

Isolamento di un Host Compromesso tramite 5-Tuple

Isolamento di un Host Compromesso tramite 5-Tuple

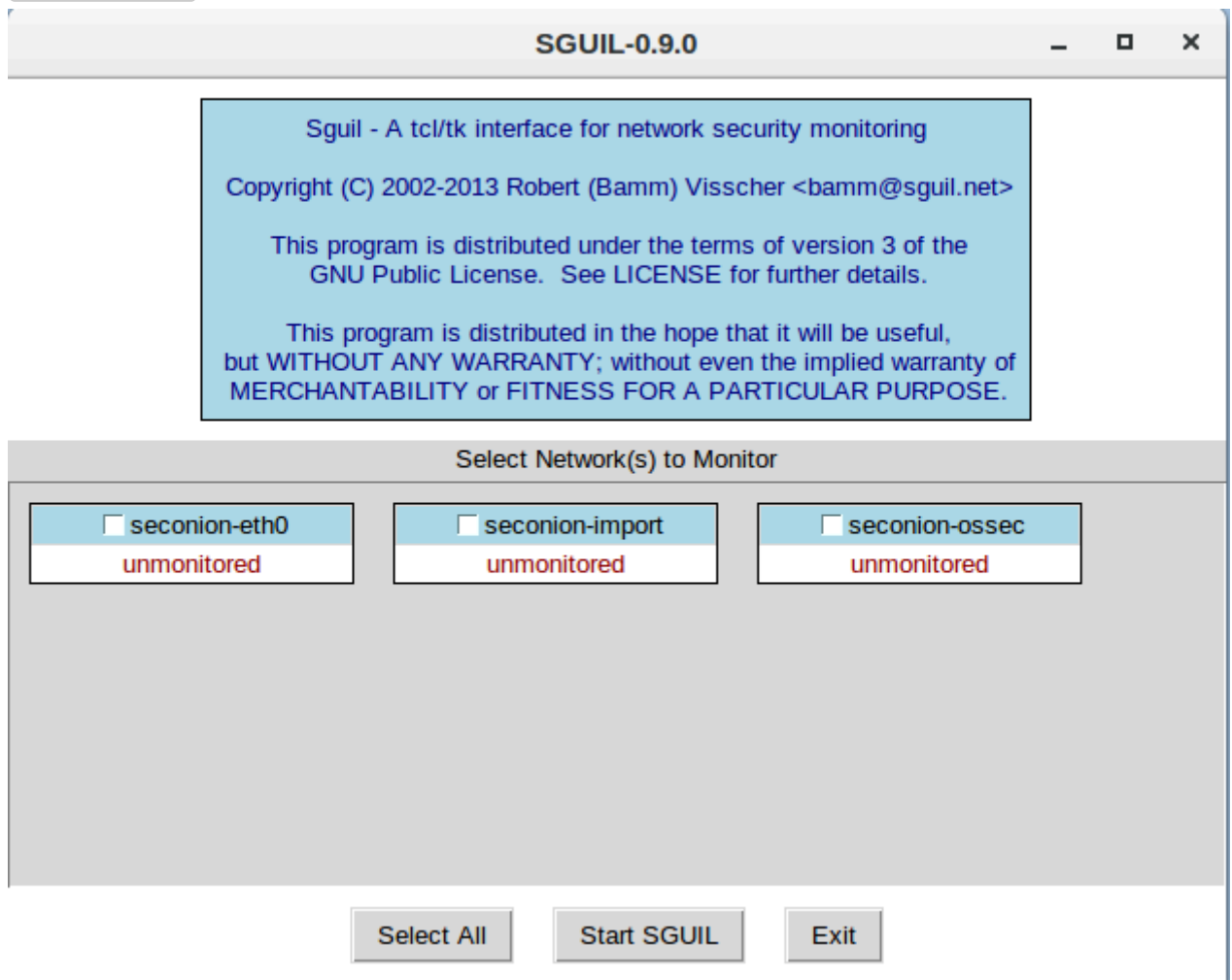
Parte 1: Revisione degli Avvisi in Sguil

1. Avvio della VM Security Onion

- Ho avviato la macchina virtuale Security Onion.
- Ho effettuato l'accesso con l'utente `analyst` e la password `cyberops`.

