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.

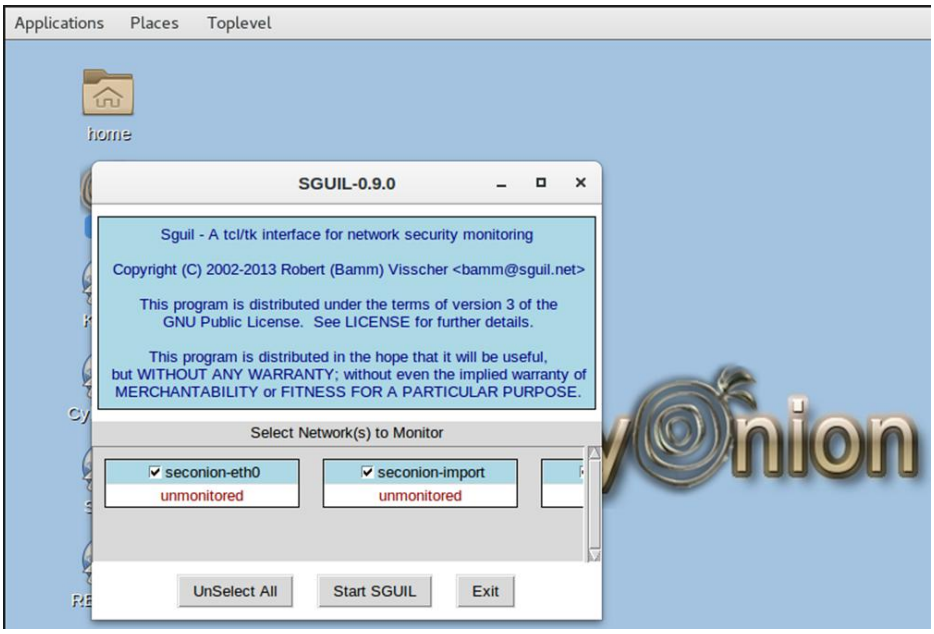
Verrà utilizzata la Macchina Virtuale CyberOps Security Onion, progettata per il monitoraggio della sicurezza di rete, il rilevamento delle intrusioni (IDS) e la gestione degli incidenti. Gli strumenti che saranno utilizzati saranno Sguil (piattaforma di Network Security Monitoring), Wireshark (analizzatore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

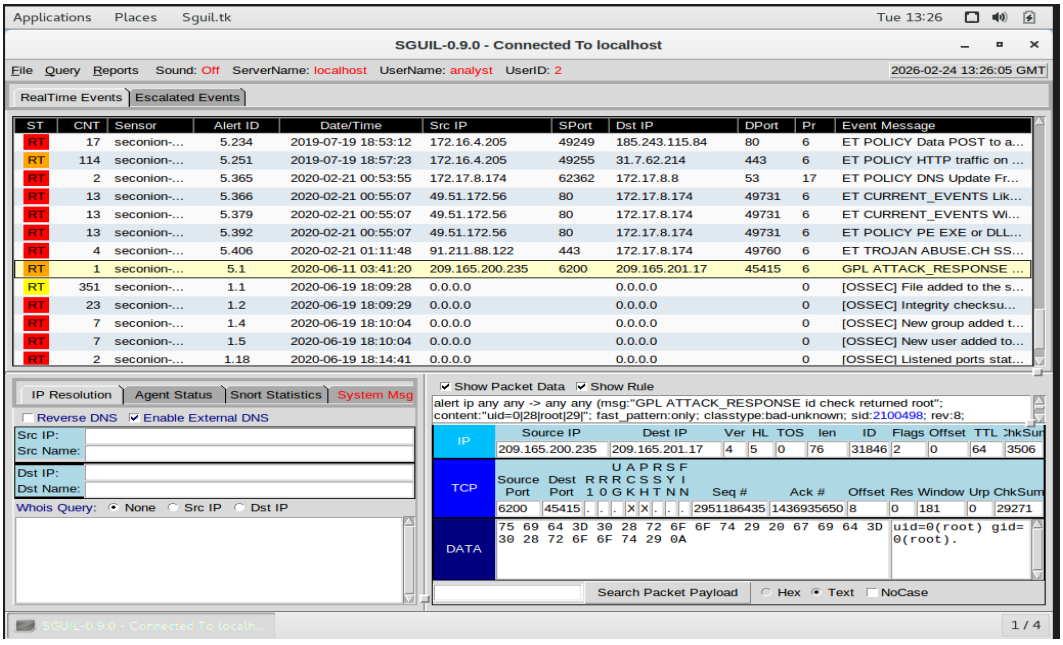
a. Viene avviata la **VM Security Onion** ed effettuato il login.
b. Si apre **Sguil** e si effettua il login. Fare clic su **Select All** per selezionare le interfacce e poi su **Start SGUIL.**



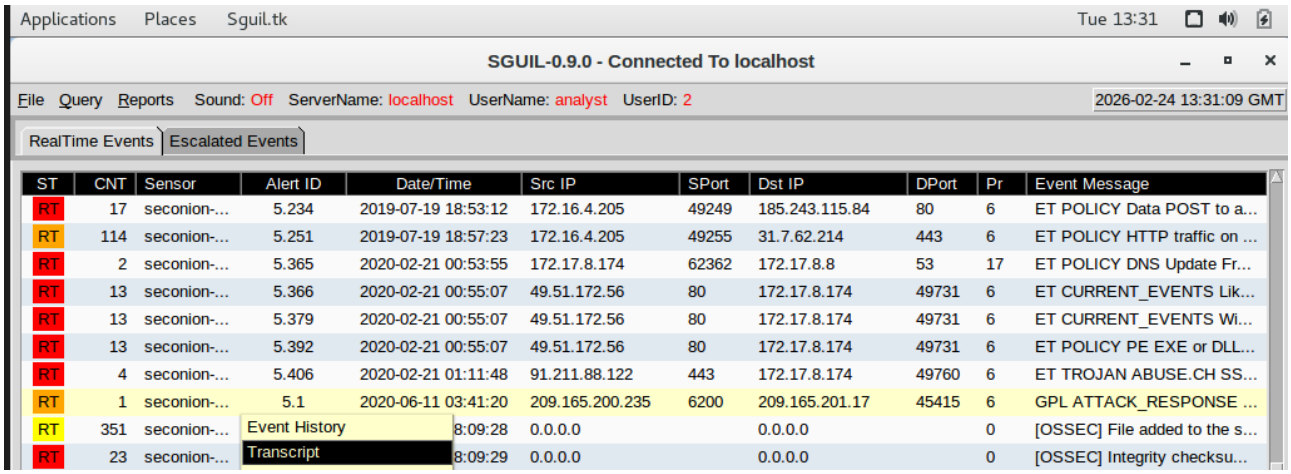
c. Si esaminano gli eventi elencati nella colonna **Event Message**. Uno di questi messaggi è **GPL ATTACK_RESPONSE id check returned root**. Questo messaggio indica che potrebbe essere stato ottenuto l'accesso root durante un attacco. L'**host 209.165.200.235** ha restituito l'accesso **root a 209.165.201.17.**

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...

