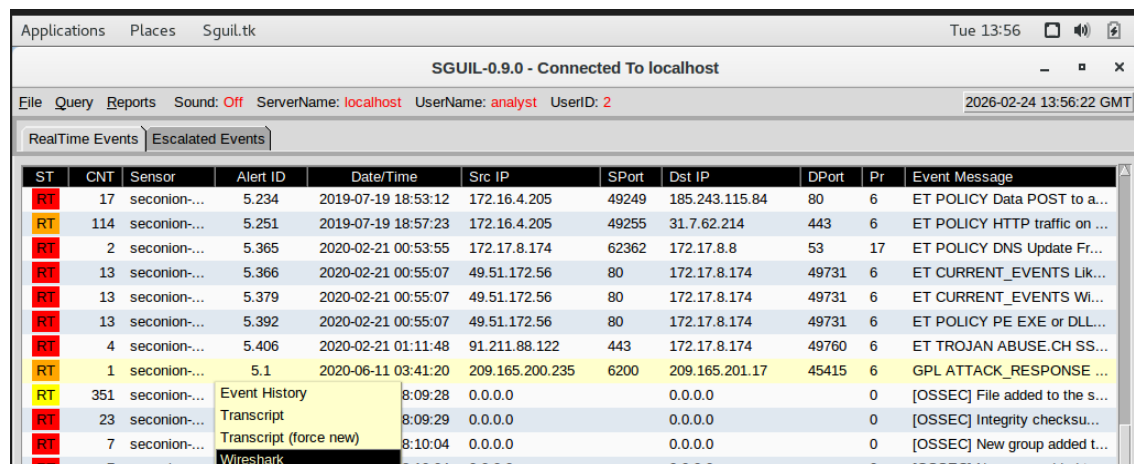
**Verifica:** L'attaccante esegue nuovamente **grep root /etc/passwd** e il server mostra entrambi gli utenti: **root** e il nuovo **myroot**.

**Uscita:** L'attaccante digita exit per chiudere la sessione corrente, lasciando però la backdoor attiva nel file **passwd**.

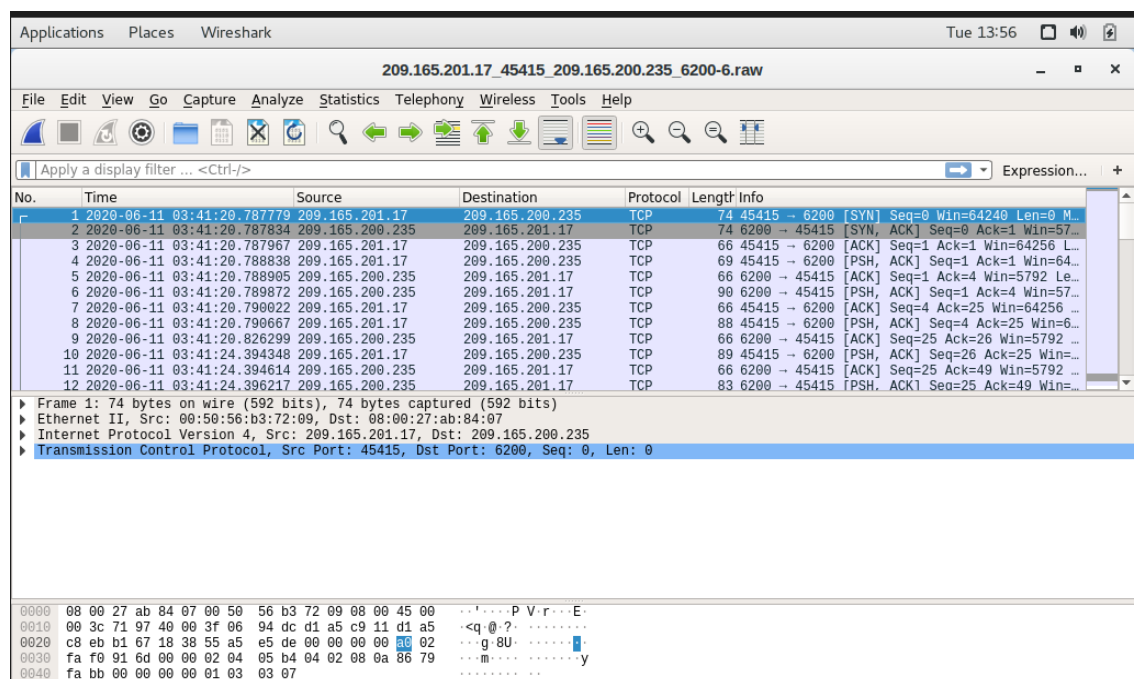
## Parte 2: Passare a Wireshark

### Istruzioni

- Si seleziona l'alert che ha fornito la trascrizione nel passo precedente. Effettua il clic con il pulsante destro sull'**ID dell'alert 5.1** e seleziona **Wireshark**. La finestra principale di **Wireshark** mostra tre viste di un pacchetto.



ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	17	seconion-...	5.234	2019-07-19 18:53:12	172.16.4.205	49249	185.243.115.84	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 ...
RT	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 Fr...
RT	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...
RT	13	seconion-...	5.379	2020-02-21 00:55:07	49.51.172.56	80	172.17.8.174	49731	6	ET CURRENT_EVENTS Wi...
RT	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...
RT	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 ...
RT	351	seconion-...		8:09:28	0.0.0.0		0.0.0.0		0	[OSSEC] File added to the s...
RT	23	seconion-...		8:09:29	0.0.0.0		0.0.0.0		0	[OSSEC] Integrity checks u...
RT	7	seconion-...		8:10:04	0.0.0.0		0.0.0.0		0	[OSSEC] New group added t...
RT	7	seconion-...		8:10:04	0.0.0.0		0.0.0.0		0	[OSSEC] New user added to...

