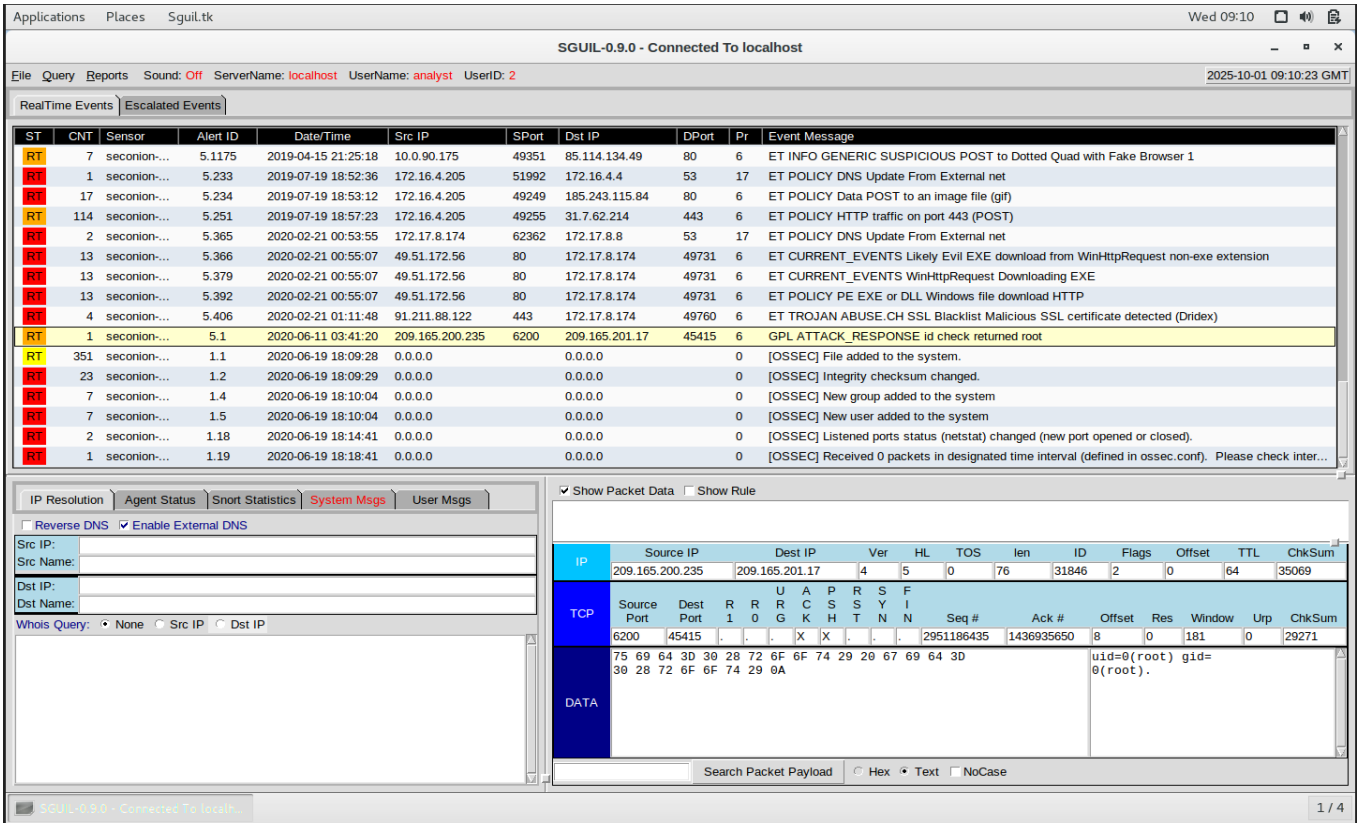
BUILD WEEK III

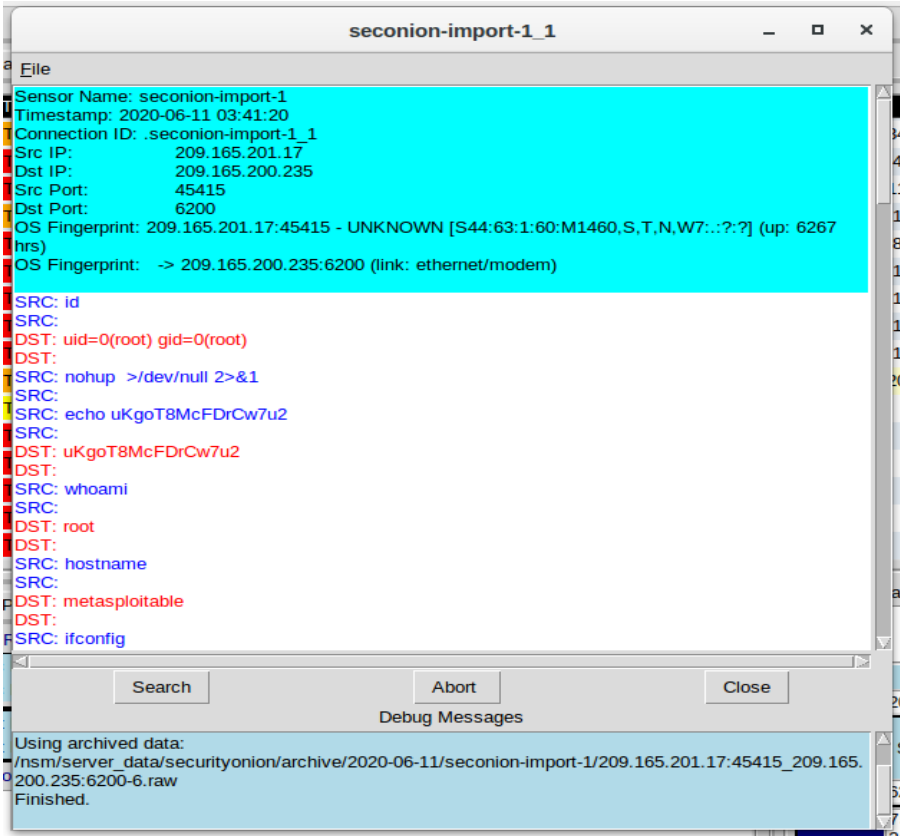
"Bonus 2: Isolare un Host Compromesso Usando la 5-Tupla"

PARTE I - SGUIL

Come da traccia andremo ad esaminare, dopo aver avviato CyberOps Security Onion, l'attacco e risponderemo alle domande:



-avvio di Sguil e ricerca del campo di nostro interesse (selezionato)-



-schermata di esempio (1)-

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

Nella schermata si potrà notare come si sono verificate 3 fasi principali che andremo ad analizzare:

- Reconnaissance — Ricognizione e raccolta informazioni
- Escalation — Escalation dei privilegi e persistenza
- Interactive Command Execution — Esecuzione dei payload e Shell

RECONNAISSANCE

Possiamo notare come siano stati usati comandi come:

- *whoami* — verifica dell'identità dell'utente corrente
- *hostname* — Identificazione del nome del server (*metaploitable*)
- *cat /etc/passwd | grep root* — lettura dei file di sistema per cercare l'utente *root* nel file degli account
- *grep root /etc/passwd* — ricerca mirata di stringhe di configurazione o account
- *cat /etc/passwd* — Raccolta (esfiltrazione) di tutti gli account utente presenti sul server

ESCALATION

In questo caso, noteremo invece comandi diversi, come:

- *nohup /bin/dev/init 2>1*

Tentativo di persistenza, l'uso di nohup (No Hang Up) serve per eseguire un processo in background, anche se il terminale viene scollegato.

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

Mannipolazione di file di sistema per la creazione di backdoor. L'attaccante aggiunge un nuovo utente (*myroot*) con UID 0 (*root*) al file */etc/passwd*, stabilendo così un accesso persistente e nascosto.

Interactive Command Execution

L'attacco si basa sull'invio di comandi di shell in sequenza:

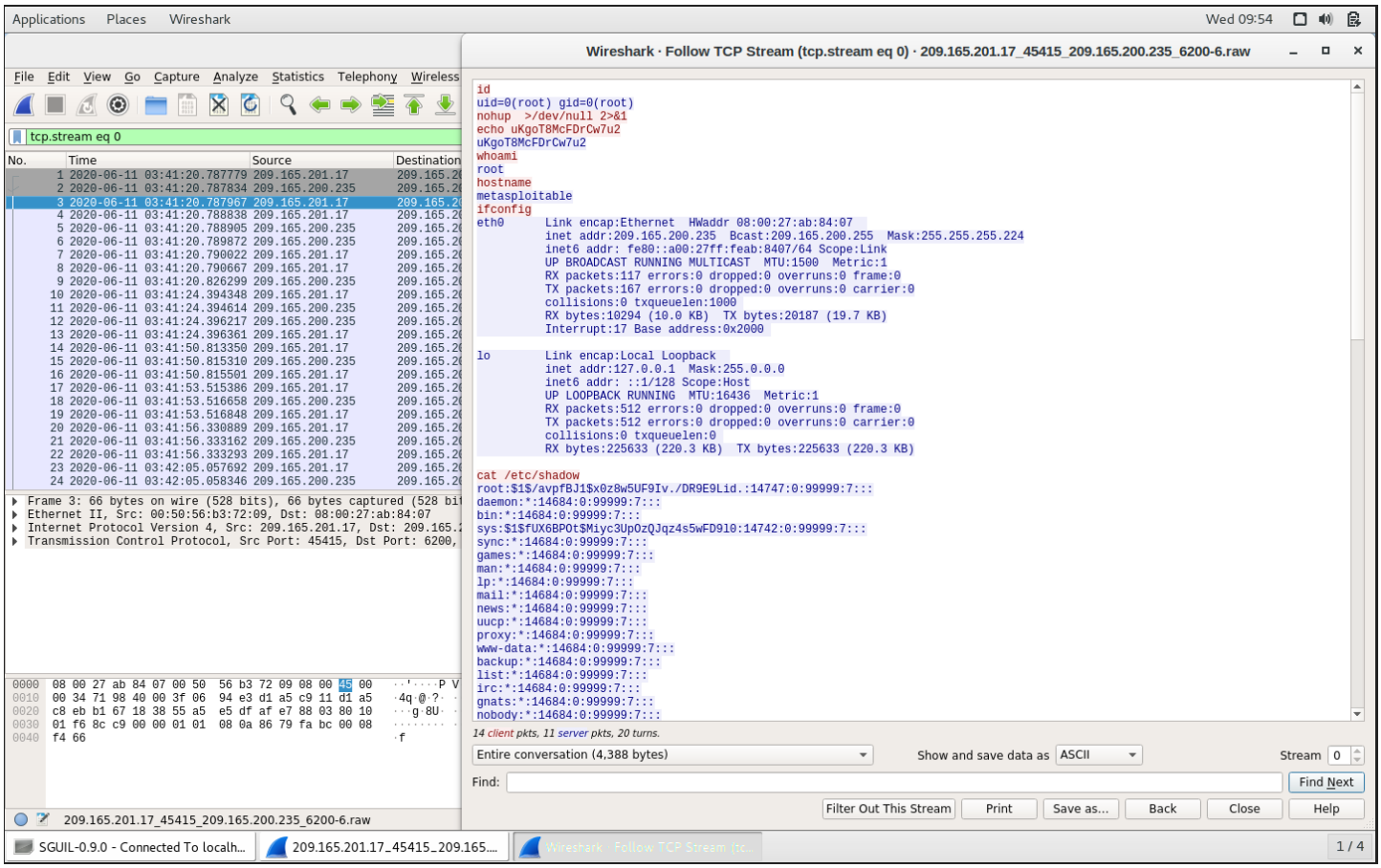
- *ush / exit* — comandi tipici di sessione di shell per avviare e chiudere la connessione
- *echo UKgTMBFeKDFwGwQxQ* — potenziale download od esecuzione di payload secondario tramite il comando echo (o simili) per scrivere dati codificati che andranno poi decodificati ed eseguiti

Riassumendo:

Le transazioni verificate tra client e server durante questo attacco sono primariamente:

1. Esecuzione remota di comandi
2. Manipolazione di file di configurazione critici
3. Transazioni di persistenza

PARTE II - WIRESHARK



-schermata di esempio (2)-

Dopo aver aperto il pacchetto indicato usando Wireshark presente nella Sguil, andremo a rispondere alle seguenti domande:

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

Il colore del testo indica la direzione dei dati, nel dettaglio:

- ROSSO indica i dati inviati dal client (attaccante) al server
- BLU indica i dati inviati dal server al client in risposta ai comandi

DOMANDA *Cosa rivela questo sul ruolo dell'attaccante sul computer bersaglio?*

Il flusso di comandi e le relative risposte indicano che l'attaccante ha assunto i privilegi di root, ottenendo un controllo quasi totale del computer bersaglio.

