

Progetto Cyber Security & Ethical Hacking

Team: Secure Sentinels

Modulo: Cybersecurity & Ethical Hacking (Epicode)

Data: 24 Febbraio 2026

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

Obiettivi

In questo laboratorio, si esamineranno i log raccolti durante lo sfruttamento di una vulnerabilità documentata per determinare gli host e il file compromessi.

- **Parte 1: Esaminare gli Alert in Sguil**
- **Parte 2: Passare a Wireshark (Pivoting)**
- **Parte 3: Passare a Kibana (Pivoting)**

La 5-tupla viene utilizzata dagli amministratori IT per identificare i requisiti per la creazione di un ambiente di rete operativo e sicuro. I componenti della 5-tupla includono un indirizzo IP e un numero di porta di origine, un indirizzo IP e un numero di porta di destinazione, il protocollo in uso nel payload dei dati.

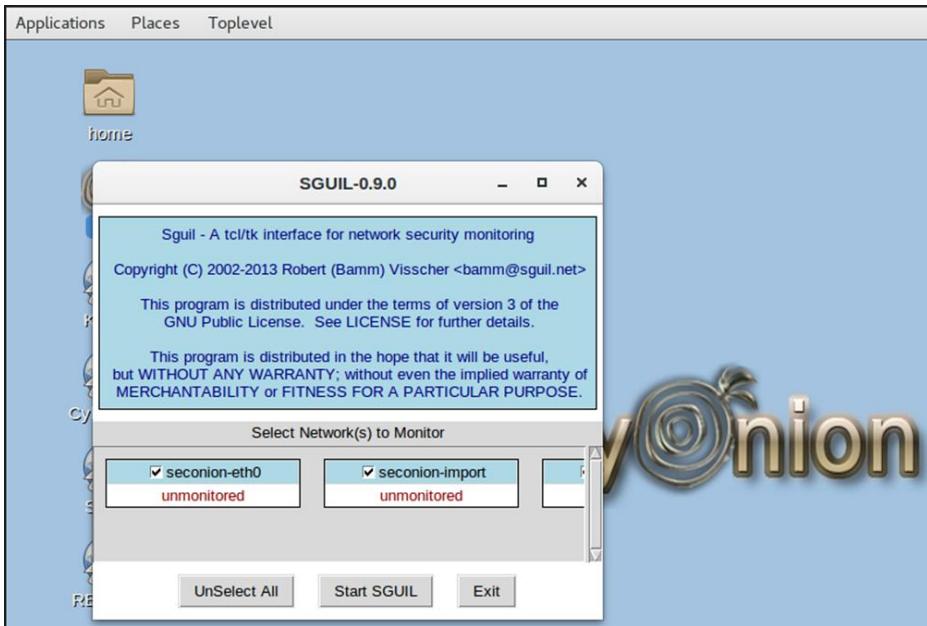
Verrà utilizzata la Macchina Virtuale CyberOps Security Onion, progettata per il monitoraggio della sicurezza di rete, il rilevamento delle intrusioni (IDS) e la gestione degli incidenti. Gli strumenti che saranno utilizzati saranno Sguil (piattaforma di Network Security Monitoring), Wireshark (analizzatore di pacchetti di rete) e Kibana (strumento di visualizzazione e analisi dei log).

Parte 1: Esaminare gli Alert in Sguil

Istruzioni

Dopo l'attacco, gli utenti non hanno più accesso al file chiamato **confidential.txt**.

- Viene avviata la **VM Security Onion** ed effettuato il login.
- Si apre **Sguil** e si effettua il login. Fare clic su **Select All** per selezionare le interfacce e poi su **Start SGUIL**.



c. Si esaminano gli eventi elencati nella colonna **Event Message**. Uno di questi messaggi è **GPL ATTACK_RESPONSE id check returned root**. Questo messaggio indica che potrebbe essere stato ottenuto l'accesso root durante un attacco. L'**host 209.165.200.235** ha restituito l'accesso root a **209.165.201.17**.

