Build Week 3 Bonus 2
Isolare un Host Compromesso Usando la 5-Tupla

Laboratorio: Bonus 2 - Isolare un Host Compromesso

Data: 24 Febbraio 2026

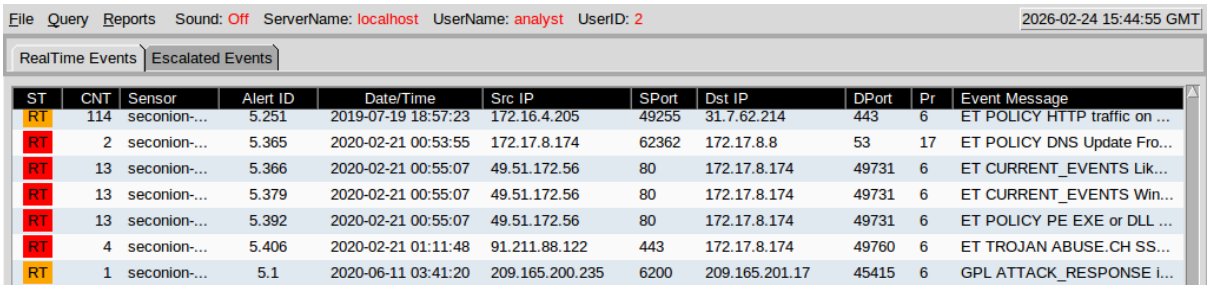
1. Obiettivi e Contesto

L'obiettivo di questo laboratorio è l'analisi di un incidente di sicurezza di rete utilizzando gli strumenti della suite Security Onion (Sguil, Wireshark, Kibana). Tramite l'identificazione della 5-Tupla (IP sorgente, Porta sorgente, IP destinazione, Porta destinazione, Protocollo) e il *pivoting* tra i vari tool, l'indagine mira a confermare la compromissione di un host, tracciare le azioni del *Threat Actor* (TA) e determinare le modalità di esfiltrazione del file confidential.txt.

2. Esecuzione e Analisi Passo-Passo

Parte 1: Esaminare gli Alert in Sguil

Dall'accesso alla console Sguil, si è proceduto all'analisi degli eventi real-time. È stato individuato un alert critico:


File Query Reports Sound: Off ServerName: localhost UserName: analyst UserID: 2 2026-02-24 15:44:55 GMT

RealTime Events | Escalated Events

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
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 Fro...
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 Win...
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 i...

- **Alert ID:** 5.1
- **Event Message:** GPL ATTACK_RESPONSE id check returned root
- **5-Tupla dell'evento (pacchetto di risposta):**
  - **Src IP (Target Server):** 209.165.200.235
  - **SPort:** 6200
  - **Dst IP (Attaccante):** 209.165.201.17
  - **DPort:** 45415
  - **Protocollo:** TCP (6)
- *Nota tecnica:* Essendo una regola "ATTACK_RESPONSE", l'IP sorgente registrato nell'alert è quello del server compromesso che sta restituendo l'output all'attaccante. La porta 6200 è tipicamente associata alla *backdoor* malevola introdotta nella

vulnerabilità di vsftpd 2.3.4.