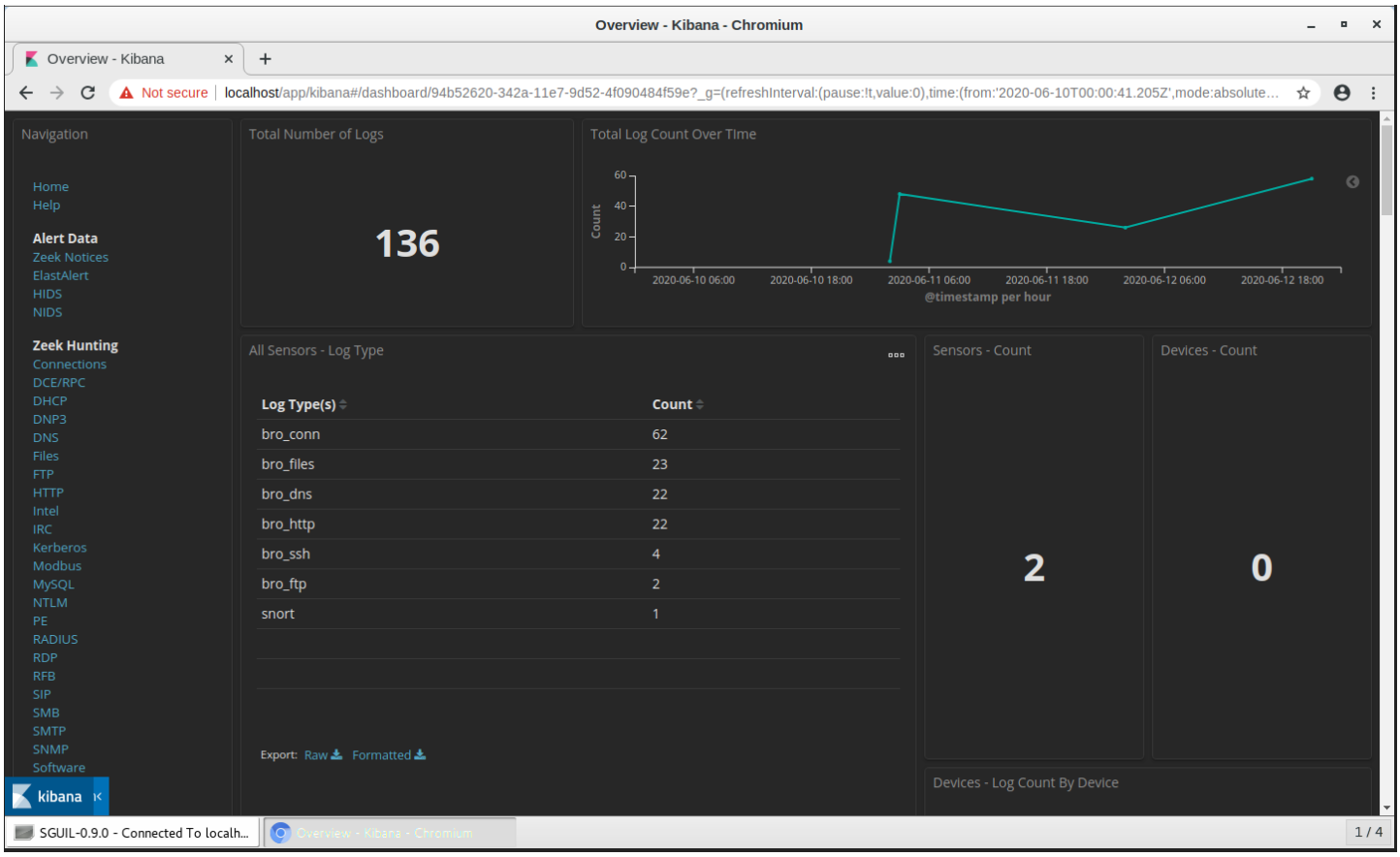
DOMANDA *Scorri il flusso TCP. Che tipo di dati ha letto l'attore della minaccia?*

Scorrendo il flusso TCP (come detto precedentemente, evidenziato in blu come risposta dal server), l'attaccante ha letto i seguenti tipi di dati di sistema:

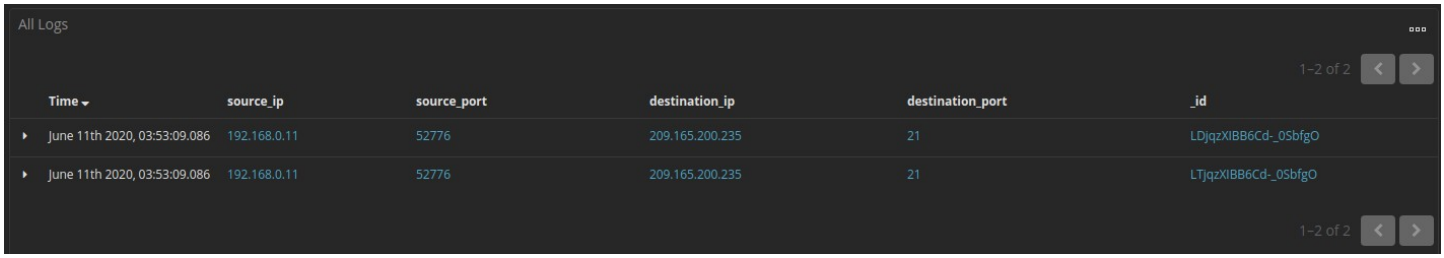
- Identità Utente output di id, che rivela i privilegi di root
- Identità Host il nome della macchina metaploitable, identifica il bersaglio

In seguito poi ha ricercato dati sulla configurazione di rete (*eth0*) usando il comando *ifconfig*.

PARTE III - KIBANA



-apertura di Kibana-



-filtro richiesto applicato-

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

Osservando il log, deduciamo che:

- IP di origine (attaccante) 192.168.0.11 Porta 52776 (porta effimera dinamica)
- IP di destinazione (server) 209.165.200.235 Porta 21 (standard FTP)

Procedendo come da traccia andiamo poi ad analizzare i log per rispondere alle domande poste:

192.168.0.11:52776_209.165.200.235:21-6-1362360228.pcap

Log entry:
{"ts":"2020-06-11T03:53:09.086840Z","uid":"C5GkeA4t8oXZdWTPr6","id.orig_h":"192.168.0.11","id.orig_p":52776,"id.resp_h":"209.165.200.235","id.resp_p":21,"user":"analyst","password":"<hidden>","command":"STOR","arg":"ftp://209.165.200.235/./confidential.txt","mime_type":"text/plain","reply_code":226,"reply_msg":"Transfer complete.","fuid":"FX1iV63eSMAEiN16S2"}

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: 52776
Dst Port: 21
OS Fingerprint: 192.168.0.11:52776 - UNKNOWN [S44:63:1:60:M1460,S,T,N,W7:.:?:?] (up: 3131 hrs)
OS Fingerprint: -> 209.165.200.235:21 (link: ethernet/modem)
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.

-analisi del log id-

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

Come possiamo vedere dall'immagine soprastante, le credenziali usate per accedere al sito FTP sono:

- USER analyst
- PASS cyberops

DOMANDA *Qual è il contenuto del file?*

close

192.168.0.11:49817_209.165.200.235:20-6-1700763525.pcap

Log entry:
{"ts":"2020-06-11T03:53:09.087738Z","uid":"C2Jv8MWV6Xg4lbb51","id.orig_h":"209.165.200.235","id.orig_p":20,"id.resp_h":"192.168.0.11","id.resp_p":49817,"proto":"tcp","service":"ftp-data","duration":0.001316070556640625,"orig_bytes":0,"resp_bytes":102,"conn_state":"SF","missed_bytes":0,"history":"ShAdfFa","orig_pkts":4,"orig_ip_bytes":216,"resp_pkts":4,"resp_ip_bytes":318,"sensorname":"seconion-import"}

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:

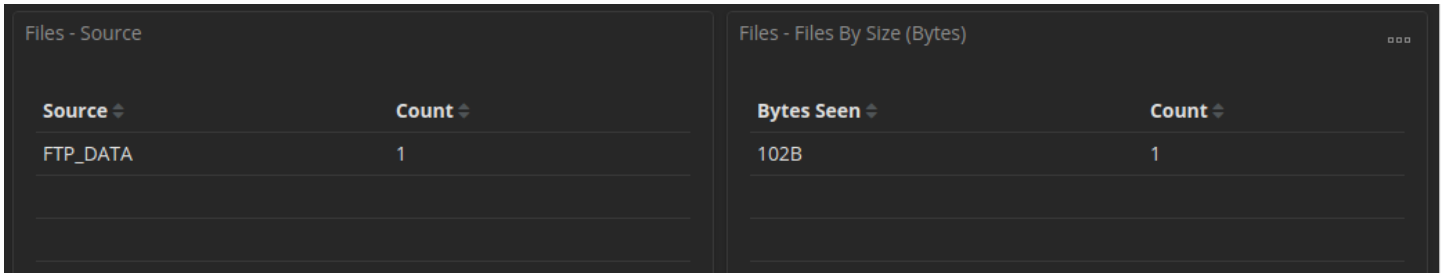
DEBUG: Using archived data: /nsm/server_data/securityonion/archive/2020-06-11/seconion-import/192.168.0.11:49817_209.165.200.235:20-6.raw
QUERY: SELECT sid FROM sensor WHERE hostname='seconion-import' AND agent_type='pcap' LIMIT 1
CAPME: Processed transcript in 0.73 seconds: 0.23 0.32 0.00 0.18 0.00

192.168.0.11:49817_209.165.200.235:20-6-1700763525.pcap

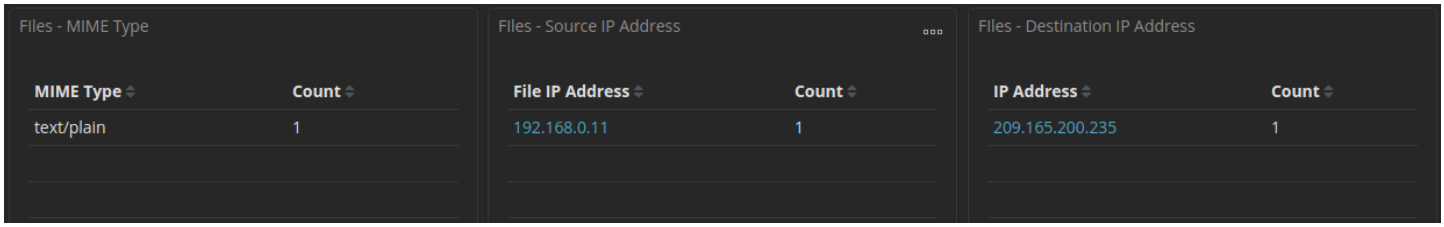
-contenuto del file-

Dopo aver ricercato il file richiesto, è chiaramente visibile il contenuto:

CONFIDENTIAL DOCUMENT
DO NOT SHARE
This document contains information about the last security breach



-files-



-MIME/source/destination-

-log FTP DATA-

DOMANDA *Quali sono i diversi tipi di file?*

A differenza delle slide, nella nostra personale analisi è stato rilevato solamente un file *plain/text.*

DOMANDA *Quali sono le sorgenti dei file elencate?*

Da come si evince dalle immagini, la sorgente è *FTP_DATA.*

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?

Da come possiamo notare:

- Tipo di MIME test/plain
- Indirizzo IP di origine 209.165.200.235
- Indirizzo IP di destinazione 192.168.0.11
- Data dell'evento 11 Giugno 2020 / 03:53:09.088

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

Questo si basa sulle precedenti conclusioni, arrivando ad ottenere la risposta data poco sopra:

CONFIDENTIAL DOCUMENT
DO NOT SHARE
This document contains information about the last security breach

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

A seguito delle informazioni raccolte,, la raccomandazione è di fermare l'attaccante immediatamente e su più livelli per proteggere il sistema:

AZIONI IMMEDIATE

- Disconnessione e blocco dell'indirizzo IP dell'attaccante
- Disabilitazione del servizio FTP, o di qualunque servizio sfruttato per l'accesso root iniziale
- Cambio delle credenziali utilizzando password più robuste
- Revoca dell'accesso di root, ovvero eliminare o disabilitare tutti gli account di root sospetti

AZIONI A LUNGO TERMINE

- Disabilitare completamente il servizio FTP per aggiornarsi al protocollo SFTP o FTPS
- Aggiornamenti di sicurezza, applicando patch che aggiorninoo e correggano l'errore che ha permesso l'attacco
- Monitoraggio maggiore, potenziando un monitoraggio in modo più efficiente del traffico e dei log sarà possibile rilevare in modo efficace tentativi di accesso o attività sospette.