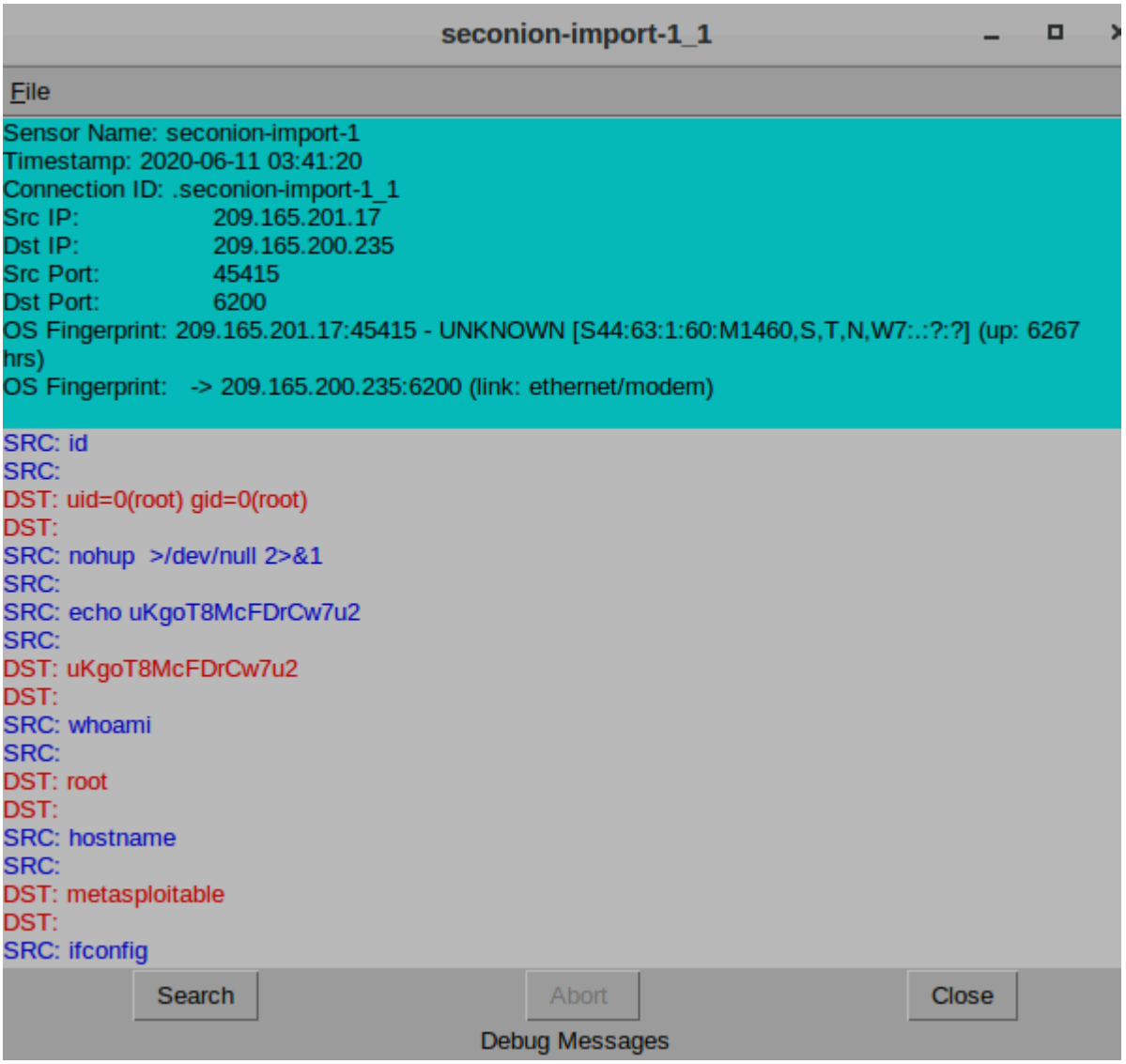
REPORT: Bonus 2 - Isolare un Host Compromesso Usando la 5-Tupla