2. Apertura di Sguil

- Ho aperto Sguil e ho effettuato il login.
- Ho selezionato `Select All` per selezionare tutte le interfacce e ho avviato Sguil cliccando su `Start SGUIL`.



Username: analyst

Password: cyberops

3. Revisione degli eventi in Sguil

- Ho esaminato gli eventi nella colonna `Event Message`.
- Ho individuato l'evento `GPL ATTACK_RESPONSE id check returned root`, che indica che un attacco ha ottenuto accesso root.
- L'host `209.165.200.235` ha restituito accesso root all'host `209.165.201.17`.

RT	seconion-imp...	2020-02-21 01:11...	91.211.88.122	443	172.17.8.174	49760	6	ET TROJAN ABUSE.CH SSL Blacklist Malicious SS...
RT	seconion-imp...	2020-06-11 03:41...	209.165.200.235	6200	209.165.201.17	45415	6	GPL ATTACK_RESPONSE id check returned root
RT	seconion-ossec	2020-06-19 18:09...	0.0.0.0		0.0.0.0		0	[OSSEC] File added to the system.

4. Esame dettagliato degli avvisi

- Ho selezionato le opzioni `Show Packet Data` e `Show Rule` per visualizzare i dettagli dell'avviso.

IP Resolution Agent Status Snort Statistics System Msg

☐ Reverse DNS ☒ Enable External DNS

Src IP:
Src Name:
Dst IP:
Dst Name:
Whois Query: ☒ None ☐ Src IP ☐ Dst IP

☒ Show Packet Data ☒ Show Rule

alert ip any any -> any any (msg:"GPL ATTACK_RESPONSE id check returned root"; content:"uid=0/root/291"; fast_pattern:only; classtype:bad-unknown; sid:2100408; rev:8;

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	hkSum
IP	209.165.200.235	209.165.201.17	4	5	0	76	31846	2	0	64	350

U A P R S F

TCP	Source Port	Dest Port	R R R C S S Y I	Seq #	Ack #	Offset	Res	Window	Urp	ChkSum
TCP	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

Search Packet Payload ☐ Hex ☒ Text ☐ NoCase

- Ho cliccato con il tasto destro sull'alert ID 5.1 e selezionato `Transcript`.

RT 1 seconion-imp... 5.1 2020-06-11 03:41

RT 351 seconion-ossec

RT 23 seconion-ossec

RT 7 seconion-ossec

RT 7 seconion-ossec

RT 2 seconion-ossec

RT 1 seconion-ossec

IP Resolution Agent Status

☐ Reverse DNS ☒ Enable External DNS

Event History
Transcript
Transcript (force new)
Wireshark
Wireshark (force new)
NetworkMiner
NetworkMiner (force new)
Bro
Bro (force new)

