QUADRO ILLEGITTIMO

Clone o furto di proprietà?

FILIPPO GIORGIO RONDO'
BUILDWEEK III

INDICE

TEORIA IN PILLOLE: 5-Tuple

La "**5-tuple**" è un insieme di cinque elementi che definiscono un flusso di comunicazione in rete.

Questi elementi sono: IP/Porta sorgente, IP/Porta destinazione, Protocollo utilizzato

TEORIA IN PILLOLE: 5-Tuple

Grazie alle 5-tuple è possibile: ricostruire l'intera sessione di comunicazione tra attaccante e vittima; identificare e tracciare specifici flussi di rete, facilitando la correlazione con altri eventi; filtrare e bloccare traffico malevolo; implementare misure difensive efficaci.

TEORIA IN PILLOLE: Sguil

***Sguil** è uno strumento di analisi del traffico di rete utilizzato per il monitoraggio della sicurezza che si integra con Snort, un IDS*

1. Visualizzare gli eventi di sicurezza (come quelli di snort)

2. Esaminare i pacchetti di rete

3. Intervenire su host compromessi

TEORIA IN PILLOLE: Trascrizioni

Le trascrizioni fanno riferimento alla registrazione dettagliata delle attività svolte durante un evento di compromissione o attacco. Queste includono: log di sistema e di rete, comandi eseguiti, allarmi e avvisi.

TEORIA IN PILLOLE: Trascrizioni

In un'analisi forense hanno un ruolo cruciale, i motivi principali sono:

1.Ricostruzione degli eventi
2.Identificare le vulnerabilità
3.Documentazione legale, poiché fungono da prove per dimostrare la natura e la gravità dell'attacco

PRESENTAZIONE PROGETTO

Strumenti utilizzati:

Cyberops Security Onion: VM, ossia il laboratorio dove si effettuerà l'attacco informatico
Sguil: piattaforma che permette di investigare sugli allarmi generati da IDS
Snort: Sistema di rilevamento delle intrusioni (IDS)
Wireshark: Strumento di monitoraggio del traffico di rete
Kibana: Distribuzione Linux che permette di correlare gli eventi ed avere una visione globale

PRESENTAZIONE PROGETTO

Scenario

Nel contesto di questo laboratorio è stato rilevato un attacco informatico su rete monitorata. Un host compromesso ha eseguito attività malevoli che coinvolgevano tentativi di accesso non autorizzato a file di sistema critici, come evidenziato dai log di /etc/shadow. L'allarme iniziale è stato generato da Snort, che ha rilevato un flusso di rete anomalo associato a tentativi di compromissione del sistema tramite accesso root. Le fasi essenziali di questo progetto sono tre: analisi con Sguil; analisi con Wireshark; analisi con Kibana

ANALISI CON SGUIL

QUESTA SEZIONE SARA' SUDDIVISA IN

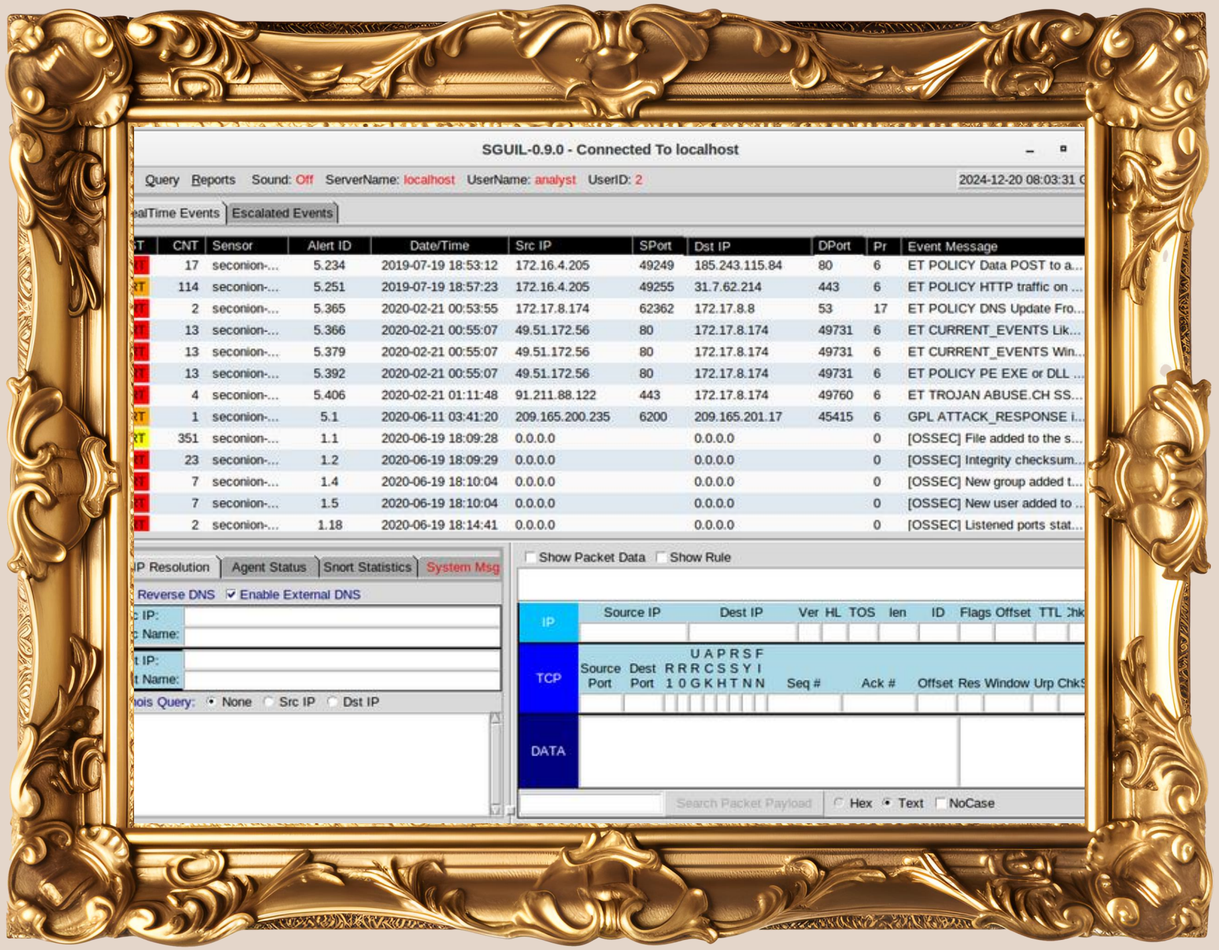
1. Esame dei pacchetti
2. Esame della regola IDS
3. Esame delle trascrizioni

ANALISI CON SGUIL - ESAME DEI PACCHETTI

1. Avviare la VM e registrarsi con le credenziali **analyst/cyberops**

Effettuare l’accesso a Sguil con le medesime credenziali. Nella colonna ‘event message’