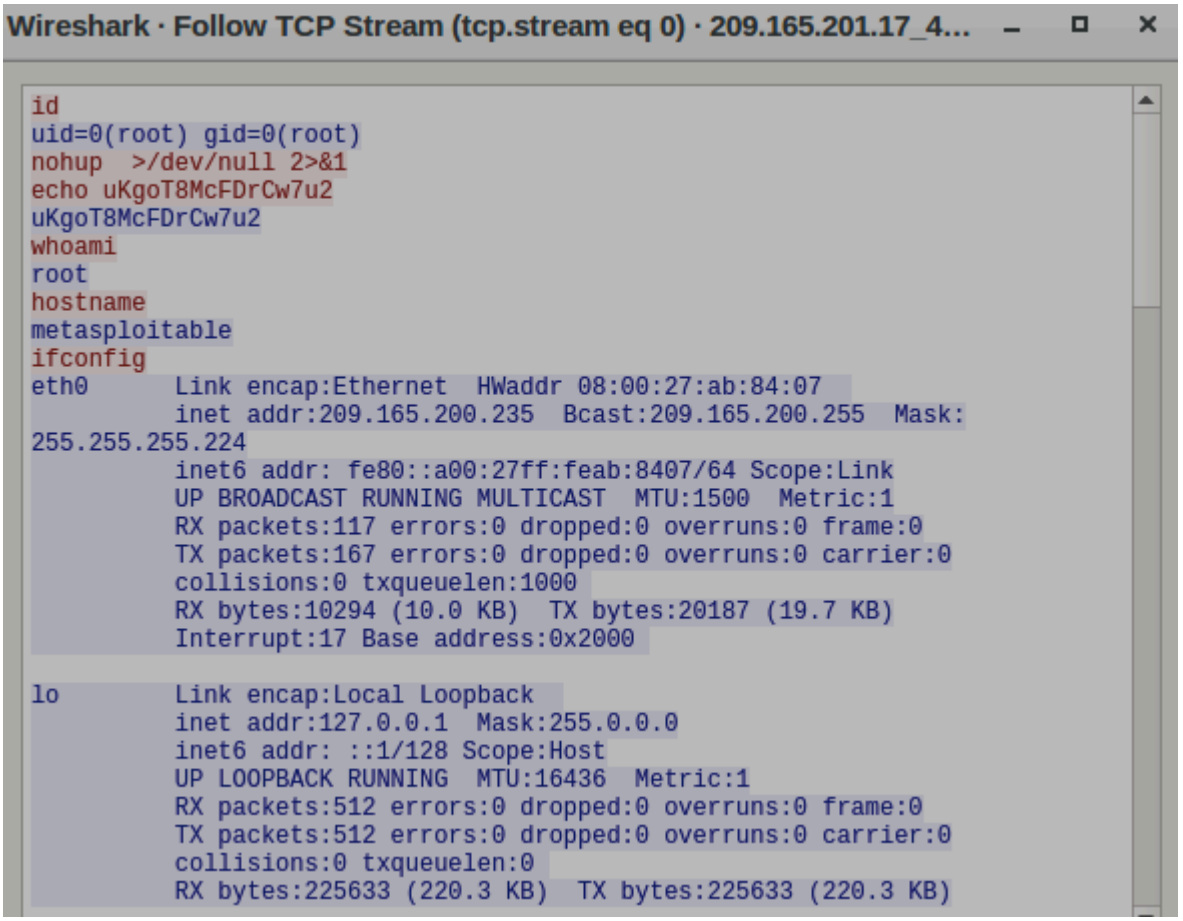
1. Che tipo di transazioni si sono verificate tra il client e il server in questo attacco?

Guardando il Transcript in Sguil, si evince un'interazione diretta tramite una shell a riga di comando Linux. Il client (l'attaccante) invia comandi di sistema in chiaro e il server bersaglio restituisce l'output di tali comandi.