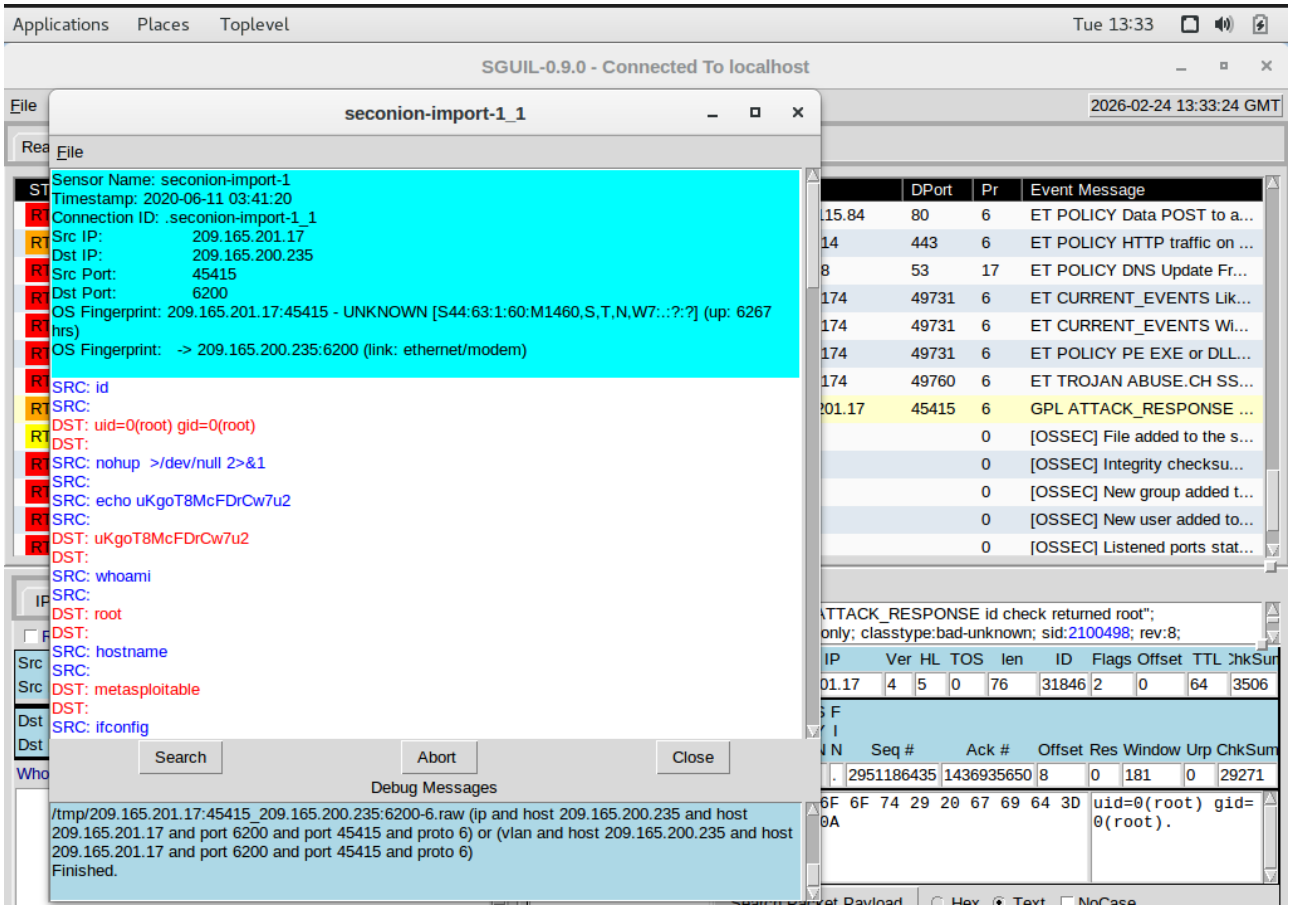
d. Si selezionano le caselle di controllo **Show Packet Data** e **Show Rule** per visualizzare ogni alert più in dettaglio

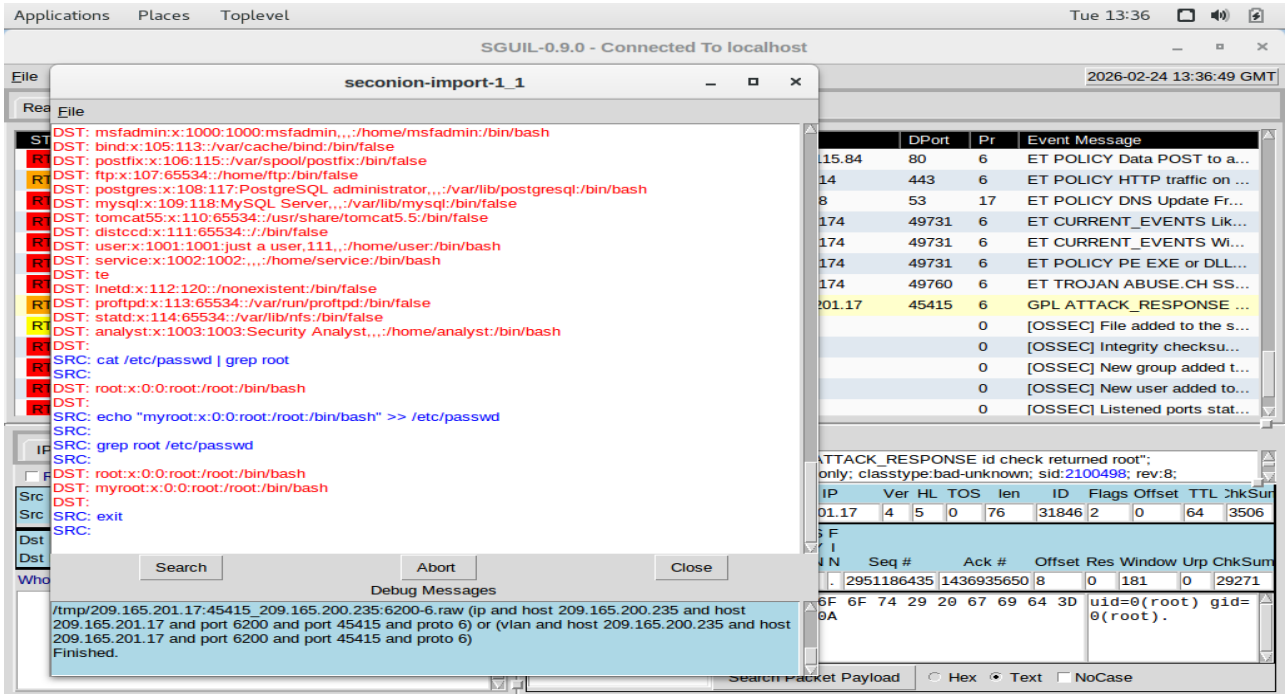


e. Si effettua il clic con il pulsante destro sull'**ID** dell'**alert 5.1** e si seleziona **Transcript**



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.