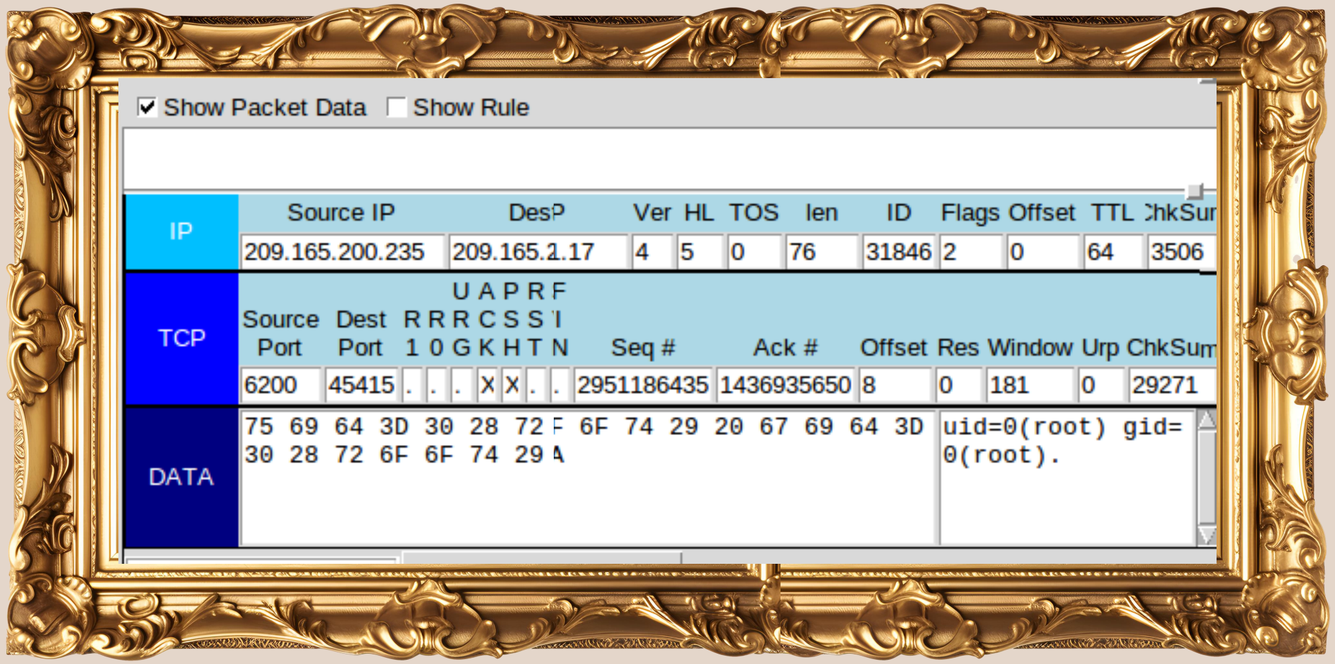
2. comparirà l’avviso di snort: ‘GPL ATTACK_RESPONSE id check turned root’, nonchè ciò che andremo ad analizzare.



ANALISI CON SGUIL - ESAME DEI PACCHETTI

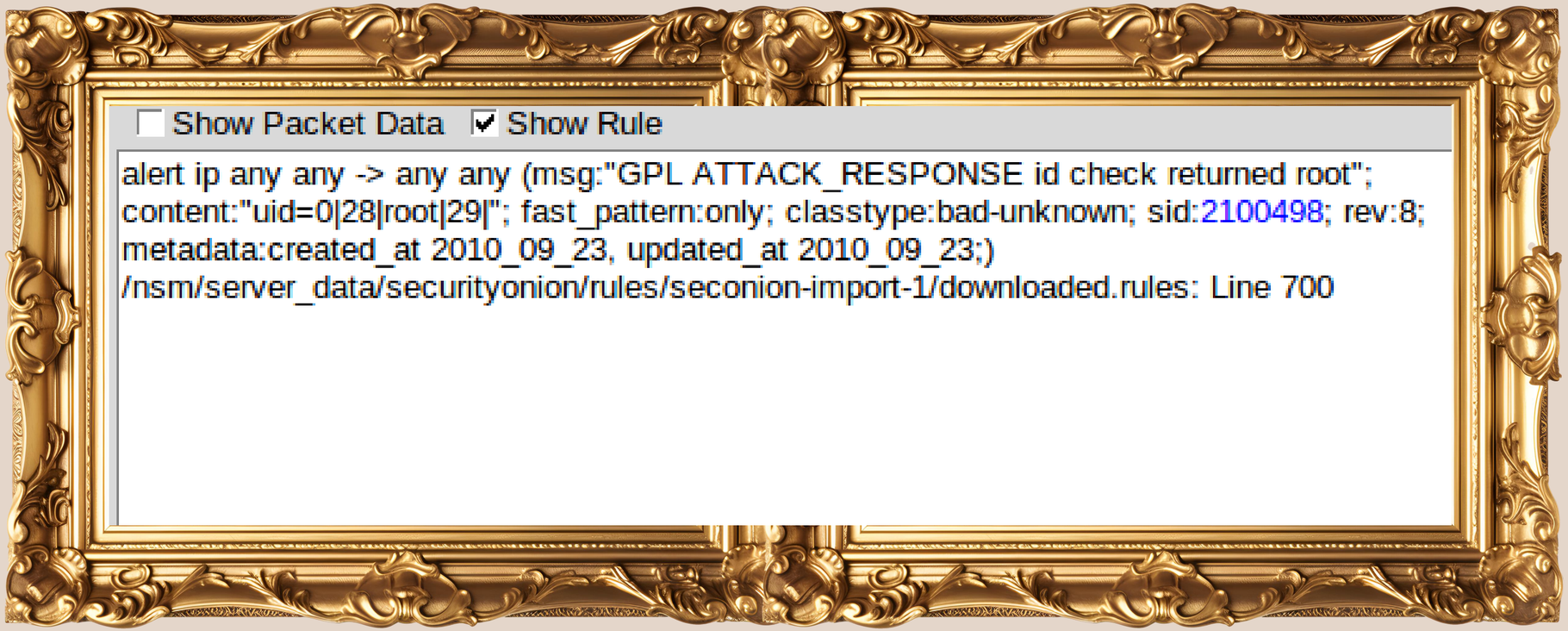
Mettiamo ora il flag nella sezione '**Show Data Packet'.** Saranno fornite le **5-Tuple** e il **payload**

3. **uid=0(root),** identificatore user, in questo caso root
   gid=0(root), identificatore di gruppo o insiemi di utenti, in questo caso gruppo root