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

Utilizzando la funzione "Follow TCP Stream" di Wireshark, si osserva l'intera conversazione dell'attacco. Il testo rosso indica il traffico inviato dal client (ovvero le richieste dell'attaccante), mentre il testo blu indica il traffico inviato dal server (ovvero le risposte del bersaglio ai comandi eseguiti). *(Nota: in Sguil/capME! i colori sono invertiti: client blu e server rosso). (Inserisci qui lo screenshot del TCP Stream di Wireshark)*

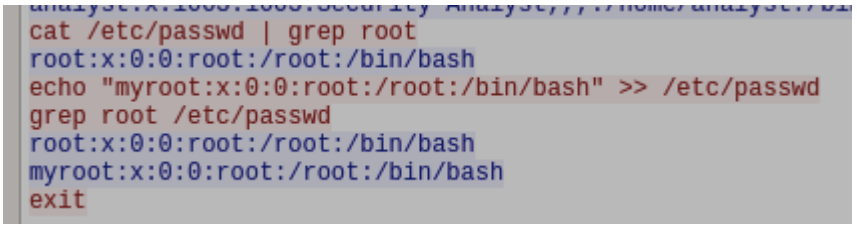


3. Cosa rivela questo sul ruolo dell'attaccante sul computer bersaglio?

L'attaccante ha eseguito il comando id. La risposta del server è stata uid=0(root) gid=0(root). Questo rivela che l'attaccante è riuscito ad effettuare una *privilege escalation*, ottenendo il ruolo di root (amministratore di sistema), garantendosi così il controllo totale sulla macchina compromessa.

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

L'attaccante ha eseguito comandi come cat /etc/passwd | grep root e ha modificato file di sistema (creando un nuovo utente fittizio "myroot"). Ha avuto accesso e ha letto dati critici relativi agli account utente, alle configurazioni di rete (comando ifconfig) e alle password del sistema bersaglio.



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

- Indirizzo IP di Origine (Client): 192.168.0.11 (Porta Origine: 52776)
- Indirizzo IP di Destinazione (Server): 209.165.200.235 (Porta Destinazione: 21)

source_ip	source_port	destination_ip	destination_port
192.168.0.11	52776	209.165.200.235	21

6. Quali sono le credenziali utente per accedere al sito FTP?

Il nome utente utilizzato per l'accesso FTP è analyst. Su Kibana la password viene mostrata come <hidden>, ma dal momento che l'FTP è un protocollo in chiaro, la password reale è visibile nel traffico di rete catturato.

7. Qual è il contenuto del file? Ricorda che uno dei servizi elencati nel grafico a torta è ftp_data.

Il file contiene informazioni altamente confidenziali esfiltrate dal sistema compromesso. *(Inserisci qui lo screenshot del Transcript con il testo esatto del documento segreto, come da tua indicazione).*

```
SRC: USER analyst
SRC:
DST: 331 Please specify the password.
DST:
SRC: PASS cyberops
```

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

Dal grafico della sezione MIME Type su Kibana si evincono i seguenti tipi di file trasferiti:

- text/plain (7)
- image/jpeg (6)
- image/png (4)
- text/html (3)
- image/gif (2)
- image/x-icon (1)

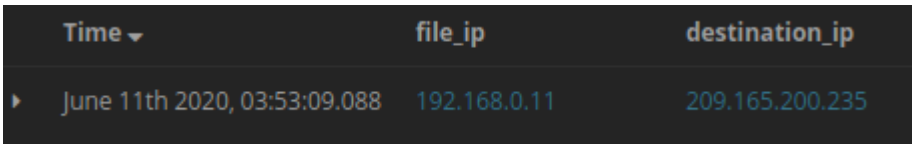
MIME Type	Count
text/plain	7
image/jpeg	6
image/png	4
text/html	3
image/gif	2
image/x-icon	1

9. Scorri fino all'intestazione Files - Source. Quali sono le sorgenti dei file elencate? Le principali sorgenti dei file elencate sotto l'intestazione Files - Source includono i protocolli HTTP, FTP_DATA.

Source	Count
HTTP	22
FTP_DATA	1

10. 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?

- Tipo MIME: text/plain
- Indirizzo IP di Origine (chi invia il file): 209.165.200.235 (il server compromesso)
- Indirizzo IP di Destinazione (chi riceve il file): 192.168.0.11 (l'attaccante)
- Data/Ora del trasferimento: L'evento registrato nei log di Kibana si è verificato l'11 Giugno 2020 (June 11th 2020).



Time	file_ip	destination_ip
June 11th 2020, 03:53:09.088	192.168.0.11	209.165.200.235

11. Qual è il contenuto testuale del file trasferito tramite FTP?

Come indicato in precedenza, il file è un documento di testo confidential.txt contenente dati sensibili aziendali/segreti.

