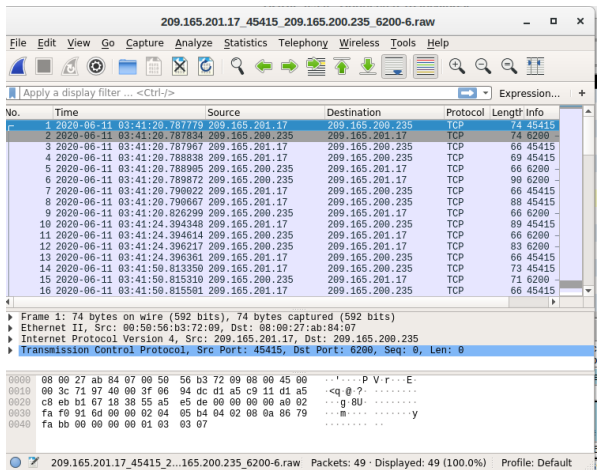
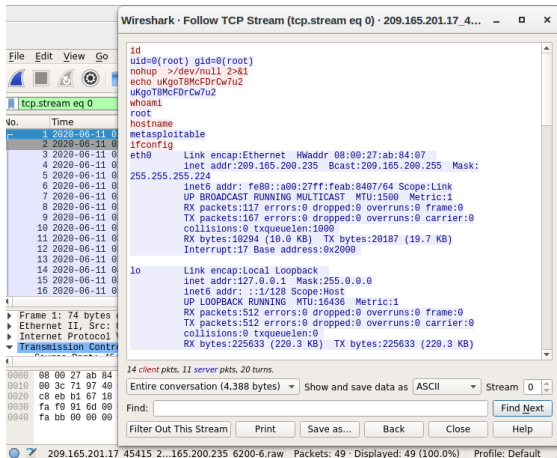


Successivamente si può analizzare l'alert con lo strumento wireshark.



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

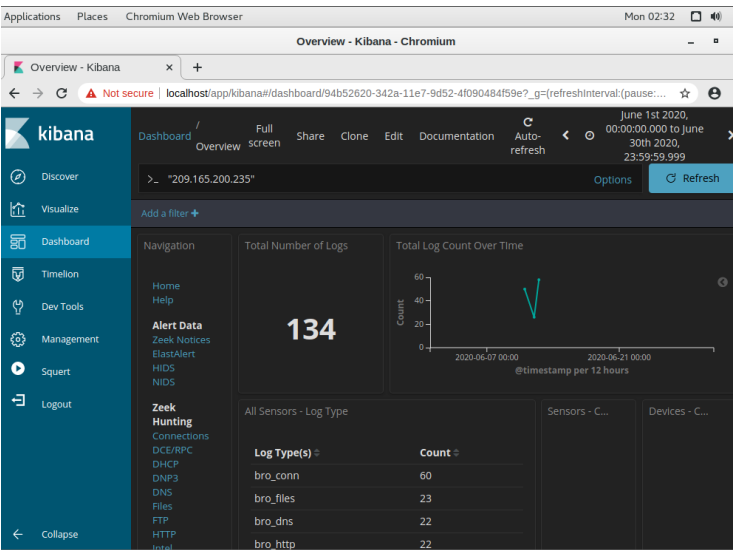


Qui si può notare che il testo in rosso è quello dell'attaccante, mentre in blu è della macchina target. Nell'immagine soprastante si può notare che l'attaccante abbia stampato a schermo tutte le configurazioni della macchina target. Infatti, l'IP di quest'ultima è 209.165.200.235 ed il suo nome è metasploitable. 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.

```
tomcat55:*:14691:0:99999:7:::
distccd:*:14698:0:99999:7:::
user:$1$HESu9xrH$K.o3G93DGoXIiQKkPmUgZ0:14699:0:99999:7:::
service:$1$SkR3ue7JZ$7GxELDupr50hp6cjZ38u//:14715:0:99999:7:::
telnetd:*:14715:0:99999:7:::
proftpd:*:14727:0:99999:7:::
statd:*:15474:0:99999:7:::
analyst:$1$uVeqE7eTSx6gczc318aD6mhx0FZqXE.:17338:0:99999:7:::
echo "myroot:::14747:0:99999:7:::" >> /etc/shadow
grep root /etc/shadow
root:$1$avprB3i5x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
myroot:::14747:0:99999:7:::
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
```

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.