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 ...
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...

d. Si selezionano le caselle di controllo **Show Packet Data** e **Show Rule** per visualizzare ogni alert più in dettaglio

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	sPort	Dst IP	oPort	Pr	Event Message
RT	17	seconion-...	5.234	2019-07-19 18:53:12	172.16.4.205	49249	185.243.115.84	80	6	ET POLICY Data POST to a...
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 Fr...
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 Wil...
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 ...
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 checksu...
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...

e. Si effettua il clic con il pulsante destro sull'**ID dell'alert 5.1** e si seleziona **Transcript**

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	Sport	Dst IP	DPort	Pr	Event Message
RT	17	seconion...	5.234	2019-07-19 18:53:12	172.16.4.205	49249	185.243.115.84	80	6	ET POLICY Data POST to a...
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 Fr...
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 Wi...
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 ...
RT	351	seconion...	Event History	8:09:28	0.0.0.0		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	0	[OSSEC] Integrity checksu...

f. Esame delle 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.

ST	DPort	Pr	Event Message
15.84	80	6	ET POLICY Data POST to a...
14	443	6	ET POLICY HTTP traffic on ...
8	53	17	ET POLICY DNS Update Fr...
174	49731	6	ET CURRENT_EVENTS Lik...
174	49731	6	ET CURRENT_EVENTS Wi...
174	49731	6	ET POLICY PE EXE or DLL...
174	49760	6	ET TROJAN ABUSE.CH SS...
201.17	45415	6	GPL ATTACK_RESPONSE ...
	0	0	[OSSEC] File added to the s...
	0	0	[OSSEC] Integrity checksu...
	0	0	[OSSEC] New group added t...
	0	0	[OSSEC] New user added to...
	0	0	[OSSEC] Listened ports stat...

File

Re

File

Sensor Name: seconion-import-1
Timestamp: 2020-06-11 03:41:20
RT Connection ID: .seconion-import-1_1
RT Src IP: 209.165.201.17
RT Dst IP: 209.165.200.235
RT Src Port: 45415
RT Dst Port: 6200
RT OS Fingerprint: 209.165.201.17:45415 - UNKNOWN [S44:63:1:60:M1460,S,T,N,W7::??:?] (up: 6267 hrs)
RT OS Fingerprint: -> 209.165.200.235:6200 (link: ethernet/modem)
RT SRC: id
RT SRC:
RT DST: uid=0(root) gid=0(root)
RT DST:
RT SRC: nohup >/dev/null 2>&1
RT SRC:
RT SRC: echo uKgoT8McFDrcw7u2
RT SRC:
RT DST: uKgoT8McFDrcw7u2
RT DST:
RT SRC: whoami
RT SRC:
RT DST: root
RT DST:
RT SRC: hostname
RT SRC:
RT DST: metasploitable
RT DST:
RT SRC: ifconfig

