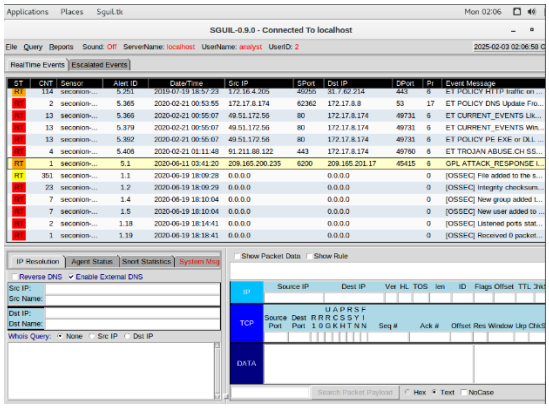
BONUS 3

Lab - Isolate Compromised Host Using 5-Tuple

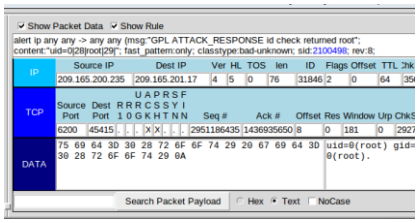
https://itexamanswers.net/27-2-14-lab-isolate-compromised-host-using-5-tuple-answers.html

ESECUZIONE ESERCIZIO

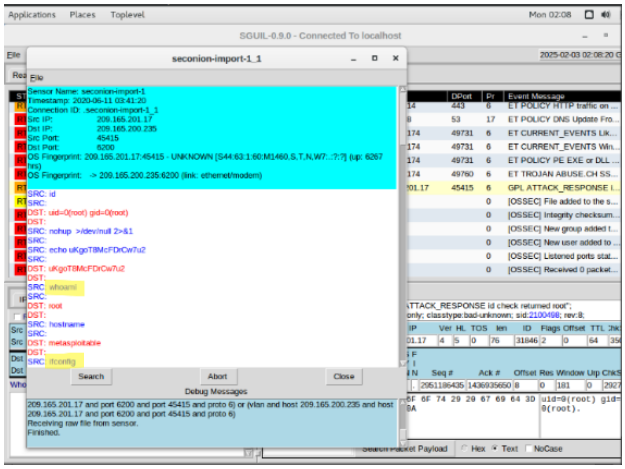
Focalizzandoci sulla voce “GPL ATTACK_RESPONSE id check returned root” si può notare che indica che un accesso root è stato ottenuto durante un attacco.



Selezionando “show packet data” e “show rule” possiamo ottenere più dettagli riguardo l’alert.

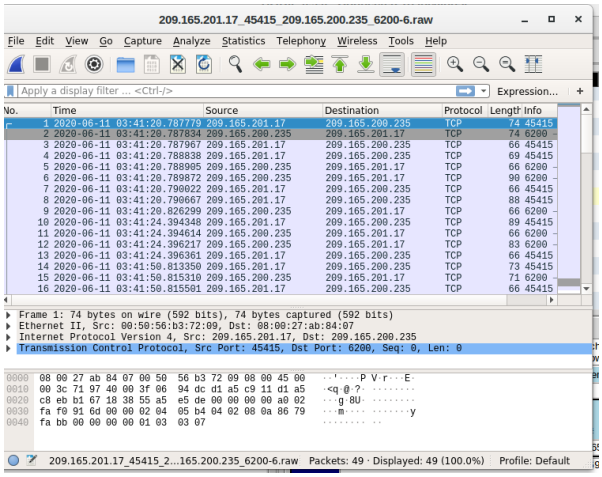


Cliccando sull’ID 5.1 e selezionando “transcript” si possono tracciare tutte le interazioni che ci sono state tra la fonte di attacco e la destinazione. Si può notare che l’attaccante ha eseguito del comandi linux sulla macchina target.