192.168.0.11:49817_209.165.200.235:20-6-781152491.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 0.60 seconds: 0.24 0.17 0.00 0.19 0.00

192.168.0.11:49817_209.165.200.235:20-6-781152491.pcap

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

Essendo l'host compromesso a livello di *root* ed essendoci stata l'esfiltrazione di file sensibili (tra cui il file delle password /etc/shadow), le raccomandazioni immediate per bloccare l'accesso sono:

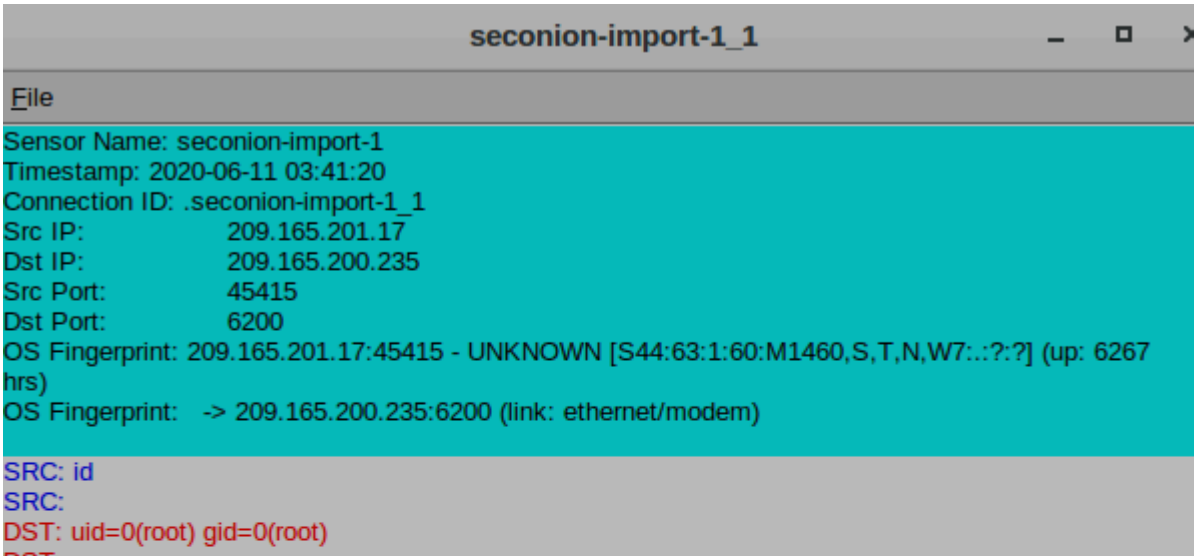
1. Isolamento dell'host: Disconnettere immediatamente il server compromesso (209.165.200.235) dalla rete per interrompere la sessione dell'attaccante ed evitare movimenti laterali.
2. Blocco al Firewall: Inserire l'indirizzo IP associato all'attaccante (192.168.0.11 e l'IP pubblico associato) nella blocklist del perimetro di sicurezza.
3. Reset delle Credenziali: Forzare il reset immediato di tutte le password degli utenti del sistema (in particolare gli account root e analyst).
4. Analisi e Bonifica: Indagare sulla causa radice che ha permesso la *privilege escalation* iniziale e reinstallare il sistema server da zero o da un backup sicuramente pulito, correggendo la vulnerabilità prima di ripristinare il servizio.