IP

Src

Src

Dst

Dst

Who

Search Abort Close

Debug Messages

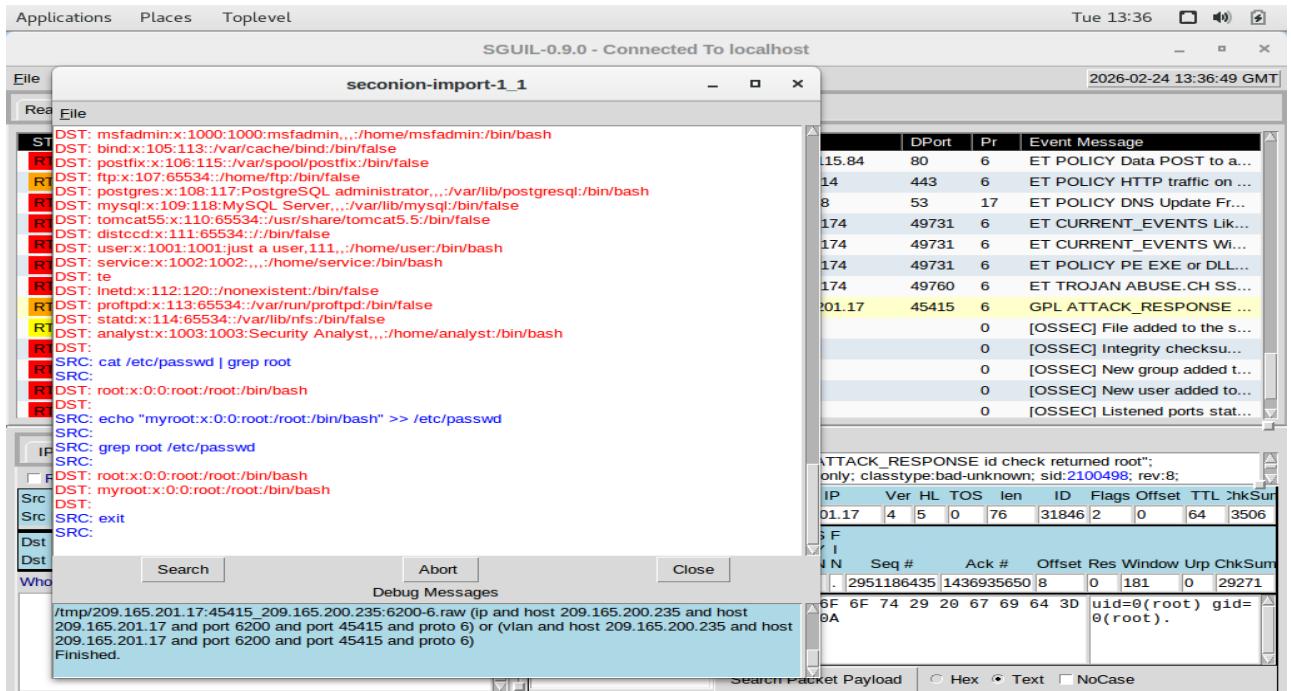
/tmp/209.165.201.17:45415_209.165.200.235:6200-6.raw (ip and host 209.165.200.235 and host 209.165.201.17 and port 6200 and port 45415 and proto 6) or (vlan and host 209.165.200.235 and host 209.165.201.17 and port 6200 and port 45415 and proto 6)

Finished.

ATTACK_RESPONSE id check returned root";
only; class:type:bad-unknown; sid:2100498; rev:8;

IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
01.17	4	5	0	76	31846	2	0	64	3506
6F	74	29	20	67	69	64	3D		
6F	6F	74	29	20	67	69	64	3D	uid=0(root) gid=0(root).
									0A

Raw Hex Text NoCase



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

Le transazioni avvenute tra il **Client** (Attaccante: **209.165.201.17**) e il **Server** (Vittima: **209.165.200.235**) sulla porta **6200/TCP** sono:

1. Fase di Esplorazione e Conferma Privilegi

l'attaccante invia comandi per capire chi è e dove si trova all'interno del sistema compromesso.

Comando id: Il server risponde con **uid=0(root) gid=0(root)**, confermando che l'attaccante ha già ottenuto i massimi privilegi (**root**).

Comando whoami: Il server conferma nuovamente l'identità dell'utente come root.

Comando hostname: Il server risponde metasploitable, indicando il nome della macchina vittima.

Comando ifconfig: L'attaccante richiede i dettagli di rete per mappare meglio l'infrastruttura.

2. Esfiltrazione di Informazioni Critiche

L'attaccante passa all'analisi degli utenti presenti sul sistema.

Comando cat /etc/passwd: Il server invia l'intero contenuto del file degli utenti (si vedono utenti come msfadmin, postgres, service, ecc.).

Filtraggio: L'attaccante usa **grep root** per isolare le informazioni relative all'utente amministratore.

3. Fase di Persistenza (Creazione Backdoor)

L'attaccante decide di non usare l'utente root esistente, ma di creare uno nuovo

Comando: echo "myroot:x:0:0:root:/root:/bin/bash" >> /etc/passwd

L'attaccante ha aggiunto un nuovo utente chiamato **myroot** con **UID 0** (identico a root). Questo gli permetterà di rientrare nel sistema in futuro con privilegi totali, anche se la password dell'utente root originale venisse cambiata.

