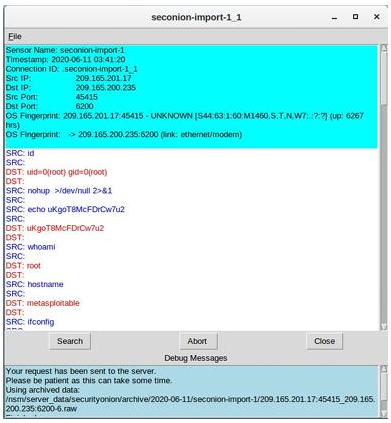
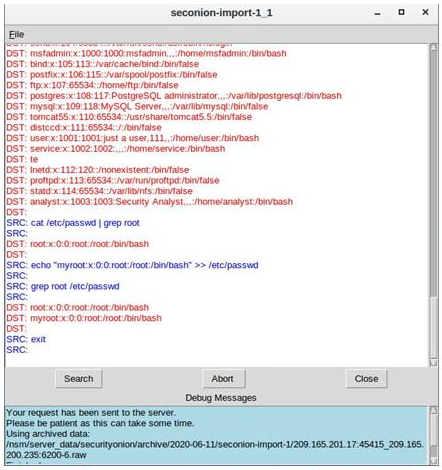
Bonus 2: Isolare un Host Compromesso Usando la 5-Tupla

f. Esamina le trascrizioni per l'alert. La trascrizione mostra le transazioni tra l'attore della minaccia (SRC) e il bersaglio (DST) durante l'attacco. L'attore della minaccia sta eseguendo comandi Linux sul bersaglio.





53

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

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

Il tipo di transazioni che si è verificato è una Ricognizione Post-Exploitation seguita dalla fase cruciale di Mantenimento dell'Accesso.

1. Ricognizione e Controllo Iniziale

I primi comandi servono all'attaccante (SRC) per confermare il suo livello di accesso e raccogliere informazioni sul bersaglio (DST).

- **Elevazione Privilegi/Verifica:**
  - SRC: id DST: uid=0(root) gid=0(root): L'attaccante ha i massimi privilegi amministrativi.
  - SRC: whoami DST: root: Conferma dell'utente.
- **Raccolta di Informazioni:**
  - SRC: hostname DST: metasploitable: Identificazione del sistema come una macchina virtuale di testing vulnerabile.
  - SRC: ifconfig: Acquisizione dei dettagli di rete.

2. Raccolta di Credenziali

L'attaccante tenta di accedere ai file di sistema che contengono le informazioni degli utenti e le password.

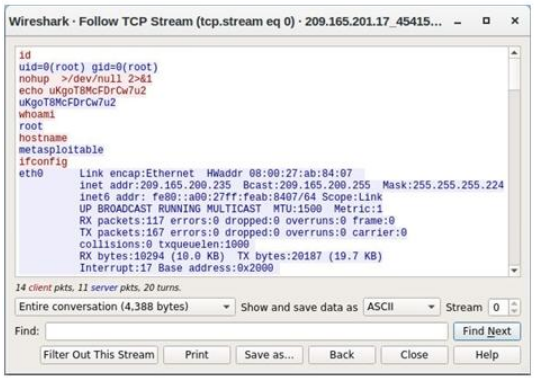
- SRC: cat /etc/shadow: Visualizza il contenuto del file /etc/shadow (dove sono archiviate le password criptate degli utenti).
- SRC: cat /etc/passwd: Visualizza il contenuto del file /etc/passwd (lista degli utenti, UID, GID, ecc.).

3. Mantenimento dell'Accesso

Creazione di una backdoor per l'accesso futuro.

- SRC: echo "myroot:x:0:0:root:/root:/bin/bash" >> /etc/passwd:
  - **Aggiunge un nuovo utente** chiamato myroot a /etc/passwd.
  - Assegna a myroot l'UID 0 e GID 0, ovvero gli stessi permessi dell'utente root.
- SRC: echo "myroot::14747:0:99999:7:::" >> /etc/shadow:
  - Aggiunge la riga corrispondente in /etc/shadow.
    L'assenza di un hash di password (myroot::) in questa parte del log è un'omissione nel log o significa che l'attaccante non ha ancora impostato la password, lasciando l'account potenzialmente disabilitato (o, in alcuni casi, usabile senza password, a seconda della configurazione del sistema).
- L'attaccante verifica l'aggiunta con i comandi grep.

b. Per visualizzare tutti i pacchetti assemblati in una conversazione TCP, fai clic con il pulsante destro su un pacchetto qualsiasi e seleziona **Follow** > **TCP Stream**.



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

Si osservano le interazioni tra client e server, in blu e in rosso, inversamente rispetto alla situazione precedente (SGUIL) e non compaiono i tag SRC e DST.