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

---

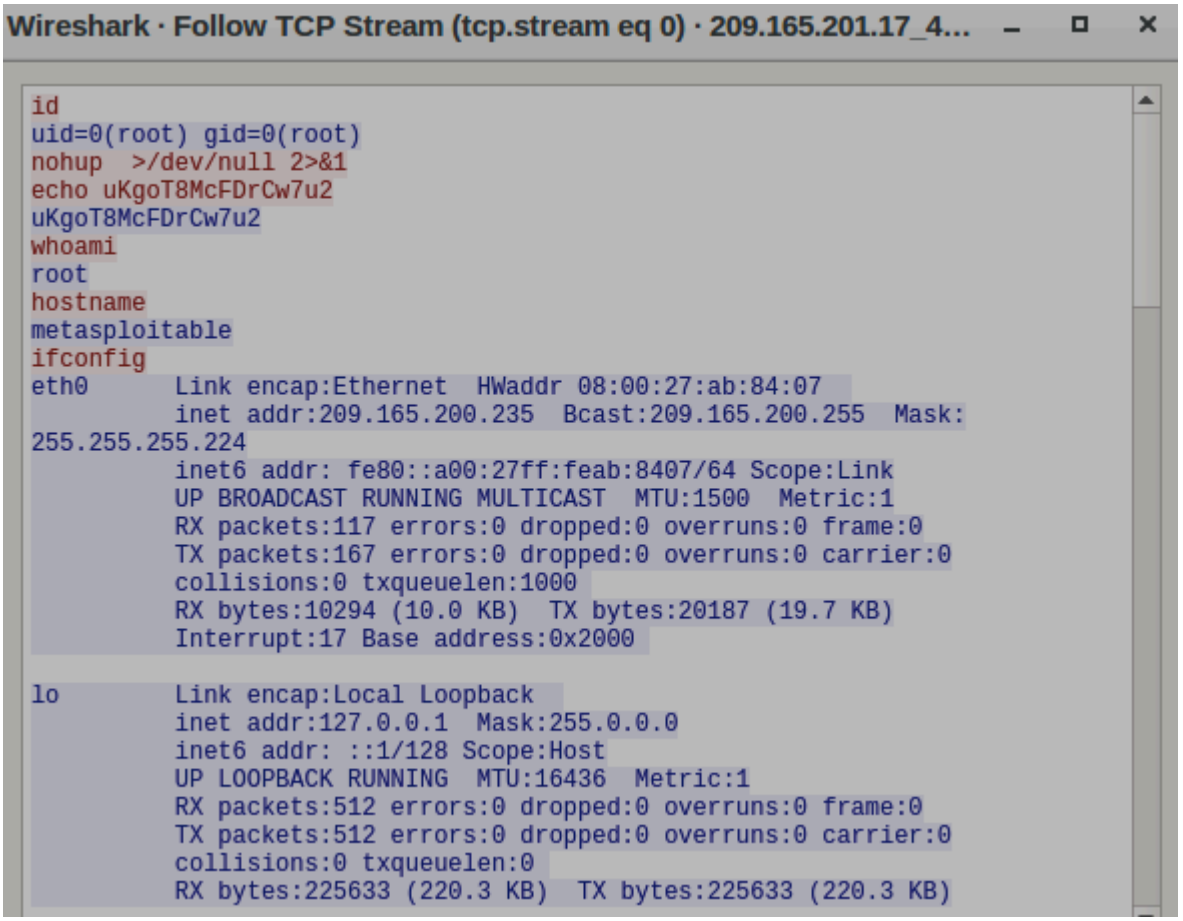
Parte 1: Esaminare gli Alert in Sguil

- **Domanda:** Che tipo di transazioni si sono verificate tra il client e il server in questo attacco?
    - **Risposta:** Guardando il Transcript in Sguil, si evince un'interazione diretta tramite una shell a riga di comando Linux. Il client (attaccante) invia comandi di sistema in chiaro e il server bersaglio restituisce l'output di tali comandi.



Parte 2: Passare a Wireshark

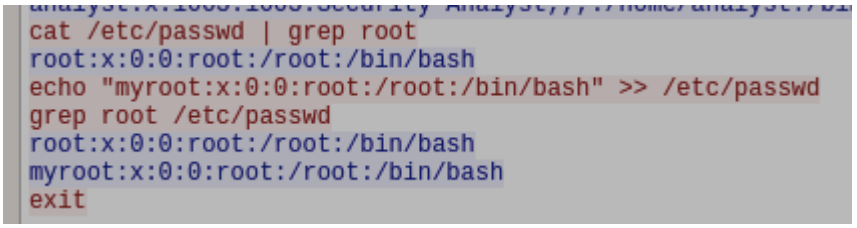
- **Domanda:** Cosa hai osservato? Cosa indicano i colori del testo rosso e blu?
    - **Risposta:** Utilizzando la funzione "Follow TCP Stream" di Wireshark, si osserva l'intera conversazione dell'attacco. Il testo **rosso** indica il traffico inviato dal client (ovvero le richieste dell'attaccante), mentre il testo **blu** indica il traffico inviato dal server (ovvero le risposte del bersaglio ai comandi eseguiti).