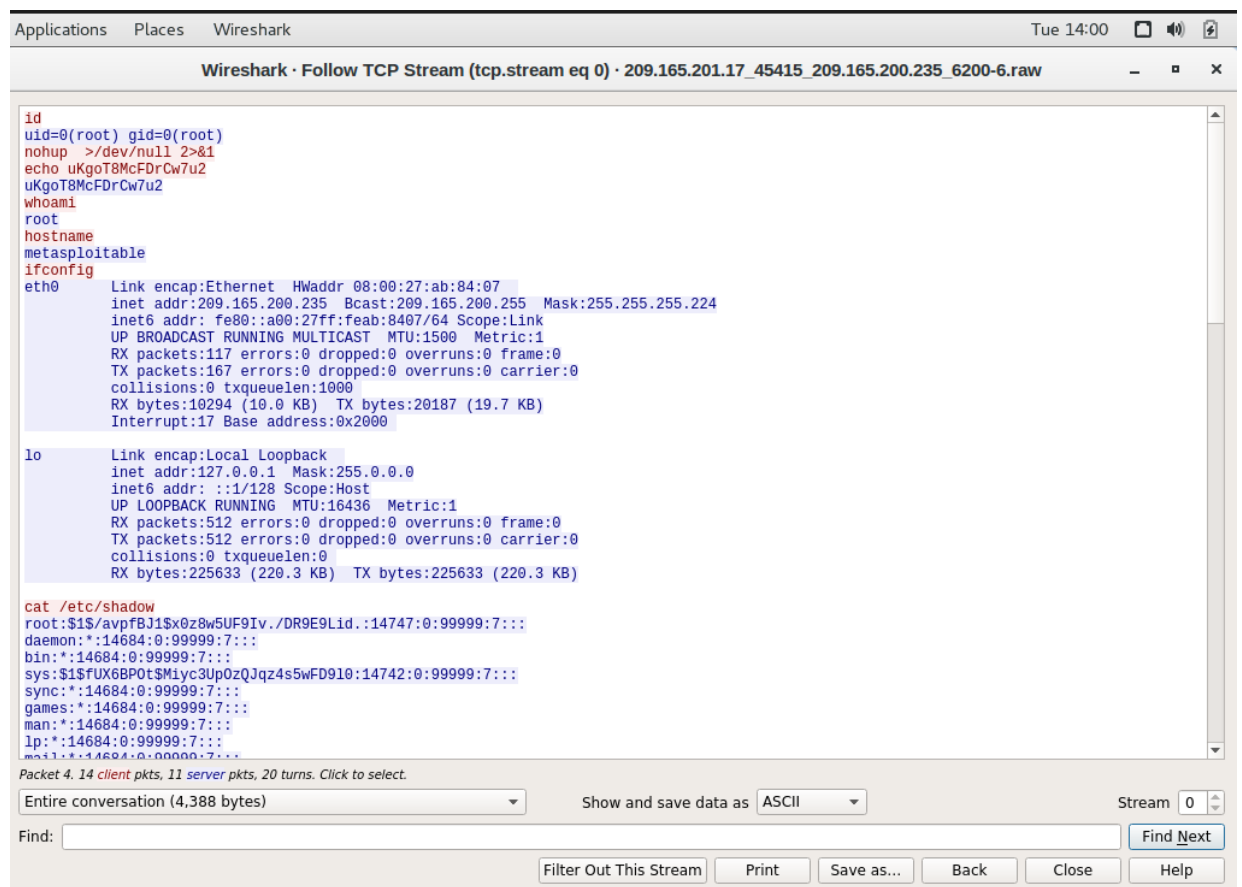
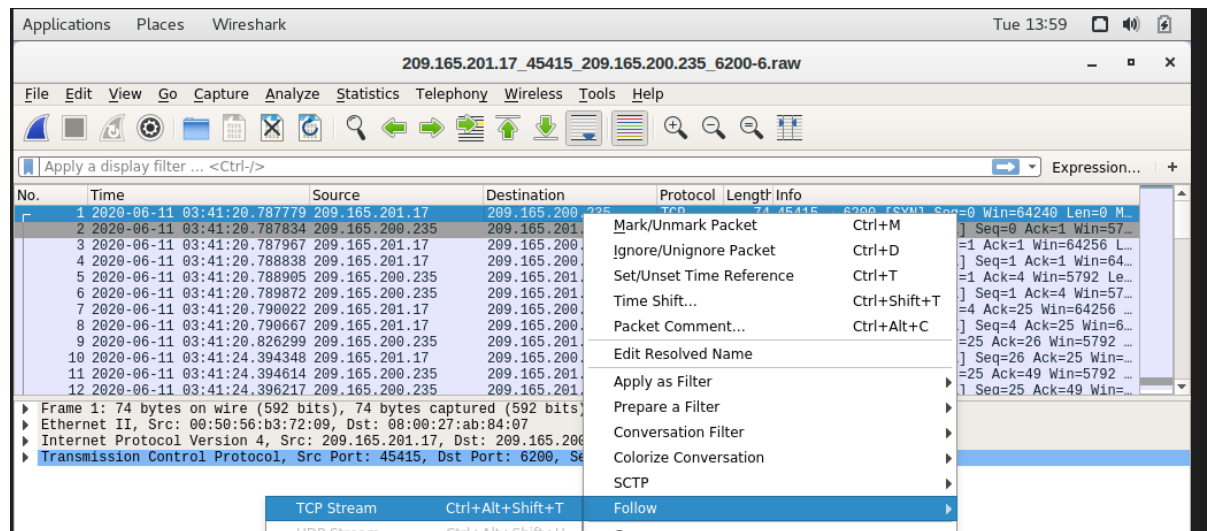