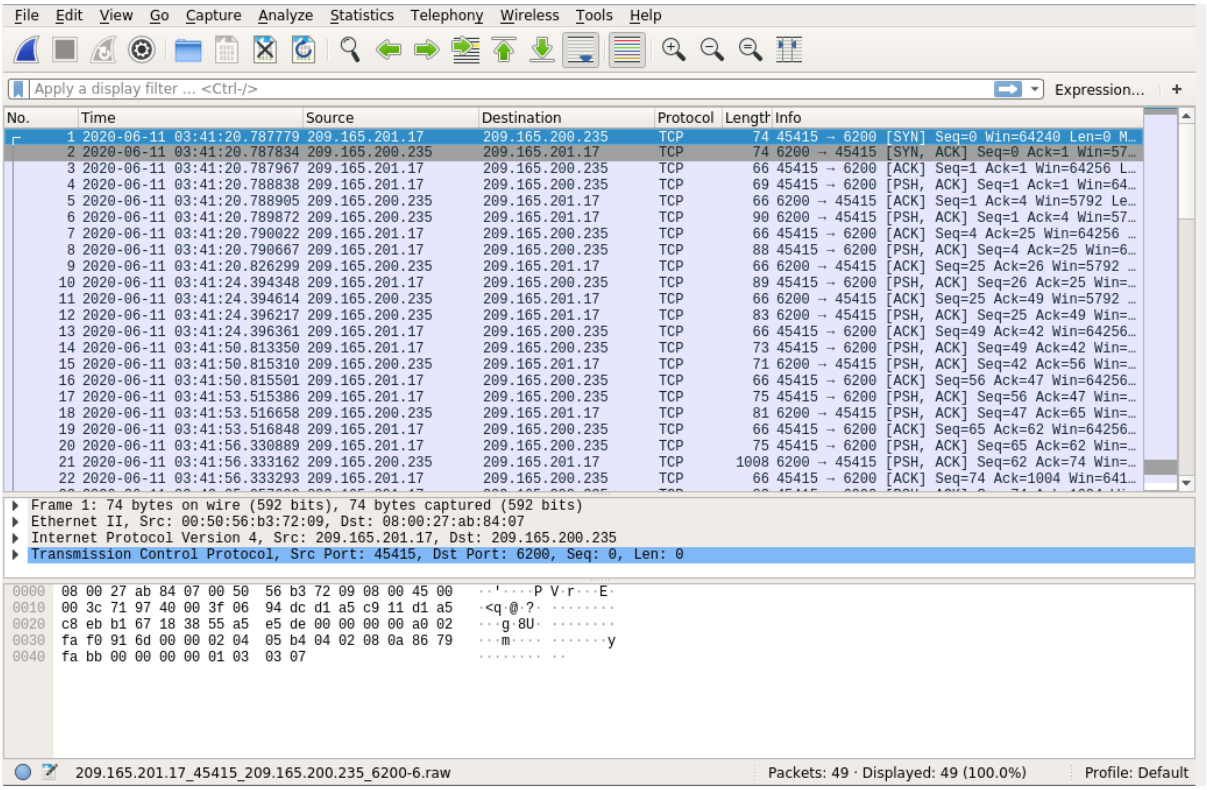
Dal transcript dell'evento, l'attaccante ha stabilito una connessione con l'host bersaglio, eseguendo comandi tipici della fase di *Post-Exploitation* o *Discovery*.

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

Risposta: Si tratta di una sessione di shell interattiva non crittografata (una *bind shell* in ascolto sulla porta 6200 dell'host compromesso). L'attaccante (client) sta inviando comandi di sistema Linux standard (id, whoami, hostname, ifconfig) e il server sta restituendo in chiaro gli output (stdout/stderr) di tali comandi.