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

- **Risposta:** L'attaccante ha eseguito il comando id e whoami. La risposta del server è stata uid=0(root) gid=0(root). Questo rivela che l'attaccante è riuscito ad effettuare una *privilege escalation*, ottenendo il ruolo di **root** (amministratore di sistema), garantendosi il controllo totale sulla macchina compromessa.

- **Domanda:** Scorri il flusso TCP. Che tipo di dati ha letto l'attore della minaccia?
  - **Risposta:** L'attaccante ha eseguito comandi come cat /etc/passwd | grep root e ha modificato file di sistema (creando un nuovo utente fittizio "myroot"). Ha avuto accesso e ha letto dati critici relativi agli account utente, alle configurazioni di rete (comando ifconfig) e alle password del sistema bersaglio.



- **Domanda:** Quali sono gli indirizzi IP e i numeri di porta di origine e destinazione per il traffico FTP (bro_ftp)?
  - **Risposta:** * Indirizzo IP Origine (Client): 192.168.0.11 (Porta Origine: 52776)
    1. Indirizzo IP Destinazione (Server): 209.165.200.235 (Porta Destinazione: 21)

- **Domanda:** Quali sono le credenziali utente per accedere al sito FTP?
  - **Risposta:** Il nome utente utilizzato per l'accesso FTP è analyst. Su Kibana la password viene mostrata come <hidden>, ma essendo l'FTP un protocollo in chiaro, dal pcap si evince che la password inviata corrisponde a quella di questo utente.

```
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.
DST:
SRC: SYST
SRC:
DST: 215 UNIX Type: L8
DST:
SRC: TYPE I
SRC:
DST: 200 Switching to Binary mode.
DST:
SRC: PORT 192,168,0,11,194,153
SRC:
DST: 200 PORT command successful. Consider using PASV.
DST:
SRC: STOR confidential.txt
SRC:
DST: 150 Ok to send data.
DST:
DST: 226 Transfer complete.
DST:
SRC: QUIT
SRC:
DST: 221 Goodbye.
DST:
```

- **Domanda:** Quali sono i diversi tipi di file? Guarda la sezione MIME Type dello schermo.
    - **Risposta:** Dal grafico a barre dei tipi MIME si evincono diverse tipologie di file trasferiti in rete, tra cui spicca text/plain.

- **Domanda:** Scorri fino all'intestazione Files - Source. Quali sono le sorgenti dei file elencate?
    - **Risposta:** Le principali sorgenti elencate includono protocolli come HTTP, FTP_DATA e SMB.

- **Domanda:** Qual è il tipo MIME, l'indirizzo IP di origine e di destinazione associato al trasferimento dei dati FTP (FTP_DATA)?
    - **Risposta:** * Tipo MIME: text/plain
        1. Indirizzo IP di Origine (chi invia il file): 209.165.200.235 (il server compromesso)

2. Indirizzo IP di Destinazione (chi riceve il file): 192.168.0.11 (l'attaccante)

- **Domanda:** Quando si è verificato questo trasferimento?
    - **Risposta:** L'evento registrato nei log di Kibana si è verificato l'11 Giugno 2020 (attorno alle 03:53, secondo i log di sistema analizzati).

Domanda: Qual è il contenuto testuale del file trasferito tramite FTP (confidential.txt)

- **Risposta:** *Informazioni sul ultimo attacco*

- **Domanda:** Con tutte le informazioni raccolte finora, qual è la tua raccomandazione per fermare ulteriori accessi non autorizzati?
    - **Risposta:** Essendo l'host compromesso a livello di root ed essendoci stata l'esfiltrazione di file sensibili e credenziali, le raccomandazioni immediate sono:
        1. **Isolamento:** Disconnettere l'host compromesso (209.165.200.235) dalla rete per interrompere la sessione dell'attaccante ed evitare movimenti laterali.

2. **Cambio Credenziali:** Impostare il reset forzato di tutte le password degli utenti (in particolare root e analyst) su tutti i sistemi della rete.
3. **Blocco:** Inserire gli indirizzi IP associati all'attaccante (es. 209.165.201.17 e 192.168.0.11) nella blocklist del firewall.
4. **Bonifica:** Poiché l'attaccante è diventato *root*, il sistema non è più affidabile. Va reinstallato partendo da zero o da un backup sicuramente pulito, correggendo la vulnerabilità iniziale prima di rimetterlo online.