No.	Time	Source	Destination	Protocol	Length	Info
1	2020-06-11 03:41:20.787779	209.165.201.17	209.165.200.235	TCP	74	45415 → 6200 [SYN] Seq=0 Win=64240 Len=0 M...
2	2020-06-11 03:41:20.787834	209.165.200.235	209.165.201.17	TCP	74	6200 → 45415 [SYN, ACK] Seq=0 Ack=1 Win=57...
3	2020-06-11 03:41:20.787967	209.165.201.17	209.165.200.235	TCP	66	45415 → 6200 [ACK] Seq=1 Ack=1 Win=64256 L...
4	2020-06-11 03:41:20.788838	209.165.201.17	209.165.200.235	TCP	69	45415 → 6200 [PSH, ACK] Seq=1 Ack=1 Win=64...
5	2020-06-11 03:41:20.788905	209.165.200.235	209.165.201.17	TCP	66	6200 → 45415 [ACK] Seq=1 Ack=4 Win=5792 Le...
6	2020-06-11 03:41:20.789872	209.165.200.235	209.165.201.17	TCP	90	6200 → 45415 [PSH, ACK] Seq=1 Ack=4 Win=57...
7	2020-06-11 03:41:20.790022	209.165.201.17	209.165.200.235	TCP	66	45415 → 6200 [ACK] Seq=4 Ack=25 Win=64256 ...
8	2020-06-11 03:41:20.790667	209.165.201.17	209.165.200.235	TCP	88	45415 → 6200 [PSH, ACK] Seq=4 Ack=25 Win=6...
9	2020-06-11 03:41:20.826299	209.165.200.235	209.165.201.17	TCP	66	6200 → 45415 [ACK] Seq=25 Ack=26 Win=5792 ...
10	2020-06-11 03:41:24.394348	209.165.201.17	209.165.200.235	TCP	89	45415 → 6200 [PSH, ACK] Seq=26 Ack=25 Win=...
11	2020-06-11 03:41:24.394614	209.165.200.235	209.165.201.17	TCP	66	6200 → 45415 [ACK] Seq=25 Ack=49 Win=5792 ...
12	2020-06-11 03:41:24.396217	209.165.200.235	209.165.201.17	TCP	83	6200 → 45415 [PSH, ACK] Seq=25 Ack=49 Win=...

Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)  
Ethernet II, Src: 00:50:56:b3:72:09, Dst: 08:00:27:ab:84:07  
Internet Protocol Version 4, Src: 209.165.201.17, Dst: 209.165.200.235  
Transmission Control Protocol, Src Port: 45415, Dst Port: 6200, Seq: 0, Len: 0

0000 08 00 27 ab 84 07 00 56 b3 72 09 08 00 45 00 ... P V r ... E  
0010 00 3c 71 97 40 00 3f 06 94 dc d1 a5 c9 11 d1 a5 ... <q @ ? ...  
0020 c8 eb b1 67 18 38 55 a5 e5 de 00 00 00 00 00 02 ... g 8U ...  
0030 fa f0 91 6d 00 00 02 04 05 b4 04 02 08 0a 86 79 ... m ... y  
0040 fa bb 00 00 00 00 01 03 03 07 ...

- b. Per visualizzare tutti i pacchetti assemblati in una conversazione **TCP**, si fa clic con il pulsante destro su un pacchetto qualsiasi e si seleziona **Follow > TCP Stream**.



### Cosa hai osservato? Cosa indicano i colori del testo rosso e blu?

Il testo rosso indica i comandi inviati dall'attaccante(client), mentre il testo blu l'output in risposta ai comandi inviati(server)

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

Il comando **whoami** eseguito dall'attaccante rivela che quest'ultimo ha ottenuto il controllo completo e senza restrizioni sul sistema bersaglio.

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

I dati letti dall'attore della minaccia sono:

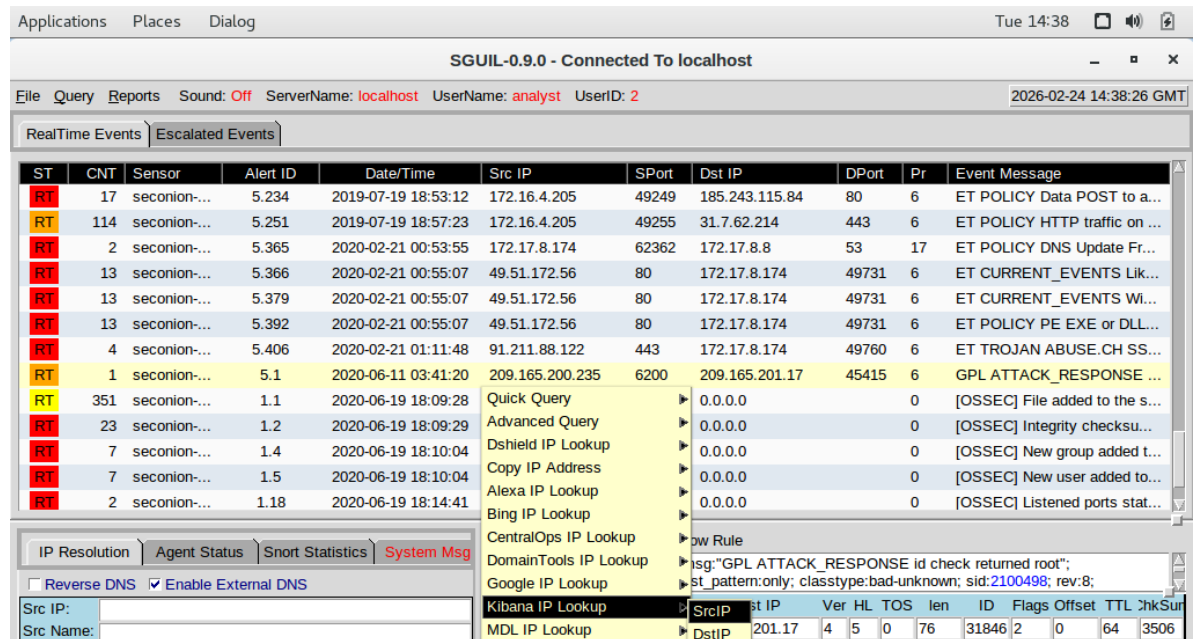
- Identità e privilegi dell'utente, confermando di operare come root
- Configurazioni di rete e host, tramite i comandi **hostname** e **ifconfig** ha letto il nome della macchina vittima (**metasploitable**) e i dettagli dell'interfaccia di rete, ip e mac
- Database degli utenti di sistema, attraverso la lettura di **/etc/passwd**, l'attaccante ha ottenuto l'elenco di tutti gli account presenti sulla macchina
- Credenziali e Hash delle password, ha visualizzato il contenuto del file shadow, ottenendo gli **hash crittografati** delle password (es. per gli utenti root, sys, service e analyst)
- Ha riletto i file di configurazione per confermare il successo dell'operazione, filtrando i file **/etc/passwd** e **/etc/shadow** tramite il comando **grep root** per verificare che il nuovo utente malevolo **myroot** fosse stato aggiunto correttamente e fosse pronto all'uso senza password.



## Parte 3: Passare a Kibana

### Istruzioni

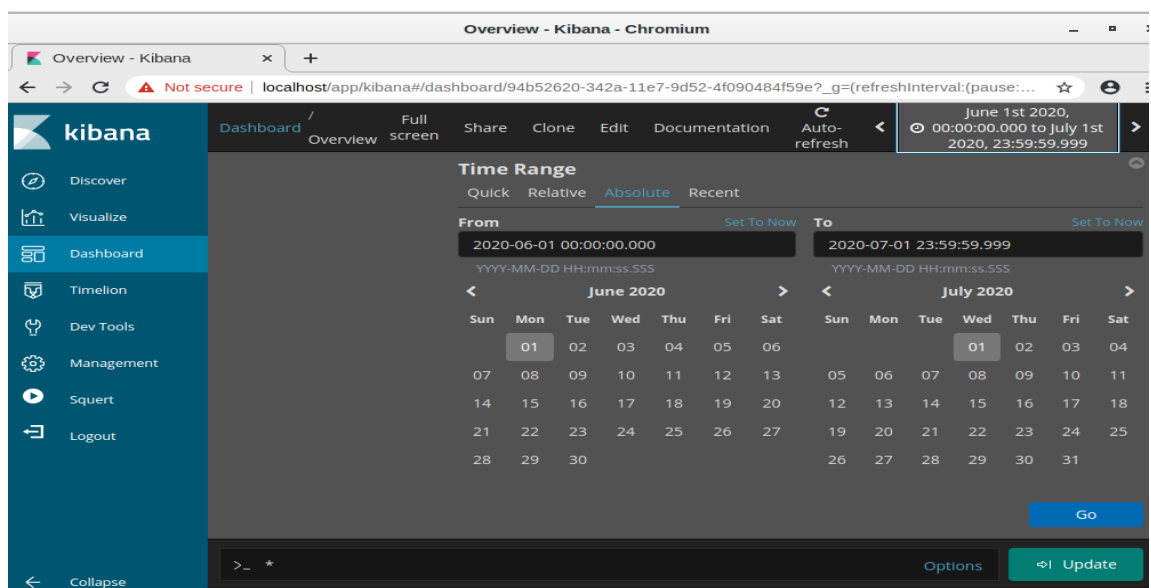
- a. Si torna a **Sguil**. Si fa clic con il pulsante destro sull'indirizzo IP di origine o di destinazione per l'**ID dell>alert 5.1** e si seleziona **Kibana IP Lookup > SrcIP**.



The screenshot shows the Sguil-0.9.0 interface. The main window displays a table of events. The event with ID 5.1 is highlighted. A right-click context menu is open, showing options like 'Quick Query', 'Advanced Query', 'Dshield IP Lookup', 'Copy IP Address', 'Alexa IP Lookup', 'Bing IP Lookup', 'CentralOps IP Lookup', 'DomainTools IP Lookup', 'Google IP Lookup', 'Kibana IP Lookup', and 'MDL IP Lookup'. The 'Kibana IP Lookup' option is selected, and a sub-menu is visible with 'SrcIP' and 'DstIP' options.

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	17	seconion-...	5.234	2019-07-19 18:53:12	172.16.4.205	49249	185.243.115.84	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 ...
RT	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 Fr...
RT	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...
RT	13	seconion-...	5.379	2020-02-21 00:55:07	49.51.172.56	80	172.17.8.174	49731	6	ET CURRENT_EVENTS Wi...
RT	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...
RT	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 ...
RT	351	seconion-...	1.1	2020-06-19 18:09:28			0.0.0.0		0	[OSSEC] File added to the s...
RT	23	seconion-...	1.2	2020-06-19 18:09:29			0.0.0.0		0	[OSSEC] Integrity checksu...
RT	7	seconion-...	1.4	2020-06-19 18:10:04			0.0.0.0		0	[OSSEC] New group added t...
RT	7	seconion-...	1.5	2020-06-19 18:10:04			0.0.0.0		0	[OSSEC] New user added to...
RT	2	seconion-...	1.18	2020-06-19 18:14:41			0.0.0.0		0	[OSSEC] Listened ports stat...