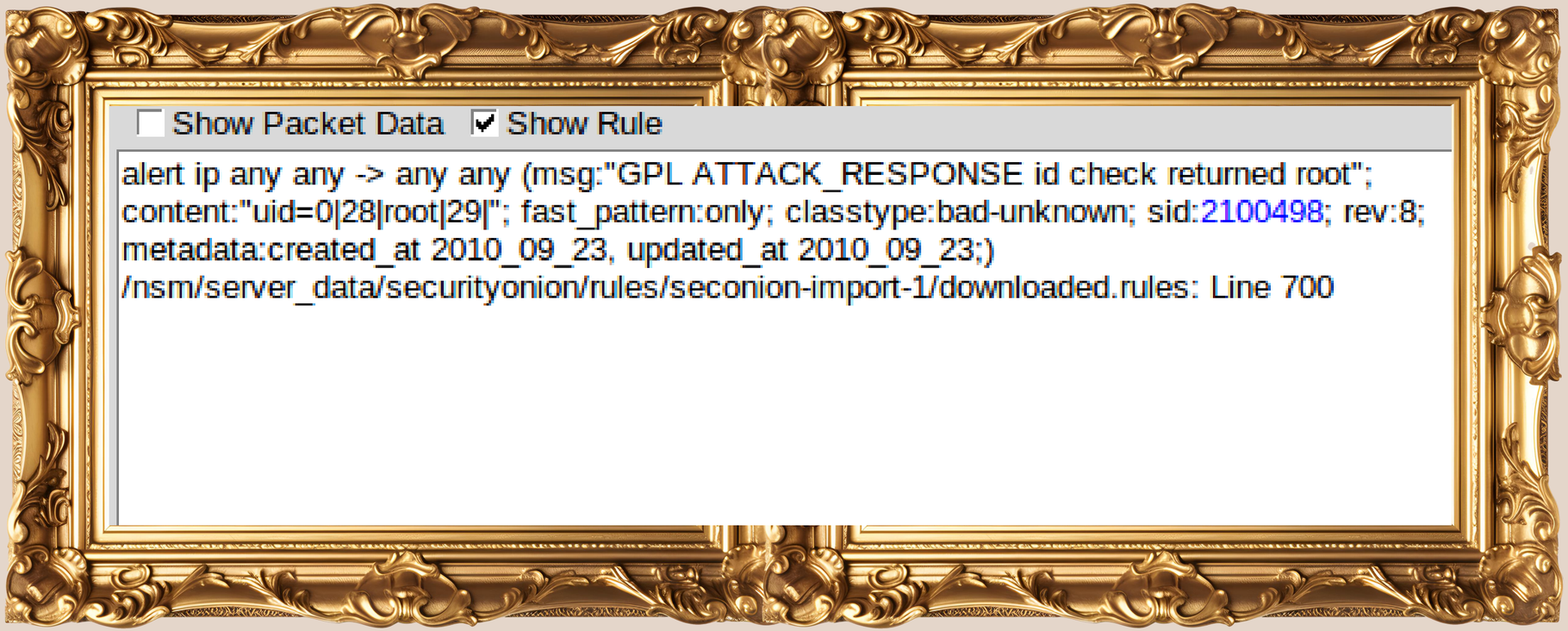
ANALISI CON SGUIL - ESAME DELLA REGOLA IDS

4. Mettiamo ora il flag nella sezione ‘**Show Rule’.** Sarà fornita la regola IDS attivata. Questa regola si basa su un concetto molto semplice: avviso di output contenenti informazioni di root. Se tale contenuto appare nel traffico di rete, è molto probabile che l’attaccante abbia già ottenuto privilegi root sul sistema target. Si tratta dunque di una regola post-exploit

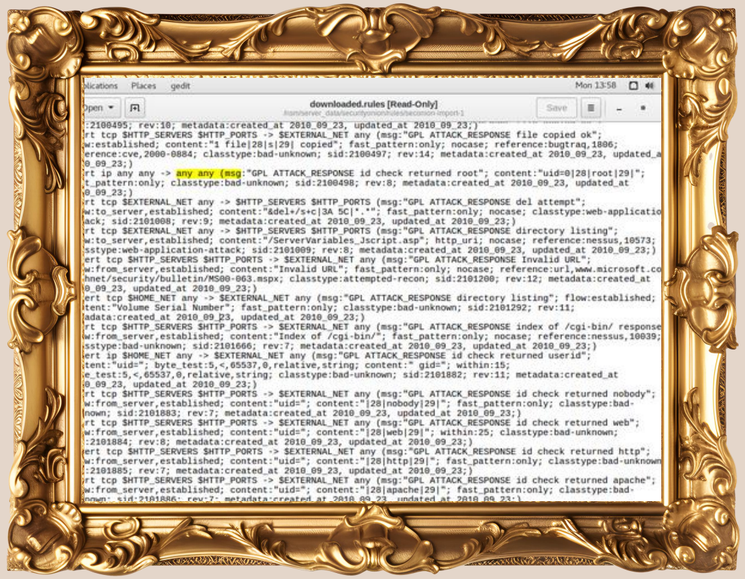


ANALISI CON SGUIL - ESAME DELLA REGOLA IDS

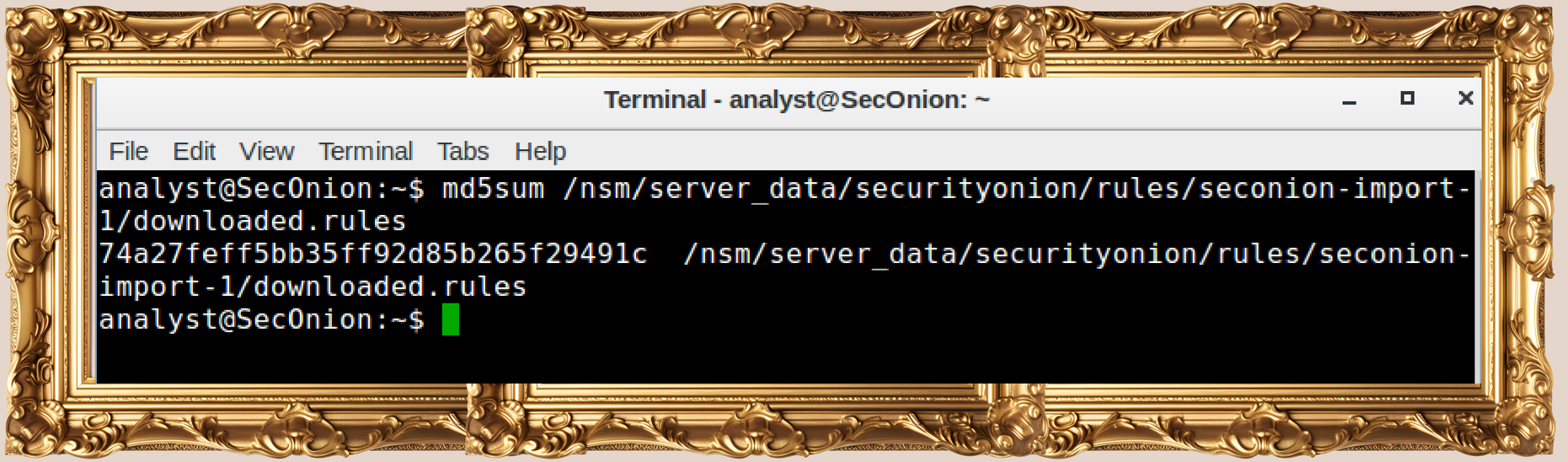
5. Il formato generale di questa regola è:
<ACTION> <PROTOCOL> <SOURCE IP> <SOURCE PORT> à <DESTINATION IP> <DESTINATION PORT> <SIGNATURES>



