

Relazione: Isolamento di Host Compromessi Utilizzando la 5-Tuple

Introduzione

Questo laboratorio si concentra sull'analisi dei log raccolti a seguito dello sfruttamento di una vulnerabilità documentata. L'obiettivo è determinare quali host e file sono stati compromessi durante l'incidente. Utilizzeremo la 5-Tuple (Indirizzo IP Sorgente, Porta Sorgente, Indirizzo IP Destinazione, Porta Destinazione, Protocollo) come concetto guida per tracciare le connessioni di rete.

Il contesto specifico riguarda un file denominato confidential.txt a cui gli utenti non hanno più accesso dopo un attacco; il nostro compito è investigare come questo file sia stato compromesso, utilizzando gli strumenti disponibili sulla macchina virtuale Security Onion.

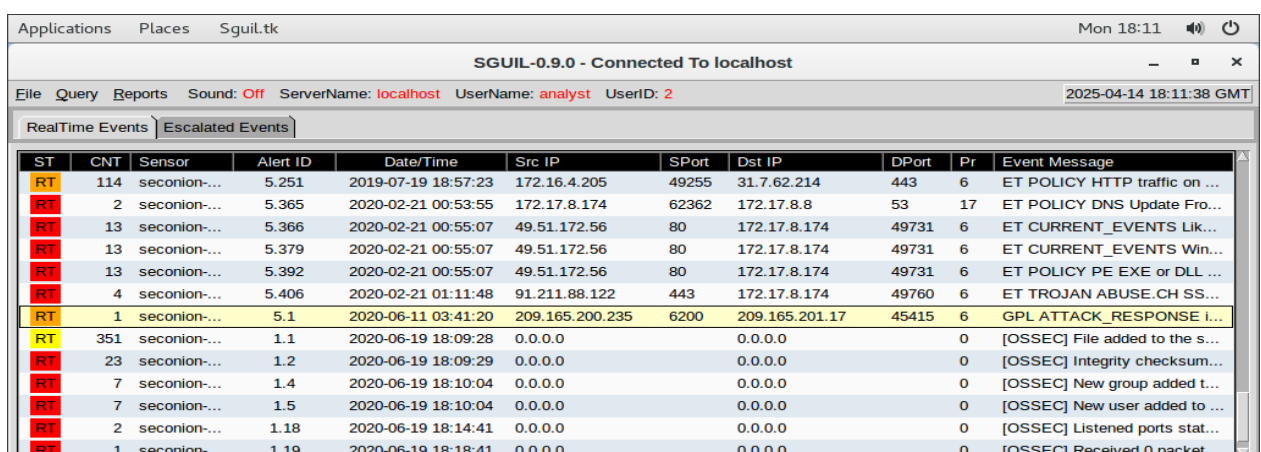
Parte 1: Esaminare gli Avvisi in Sguil

Il primo passo è stato avviare la VM Security Onion ed effettuare l'accesso come utente analyst.

Successivamente, abbiamo aperto Sguil, uno strumento di analisi degli avvisi di sicurezza di rete, selezionando tutte le interfacce monitorate.

Nella console principale di Sguil, abbiamo esaminato gli eventi in tempo reale.

Un avviso in particolare ha attirato la nostra attenzione: "GPL ATTACK_RESPONSE id check returned root" (nell'esempio del lab, Alert ID 5.1). Questo messaggio suggerisce che un comando eseguito sull'host di destinazione (209.165.200.235) ha restituito un output indicante privilegi di root (uid=0), probabilmente a seguito di un attacco proveniente dall'host sorgente (209.165.201.17).



ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	114	seconion-...	5.251	2019-07-19 18:57:23	172.16.4.205	49255	31.7.62.214	443	6	ET POLICY HTTP traffic on ...
RT	2	seconion-...	5.365	2020-02-21 00:53:55	172.17.8.174	62362	172.17.8.8	53	17	ET POLICY DNS Update Fro...
RT	13	seconion-...	5.366	2020-02-21 00:55:07	49.51.172.56	80	172.17.8.174	49731	6	ET CURRENT_EVENTS Lik...
RT	13	seconion-...	5.379	2020-02-21 00:55:07	49.51.172.56	80	172.17.8.174	49731	6	ET CURRENT_EVENTS Win...
RT	13	seconion-...	5.392	2020-02-21 00:55:07	49.51.172.56	80	172.17.8.174	49731	6	ET POLICY PE EXE or DLL ...
RT	4	seconion-...	5.406	2020-02-21 01:11:48	91.211.88.122	443	172.17.8.174	49760	6	ET TROJAN ABUSE.CH SS...
RT	1	seconion-...	5.1	2020-06-11 03:41:20	209.165.200.235	6200	209.165.201.17	45415	6	GPL ATTACK_RESPONSE I...
RT	351	seconion-...	1.1	2020-06-19 18:09:28	0.0.0.0		0.0.0.0		0	[OSSEC] File added to the s...
RT	23	seconion-...	1.2	2020-06-19 18:09:29	0.0.0.0		0.0.0.0		0	[OSSEC] Integrity checksum...
RT	7	seconion-...	1.4	2020-06-19 18:10:04	0.0.0.0		0.0.0.0		0	[OSSEC] New group added t...
RT	7	seconion-...	1.5	2020-06-19 18:10:04	0.0.0.0		0.0.0.0		0	[OSSEC] New user added to ...
RT	2	seconion-...	1.18	2020-06-19 18:14:41	0.0.0.0		0.0.0.0		0	[OSSEC] Listened ports stat...
RT	1	seconion-...	1.19	2020-06-19 18:18:41	0.0.0.0		0.0.0.0		0	[OSSEC] Received 0 packet...

Per ottenere maggiori dettagli, abbiamo selezionato le caselle "Show Packet Data" e "Show Rule". Questo ha mostrato informazioni aggiuntive sotto l'elenco degli eventi, inclusa la regola Snort che ha generato l'avviso e uno snippet dei dati del pacchetto contenente uid=0(root) gid=0(root), confermando l'ottenimento dei privilegi di root.

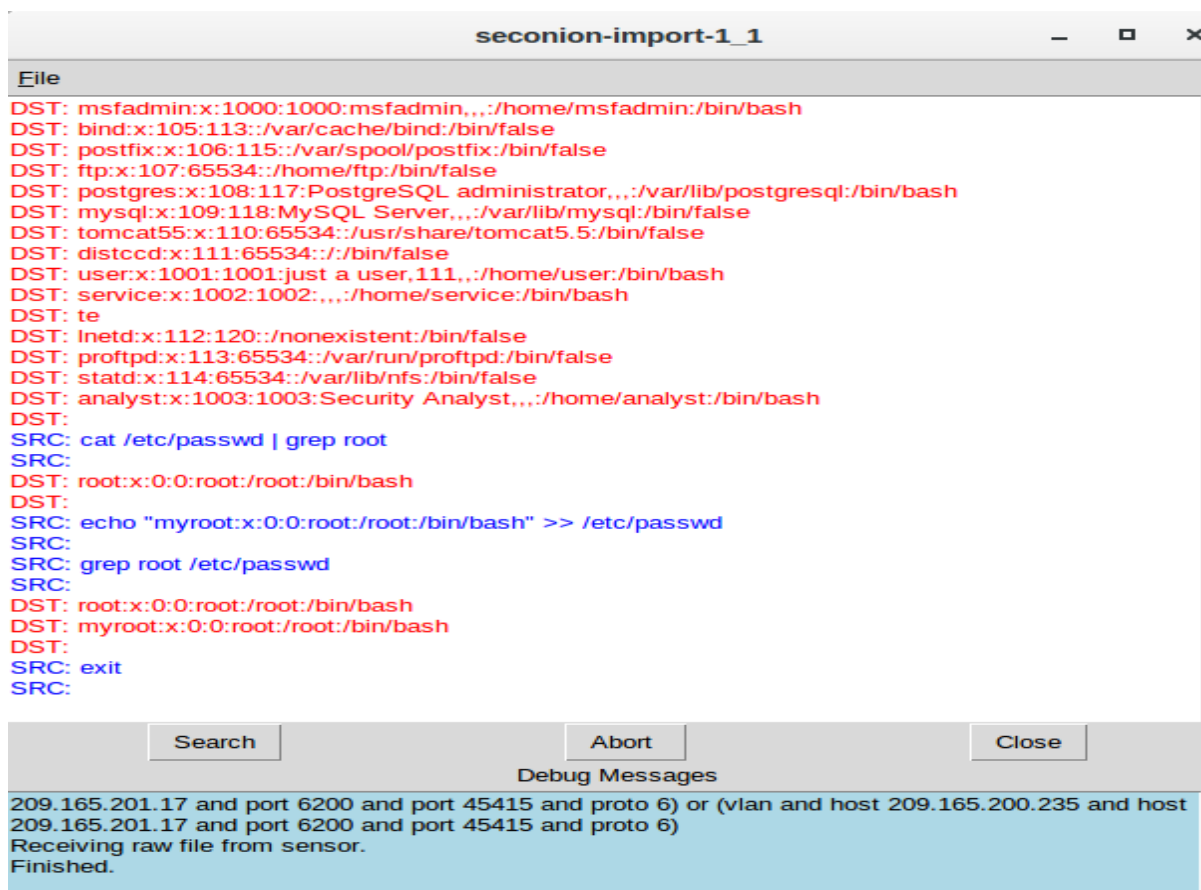
<input checked="" type="checkbox"/> Show Packet Data <input checked="" type="checkbox"/> Show Rule alert ip any any -> any any (msg:"GPL ATTACK_RESPONSE id check returned root"; content:"uid=0 28 root 29 "; fast_pattern:only; classtype:bad-unknown; sid:2100498; rev:8;													
IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum		
	209.165.200.235	209.165.201.17	4	5	0	76	31846	2	0	64	3506		
TCP	Source Port	Dest Port	RRR	SS	SY	I	Seq #	Ack #	Offset	Res	Window	Urp	ChkSum
	6200	45415	.	.	X	X	2951186435	1436935650	8	0	181	0	29271
DATA	75 69 64 3D 30 28 72 6F 6F 74 29 20 67 69 64 3D uid=0(root) gid=0(root). 30 28 72 6F 6F 74 29 0A												