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 u**id=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**

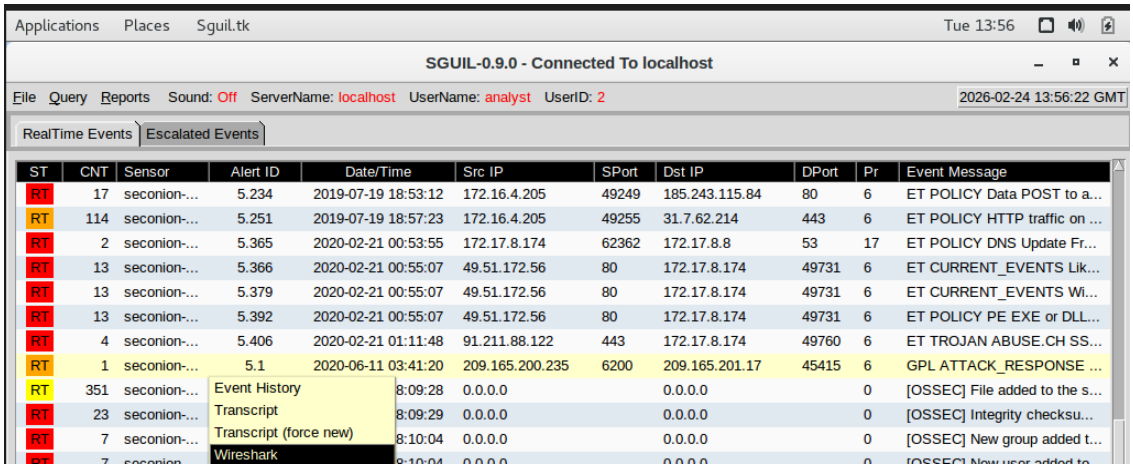
   Verifica: L'attaccante esegue nuovamente **grep root /etc/passwd** e il server mostra entrambi gli utenti: **root** e il nuovo **myroot**.

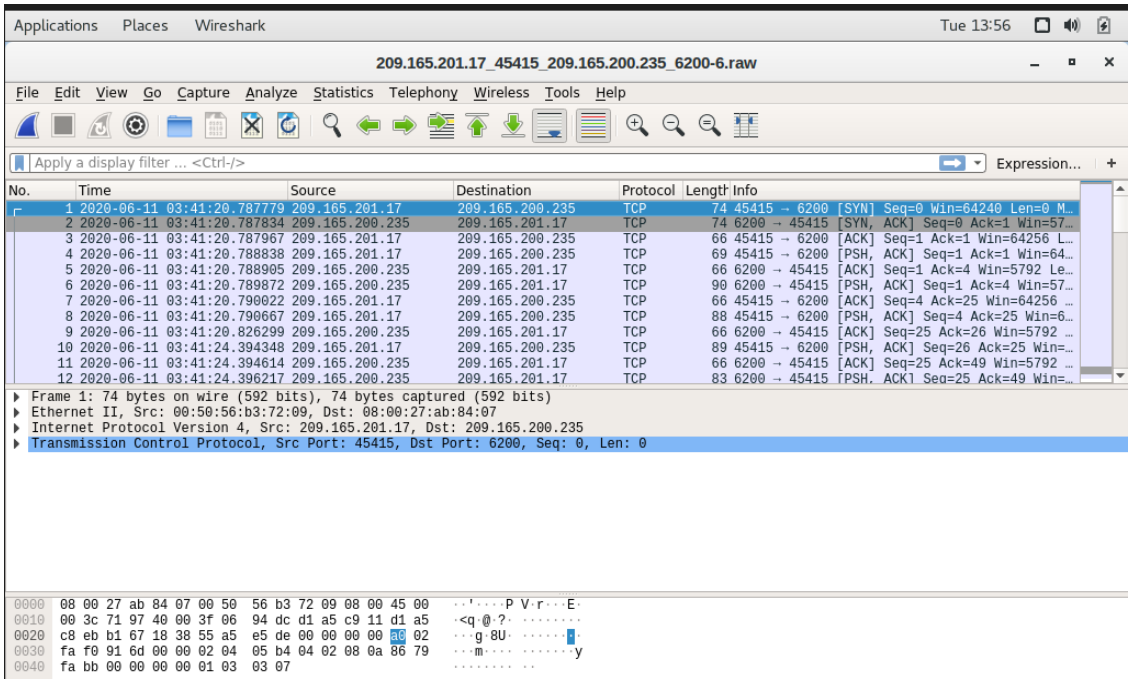
Uscita: L'attaccante digita exit per chiudere la sessione corrente, lasciando però la backdoor attiva nel file **passwd.**