ANALISI CON SGUIL - ESAME DELLA REGOLA IDS

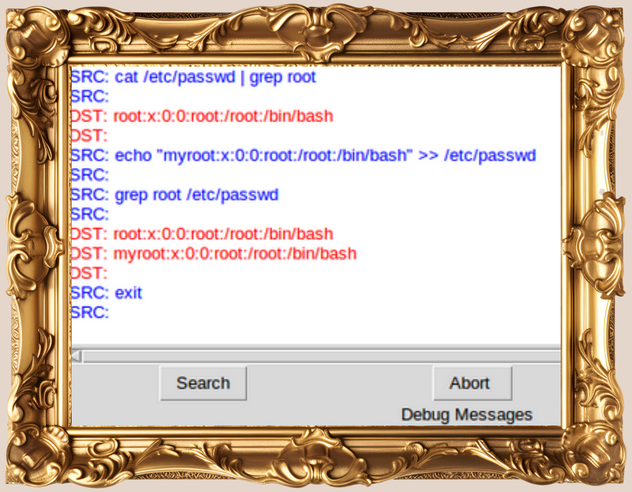


6. Controllo dell'integrità della regola:
   - hash
   - data di modifica
   - Utilizzo del SID



ANALISI CON SGUIL - ESAME DELLE TRASCRIZIONI

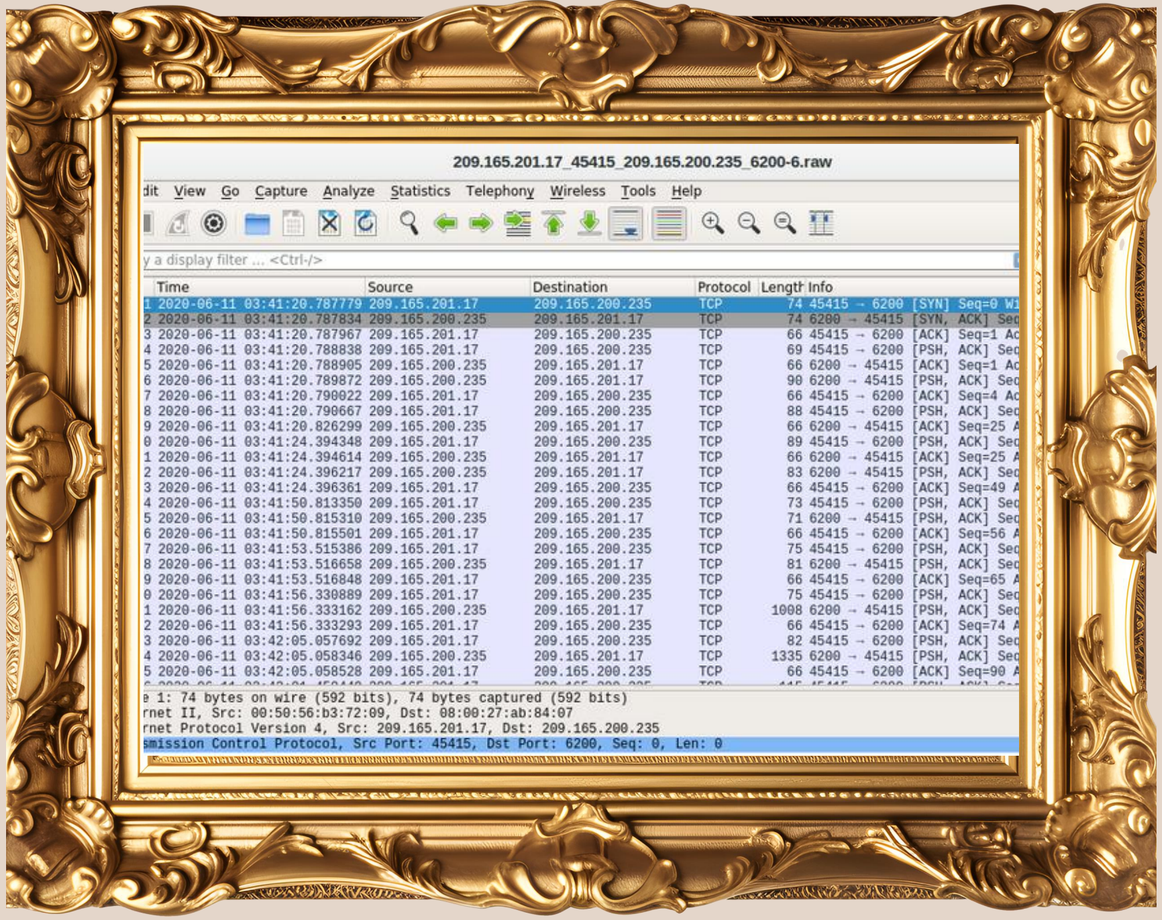
7. Facendo doppio click nella colonna ‘Alert ID’ e andando poi su ‘Transcript’ è possibile visionare tutte le trascrizioni.



ANALISI CON WIRESHARK

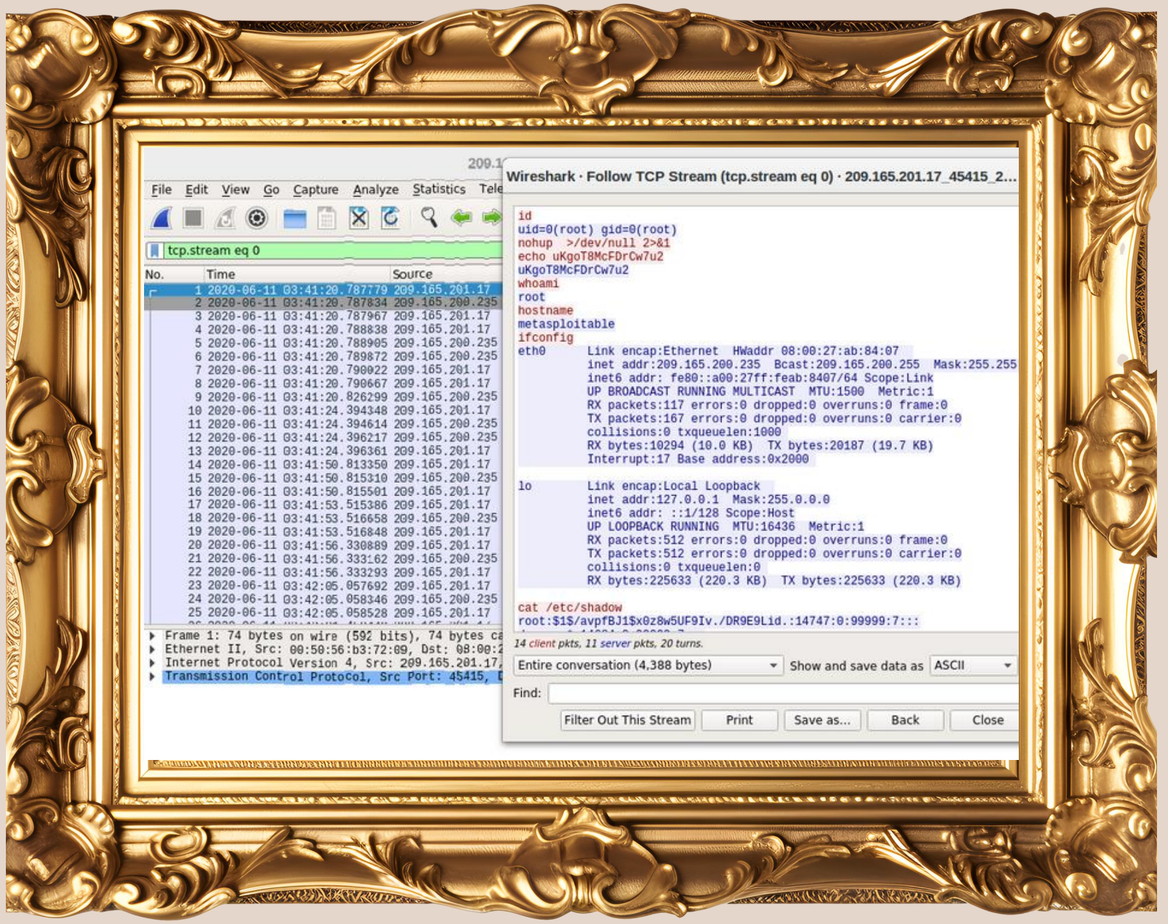
Cattura di rete

Per visualizzare la cattura di wireshark il processo è identico alle tascrizioni: tasto destro nella colonna ‘id alert’ > ‘Wireshark’.Notiamo che i pacchetti trasmessi utilizzano tutti il protocollo TCP.