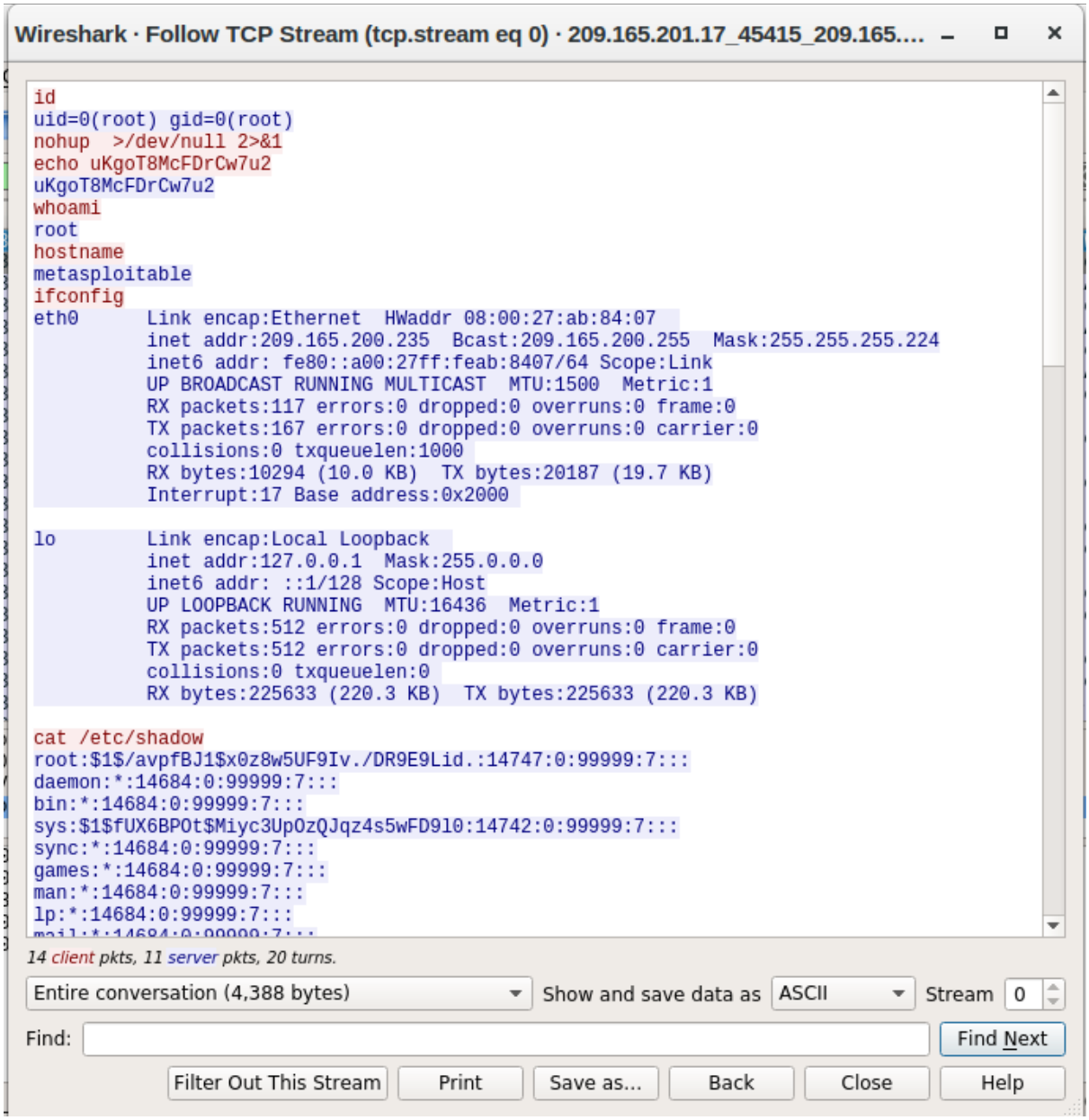
Parte 2: Passare a Wireshark (Pivoting)

Per un'analisi approfondita a livello di pacchetto, si è effettuato il *pivoting* su Wireshark partendo dall'alert 5.1 in Sguil, utilizzando la funzione "Follow TCP Stream".



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

Risposta: Il "TCP Stream" riassembla il payload della comunicazione mostrando l'esatta interazione a riga di comando. Il colore **rosso** rappresenta il traffico originato dal client (l'attore della minaccia che invia i comandi), mentre il colore **blu** rappresenta il traffico generato dal server (l'output restituito dall'host compromesso).



Domanda: Cosa rivela questo sul ruolo dell'attaccante sul computer bersaglio?

Risposta: L'output del comando id mostra uid=0(root) gid=0(root). Questo rivela che l'attaccante ha ottenuto l'escalation dei privilegi massima: opera come amministratore di sistema (root) e ha controllo totale e incontrastato sulla macchina bersaglio (hostname: *metasploitable*).

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

```
SRC: ifconfig
SRC:
DST: eth0      Link encap:Ethernet  HWaddr 08:00:27:ab:84:07
DST:           inet addr:209.165.200.235  Bcast:209.165.200.255  Mask:255.255.255.224
DST:           inet6 addr: fe80::a00:27ff:feab:8407/64 Scope:Link
DST:           UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
DST:           RX packets:117 errors:0 dropped:0 overruns:0 frame:0
DST:           TX packets:167 errors:0 dropped:0 overruns:0 carrier:0
DST:           collisions:0 txqueuelen:1000
DST:           RX bytes:10294 (10.0 KB)  TX bytes:20187 (19.7 KB)
DST:           Interrupt:17 Base address:0x2000
DST:
DST: lo        Link encap:Local Loopback
DST:           inet addr:127.0.0.1  Mask:255.0.0.0
DST:           inet6 addr: ::1/128 Scope:Host
DST:           UP LOOPBACK RUNNING  MTU:16436  Metric:1
DST:           RX packets:512 errors:0 dropped:0 overruns:0 frame:0
DST:           TX packets:512 errors:0 dropped:0 overruns:0 carrier:0
DST:           collisions:0 txqueuelen:0
DST:           RX bytes:225633 (220.3 KB)  TX bytes:225633 (220.3 KB)
DST:
DST:
```