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.

All Logs					
Time	source_ip	source_port	destination_ip	destination_port	_id
June 11th 2020, 03:53:09.086	192.168.0.11	52776	209.165.200.235	21	LDJqzXIBB6Cd-0SbfgO
June 11th 2020, 03:53:09.086	192.168.0.11	52776	209.165.200.235	21	L7JqzXIBB6Cd-0SbfgO

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.

```
Log entry:
[{"ts": "2020-06-11T03:53:09.086840Z", "uid": "CSGkeA4t8oXZdWTPv6", "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.", "fluid": "FX1V63eSMAEIN16S2"}]

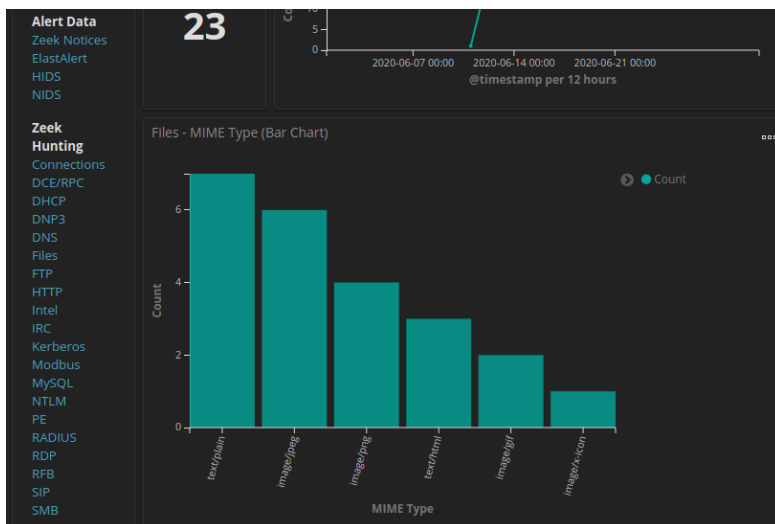
Sensor Name: seconion-import
Timestamp: 2020-06-11 03:53:09
Connection ID: CL1
Src IP: 192.168.0.11
Src Port: 209.165.200.235
Dst IP: 192.168.0.11
Dst Port: 52776
OS Fingerprint: 192.168.0.11:52776 - UNKNOWN [S44.63.1.60.M1460.S.T.N.W7.:?:?] (up: 3131 hrs)
OS Fingerprint -> 209.165.200.235:21 (link: ethernet/modem)
DST: 220 (vsFTPD 2.3.4)
```

Nell'altro leggiamo le credenziali per entrare in ftp.

```
SRC: 220 (vsFTPD 2.3.4)
DST: 21
OS Fingerprint: 192.168.0.11:52776 - UNKNOWN
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.
DST:
```

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.

SMTP	
SNMP	
Software	
SSH	
SSL	
Syslog	
Tunnels	
Weird	
X.509	
Host Hunting	

Files - Source	
Source	Count
HTTP	22
FTP_DATA	1

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

Files - Logs

1-1 of 1

Time	file_ip	destination_ip	source	uid	fuid	_id
June 11th 2020, 03:53:09.088	192.168.0.11	209.165.200.235	FTP_DATA	C2jv8MWV6Xg4lb51	FX1N63eSMAEIN16S2	KDlq2XlBB6Cd-_05Vfly

1-1 of 1

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":["C2jv8MWV6Xg4lb51"],"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,"timeout":false,"md5":"e7bc9c20b0d5666365379c91294d536b","sha1":"7f754ace0342f61f8e63a10824ee11b330725"}

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