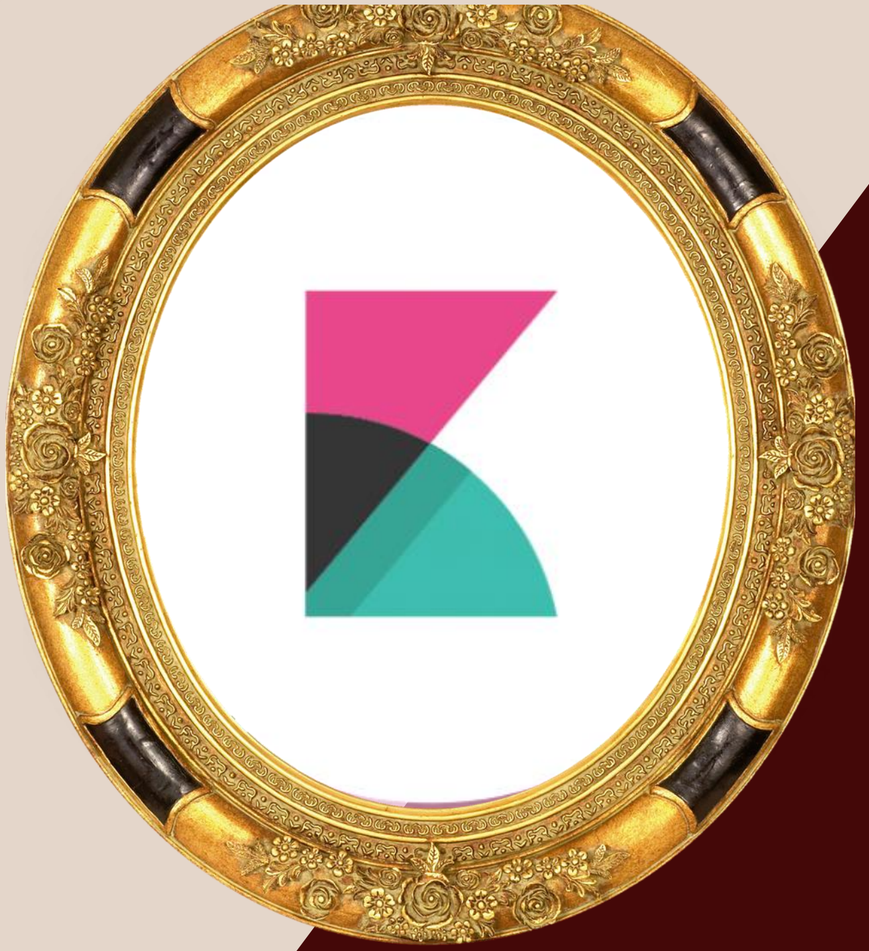
ANALISI CON WIRESHARK

Da qui, con tasto destro su un pacchetto > ‘follow’> ‘tcp stream’ è possibile visionare in maniera ordinata tutti i pacchetti scambiati dall’attaccante con l’host compromesso. I dati che vengono riportati sono molto simili alle trascrizioni viste su Sguil