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

Risposta: Dagli screenshot del flusso TCP emerge chiaramente che l'attore della minaccia ha esfiltrato dati critici e stabilito persistenza:

1. Ha eseguito cat /etc/passwd e cat /etc/shadow per leggere l'elenco degli utenti di sistema e rubare gli hash delle password (come evidenziato dalla riga rubata root:1/avpfBJ1...).

```
SRC: cat /etc/passwd
SRC:
DST: root:x:0:0:root:/root:/bin/bash
DST: daemon:x:1:1:daemon:/usr/sbin:/bin/sh
DST: bin:x:2:2:bin:/bin:/bin/sh
DST: sys:x:3:3:sys:/dev:/bin/sh
DST: sync:x:4:65534:sync:/bin:/bin/sync
DST: games:x:5:60:games:/usr/games:/bin/sh
```

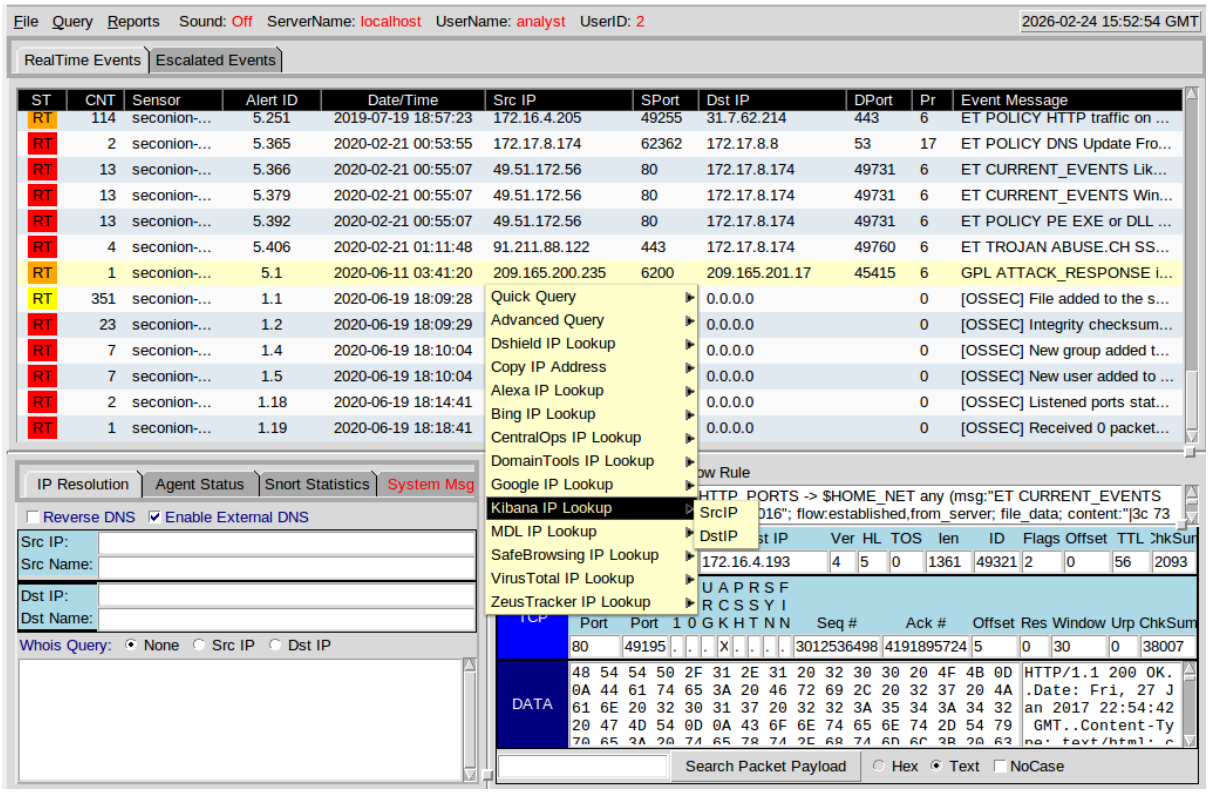
```
SRC: cat /etc/shadow
SRC:
DST: root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
DST: daemon:*:14684:0:99999:7:::
DST: bin:*:14684:0:99999:7:::
DST: sys:$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:14742:0:99999:7:::
DST: sync:*:14684:0:99999:7:::
DST: games:*:14684:0:99999:7:::
```