5. Analisi dei transcript

- Ho analizzato i dati dei transcript per comprendere le interazioni tra il client (attaccante) e il server (target).
- L'attaccante con IP `209.165.201.17` ha ottenuto accesso root al sistema con IP `209.165.200.235`.
- L'attaccante ha esplorato il file system, copiato il file `shadow` e modificato i file `/etc/shadow` e `/etc/passwd`.

```
DST: klog:x:200:20:/nonexistent:/bin/false
DST: sshd:x:104:65534:/var/run/sshd:/usr/sbin/nologin
DST: msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
DST: bind:x:105:113:/var/cache/bind:/bin/false
DST: postfix:x:106:115:/var/spool/postfix:/bin/false
DST: ftp:x:107:65534:/home/ftp:/bin/false
DST: postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
DST: mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
DST: tomcat55:x:110:65534:/usr/share/tomcat5.5:/bin/false
DST: distccd:x:111:65534:/bin/false
DST: user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
DST: service:x:1002:1002,,,:/home/service:/bin/bash
DST: te
DST: inetd:x:112:120:/nonexistent:/bin/false
DST: proftpd:x:113:65534:/var/run/proftpd:/bin/false
DST: statd:x:114:65534:/var/lib/nfs:/bin/false
DST: analyst:x:1003:1003:Security Analyst,,,:/home/analyst:/bin/bash
DST:
SRC: cat /etc/passwd | grep root
SRC:
DST: root:x:0:0:root:/root:/bin/bash
DST:
SRC: echo "myroot:x:0:0:root:/root:/bin/bash" >> /etc/passwd
SRC:
SRC: grep root /etc/passwd
SRC:
DST: root:x:0:0:root:/root:/bin/bash
DST: myroot:x:0:0:root:/root:/bin/bash
DST:
SRC: exit
SRC:
```

Search

Abort

Debug Mess

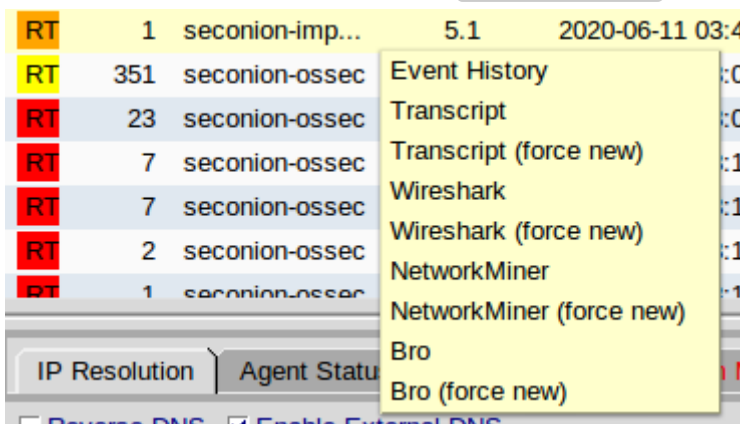
1001000000

Creating unique data file: /usr/sbin/tcpdump -r /nsm/sensor_data/seconion-import/dailylogs/

Parte 2: Pivot su Wireshark

1. Apertura di Wireshark

- Ho cliccato con il tasto destro sull'alert ID 5.1 e selezionato Wireshark.



- Ho esaminato la visualizzazione principale di Wireshark.

209.165.201.17_45415_209.165.200.235_6200-6.raw

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
1	2020-06-11 03:41:20.787779	209.165.201.17	209.165.200.235	TCP	74	45415
2	2020-06-11 03:41:20.787834	209.165.200.235	209.165.201.17	TCP	74	6200
3	2020-06-11 03:41:20.787967	209.165.201.17	209.165.200.235	TCP	66	45415
4	2020-06-11 03:41:20.788838	209.165.201.17	209.165.200.235	TCP	69	45415
5	2020-06-11 03:41:20.788905	209.165.200.235	209.165.201.17	TCP	66	6200
6	2020-06-11 03:41:20.789872	209.165.200.235	209.165.201.17	TCP	90	6200
7	2020-06-11 03:41:20.790022	209.165.201.17	209.165.200.235	TCP	66	45415
8	2020-06-11 03:41:20.790667	209.165.201.17	209.165.200.235	TCP	88	45415