Per comprendere l'intera interazione, abbiamo fatto clic con il pulsante destro del mouse sull'Alert ID 5.1 e abbiamo selezionato "Transcript".

RT	4	seconion-...	5.406	2020-02-21 01:11:48	91.211.88.122	443	172.17.8.174
RT	1	seconion-...	5.1	2020-06-11 03:41:20	209.165.200.235	6200	209.165.201.17
RT	351	seconion-...	Event History	8:09:28	0.0.0.0		0.0.0.0
RT	23	seconion-...	Transcript	8:09:29	0.0.0.0		0.0.0.0
RT	7	seconion-...	Transcript (force new)	8:10:04	0.0.0.0		0.0.0.0

La finestra della trascrizione mostra la comunicazione tra l'IP sorgente (SRC - l'attaccante, 209.165.201.17) e l'IP destinazione (DST - la vittima, 209.165.200.235) [source: 20]. Si può osservare l'attaccante eseguire comandi Linux standard sulla macchina target.

seconion-import-1_1	
File Sensor Name: seconion-import-1 Timestamp: 2020-06-11 03:41:20 Connection ID: .seconion-import-1_1 Src IP: 209.165.201.17 Dst IP: 209.165.200.235 Src Port: 45415 Dst Port: 6200 OS Fingerprint: 209.165.201.17:45415 - UNKNOWN [S44:63:1:60:M1460,S,T,N,W7:..?:?] (up: 6267 hrs) OS Fingerprint: -> 209.165.200.235:6200 (link: ethernet/modem)	
SRC: id SRC: DST: uid=0(root) gid=0(root) DST: SRC: nohup >/dev/null 2>&1 SRC: echo uKgoT8McFDrCw7u2 SRC: uKgoT8McFDrCw7u2 DST: SRC: whoami SRC: DST: root DST: SRC: hostname SRC: DST: metasploitable DST: SRC: ifconfig	
Search	Abort Close
Debug Messages 209.165.201.17 and port 6200 and port 45415 and proto 6) or (vlan and host 209.165.200.235 and host 209.165.201.17 and port 6200 and port 45415 and proto 6) Receiving raw file from sensor. Finished.	



Dalla trascrizione emerge chiaramente che l'attaccante (209.165.201.17) ha ottenuto accesso come root sulla macchina target (209.165.200.235). Ha eseguito comandi per identificarsi (whoami, id), ottenere informazioni sulla macchina (hostname, ifconfig), visualizzare file sensibili come /etc/passwd (e presumibilmente /etc/shadow), e infine ha modificato il file /etc/passwd per aggiungere un nuovo utente (myroot) con privilegi di root.

Parte 2: Passare a Wireshark

Per un'analisi a livello di pacchetto, Sguil permette di passare direttamente a Wireshark. Abbiamo fatto clic con il pulsante destro del mouse sull'Alert ID 5.1 e selezionato "Wireshark".