ANALISI CON WIRESHARK

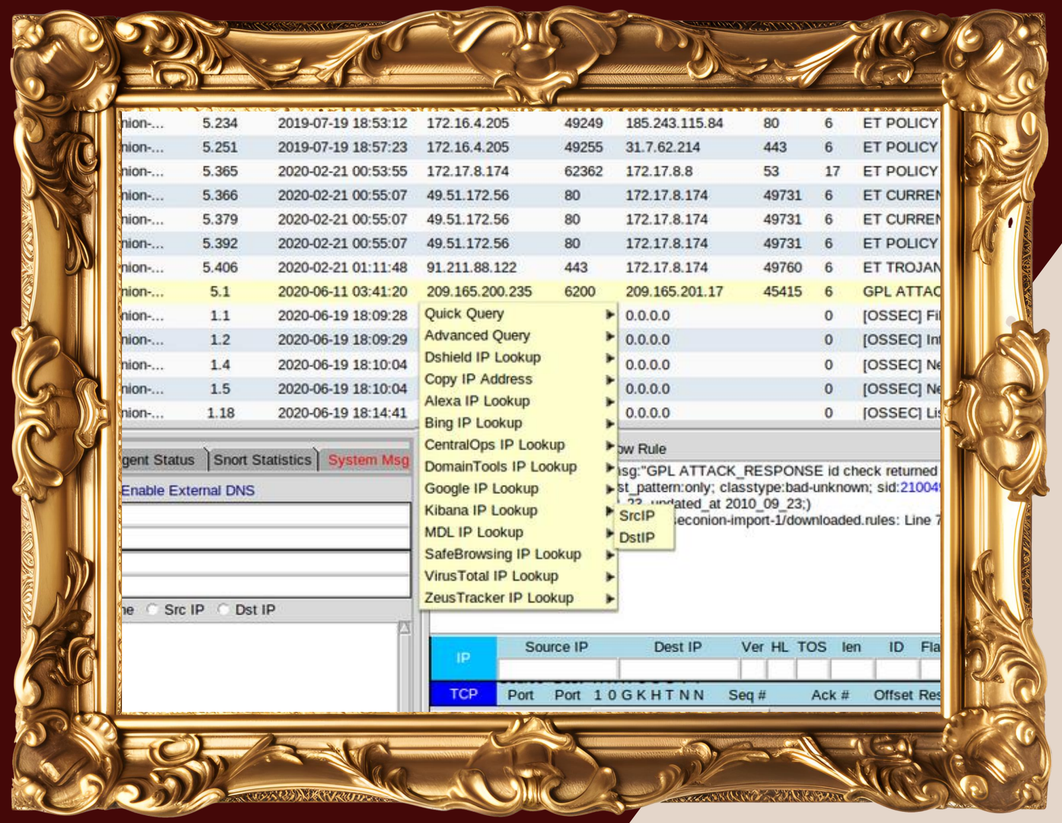
ANALISI CON KIBANA



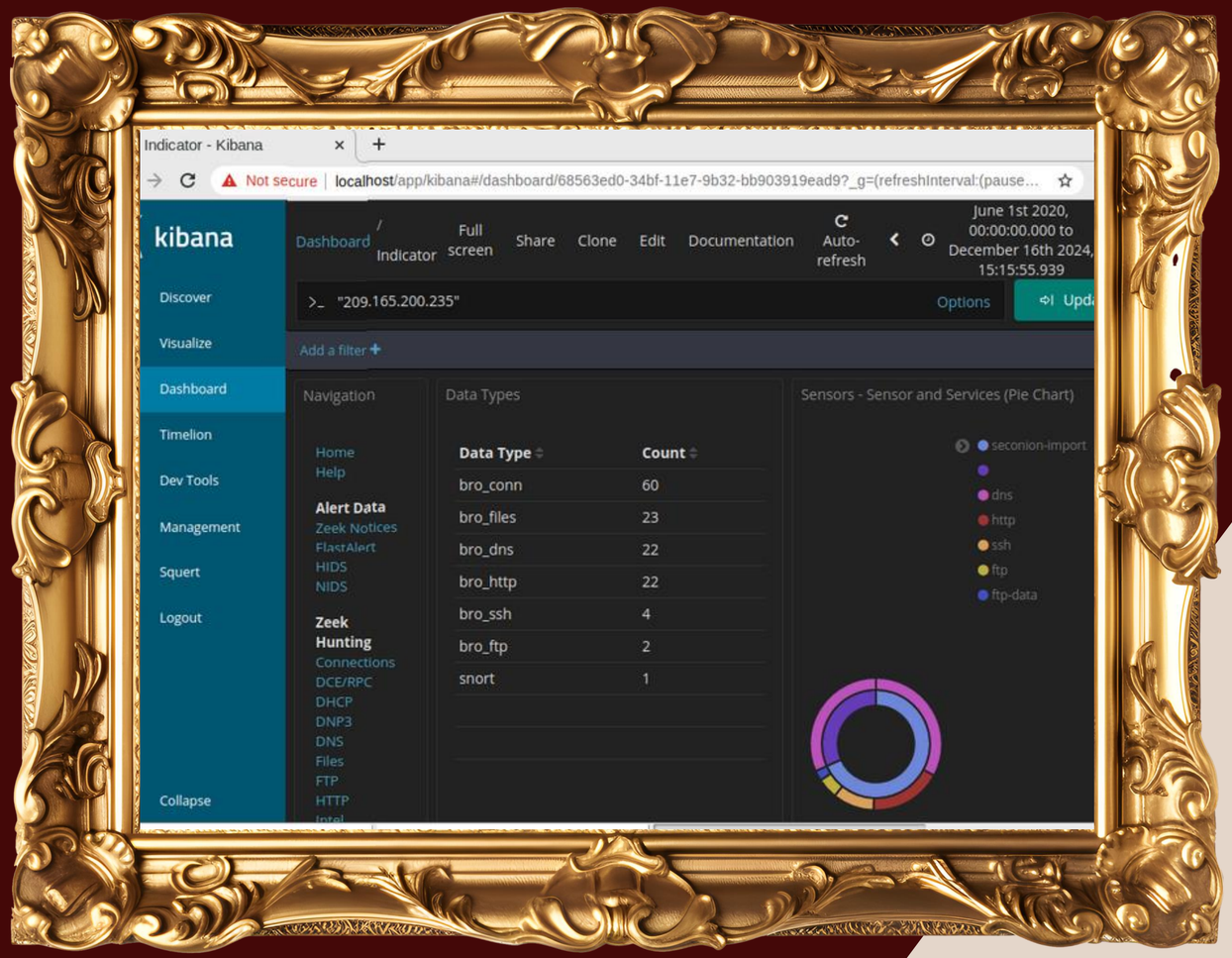
IN QUESTA SEZIONE ESPLOREREMO

- *FTP*
- *FILES*

ESAME CON KIBANA - FTP

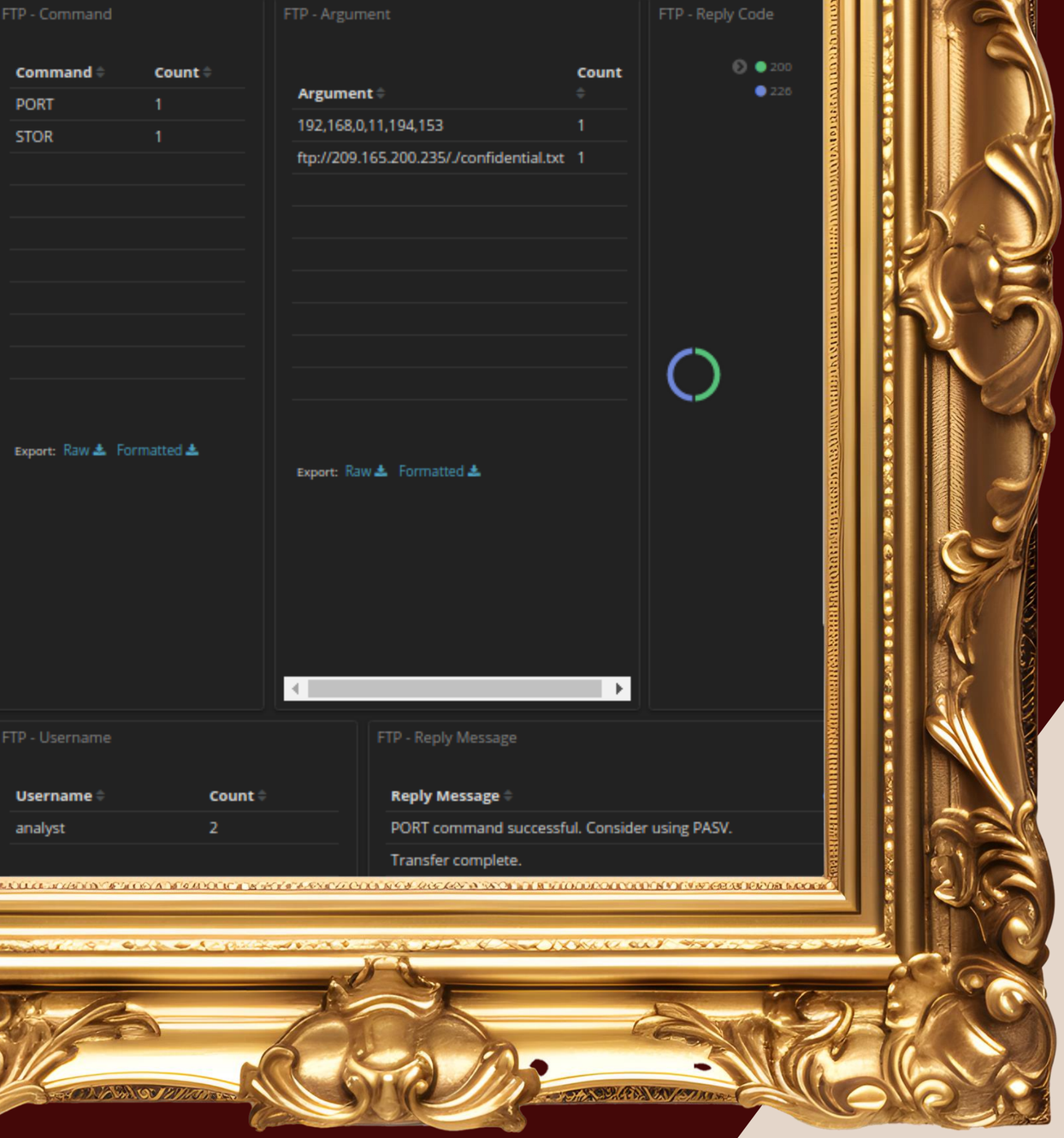


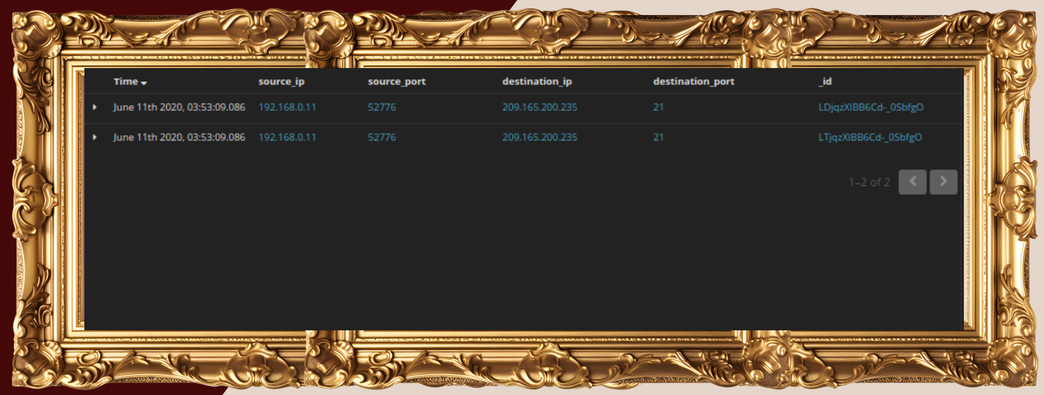
1. Nella colonna ‘SRC IP’ tasto destro > ‘Kibana IP lookup’ > SrcIP’ in modo da visualizzare le informazioni su Kibana



2. Importante filtrare le informazioni, inserendo il range di tempo necessario e inserire l'ip interessato, in questo caso quello sorgente

ESAME CON KIBANA - FTP





3. Filtrando la richiesta su bro_ftp notiamo che sono stati effettuati due log su FTP. Il motivo è semplice: Il protocollo FTP utilizza due connessioni separate per trasferire i dati, una per il controllo e una per i dati, per via della sua architettura progettuale

ESAME CON KIBANA - FTP

ESAME CON KIBANA - FTP

4.

I punti chiave riscontrabili in questo log sono:

- ftp command = PORT
- Message = Port command successful e credenziali usate
- Mimetype: text/plan

In sintesi questo log è utilizzato per copiare il file dal server

t	destination_geo.region_name	California
t	destination_geo.timezone	America/Los_Angeles
💻	destination_ip	209.165.200.235
t	destination_ips	209.165.200.235
#	destination_port	21
t	event_type	bro_ftp