4. Verifica e Chiusura

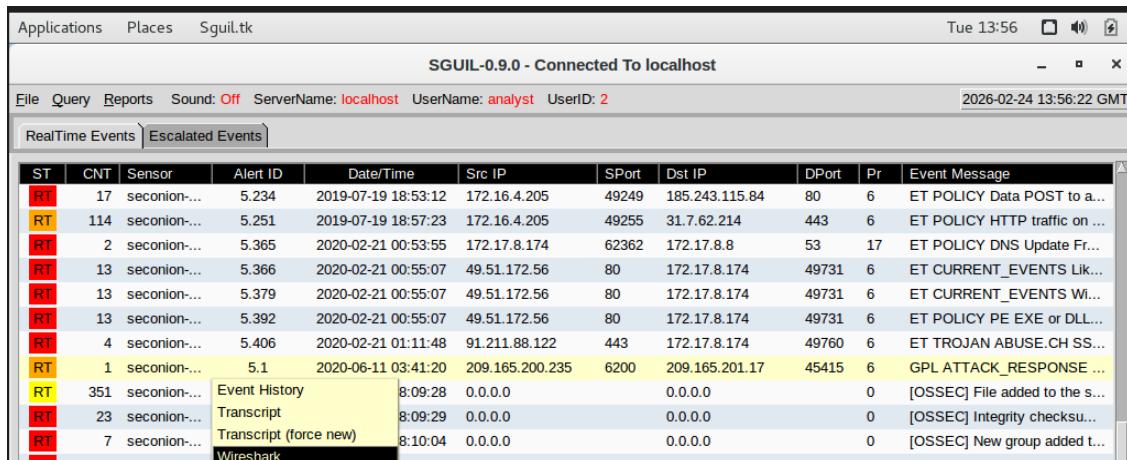
Verifica: L'attaccante esegue nuovamente **grep root /etc/passwd** e il server mostra entrambi gli utenti: **root** e il nuovo **myroot**.

Uscita: L'attaccante digita exit per chiudere la sessione corrente, lasciando però la backdoor attiva nel file **passwd**.