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	114	seconion-...	5.251	2019-07-19 18:57:23	172.16.4.205	49255	31.7.62.214	443	6	ET POLICY HTTP traffic on ...
RT	2	seconion-...	5.365	2020-02-21 00:53:55	172.17.8.174	62362	172.17.8.8	53	17	ET POLICY DNS Update Fro...
RT	13	seconion-...	5.366	2020-02-21 00:55:07	49.51.172.56	80	172.17.8.174	49731	6	ET CURRENT_EVENTS Lik...
RT	13	seconion-...	5.379	2020-02-21 00:55:07	49.51.172.56	80	172.17.8.174	49731	6	ET CURRENT_EVENTS Win...
RT	13	seconion-...	5.392	2020-02-21 00:55:07	49.51.172.56	80	172.17.8.174	49731	6	ET POLICY PE EXE or DLL ...
RT	4	seconion-...	5.406	2020-02-21 01:11:48	91.211.88.122	443	172.17.8.174	49760	6	ET TROJAN ABUSE.CH SS...
RT	1	seconion-...	5.1	2020-06-11 03:41:20	209.165.200.235	6200	209.165.201.17	45415	6	GPL ATTACK_RESPONSE i...
RT	351	seconion-...	Event History	8:09:28	0.0.0.0		0.0.0.0		0	[OSSEC] File added to the s...
RT	23	seconion-...	Transcript	8:09:29	0.0.0.0		0.0.0.0		0	[OSSEC] Integrity checksum...
RT	7	seconion-...	Transcript (force new)	8:10:04	0.0.0.0		0.0.0.0		0	[OSSEC] New group added t...
RT	7	seconion-...	Wireshark	8:10:04	0.0.0.0		0.0.0.0		0	[OSSEC] New user added to ...
RT	2	seconion-...	Wireshark (force new)	8:14:41	0.0.0.0		0.0.0.0		0	[OSSEC] Listened ports stat...
RT	1	seconion-...	NetworkMiner	8:18:41	0.0.0.0		0.0.0.0		0	[OSSEC] Received 0 packet...
			NetworkMiner (force new)							
			Bro							
			Bro (force new)							

Wireshark si è aperto mostrando i pacchetti relativi all'avviso selezionato

The screenshot shows the Wireshark interface with a packet capture of a TCP connection. The packet list shows a sequence of packets from 209.165.201.17 to 209.165.200.235. The packet details pane shows the selected packet (Frame 1) with Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol fields. The packet bytes pane shows the raw data in hexadecimal and ASCII.

Similmente a quanto fatto con la trascrizione di Sguil, abbiamo utilizzato la funzione "Segui flusso TCP" di Wireshark per ricostruire la conversazione. Abbiamo fatto clic con il pulsante destro su un pacchetto della comunicazione e scelto Segui > Flusso TCP

La finestra "Follow TCP Stream" in Wireshark mostra la stessa interazione vista nella trascrizione di Sguil . Il testo rosso rappresenta i dati inviati dall'attaccante (client, 209.165.201.17), mentre il testo blu rappresenta i dati inviati dalla vittima (server, 209.165.200.235) .