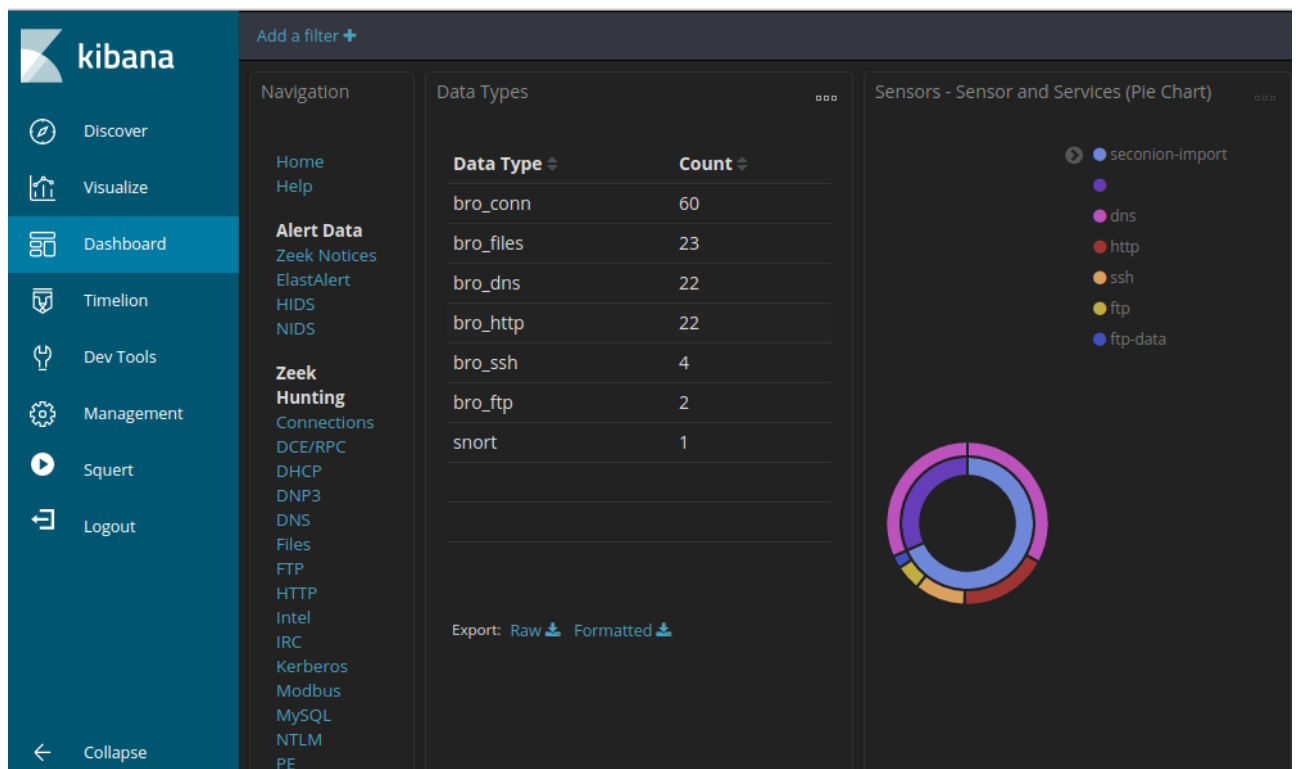
- b. Se l'intervallo di tempo è impostato sulle ultime 24 ore, cambia a Giugno 2020 in modo che l'11 giugno sia incluso nell'intervallo. Si usa la scheda Absolute per cambiare l'intervallo di tempo.



The screenshot shows the Kibana interface. The 'Time Range' section is visible, with the 'Absolute' tab selected. The date range is set from 2020-06-01 00:00:00.000 to 2020-07-01 23:59:59.999. A calendar view is visible below the date range, showing June 2020 and July 2020. The date 01 is highlighted in June 2020.

- c. Nei risultati visualizzati, c'è un elenco di diversi tipi di dati. Ti è stato detto che il file confidential.txt non è più accessibile. Nel grafico a torta "**Sensors - Sensors and Services**", sono presenti **ftp** e **ftp-data**. Determineremo se **FTP** è stato usato per rubare il file.





- d. Filtriamo per **bro\_ftp**. Si passa il mouse sullo spazio vuoto accanto al conteggio dei tipi di dati **bro\_ftp**. Si seleziona **+** per filtrare solo il traffico relativo a **FTP**



- e. Si scorre verso il basso fino a **All Logs**. Ci sono due voci elencate.