2. Successivamente, **ha creato una backdoor persistente**: ha usato il comando echo "myroot:x:0:0:root:/root:/bin/bash" >> /etc/passwd per inserire un nuovo utente chiamato myroot con privilegi amministrativi (UID e GID 0:0), aggiungendo poi il relativo record senza password con echo "myroot::14747:0:99999:7:::" >> /etc/shadow, garantendosi futuri accessi silenti.

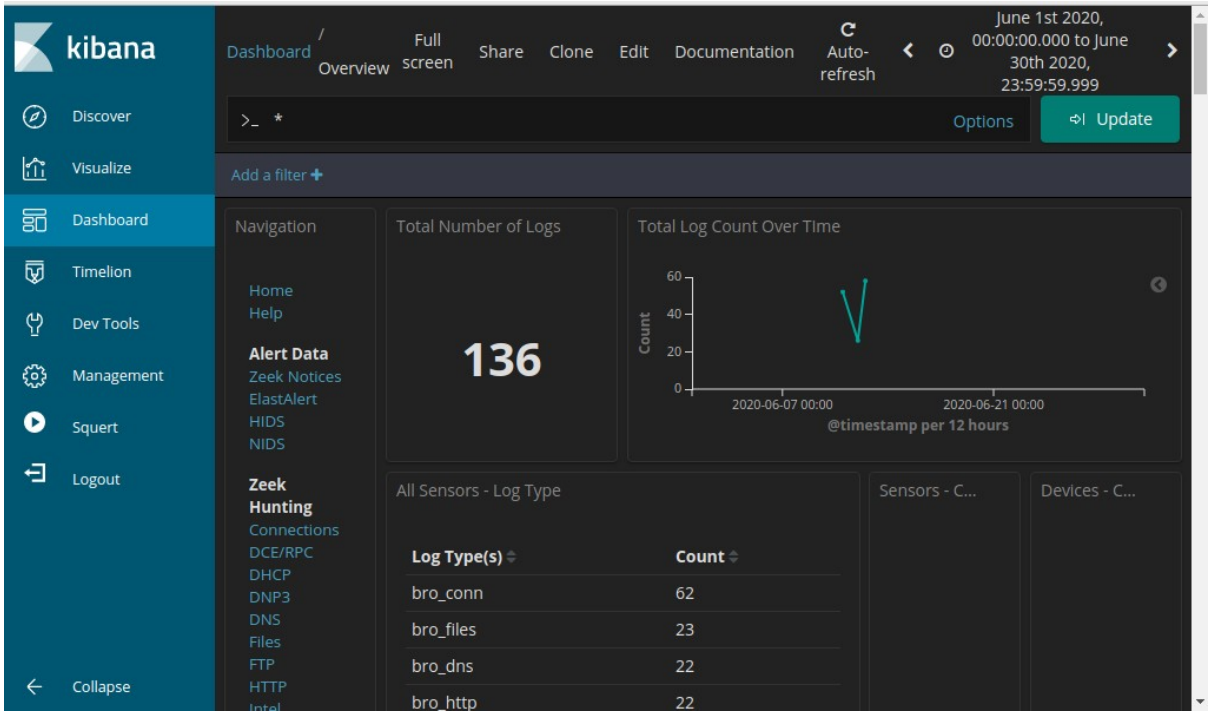
```
SRC: echo "myroot::14747:0:99999:7:::" >> /etc/shadow
SRC:
SRC: grep root /etc/shadow
SRC:
DST: root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
DST: myroot::14747:0:99999:7:::
DST:
SRC: cat /etc/passwd | grep root
SRC:
DST: root:x:0:0:root:/root:/bin/bash
DST:
SRC: echo "myroot:x:0:0:root:/root:/bin/bash" >> /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:
```