Wireshark · Follow TCP Stream (tcp.stream eq 0) · 209.165.201.17_4... — □ ×

```
id
uid=0(root) gid=0(root)
nohup >/dev/null 2>&1
echo uKgoT8McFDrCw7u2
uKgoT8McFDrCw7u2
whoami
root
hostname
metasploitable
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:ab:84:07
          inet addr:209.165.200.235  Bcast:209.165.200.255  Mask:
          255.255.255.224
          inet6 addr: fe80::a00:27ff:feab:8407/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:117 errors:0 dropped:0 overruns:0 frame:0
          TX packets:167 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:10294 (10.0 KB)  TX bytes:20187 (19.7 KB)
          Interrupt:17 Base address:0x2000

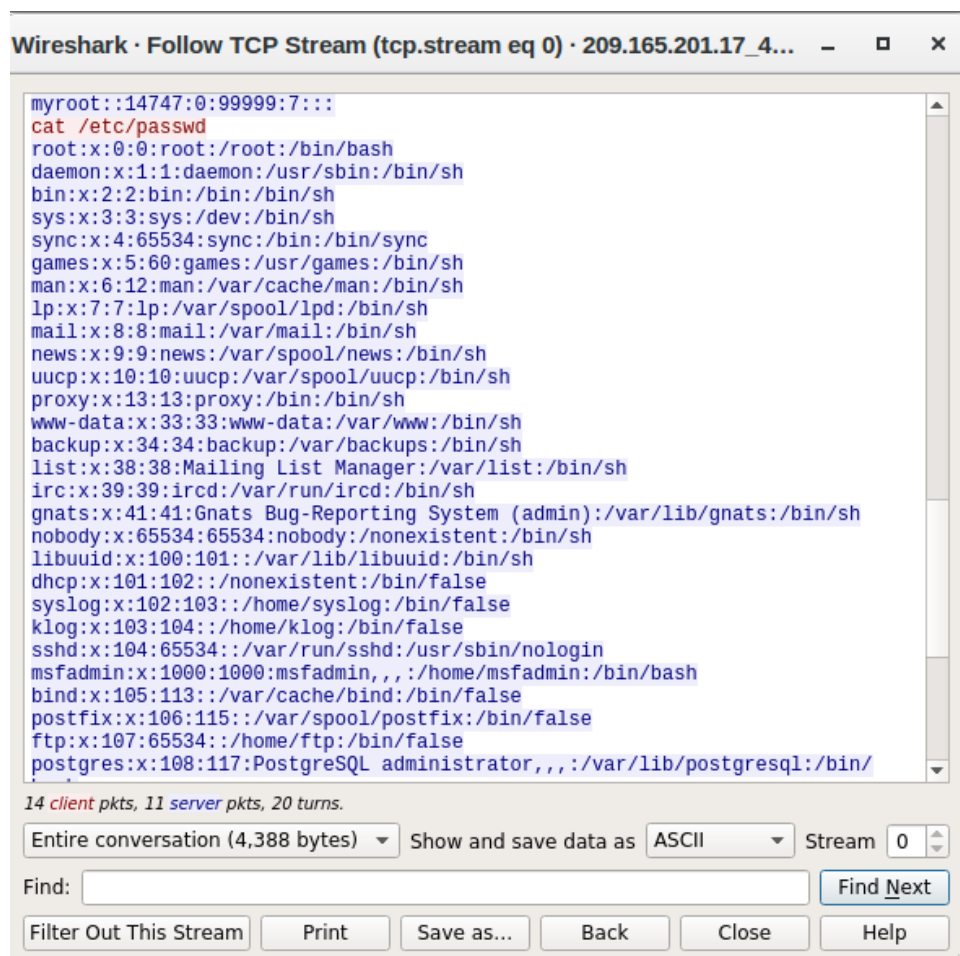
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:512 errors:0 dropped:0 overruns:0 frame:0
          TX packets:512 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:225633 (220.3 KB)  TX bytes:225633 (220.3 KB)
```

14 *client* pkts, 11 *server* pkts, 20 turns.

Entire conversation (4,388 bytes) ▾ Show and save data as ASCII ▾ Stream 0 ▾

Find:

Il comando `whoami` che restituisce `root` conferma nuovamente che l'attaccante operava con i massimi privilegi sulla macchina target (`metasploitable`, IP 209.165.200.235). Scorrendo la finestra, abbiamo potuto rivedere l'output del comando `cat /etc/passwd`, confermando che l'attaccante ha letto le informazioni sugli account utente.



Parte 3: Pivot a Kibana

Per ottenere una visione più ampia dell'attività relativa agli indirizzi IP coinvolti, siamo tornati a Sguil e abbiamo utilizzato la funzionalità di "pivot" verso Kibana. Abbiamo fatto clic con il pulsante destro sull'indirizzo IP di origine (o destinazione) dell'Alert ID 5.1 e scelto Kibana IP Lookup > SrcIP.

RT

4

seconion-...

5.406

2020-02-21 01:11:48

91.211.88.122

443

172.17.8.174

49760

6

ET TROJAN ABUSE.CH SS...

RT

1

seconion-...

5.1

2020-06-11 03:41:20

209.165.200.235

6200

209.165.201.17

45415

6

GPL ATTACK_RESPONSE i...

RT

351

seconion-...

1.1

2020-06-19 18:09:28

Quick Query

0.0.0.0

0

[OSSEC] File added to the s...

RT

23

seconion-...

1.2

2020-06-19 18:09:29

Advanced Query

0.0.0.0

0

[OSSEC] Integrity checksum...

RT

7

seconion-...

1.4

2020-06-19 18:10:04

Dshield IP Lookup

0.0.0.0

0

[OSSEC] New group added t...

RT

7

seconion-...

1.5

2020-06-19 18:10:04

Copy IP Address

0.0.0.0

0

[OSSEC] New user added to ...

RT

2

seconion-...