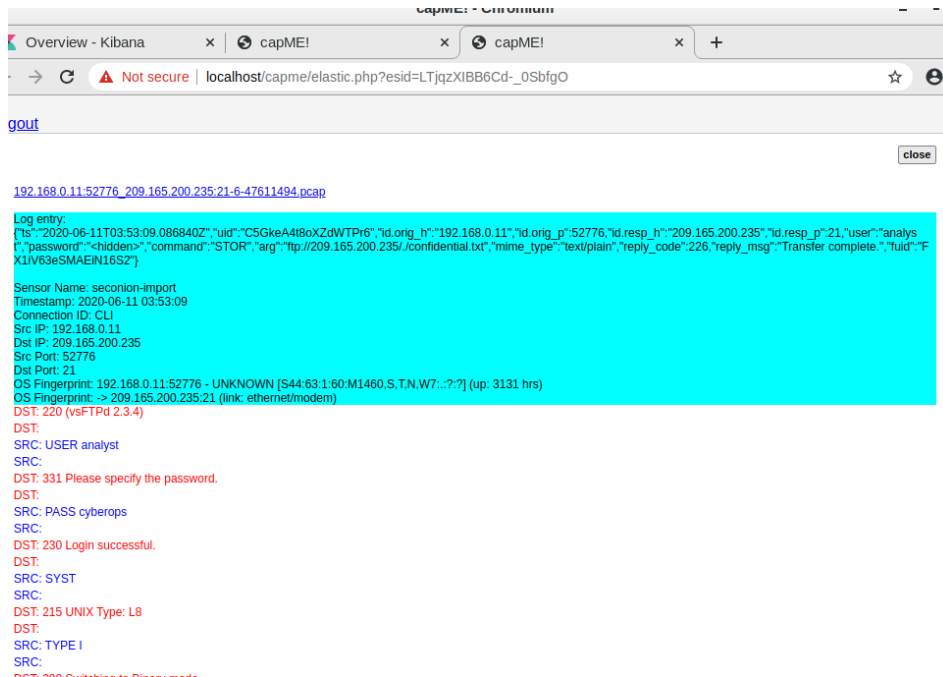
All Logs						
Time	source_ip	source_port	destination_ip	destination_port	_id	
June 11th 2020, 03:53:09.086	192.168.0.11	52776	209.165.200.235	21	LDjqzXIB B6Cd_0 SbfgO	
June 11th 2020, 03:53:09.086	192.168.0.11	52776	209.165.200.235	21	LTjqzXIB B6Cd_0 SbfgO	

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

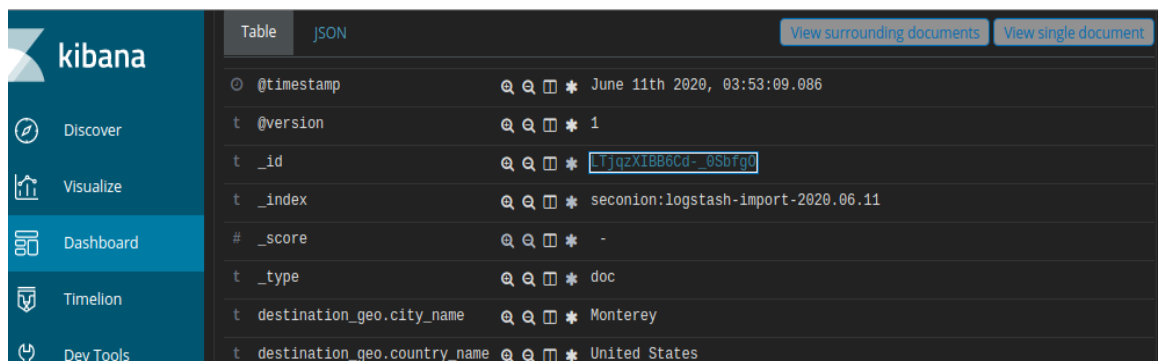
Ip di origine (**source\_ip**) **192.168.0.11**, porta **52776**

Ip di destinazione (**destination\_ip**) **209.165.200.235**, porta **21**

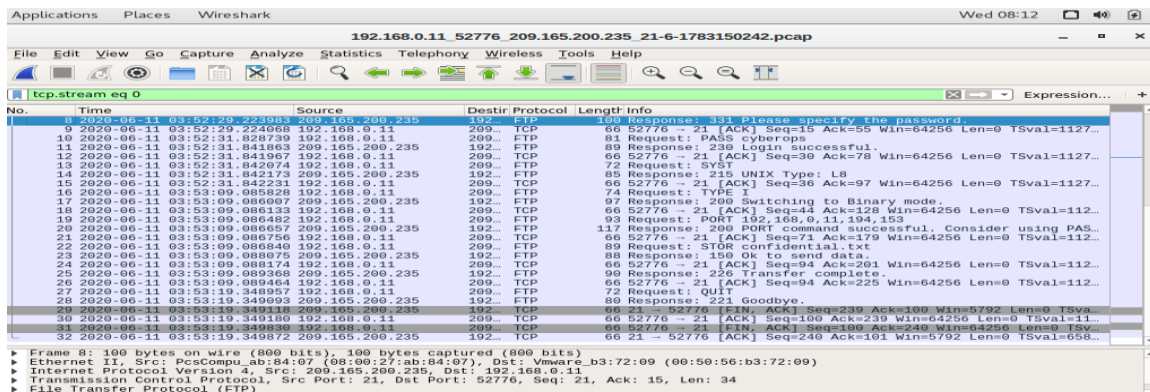
- f. Si espande e si esaminano entrambe le voci di log. In una di queste voci, il campo **ftp\_argument** ha una voce di **ftp://209.165.200.235/./confidential.txt**. Si esamina anche il messaggio nella voce di log per saperne di più su questo evento



- g. All'interno della stessa voce di log, scorri fino al campo **alert\_id** e fai clic sul link.



- h. Si esamina la trascrizione per le transazioni tra l'attaccante e il bersaglio. Si scarica il pcap per esaminare il traffico usando **Wireshark**.



Quali sono le credenziali utente per accedere al sito FTP?