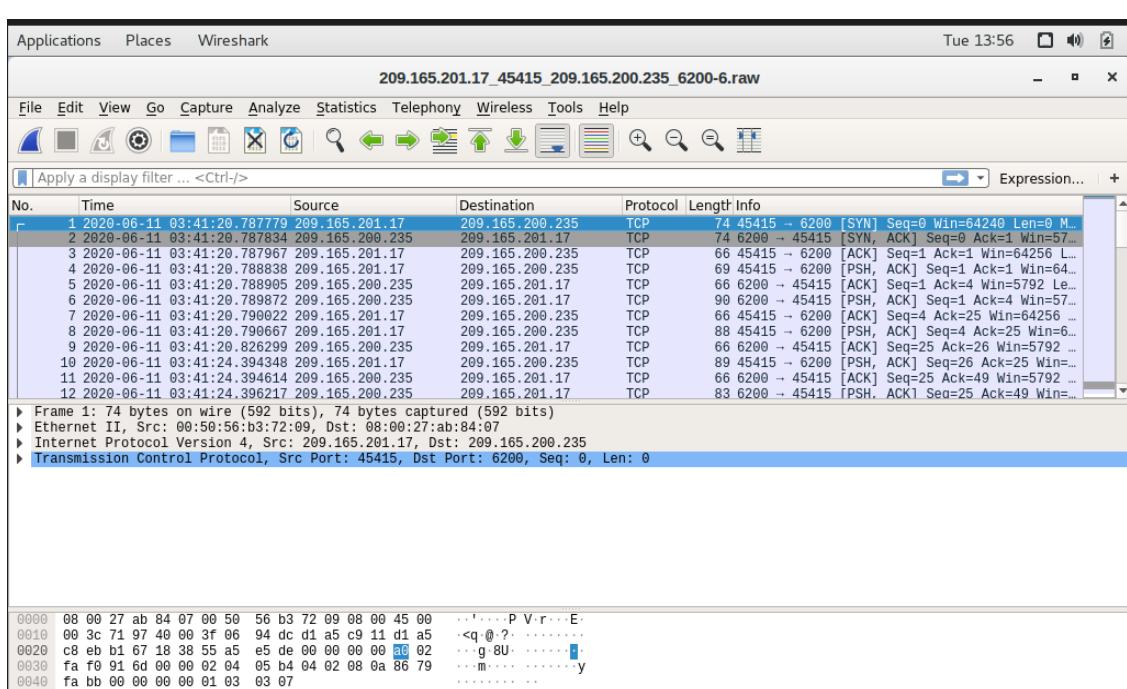
Parte 2: Passare a Wireshark

Istruzioni

- Si seleziona l'alert che ha fornito la trascrizione nel passo precedente. Effettua il clic con il pulsante destro sull'**ID dell'alert 5.1** e seleziona **Wireshark**. La finestra principale di **Wireshark** mostra tre viste di un pacchetto.



The screenshot shows the SGUIL interface with a list of alerts. Alert 5.1 is selected and highlighted in yellow. The details for this alert are shown in the main pane: Date/Time 2020-06-11 03:41:20, Src IP 209.165.200.235, Dst IP 209.165.201.17, Sport 6200, DPort 45415, and Pr 6. The event message is "GPL ATTACK_RESPONSE ...". Below the alert list, there are tabs for "RealTime Events" and "Escalated Events".



The screenshot shows the Wireshark interface with the captured traffic for the selected alert. The packet list shows 12 TCP packets between 209.165.201.17 and 209.165.200.235. The details view shows the first few packets, and the bytes view shows the raw hex and ASCII data. A tooltip at the bottom indicates the frame details: "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:84:97 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".

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

The screenshot shows two instances of the Wireshark application. The top instance is titled "209.165.201.17_45415_209.165.200.235_6200-6.raw" and displays a list of network packets. A context menu is open over the second packet (a SYN packet) with the option "Follow" selected under the "TCP Stream" submenu. The bottom instance is titled "Wireshark · Follow TCP Stream (tcp.stream eq 0) · 209.165.201.17_45415_209.165.200.235_6200-6.raw" and shows the detailed content of the selected TCP stream, including the SYN packet and its response.

```

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)

cat /etc/shadow
root:$1$avpfBj1$0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$UX6BP0t$MiyC3Up0zQJqz4s5wFD910:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp*:14684:0:99999:7:::
mail:*:14684:0:99999:7:::
www-data:*:14684:0:99999:7:::
Packet 4. 14 client pkts, 11 server pkts, 20 turns. Click to select.
Entire conversation (4,388 bytes) Show and save data as ASCII Stream [0]
Find: Find Next Filter Out This Stream Print Save as... Back Close Help

```

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

Il testo rosso indica i comandi inviati dall'attaccante(client), mentre il testo blu l'output in risposta ai comandi inviati(server)

L'attaccante esegue il comando whoami sul bersaglio. Cosa rivela questo sul ruolo dell'attaccante sul computer bersaglio?

Il comando **whoami** eseguito dall'attaccante rivela che quest'ultimo ha ottenuto il controllo completo e senza restrizioni sul sistema bersaglio.

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

I dati letti dall'attore della minaccia sono:

- Identità e privilegi dell'utente, confermando di operare come root
- Configurazioni di rete e host, tramite i comandi **hostname** e **ifconfig** ha letto il nome della macchina vittima (**metasploitable**) e i dettagli dell'interfaccia di rete, ip e mac
- Database degli utenti di sistema, attraverso la lettura di **/etc/passwd**, l'attaccante ha ottenuto l'elenco di tutti gli account presenti sulla macchina
- Credenziali e Hash delle password, ha visualizzato il contenuto del file shadow, ottenendo gli **hash crittografati** delle password (es. per gli utenti root, sys, service e analyst)
- Ha riletto i file di configurazione per confermare il successo dell'operazione, filtrando i file **/etc/passwd** e **/etc/shadow** tramite il comando **grep root** per verificare che il nuovo utente malevolo **myroot** fosse stato aggiunto correttamente e fosse pronto all'uso senza password.