Parte 2: Passare a Wireshark

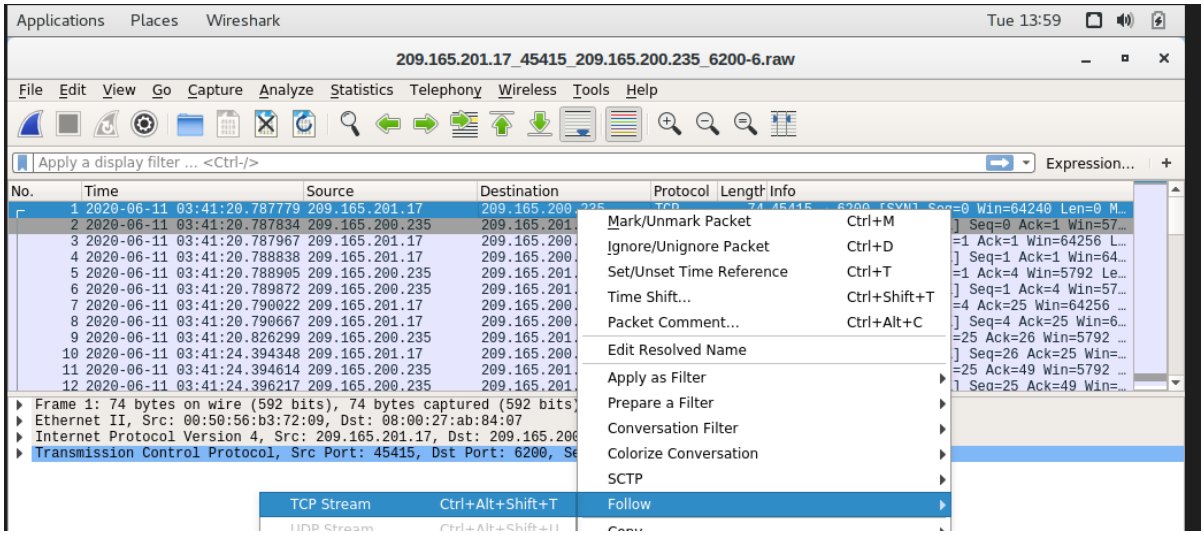
Istruzioni

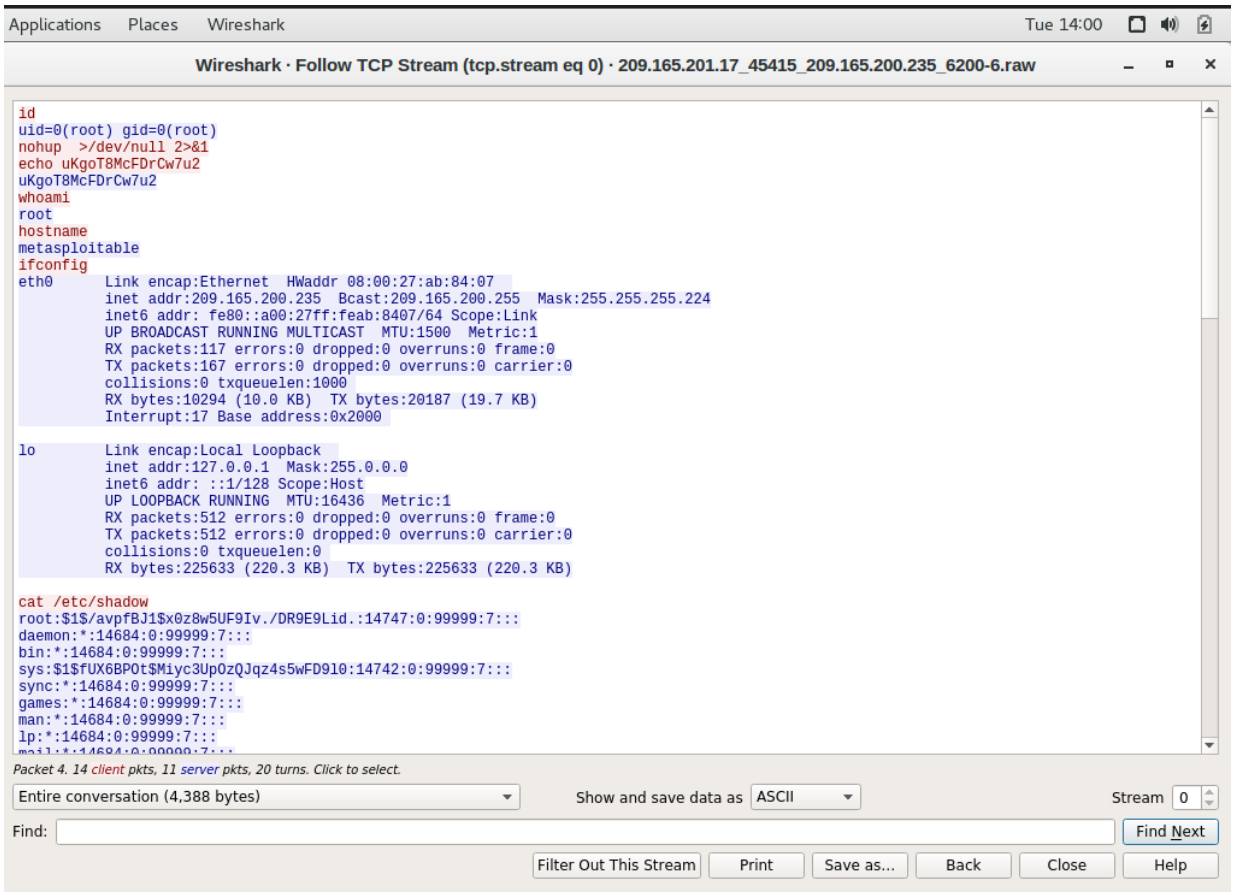
a. Si seleziona l'alert che ha fornito la trascrizione nel passo precedente. Effettua il clic con il pulsante destro sull'**ID dell'alert 5.1** e seleziona **Wireshark**. La finestra principale di **Wireshark** mostra tre viste di un pacchetto.





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?

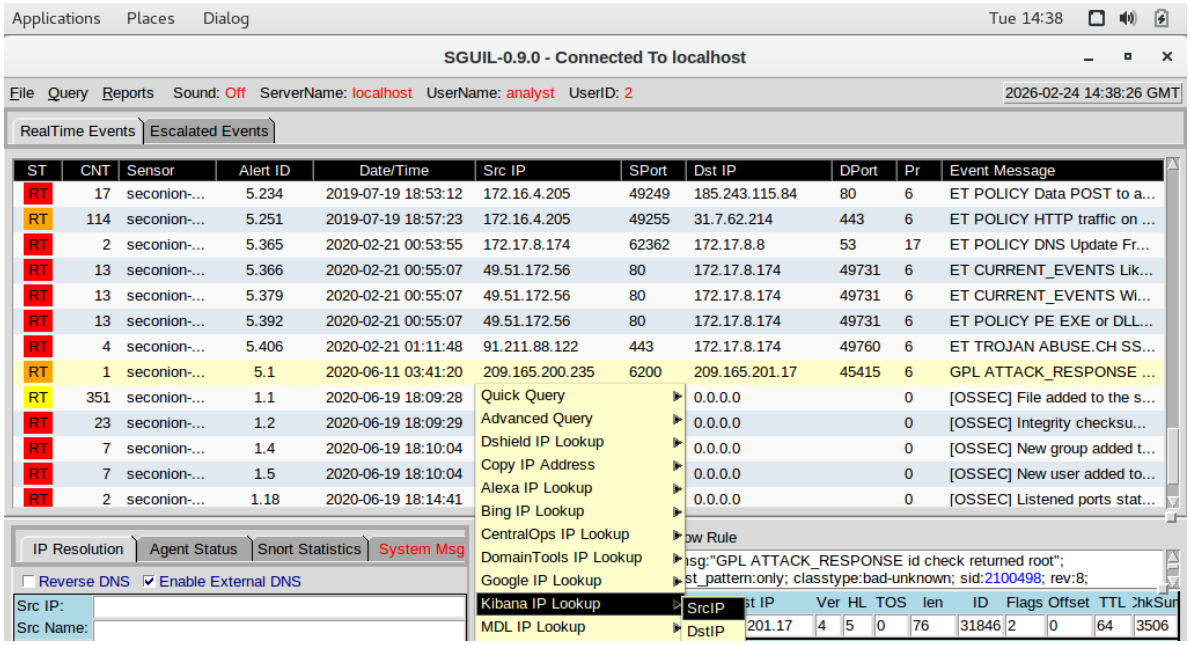
I dati letti dall'attore della minaccia sono:

- Identità e privilegi dell'utente, confermando di operare come root
- Configurazioni di rete e host, tramite i comandi **hostname** e **ifconfing** 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.

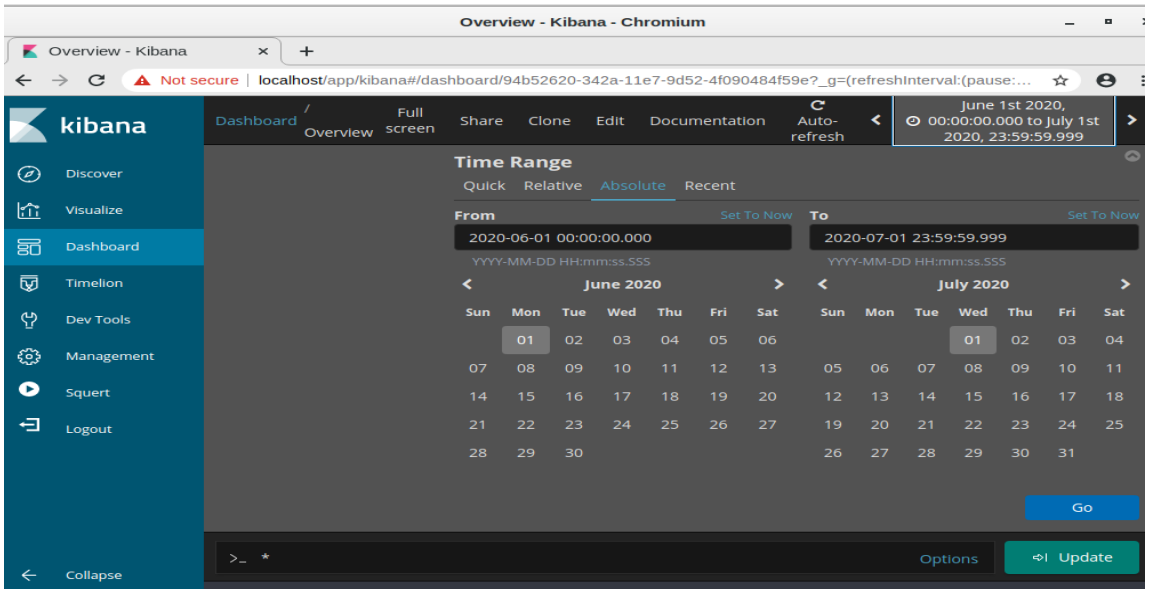
Parte 3: Passare a Kibana

Istruzioni

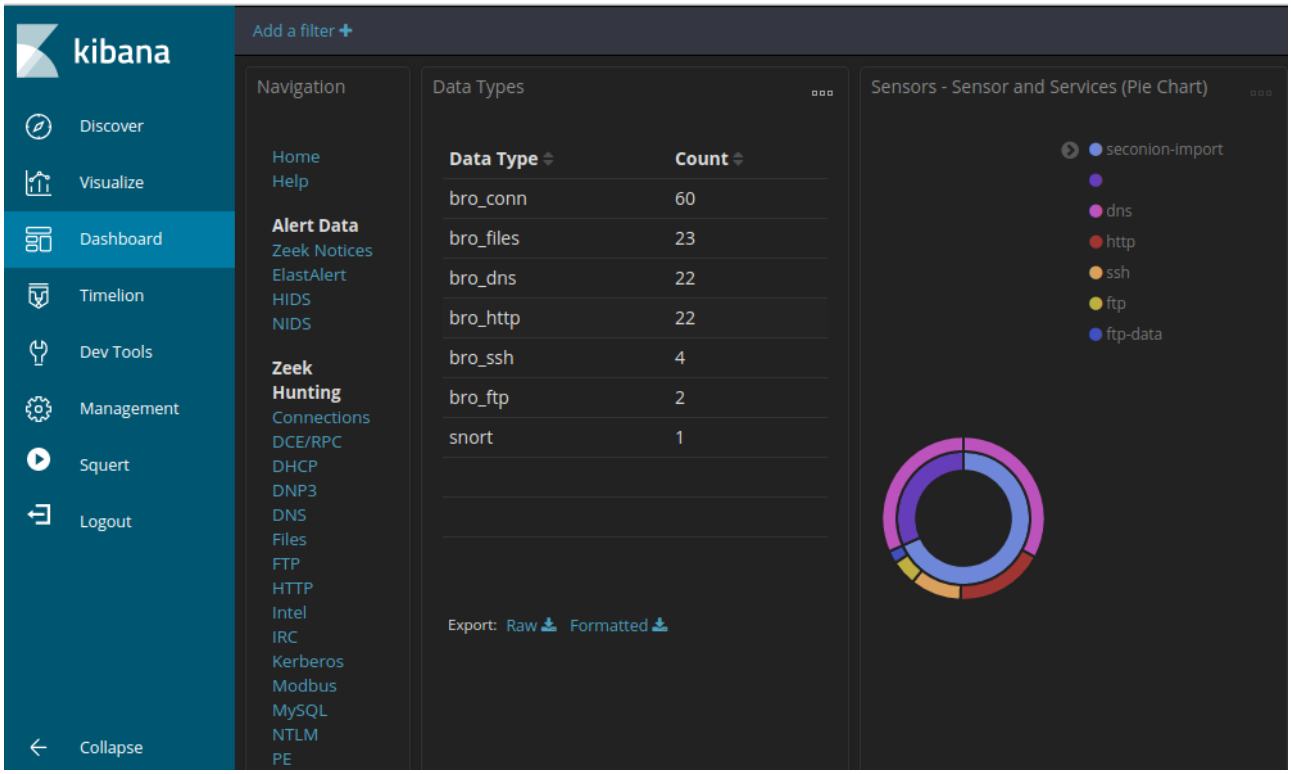
a. Si torna a **Sguil**. Si fa clic con il pulsante destro sull'indirizzo IP di origine o di destinazione per l'**ID dell'alert 5.1** e si seleziona **Kibana IP Lookup > SrcIP.**



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.