1.18

2020-06-19 18:14:41

Alexa IP Lookup

0.0.0.0

0

[OSSEC] Listened ports stat...

RT

1

seconion-...

1.19

2020-06-19 18:18:41

Bing IP Lookup

0.0.0.0

0

[OSSEC] Received 0 packet...

CentralOps IP Lookup

DomainTools IP Lookup

Google IP Lookup

Kibana IP Lookup

MDL IP Lookup

SafeBrowsing IP Lookup

VirusTotal IP Lookup

ZeusTracker IP Lookup

IP Resolution

Agent Status

Snort Statistics

System Msg

☐ Reverse DNS

☒ Enable External DNS

Src IP:

Src Name:

Dst IP:

Dst Name:

Seq #

Ack #

Offset

Res

Window

Urp

ChkS

sg:"GPL ATTACK_RESPONSE id check returned root";

srcip:only; classtype:bad-unknown; sid:2100498; rev:8;

dstip:209.165.201.17

4

5

0

76

31846

2

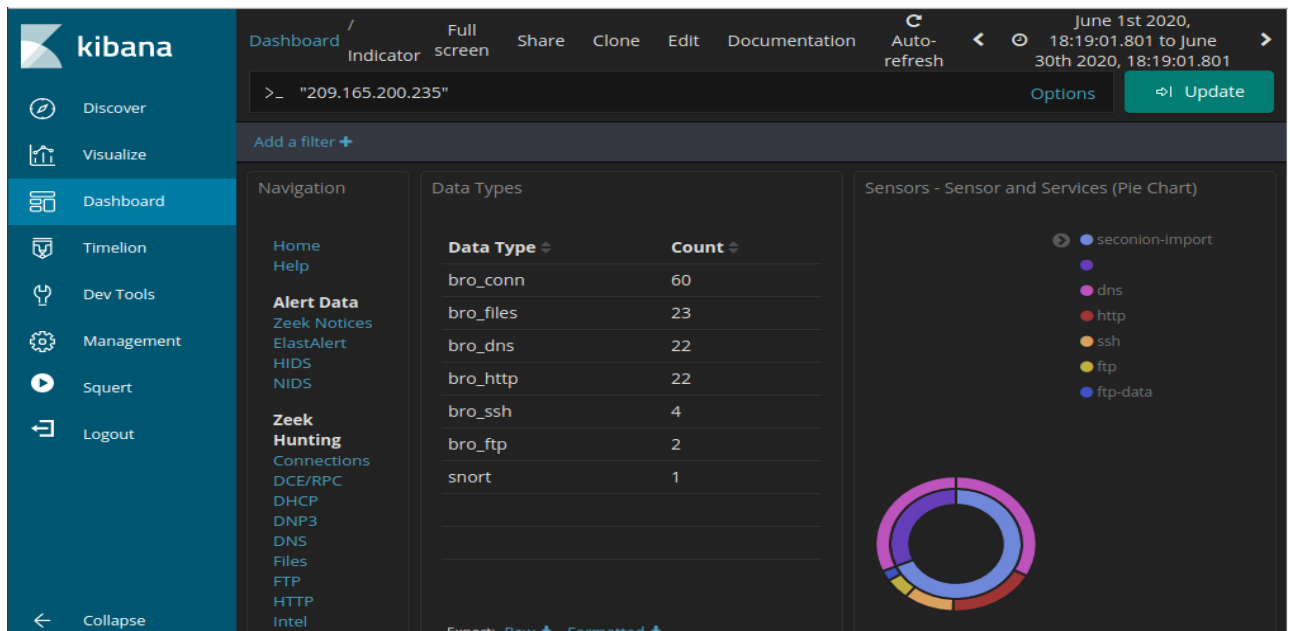
0

64

350

Dopo aver effettuato l'accesso a Kibana (utente analyst, password cyberops) e aver eventualmente gestito avvisi di sicurezza del browser, ci siamo assicurati che l'intervallo di tempo includesse la data dell'attacco (11 giugno 2020), modificando l'intervallo tramite la scheda "Assoluto" se necessario.

La dashboard di Kibana mostrava vari tipi di log associati all'indirizzo IP selezionato. Dato che il problema iniziale riguardava il file confidential.txt reso inaccessibile, abbiamo cercato indizi su come potesse essere stato manipolato. Nel grafico a torta "Sensors - Sensor and Services", abbiamo notato la presenza dei tipi di log ftp e ftp-data, suggerendo un possibile coinvolgimento del protocollo FTP.