L'attaccante esegue il comando whoami sul bersaglio.

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

Il comando whoami rivela all'attaccante il suo ruolo di root.

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

L'attore della minaccia ha letto le informazioni degli utenti e le password contenute nei file di sistema

```
cat /etc/shadow
root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:14742:0:99999:7:::
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
```

a. Torna a Sguil. Fai clic con il pulsante destro sull'indirizzo IP di origine o di destinazione per l'ID dell'alert 5.1 e seleziona **Kibana IP Lookup** > **SrcIP**.

d. Filtriamo per **bro_ftp**. Passa il mouse sullo spazio vuoto accanto al conteggio dei tipi di dati bro_ftp. Seleziona **+** per filtrare solo il traffico relativo a FTP come mostrato in figura.

e. Scorri verso il basso fino a **All Logs**. Ci sono due voci elencate.

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

Time	source_ip	source_port	destination_ip
June 11th 2020, 03:53:09.086	192.168.0.11	52776	209.165.200.235
June 11th 2020, 03:53:09.086	192.168.0.11	52776	209.165.200.235

destination_port	_id
21	LDjqzXIBB6Cd-_0SbfgO
21	LTjqzXIBB6Cd-_0SbfgO

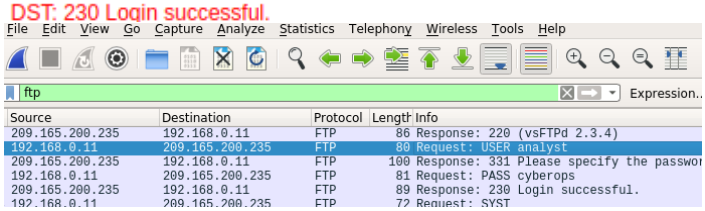
f. Espandi ed esamina entrambe le voci di log. In una di queste voci, il campo ftp_argument ha una voce di ftp://209.165.200.235/./confidential.txt. Esamina anche il messaggio nella voce di log per saperne di più su questo evento.

g. All'interno della stessa voce di log, scorri di nuovo verso l'alto fino al campo alert **_id** e fai clic sul link.

h. Esamina la trascrizione per le transazioni tra l'attaccante e il bersaglio. Se lo desideri, puoi scaricare il pcap ed esaminare il traffico usando Wireshark.

Quali sono le credenziali utente per accedere al sito FTP?

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.



Le credenziali utente per accedere al sito FTP risultano essere:

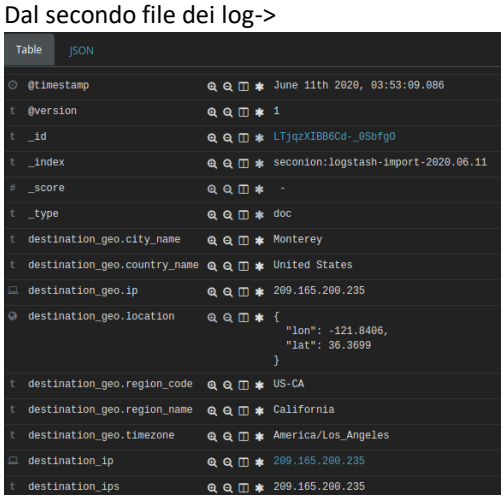
USER: analyst

PASS: cyberops

i. Ora che hai verificato che l'attaccante ha usato FTP per copiare il contenuto del file confidential.txt e poi cancellarlo dal bersaglio. **Qual è il contenuto del file? Ricorda che uno dei servizi elencati nel grafico a torta è ftp_data.**

Qui si mostra il percorso seguito per giungere alla risposta:

Dal secondo file dei log->



Time	source_ip	source_port	destination_ip	destination_port	_id
June 11th 2020, 03:54:54.173	209.165.201.17	46450	209.165.200.235	22	KzjqzXIBB6Cd-_0SZvhc
June 11th 2020, 03:54:54.172	209.165.201.17	46450	209.165.200.235	22	GjjqzXIBB6Cd-_0SS_gy
June 11th 2020, 03:53:09.088	-	-	209.165.200.235	-	KDjqzXIBB6Cd-_0SVfiy
June 11th 2020, 03:53:09.087	209.165.200.235	20	192.168.0.11	49817	DzjqzXIBB6Cd-_0SS_gy
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	LTjqzXIBB6Cd-_0SbfgO

Trovata porta di destinazione effimera 49817, che avevamo rilevato anche in precedenza da questi dati dove compare

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:

PORT 192,168,0,11,164,153.