t	ftp_argument	192,168,0,11,194,153
t	ftp_command	PORT
t	host	d68c9360b6ae
t	ips	209.165.200.235, 192.168.0.11
t	message	{"ts":"2020-06-11T03:53:09.086482Z","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":"PORT","arg":"192,168,0,11,194,153","reply_code":200,"reply_msg":"PORT command successful. Consider using PASV.","data_channel.passive":false,"data_channel.orig_h":"209.165.200.235","data_channel.resp_h":"192.168.0.11","data_channel.resp_p":49817}
t	password	<hidden>
t	path	/nsm/import/bro/bro-sak0dUdf/ftp.log
t	reply_code	200
t	reply_message	PORT command successful. Consider using PASV.
💻	source_ip	192.168.0.11
t	source_ips	192.168.0.11
#	source_port	52776
t	tags	bro, import

5.

I punti chiave riscontrabili in questo log sono:

- ftp command = STOR
- Message = ftp://ip/./confidential.txt e credenziali usate
- Mimetype: text/plan

In sintesi questo log è utilizzato per copiare il file dal server

ESAME CON KIBANA - FTP

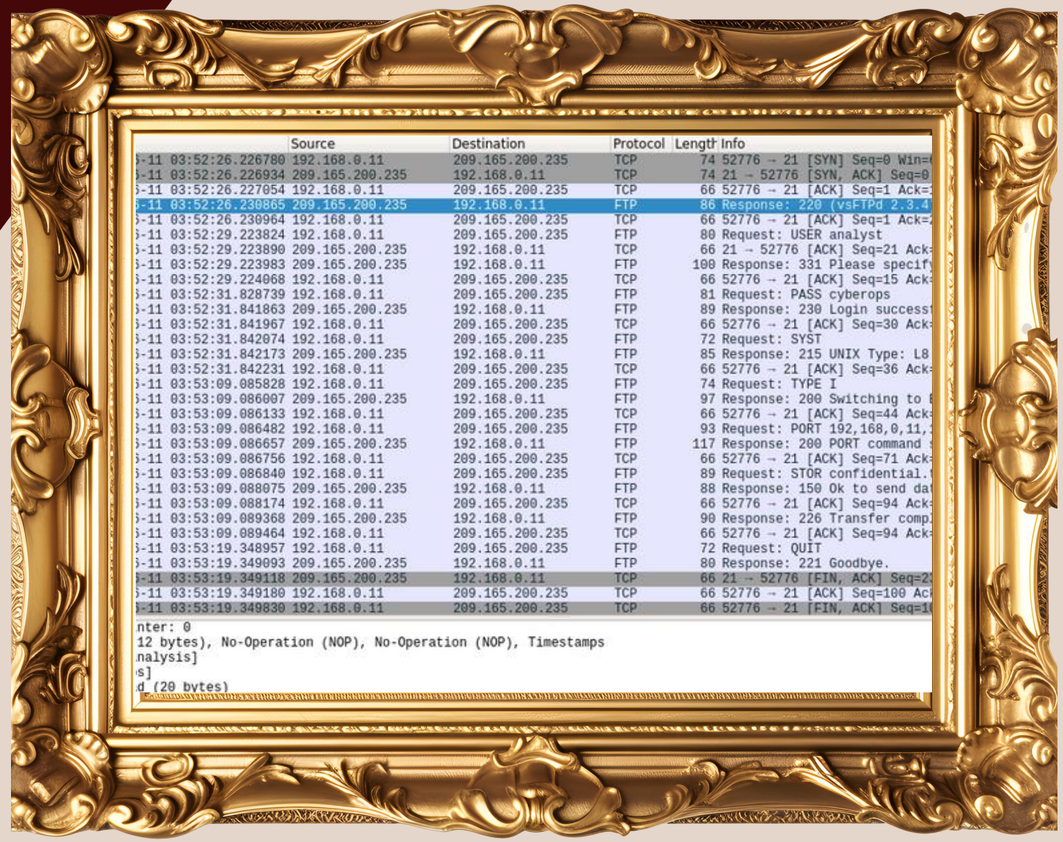
6. I punti chiave riscontrabili in questo log sono:

- ftp command = STOR
- Message = ftp://ip/./confidential.txt e credenziali usate
- Mimetype: text/plan

In sintesi questo log è utilizzato per copiare il file dal server

Kibana permette di analizzare le trascrizioni, fornendo anche i file wireshark inerenti ai log FTP

7.