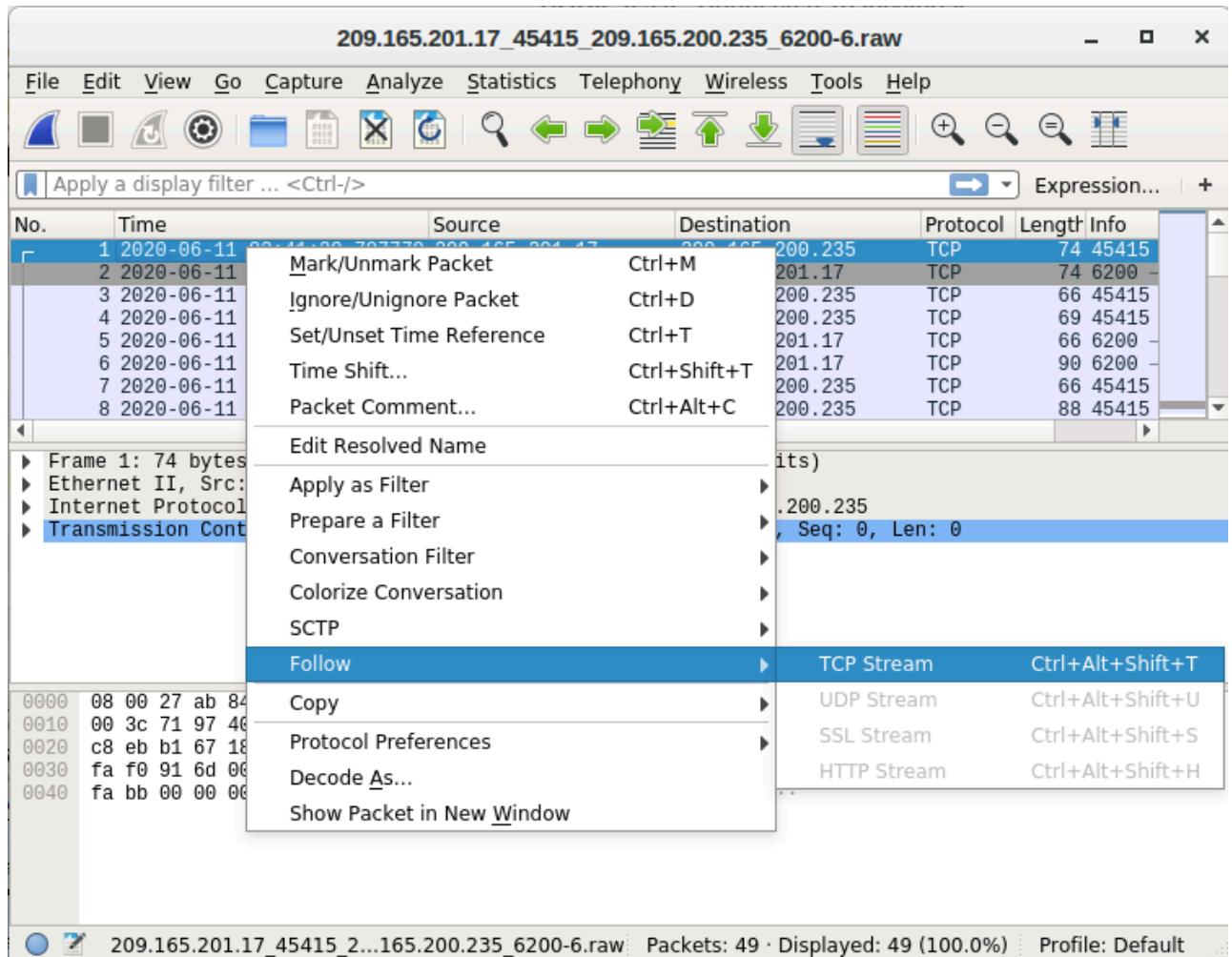
▶ Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
 ▶ Ethernet II, Src: 00:50:56:b3:72:09, Dst: 08:00:27:ab:84:07
 ▶ Internet Protocol Version 4, Src: 209.165.201.17, Dst: 209.165.200.235
 ▶ Transmission Control Protocol, Src Port: 45415, Dst Port: 6200, Seq: 0, Len: 0