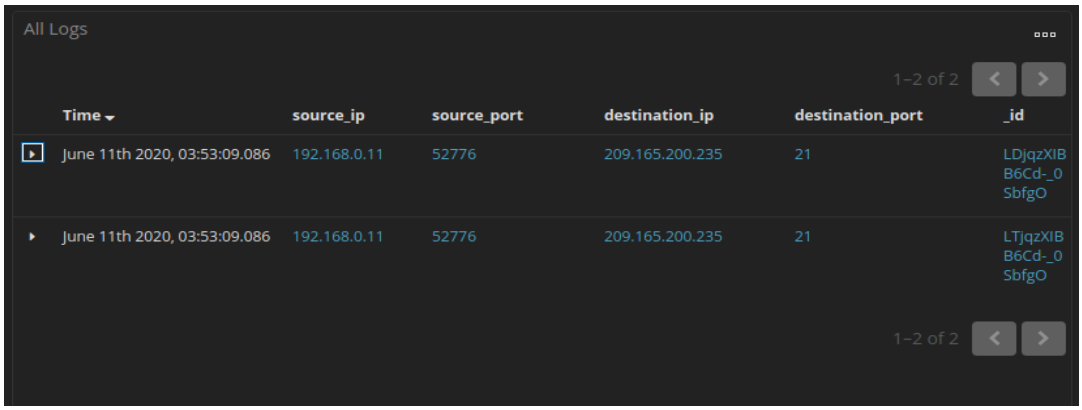


c. Nei risultati visualizzati, c'è un elenco di diversi tipi di dati. Ti è stato detto che il file confidential.txt non è più accessibile. Nel grafico a torta "**Sensors - Sensors and Services**", sono presenti **ftp** e **ftp-data**. Determineremo se **FTP** è stato usato per rubare il file.



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**

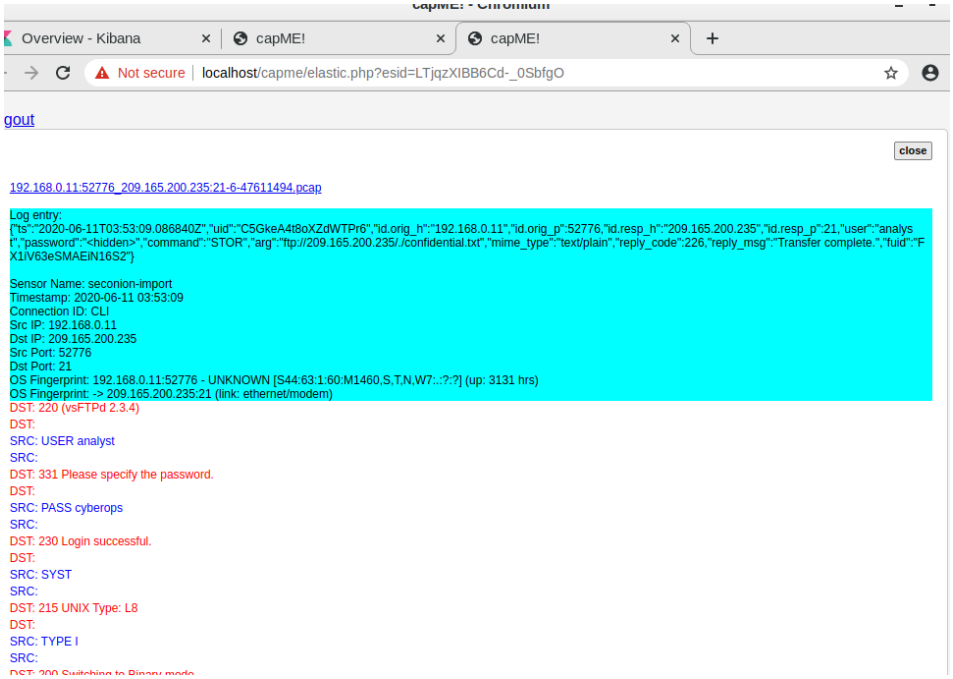
e. Si scorre verso il basso fino a **All Logs**. Ci sono due voci elencate.



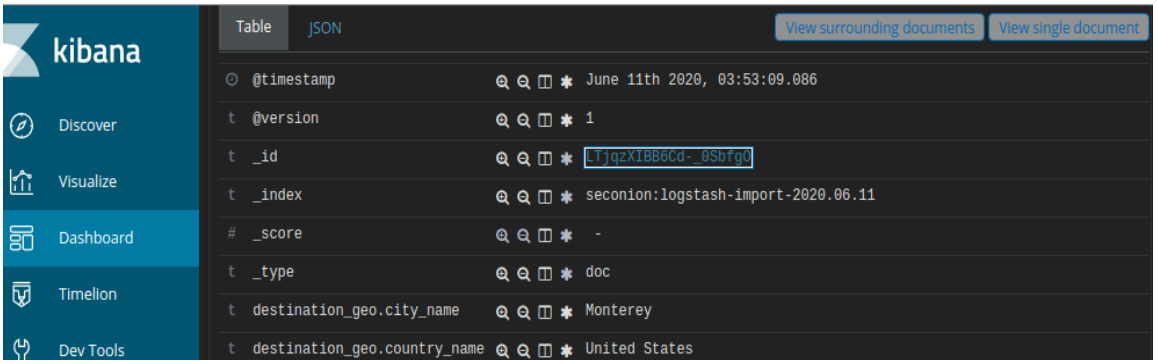
Quali sono gli indirizzi IP e i numeri di porta di origine e destinazione per il traffico FTP?