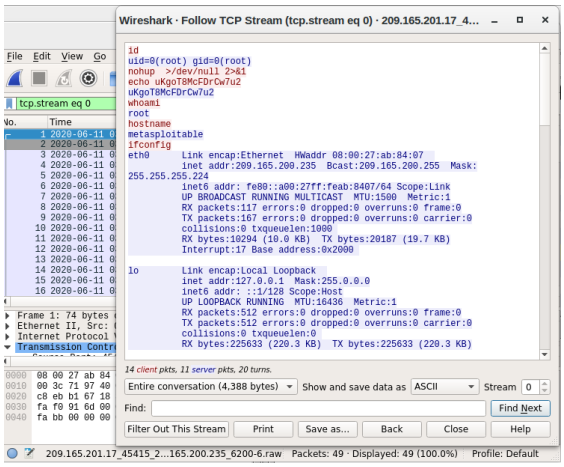


Quindi si può vedere che l’attaccante 209.165.201.27 è riuscito ad ottenere l’accesso root sulla macchina 209.165.200.235.

Successivamente si può analizzare l’alert con lo strumento wireshark.



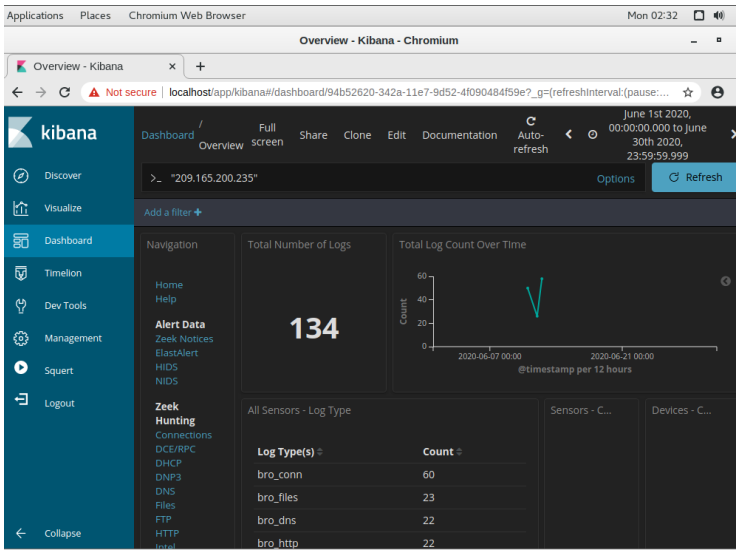
Selezionando il TCP Flow su un qualsiasi pacchetto si può osservare il flusso assemblato di pacchetti TCP.



Qui si può notare che il testo in rosso è quello dell'attaccante, mentre in blu è della macchina target. Nell'immagine soprastante si può notare che l'attaccante abbia stampato a schermo tutte le configurazioni della macchina target. Infatti, l'IP di quest'ultima è 209.165.200.235 ed il suo nome è metasploitable. Tramite il comando whoami l'attaccante si è assicurato di avere il privilegio di root sulla macchina target. E successivamente ha copiato il file shadow ed editato i file /etc/passwd e /etc/shadow.

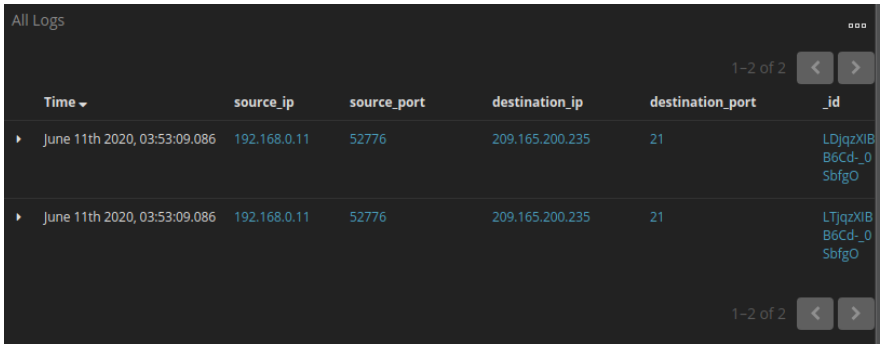
Successivamente, dopo aver acceduto a Kibana tramite username e password (analyst, cyberops), si deve impostare un range di data che include tutto il mese di giugno del 2020.

Ci sono molti tipi di data, ma ci dobbiamo concentrare sui dati ftp.