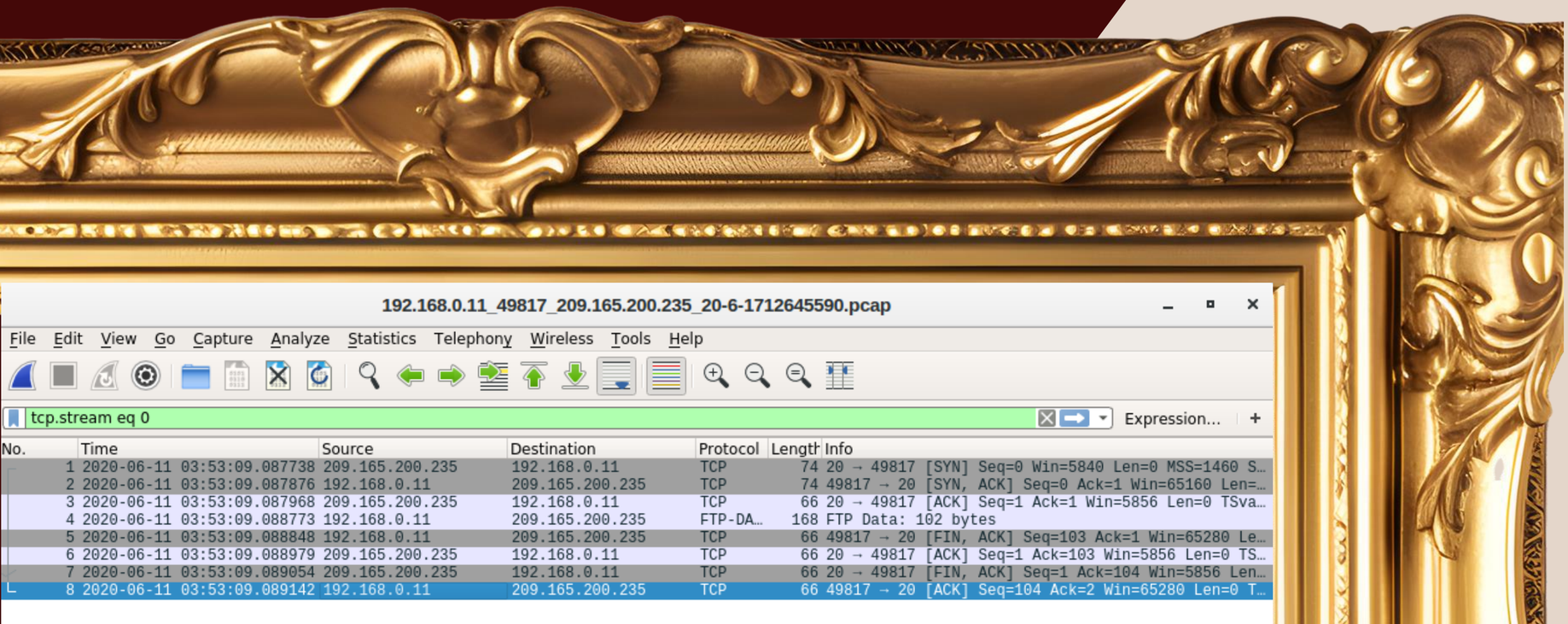
ESAME CON KIBANA - FTP

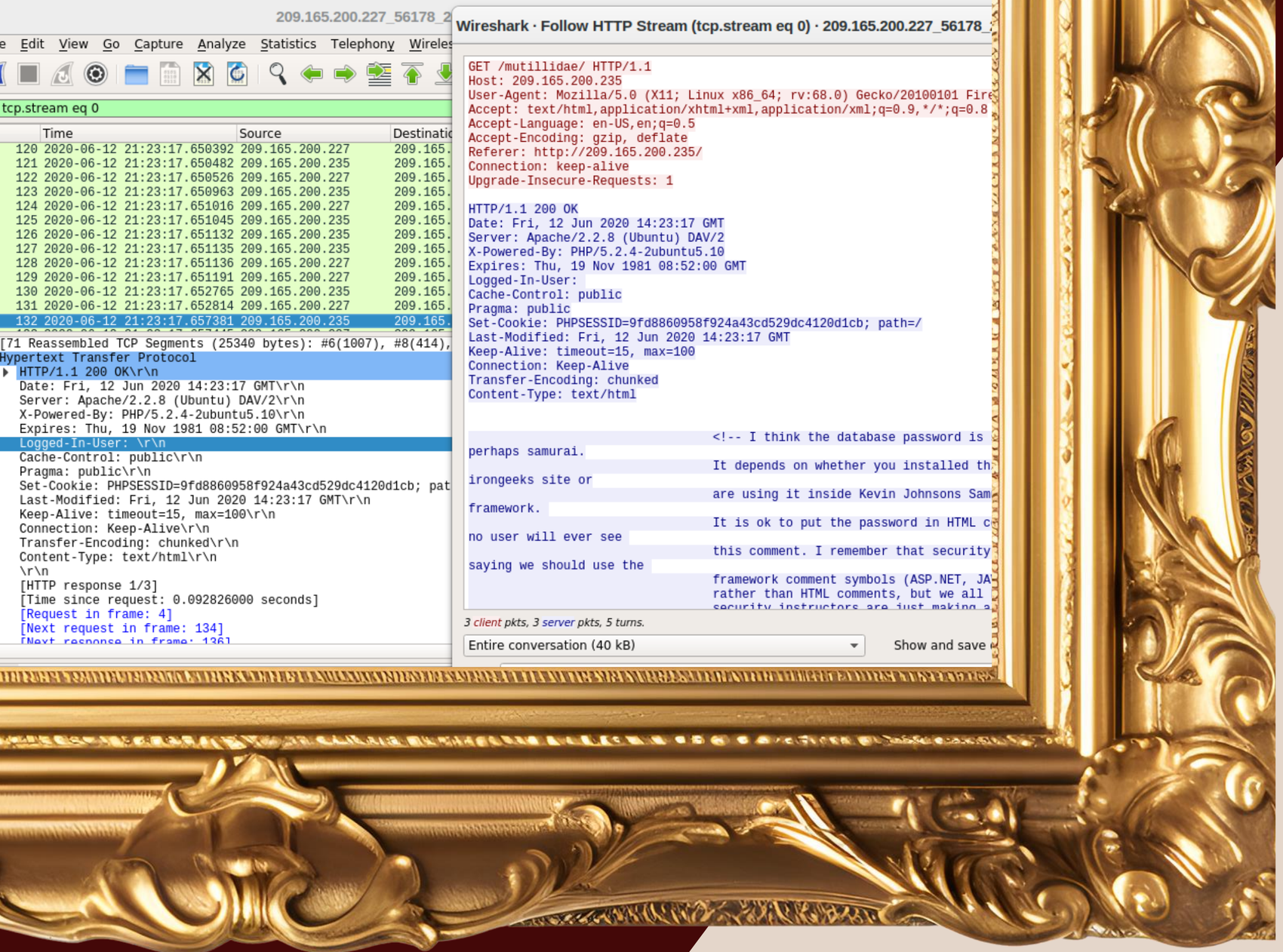
ESAME CON KIBANA - FILES

7. Per studiare tutti i file registrati, nella sezione ‘Zeek Hunting’ > Files. Durante il mese di giugno 2020, i file registrati sono 23

ESAME CON KIBANA - FILES

7. Per quanto riguarda il file FTP_DATA, si tratta del file ‘confidential.txt’ che è stato rubato





7. ESAME CON KIBANA - FILES

COSA FARE IN UNO SCENARIO SIMILE?

- *Confermare l'attacco*
- *Individuare i vettori d'attacco*
- *Acquisizione di prove*
- *Rimuovere l'host compromesso e ristabilire l'ecosistema*

PREVENZIONI

- *Politiche di sicurezza robuste*
- *Implementare patch di sicurezza*
- *Migliorare il monitoraggio e la visibilità*
- *Ridurre l'esposizione di rete*
- *Test di vulnerabilità*
- *Istruzione dei dipendenti*

GRAZIE PER L'ATTENZIONE