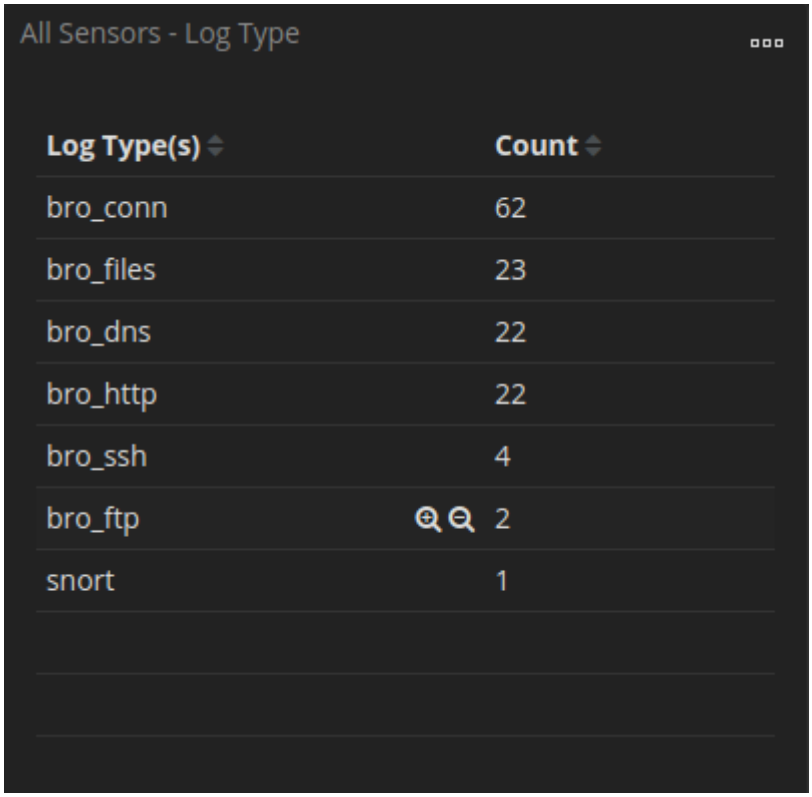
Parte 3: Passare a Kibana (Pivoting)

Per rintracciare l'esfiltrazione del file confidential.txt, si è passati a Kibana effettuando un "Kibana IP Lookup" da Sguil.



Consultando la Dashboard principale e analizzando il riepilogo per tipologia di log, sono stati identificati **136 log totali**, di cui **2 log** appartenenti alla categoria bro_ftp.

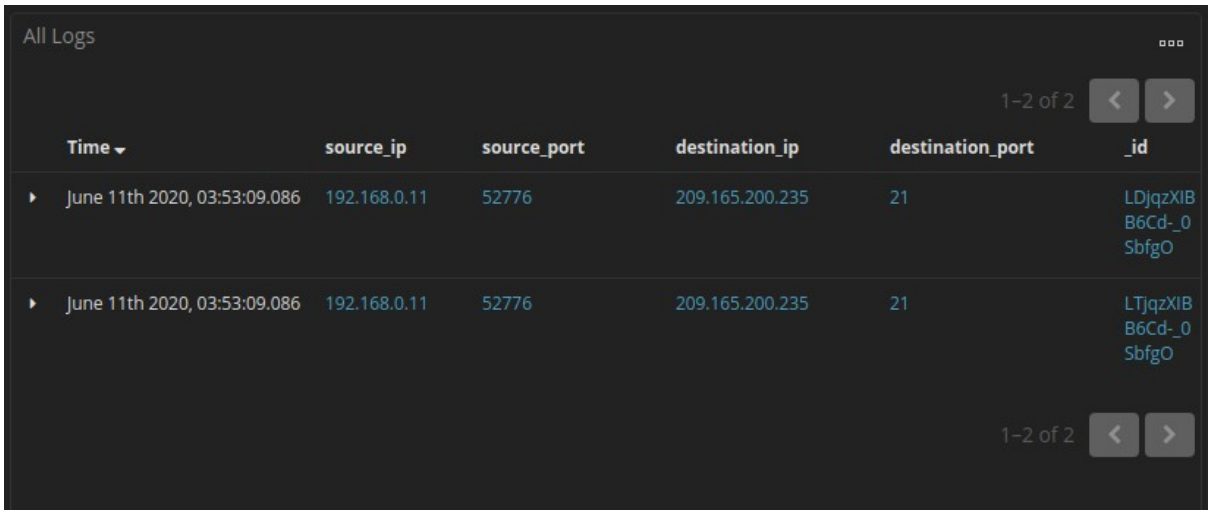




Domanda: Quali sono gli indirizzi IP e i numeri di porta di origine e destinazione per il traffico FTP?