0000	08 00 27 ab 84 07 00 50 56 b3 72 09 08 00 45 00	..'....P V.r...E.
0010	00 3c 71 97 40 00 3f 06 94 dc d1 a5 c9 11 d1 a5	<q.@.?.....
0020	c8 eb b1 67 18 38 55 a5 e5 de 00 00 00 00 a0 02	...g·8U.....
0030	fa f0 91 6d 00 00 02 04 05 b4 04 02 08 0a 86 79	...m.....y
0040	fa bb 00 00 00 00 01 03 03 07

209.165.201.17 45415 2...165.200.235 6200-6.raw Packets: 49 · Displayed: 49 (100.0%) Profile: Default

2. Analisi del flusso TCP

- Ho cliccato con il tasto destro su un pacchetto e selezionato `Follow > TCP Stream`.



- Il flusso TCP ha mostrato la transazione tra l'attaccante (testo rosso) e il target (testo blu).
- L'hostname del target è `metasploitable`, con IP `209.165.200.235`.

```
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)
```

3. Comando whoami dell'attaccante

- L'attaccante ha eseguito `whoami`, ottenendo la risposta `root`, confermando il controllo del sistema.

```
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...?:?]
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:
SRC: echo uKgoT8McFDrCw7u2
SRC:
DST: uKgoT8McFDrCw7u2
DST:
SRC: whoami
SRC:
DST: root
DST:
SRC: hostname
SRC:
DST: metasploitable
DST:
SRC: ifconfig
SRC:
DST: eth0 Link encap:Ethernet HWaddr 08:00:27:ab:84:07
DST: 1: 1: 000 105 000 005 0: 1: 000 105 000 005 1: 1: 005 005 005 001
```

4. Dati analizzati nel flusso TCP

- Ho scansionato il flusso TCP alla ricerca dei dati letti dall'attaccante.

- L'attaccante ha consultato informazioni sugli account utente.

```
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
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
atd:x:114:65534::/var/lib/atd:/bin/false
```

5. Chiusura di Wireshark

- Ho chiuso la finestra del flusso TCP e poi Wireshark.

Parte 3: Pivot su Kibana

1. Accesso a Kibana

- Sono tornata su Sguil, ho cliccato con il tasto destro sull'IP `209.165.200.235` e selezionato

```
Kibana IP Lookup > SrcIP.
```


RT	1	seconion-imp...	5.1	2020-06-11 03:41...	209.165.200.235	6200	209.165.201.1
RT	351	seconion-ossec	1.1	2020-06-19 18:09...	Quick Query		0.0
RT	23	seconion-ossec	1.2	2020-06-19 18:09...	Advanced Query		0.0
RT	7	seconion-ossec	1.4	2020-06-19 18:10...	Dshield IP Lookup		0.0
RT	7	seconion-ossec	1.5	2020-06-19 18:10...	Copy IP Address		0.0
RT	2	seconion-ossec	1.18	2020-06-19 18:14...	Alexa IP Lookup		0.0
RT	1	seconion-ossec	1.10	2020-06-19 18:18...	Bing IP Lookup		0.0