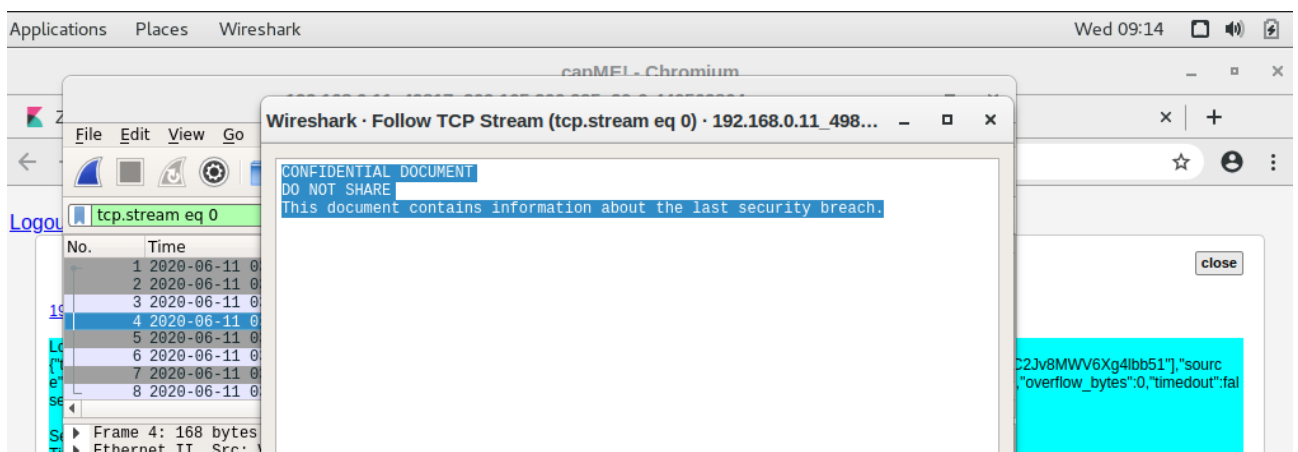
Le credenziali utente sono username **analyst** e password **cyberops**

- i. Verificato che l'attaccante ha usato **FTP** per copiare il contenuto del file confidential.txt per poi cancellarlo dal bersaglio.

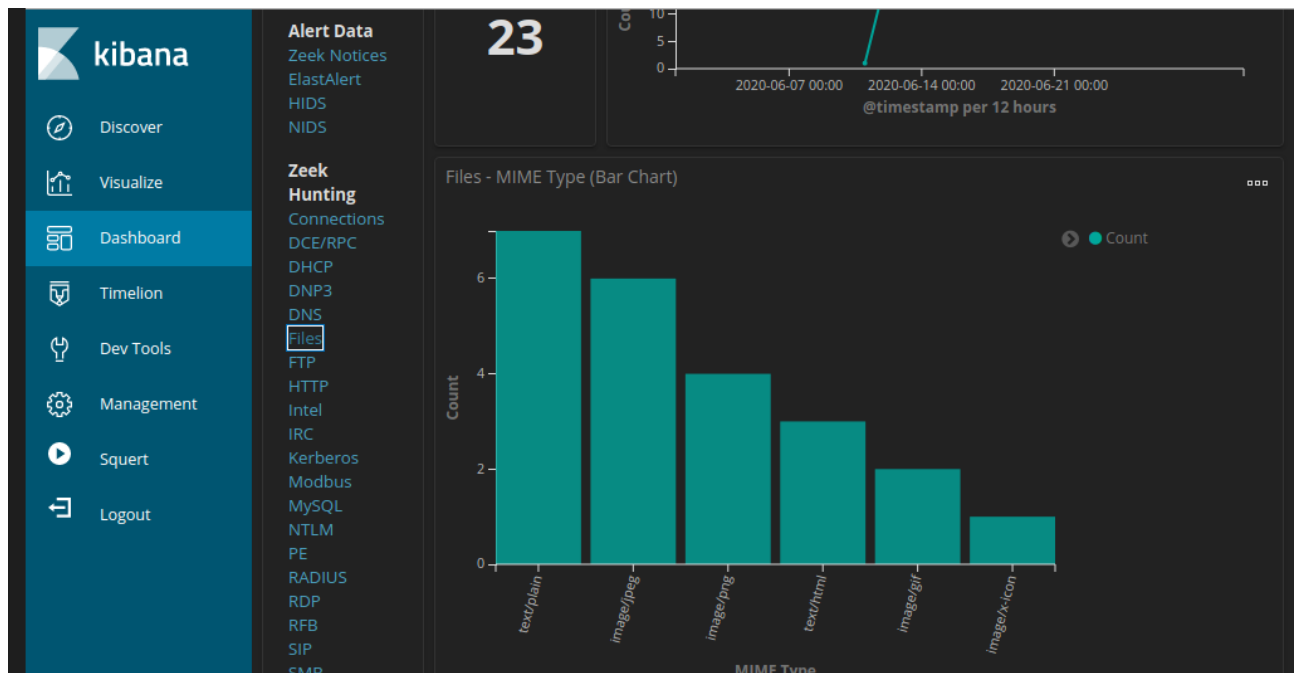
**Qual è il contenuto del file?**

Il contenuto del file è "CONFIDENTIAL DOCUMENT DO NOT SHARE

[...]"



- j. Si naviga in cima alla dashboard. Si seleziona **Files** sotto l'intestazione **Zeek Hunting** nel pannello di sinistra



Quali sono i diversi tipi di file? Guarda la sezione MIME Type dello schermo. Scorri fino all'intestazione Files - Source.

Quali sono le sorgenti dei file elencate?

I diversi tipi di file sono **text/plain**, **image/jpeg**, **image/png**, **text/html**, **image/gif**, **image/x-icon**.