Risposta: Analizzando i log FTP in Kibana (bro_ftp), il traffico per il furto del file è avvenuto tra:

- **IP Origine (Client Attaccante):** 192.168.0.11 (Porta effimera 52776 per il controllo, 49817 per i dati)
- **IP Destinazione (Server Compromesso):** 209.165.200.235 (Porta standard 21 per il comando, 20 per il trasferimento dati FTP_DATA).



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

Risposta: L'analisi del TCP Stream relativo alla connessione FTP verso vsFTPd 2.3.4 (visibile in Wireshark) mostra che l'attaccante ha effettuato un login valido inviando il comando USER analyst seguito da PASS cyberops. Le credenziali compromesse sono quindi **analyst / cyberops**.

```
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.
```

Proseguendo l'analisi nella dashboard "Zeek Hunting" -> "Files":

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

Risposta: Come si evince dal grafico a barre generato, i tipi MIME registrati sono: text/plain, image/jpeg, image/png, text/html, image/gif, image/x-icon.

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

Risposta: Le sorgenti (protocolli che hanno originato il trasferimento di file) elencate sono HTTP (Count 22) e FTP_DATA (Count 1). L'unica occorrenza di FTP_DATA coincide con il nostro file esfiltrato.

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:

- **MIME Type:** text/plain
- **File IP Address (Host mittente del file):** 192.168.0.11
- **Destination IP Address:** 209.165.200.235
- **Timestamp:** Il trasferimento si è verificato l'11 Giugno 2020, alle 03:53:09 UTC.

Files - MIME Type

MIME Type	Count
text/plain	1

Files - Source IP Address

File IP Address	Count
192.168.0.11	1

Files - Destination IP Address

IP Address	Count
209.165.200.235	1

Files - Logs

1–1 of 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

1–1 of 1

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

Risposta: Ispezionando il transcript della connessione FTP_DATA (ID connessione C2Jv8MWV6Xg4lbb51), il contenuto in chiaro del file confidential.txt scaricato è:

"CONFIDENTIAL DOCUMENT"

"DO NOT SHARE"

"This document contains information about the last security breach."

3. Conclusioni e Raccomandazioni Strategiche

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

Risposta:

Essendo di fronte ad un host server pienamente compromesso, le misure correttive devono essere immediate e strutturate:

1. **Isolamento dell'Host:** Disconnettere fisicamente o logicamente l'host compromesso (209.165.200.235) dal resto della rete aziendale per prevenire il movimento laterale.
2. **Rimozione della Backdoor di Sistema:** Ripulire i file critici del sistema operativo eliminando immediatamente l'account fittizio myroot creato dall'attaccante all'interno di /etc/passwd e /etc/shadow.
3. **Blocco sul Firewall (ACL):** Configurare regole di drop immediato sui dispositivi perimetrali per bloccare il traffico verso e dagli indirizzi IP utilizzati dall'attaccante (209.165.201.17 e 192.168.0.11) e bloccare la porta anomala 6200.
4. **Gestione Identità (Password Reset):** Poiché l'attaccante ha rubato il file /etc/shadow e ha mostrato di conoscere le credenziali dell'utente analyst, **tutti** gli hash delle password risultano compromessi. È tassativo forzare il reset delle password per tutti gli utenti di sistema e revocare eventuali chiavi SSH.
5. **Remediation & Rebuild:** Eliminare la vulnerabilità iniziale (aggiornando/rimuovendo il servizio vsFTPd 2.3.4 che contiene la backdoor nota). Tuttavia, considerando l'escalation totale a root, la *best practice* raccomanda di radere al suolo l'host e ricostruirlo da un backup certificato o da un'immagine sicura.