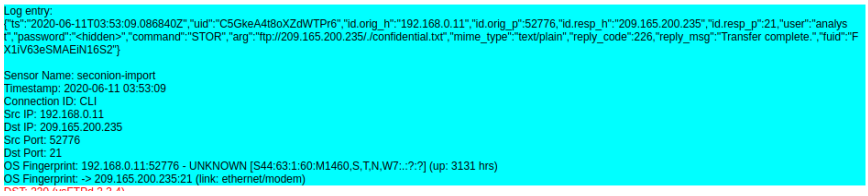


Log Type(s)	Count
bro_conn	60
bro_files	23
bro_dns	22
bro_http	22
bro_ssh	4
bro_ftp	2
snort	1

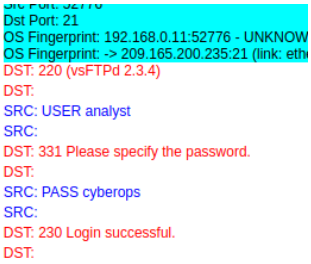
Filtrando bro_ftp e scorrendo verso “all logs” si può notare che l’ip sorgente e la rispettiva porta sono 192.168.0.11:52776 e quelli di destinazione sono 209.165.200.235:21.



Analizzando i file di entrambi i log si può vedere come in uno di questi l'argomento è ftp://209.165.200.235/./confidential.txt.

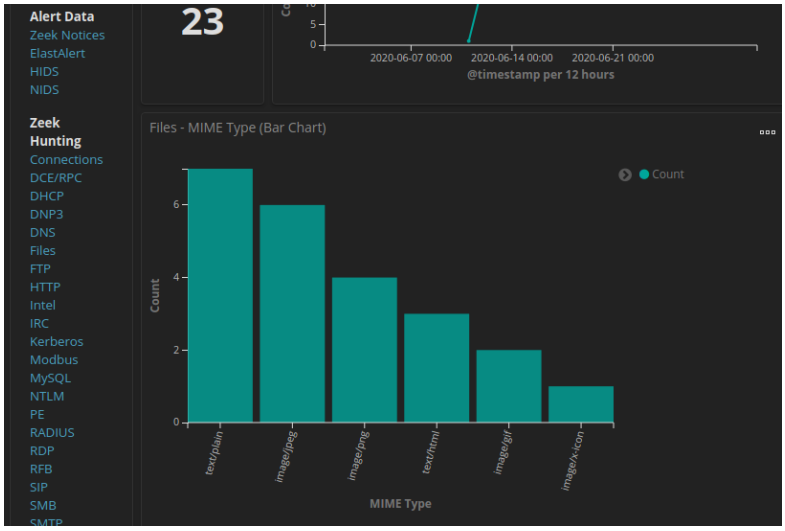


Nell'altro leggiamo le credenziali per entrare in ftp.

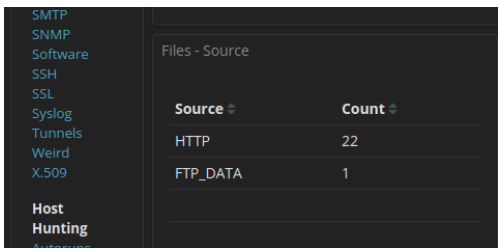


Quindi, dopo aver appurato che l'attaccante sia entrato con ftp ed abbia copiato confidential.txt e cancellato successivamente dal target, bisogna capire quale era il contenuto dei file.

Navigando verso l'inizio della dashboard si può notare la voce "files" sotto "zeek hunting" , selezionandola si può analizzare il grafico, il quale indica che i tipo di file sono principalmente testi e immagini.



Scorrendo verso il basso si può leggere l'origine dei file, ed in questo le origini sono HTTP e FTP_DATA. Dopo aver cliccato su FTP_DATA, si deve scorrere verso il basso per visualizzare i risultati del filtraggio.



Nei logs si può vedere l'ip sorgente e quello di destinazione, nonché la data in cui è stato trasferito.

Selezionando il link sotto _id si può leggere che il file è un documento riservato da non condividere, che contiene informazioni riguardo l'ultima violazione di sicurezza.

192.168.0.11:49817_209.165.200.235:20-6-1406027801.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:

Raccomandazioni

Per evitare accessi non autorizzati:

- Autenticazione forte
- Gestione degli accessi e dei privilegi
- Protezione della rete