IP Resolution
Agent Status
Snort Statistics
System Message

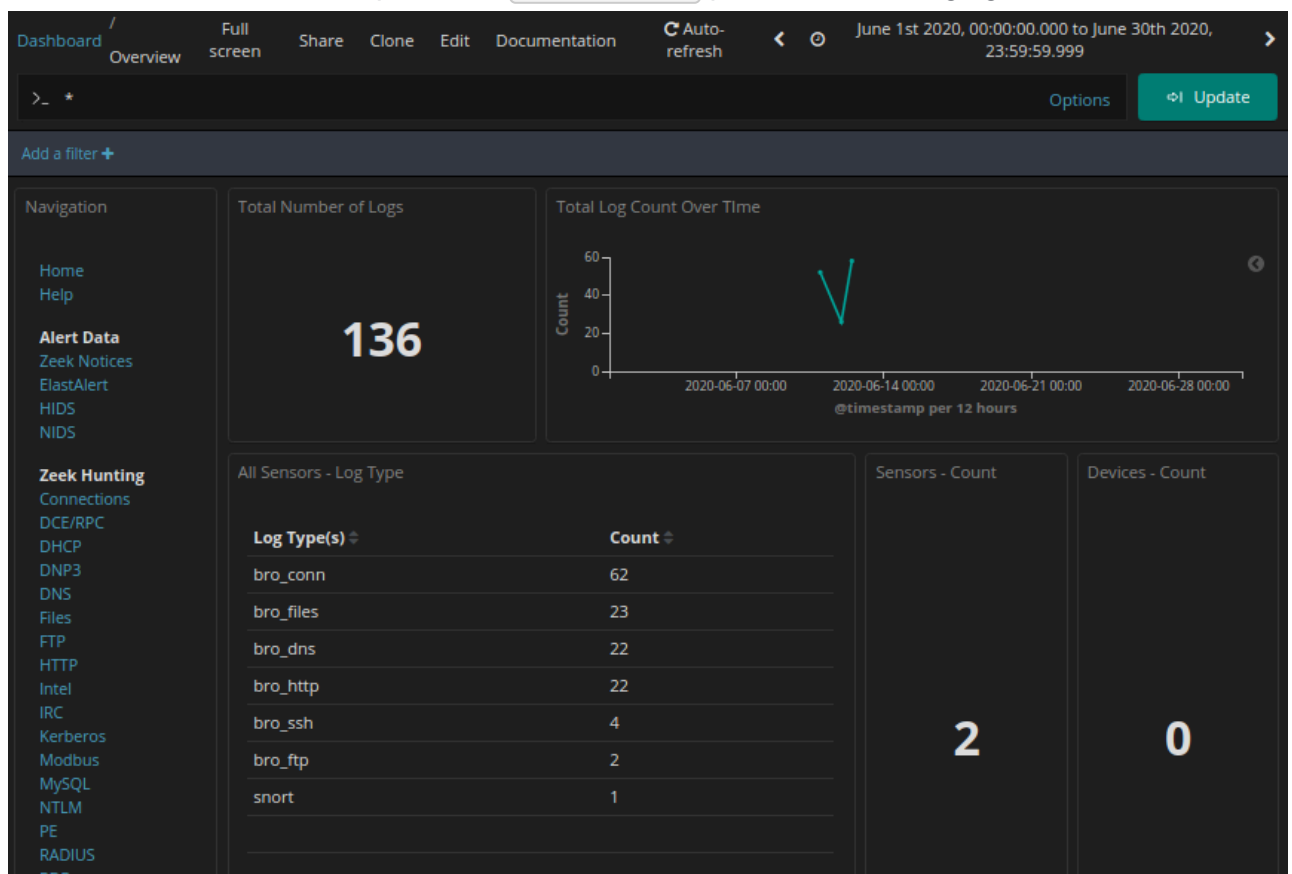
Reverse DNS
☒ Enable External DNS

Src IP:
Src Name:
Dst IP:
Dst Name:

Quick Query
Advanced Query
Dshield IP Lookup
Copy IP Address
Alexa IP Lookup
Bing IP Lookup
CentralOps IP Lookup
DomainTools IP Lookup
Google IP Lookup
Kibana IP Lookup
MDL IP Lookup
SafeBrowsing IP Lookup
VirusTotal IP Lookup
ZeusTracker IP Lookup

SrcIP
DstIP
U A P R S
R C S S Y
G K H T N

- Ho effettuato il login con l'utente `analyst` e la password `cyberops`.
- Ho cambiato l'intervallo temporale su `Giugno 2020` per includere l'11 giugno.