Ip di origine (**source_ip**) **192.168.0.11**, porta **52776**
Ip di destinazione (**destination_ip**) **209.165.200.225**, porta **21**

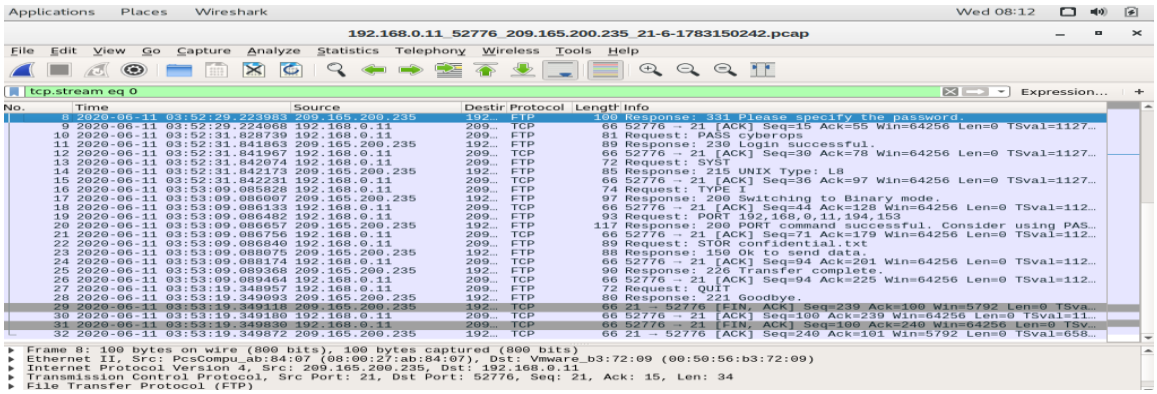
f. Si espande e si esaminano entrambe le voci di log. In una di queste voci, il campo **ftp_argument** ha una voce di **ftp://209.165.200.235/./confidential.txt.** Si esamina anche il messaggio nella voce di log per saperne di più su questo evento



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



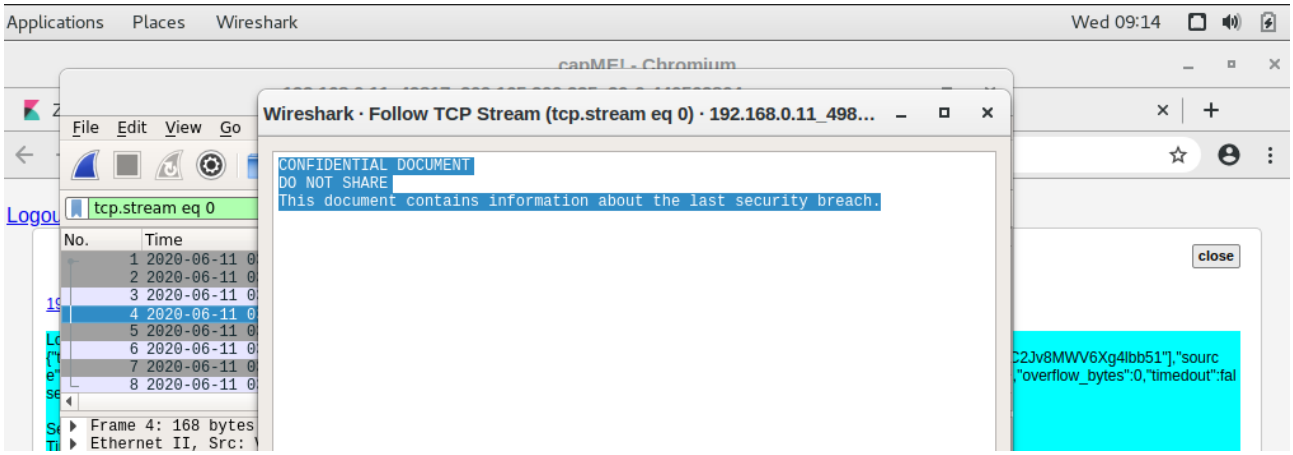
h. Si esamina la trascrizione per le transazioni tra l'attaccante e il bersaglio. Si scarica il pcap per esaminare il traffico usando **Wireshark.**



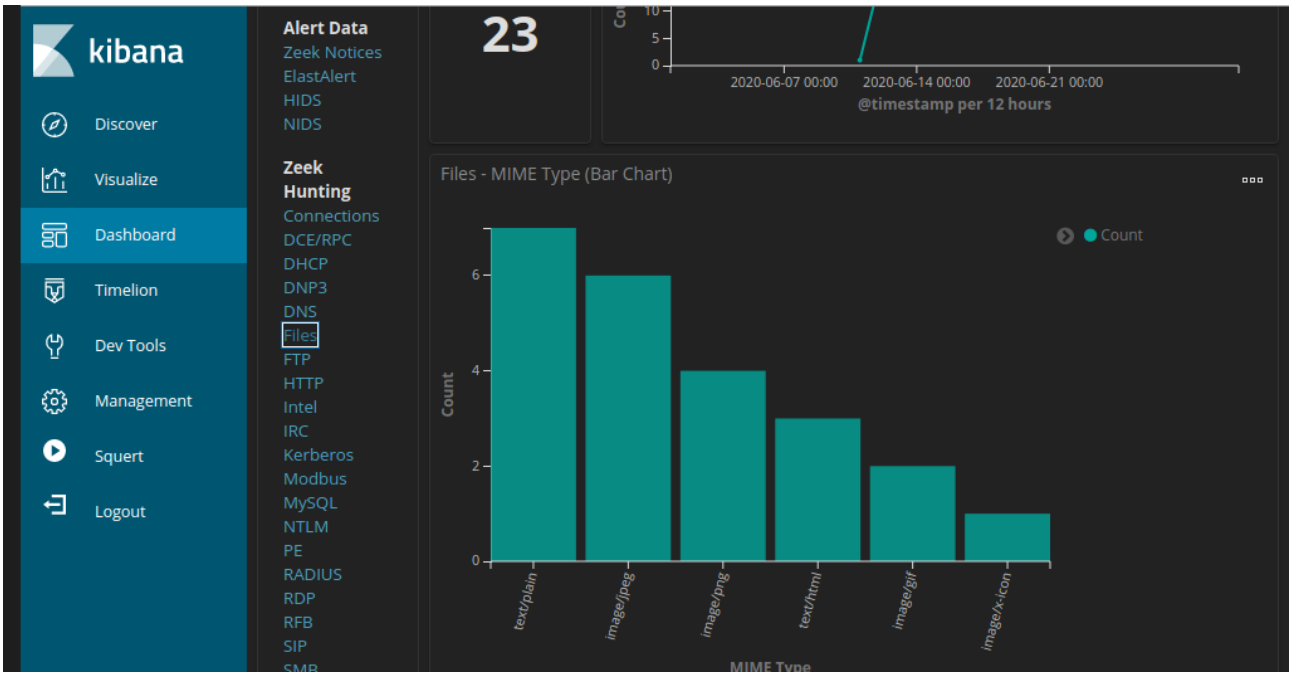
Quali sono le credenziali utente per accedere al sito FTP?