Files - MIME Type		Files - Source IP Address		Files - Destination IP Address	
MIME Type	Count	File IP Address	Count	IP Address	Count
text/plain	7	209.165.200.235	22	209.165.200.227	22
image/jpeg	6	192.168.0.11	1	209.165.200.235	1
image/png	4				
text/html	3				
image/gif	2				
image/x-icon	1				

Le sorgenti (File -Source) sono **HTTP** e **FTP\_DATA**

Files - Source

Source ▾	Count ▾
HTTP	22
FTP_DATA	1

Files - Files By Size (Bytes)

Bytes Seen ▾	Count ▾
99.685KB	1
70.19KB	1
55.912KB	1
50.438KB	1
38.326KB	1
23.687KB	1
23.11KB	1
22.569KB	1
12.137KB	1
10.032KB	1

k. Si filtra per **FTP\_DATA** passando il mouse sullo spazio vuoto accanto al conteggio per **FTP\_DATA** e si fa clic su **+**

I. Si scorre verso il basso per esaminare i risultati filtrati. Qual è il tipo MIME, l'indirizzo IP di origine e di destinazione associato al trasferimento dei dati FTP?

Il tipo **MIME** è **text/plain**, l'indirizzo ip di origine è **192.168.0.11** e indirizzo ip di destinazione è **209.165.200.235**

Files - MIME Type		Files - Source IP Address		Files - Destination IP Address	
MIME Type	Count	File IP Address	Count	IP Address	Count
text/plain	1	192.168.0.11	1	209.165.200.235	1

**Quando si è verificato questo trasferimento?**

Il trasferimento si è verificato in data 11/06/2020 alle 03:53

Time ▾	file_ip	destination_ip	source	uid	fuid	_id
▶ June 11th 2020, 03:53:09.088	192.168.1.1	209.165.200.235	FTP_DATA	C2jv8MWW6Xg4lbb51	FX11V63eSMAEIN16S2	KDjqzXIBB6Cd-05vfiy

m. Nei log dei file, espandi la voce associata ai dati FTP. Fai clic sul link associato all'**alert\_id**.

### Qual è il contenuto testuale del file trasferito tramite FTP?

Tramite la dashboard **Files** (nella suite **Zeek Hunting di Kibana**), l'indagine è stata ristretta alla categoria di traffico **FTP\_DATA**. Accedendo alla trascrizione del singolo evento di trasferimento, è stato possibile visualizzare il dump testuale del payload di rete.

Il contenuto del file è "CONFIDENTIAL DOCUMENT DO NOT SHARE [...]"

[Logout](#) close

[192.168.0.11:49817\\_209.165.200.235:20-6-370252123.pcap](#)

Log entry:  
[{"ts":"2020-06-11T03:53:09.088773Z","uid":"FX1IV63eSMAEIN16S2","tx\_hosts":["192.168.0.11"],"rx\_hosts":["209.165.200.235"],"conn\_uids":["C2Jv8MWV6Xg4Ibb51"],"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,"timeout":false,"md5":"e7bc9c20bfd5666365379c91294d536b","sha1":"77f54ace0342f6161f6e63a10824ee1b330725"}]

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 0.28 seconds: 0.05 0.12 0.00 0.10 0.00

[192.168.0.11:49817\\_209.165.200.235:20-6-370252123.pcap](#)

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

## Conclusioni e Protocollo di Rimediazione (Incident Response)

L'indagine ha permesso la ricostruzione integrale dell'incidente: l'attaccante ha violato il perimetro (Ottenimento Accesso), ha innalzato i privilegi al livello di sistema (Privilege Escalation), ha impiantato una backdoor in **/etc/passwd** (Persistenza), ha compromesso le credenziali FTP legittime e ha completato l'obiettivo esfiltrando documenti riservati prima di attuare tattiche di sabotaggio (Data Wiping/Evasion).

Per il contenimento e l'eradicazione della minaccia, si impone il seguente piano d'azione immediato:

1. **Quarantena dell'Asset:** Disconnessione fisica e logica (tramite regole switch/VLAN quarantine) dell'host 209.165.200.235 dalla rete aziendale di produzione.

2. **Mitigazione Perimetrale:** Implementazione di regole di blocco (Drop/Deny) sull'infrastruttura Firewall/IPS per interdire ogni comunicazione bidirezionale con l'indirizzo IP malevolo 209.165.201.17.
3. **Eradicazione della Backdoor:** Pulizia manuale del sistema infetto, procedendo alla cancellazione della riga associata all'account **myroot** sia dal file **/etc/passwd** che dal file crittografato **/etc/shadow**.
4. **Bonifica delle Credenziali e Hardening:** Invalidare e forzare il reset delle password per tutti gli account di sistema (in particolare l'utente **analyst** e l'amministratore **root**). Infine, **deprecare** l'utilizzo del protocollo FTP in favore di alternative sicure basate su cifratura asimmetrica, quali SFTP o FTPS.
5. **Identificazione dello host interno:** L'indirizzo **192.168.0.11** appartiene ad una classe di indirizzi privati, ciò significa che rappresenta un dispositivo all'interno della rete locale LAN. Attraverso Kibana, questo IP risulta essere la sorgente (**Source IP**) della sessione **FTP** che ha prelevato il file **confidential.txt** del server compromesso. L'attaccante dopo aver preso il controllo del server potrebbe aver utilizzato lo host **192.168.0.11** come pivoting (movimento laterale) per prelevare i dati sensibili. poiché **Wireshark** ha mostrato che l'attaccante ha rubato i file delle password (**/etc/shadow**), è molto probabile che abbia usato quelle credenziali per autenticarsi tramite FTP da questo host interno e scaricare il documento. L'host **192.168.0.11** quindi, deve essere oggetto di analisi. Risulta necessario verificare se all'interno del dispositivo associato a questo host sono stati installati Malware e che tipo di violazione ha subito.