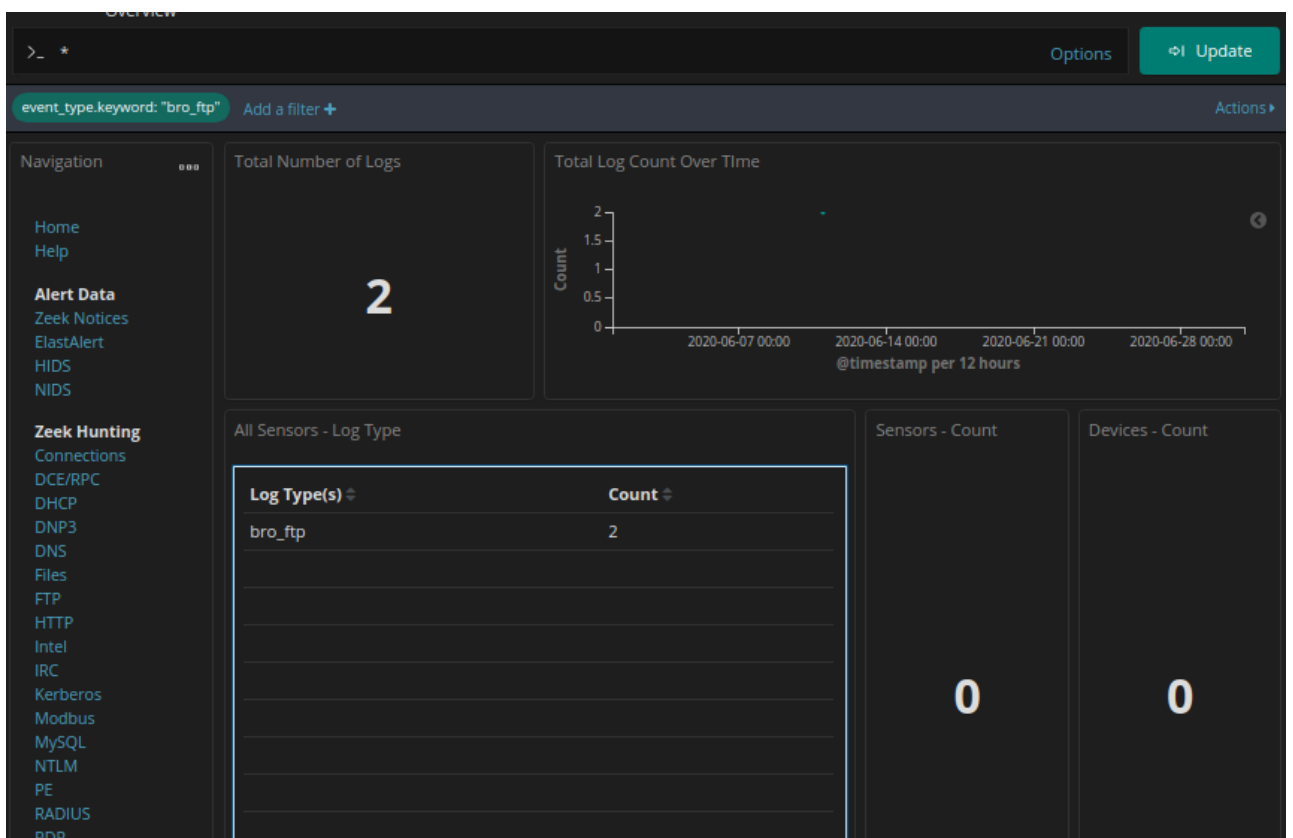
2. Identificazione del protocollo FTP

- Nella sezione `Sensors - Sensors and Services (Pie Chart)`, ho notato la presenza di `ftp`.

- Ho filtrato per `bro_ftp` cliccando su `+` accanto al conteggio.