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 [...]”

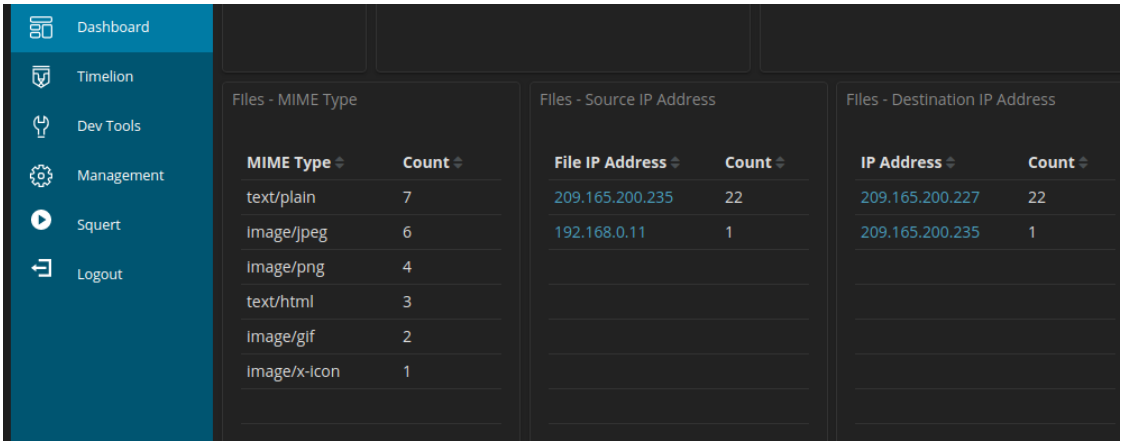


j. Si naviga in cima alla dashboard. Si seleziona **Files** sotto l'intestazione **Zeek Hunting** nel pannello di sinistra

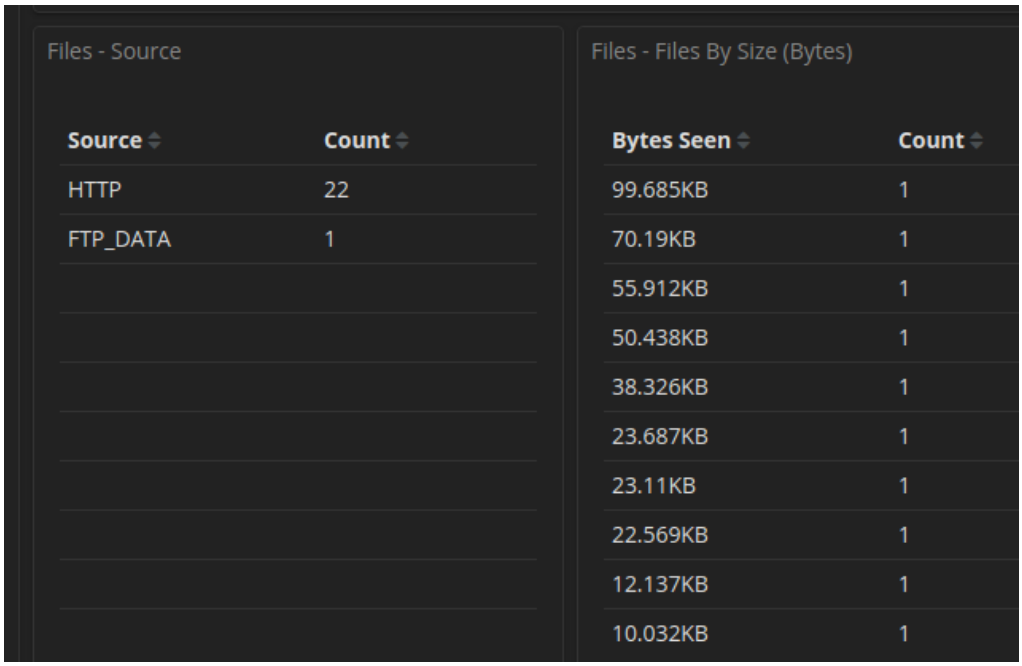


Quali sono i diversi tipi di file? Guarda la sezione MIME Type dello schermo. Scorri fino all'intestazione Files - Source.
Quali sono le sorgenti dei file elencate?

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



Le sorgenti (**File -Source**) sono **HTTP** e **FTP_DATA**



Files - Source

Source	Count
HTTP	22
FTP_DATA	1

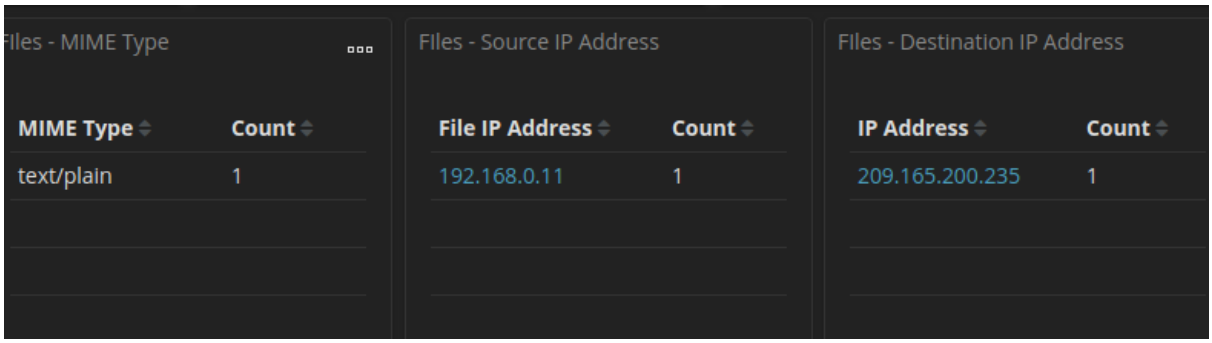
Files - Files By Size (Bytes)

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 **+**

l. 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 i**p di origine è 192.168.0.11** e indirizzo **ip di destinazione è 209.165.200.235**



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

Quando si è verificato questo trasferimento?

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

1–1 of 1

Time	file_ip	destination_ip	source	uid	fuid	_id
June 11th 2020, 03:53:09.088	192.16 1	209.165.200.235	FTP_DATA	C2Jv8MWV6X g4lbb51	FX1iV63eSMA EiN16S2	KDJqzXIBB6Cd -_0SVfiy

1–1 of 1

m. Nei log dei file, espandi la voce associata ai dati FTP. Fai clic sul link associato all'a**lert _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 [...]”

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.