Per investigare l'attività FTP, abbiamo filtrato i risultati per il tipo di log bro_ftp (log del protocollo di controllo FTP generati da Zeek/Bro). Abbiamo passato il mouse accanto al conteggio per bro_ftp e cliccato sull'icona + per applicare il filtro.

bro_ssh	4
bro_ftp	2
snort	

A tooltip 'Filter for value' is visible next to the 'bro_ftp' count of 2.

Scorrendo verso il basso fino alla sezione "All Logs" (ora filtrata), abbiamo trovato due voci relative al controllo FTP. Queste voci mostravano una comunicazione tra l'IP sorgente **192.168.0.11** (porta 52776) e l'IP destinazione **209.165.200.235** (porta 21, la porta standard per il controllo FTP).

Time	source_ip	source_port	destination_ip	destination_port	uid
June 11th 2020, 03:53:09.086	192.168.0.11	52776	209.165.200.235	21	C5GkeA4t8oXZdWTPR6
June 11th 2020, 03:53:09.086	192.168.0.11	52776	209.165.200.235	21	C5GkeA4t8oXZdWTPR6

Espandendo i dettagli di una di queste voci di log, abbiamo trovato un campo `ftp_argument` contenente `ftp://209.165.200.235/./confidential.txt` . Questo indicava un comando FTP relativo a quel file specifico. Per vedere l'intera sessione FTP, abbiamo cliccato sul link nel campo `_id` della voce di log

All Logs					
Time	Source IP	Source Port	Destination IP	Destination Port	...
June 11th 2020, 03:53:09.086	192.168.0.11	52776	209.165.200.235	21	C5GkeA4t8oXZdWTPR6
Table JSON View surrounding documents View source					
@timestamp	June 11th 2020, 03:53:09.086				
@version	1				
_id	LDiaqzXIBB6Cd- 0Sbfa0				
_index	seconion:logstash-import-2020.06.11				
_score	-				

Questo ci ha portato nuovamente all'interfaccia capME!, mostrando la trascrizione della sessione FTP . Analizzando la trascrizione, abbiamo identificato le credenziali utilizzate per l'accesso FTP:

close

[192.168.0.11:52776_209.165.200.235:21-6-107098227.pcap](#)

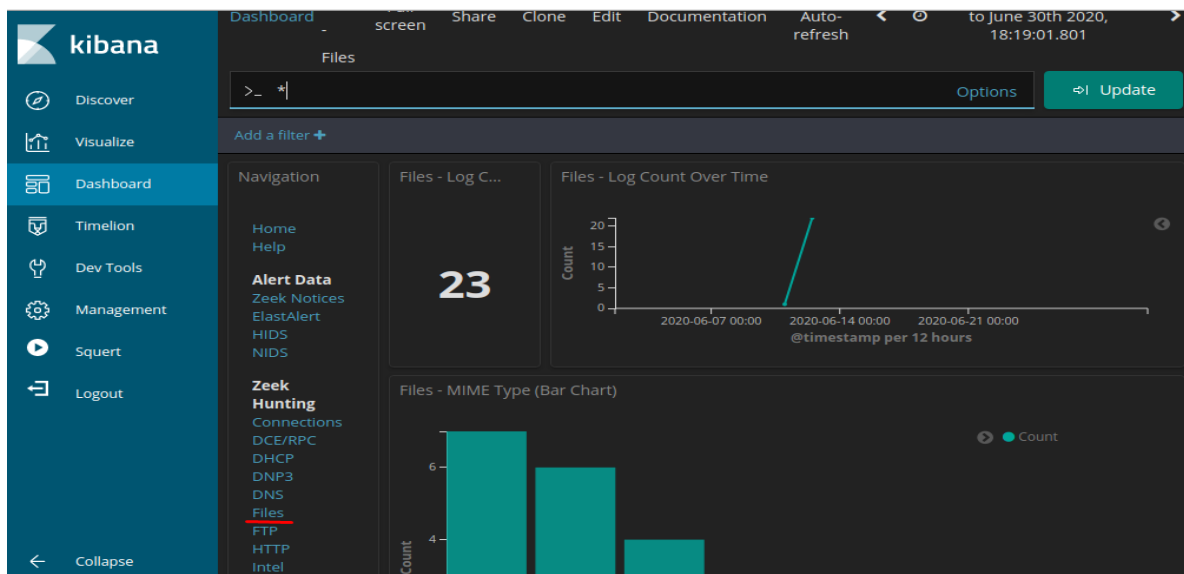
Log entry:
{\"ts\":\"2020-06-11T03:53:09.086840Z\",\"uid\":\"C5GkeA4t8oXZdWTPR6\",\"id.orig_h\":\"192.168.0.11\",\"id.orig_p\":52776,\"id.resp_h\":\"209.165.200.235\",\"id.resp_p\":21,\"user\":\"analyst\",\"password\":\"<hidden>\",\"command\":\"STOR\",\"arg\":\"ftp://209.165.200.235/./confidential.txt\",\"mime_type\":\"text/plain\",\"reply_code\":\"226\",\"reply_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:

- **Username:** analyst
- **Password:** cyberops

La trascrizione mostra anche il comando STOR `ftp://209.165.200.235/./confidential.txt` , che indica un'operazione di upload (memorizzazione) del file `confidential.txt` dal client (192.168.0.11) al server (209.165.200.235) utilizzando le credenziali dell'utente analyst.

Per visualizzare il contenuto effettivo del file trasferito, dovevamo analizzare i log relativi al trasferimento dati FTP (`ftp-data`). Siamo tornati alla dashboard di Kibana, abbiamo rimosso il filtro `bro_ftp`, e abbiamo navigato nella sezione "Files" sotto "Zeek Hunting" .



Qui, nella sezione "Files - Source", abbiamo visto che i file registrati provenivano da HTTP e FTP_DATA. Abbiamo filtrato per FTP_DATA cliccando sull'icona + corrispondente.

Files - Source	
Source	Count
HTTP	22
FTP_DATA	1

I risultati filtrati mostravano un singolo trasferimento di file:

- **Tipo MIME:** text/plain
- **IP Sorgente (chi ha inviato):** 192.168.0.11
- **IP Destinazione (chi ha ricevuto):** 209.165.200.235
- **Timestamp:** 11 giugno 2020, 03:53:09.088

Files - MIME Type		Files - Source IP Address		Files - Destination IP Address	
MIME Type	Count	File IP Address	Count	IP Address	Count
text/plain	1	192.168.0.11	1	209.165.200.235	1

Espandendo questa voce di log e cliccando nuovamente sul link `_id`, siamo stati portati alla trascrizione capME! per la connessione dati FTP. Essa mostrava il contenuto effettivo del file `confidential.txt` trasferito:

[Logout](#)

close

[192.168.0.11:49817_209.165.200.235:20-6-67833155.pcap](#)
Log entry:
{"ts":"2020-06-11T03:53:09.088773Z","fluid":"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,"timeout":false,"md5":"e7bc9c20bfd5666365379c91294d536b","sha1":"7f54acee0342f6161f8e63a10824ee11b330725"}

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 0.59 seconds: 0.12 0.36 0.00 0.11 0.00

[192.168.0.11:49817_209.165.200.235:20-6-67833155.pcap](#)

Il contenuto del file era: "CONFIDENTIAL DOCUMENT DO NOT SHARE This document contains information about the last security breach." .

Raccomandazioni e Conclusioni

L'analisi ha rivelato due eventi principali:

1. Un attacco riuscito che ha portato all'ottenimento di privilegi di root sull'host 209.165.200.235 da parte dell'attaccante all'indirizzo 209.165.201.17.
L'attaccante ha aggiunto un utente root backdoor (myroot).
2. Un trasferimento FTP del file confidential.txt dall'host 192.168.0.11 all'host 209.165.200.235, utilizzando le credenziali valide dell'utente analyst (analyst/cyberops).

Questi eventi potrebbero essere correlati o separati. Tuttavia, l'uso delle credenziali analyst per il trasferimento FTP è un grave problema di sicurezza.

Come minimo, la raccomandazione immediata è di **cambiare la password dell'utente analyst** su tutti i sistemi in cui viene utilizzata, in particolare sugli host identificati nei log (209.165.200.235 e 192.168.0.11) [source: 81, 82].

Inoltre, è necessario indagare e rimuovere l'account myroot dall'host 209.165.200.235 e identificare e correggere la vulnerabilità che ha permesso l'accesso root iniziale dall'IP 209.165.201.17.

Questo laboratorio ha dimostrato l'efficacia dell'utilizzo combinato di Sguil, Wireshark e Kibana per analizzare un incidente di sicurezza, partendo da un avviso iniziale e "pivotando" tra i diversi strumenti per raccogliere dettagli a livello di pacchetto, di flusso e di log aggregati, fino a ricostruire le azioni dell'attaccante e identificare le credenziali e i dati compromessi.