All Sensors - Log Type

Log Type(s) ▾	Count ▾
bro_conn	62
bro_files	23
bro_dns	22
bro_http	22
bro_ssh	4
bro_ftp	2
snort	1



3. Analisi del traffico FTP

- Ho trovato due voci di log relative al traffico FTP.
- **IP sorgente:** `192.168.0.11:52776`
- **IP destinazione:** `209.165.200.235:21`

1-2 of 2

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	LTjqzXIBB6Cd-_0SbfgO

1-2 of 2

4. Esame degli argomenti FTP

- Tramite capMe! ho trovato il trasferimento del file `confidential.txt`.

```
OS Fingerprint: -> 209.165.200.235:21 (link: ethernet/modem)
DST: 220 (vsFTPD 2.3.4)
SRC:
DST:
SRC: USER analyst
SRC:
DST: 331 Please specify the password.
DST:
SRC: PASS cyberops
SRC:
DST: 230 Login successful.
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:
SRC: STOR confidential.txt
SRC:
DST: 150 Ok to send data.
DST:
DST: 226 Transfer complete.
DST:
SRC: QUIT
SRC:
DST: 221 Goodbye.
DST:
```

5. Credenziali FTP utilizzate

- L'attaccante ha usato le credenziali:

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

```
Log entry:
{"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":"","analys
r","password":"","command":"PORT","arg":"192.168.0.11,194.153","reply_code":200,"reply_msg":"PORT command successful. Consider using PASV.,"data_channel.p
assive":false,"data_channel.orig_h":"209.165.200.235","data_channel.resp_h":"192.168.0.11","data_channel.resp_p":49817}

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)
```

6. Analisi dei dati FTP

- Ho filtrato per `FTP_DATA` nella dashboard di Kibana.
- Ho analizzato il tipo di file e la fonte del trasferimento:
 - **MIME Type:** `text/plain`
 - **IP sorgente:** `192.168.0.11`
 - **IP destinazione:** `209.165.200.235`

- **Data del trasferimento:** 11 giugno 2020, 3:53 AM

[illegible]

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	C2jv8MWW6Xg4lbb51	FX1V63eSMAEiN16S2	KDjqzXIBB6Cd_0SVfij

7. Contenuto del file `confidential.txt`

- Ho espanso i log relativi al trasferimento FTP e aperto l'`alert_id`.
- Il contenuto del file trasferito era:

CONFIDENTIAL DOCUMENT

DO NOT SHARE

This document contains information about the last security breach.

[192.168.0.11:49817 209.165.200.235:20-6-1938136318.pcap](#)

Log entry:

```
["ts": "2020-06-11T03:53:09.088773Z", "uid": "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": "e7bc9c20bdf5666365379c91294d3d3b", "sha1": "17f54ace0c342f61618f3ca10824ee11b330725"]
```

Sensor Name: seconion-import

Timestamp: 2020-06-11 03:53:09

Connection ID: 0

Src IP: 192.168.0.11

Dst IP: 209.165.

Src Port: 49152

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/securityunion/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 0.55 seconds: 0.18 0.21 0.00 0.15 0.00

[192.168.0.11:49817 209.165.200.235:20-6-1938136318.pcap](#)

Raccomandazioni per la Sicurezza

Con le informazioni raccolte, ho identificato una violazione di sicurezza. Per prevenire ulteriori accessi non autorizzati, consiglio:

1. Cambio password immediato

- La password dell'utente `analyst` deve essere cambiata su tutti i sistemi coinvolti (`209.165.200.235` e `192.168.0.11`).

2. Restrizioni sull'accesso FTP

- Limitare l'uso di FTP o implementare SFTP per la protezione dei dati.

3. Monitoraggio dei log di sistema

- Attivare un sistema di monitoraggio attivo per rilevare accessi sospetti.

4. Implementazione di autenticazione a più fattori (MFA)

- Proteggere gli account critici con autenticazione a più fattori.

5. Verifica dell'integrità dei file di sistema

- Controllare `/etc/shadow` e `/etc/passwd` per modifiche non autorizzate.

Conclusione

L'analisi ha rivelato che l'attaccante ha ottenuto accesso root a un sistema compromesso e ha trasferito dati sensibili tramite FTP. Le contromisure suggerite aiuteranno a mitigare il rischio di futuri attacchi simili.