Facendo qualche ricerca abbiamo scoperto che
PORT a1,a2,a3,a4,p1,p2, corrisponde:

a1.a2.a3.a4 è l'indirizzo IP. -> 192.168.0.11
Il numero di porta è dato da (p1 * 256) + p2 -> 49817

49817	DzjqzXIBB6Cd-_0SS_gy

Cliccando su questo file abbiamo trovato il contenuto del documento compromesso

192.168.0.11:49817_209.165.200.235:20-6-440647835.pcap

Log entry:
{"ts":"2020-06-11T03:53:09.087738Z","uid":"C2Jv8MWV6Xg4Ibb51","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":0.0013160705566406250,"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:

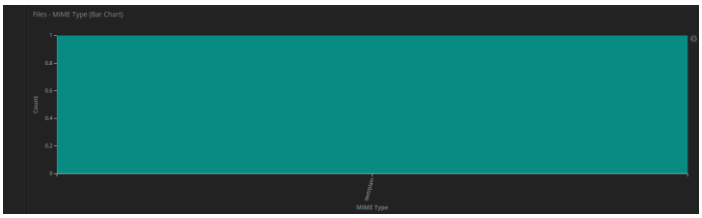
DEBUG: Using archived data: /nsm/server_data/securityonion/archive/2020-06-11/seconion-import/192.168.0.11:49817_209.165.200.235:20-6.raw
QUERY: SELECT sid FROM sensor WHERE hostname='seconion-import' AND agent_type='pcap' LIMIT 1
CAPME: Processed transcript in 0.26 seconds: 0.06 0.12 0.00 0.08 0.00

192.168.0.11:49817_209.165.200.235:20-6-440647835.pcap

j. Naviga in cima al dashboard. Seleziona **Files** sotto l'intestazione Zeek Hunting nel pannello di sinistra, come mostrato in figura. Questo ti permetterà di esaminare i tipi di file che sono stati registrati.

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

Scorri fino all'intestazione Files - Source. Quali sono le sorgenti dei file elencate?



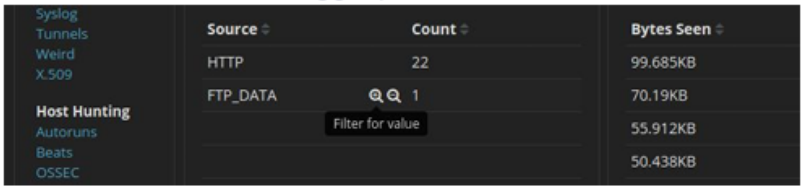
Si vede solo un tipo di file ed è di tipo text/plain.

Files - Source

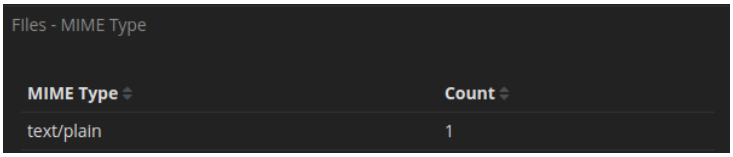
Source	Count
FTP_DATA	1

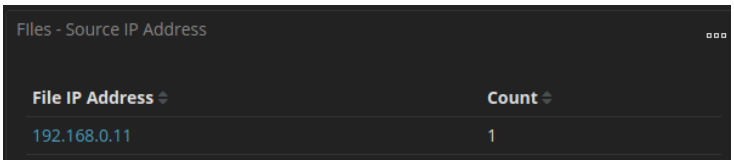
La sorgente è FTP_DATA.

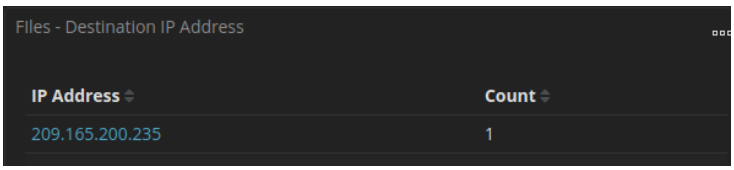
k. Filtra per **FTP_DATA** passando il mouse sullo spazio vuoto accanto al conteggio per FTP_DATA e fai clic su **+**.

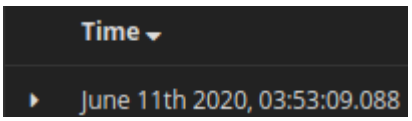


l. Scorri verso il basso per esaminare i risultati filtrati.
Qual è il tipo MIME, l'indirizzo IP di origine e di destinazione associato al trasferimento dei dati FTP? Quando si è verificato questo trasferimento?









m. Nei log dei file, espandi la voce associata ai dati FTP. Fai clic sul link associato all'alert **_id**.
Qual è il contenuto testuale del file trasferito tramite FTP?

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

Si raccomanda di scollegare la macchina da internet,
effettuare la cancellazione dell'utente "myroot" creato dall'attaccante,
cambiare le password di root e analyst, aggiornare FTP a FTPS/SFTP e di usare delle policy di sicurezza.