Parte 3: Passare a Kibana

Istruzioni

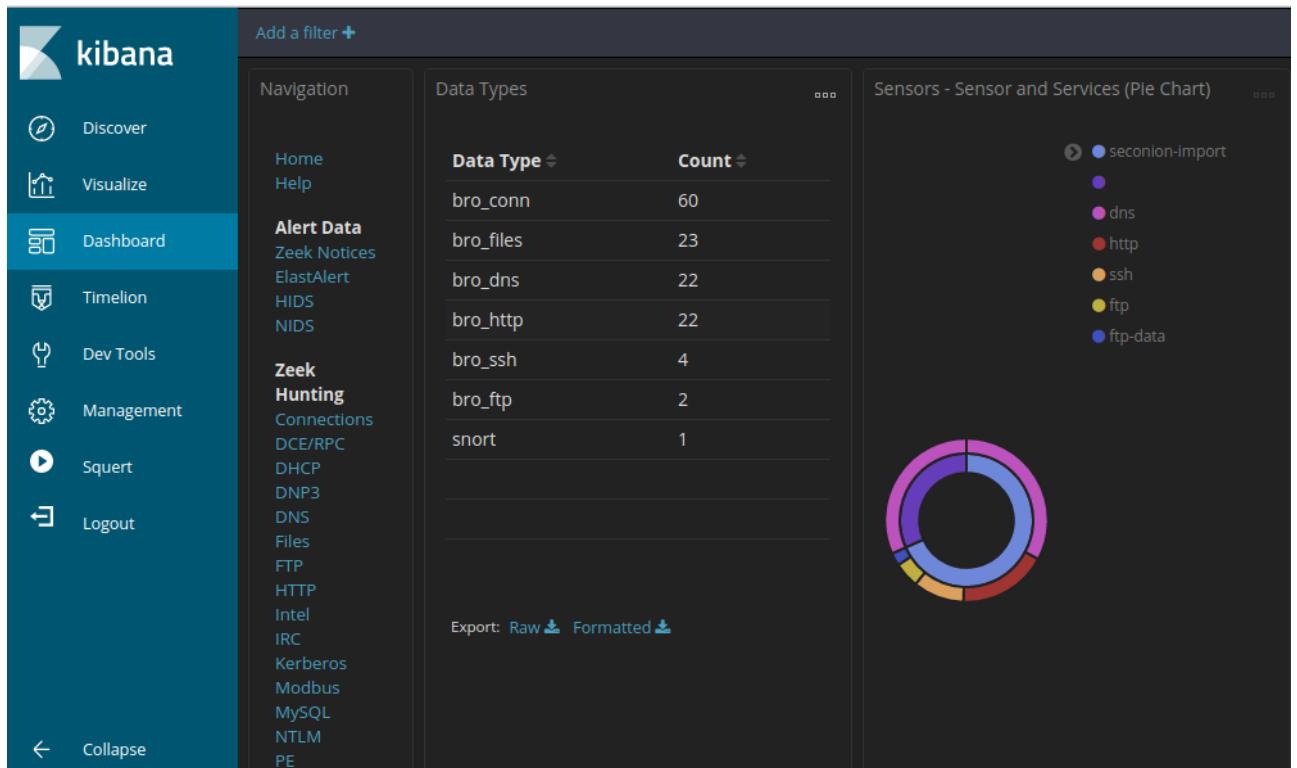
- Si torna a **Sguil**. Si fa clic con il pulsante destro sull'indirizzo IP di origine o di destinazione per l'**ID dell'alert 5.1** e si seleziona **Kibana IP Lookup > SrcIP**.

The screenshot shows the Sguil interface with a list of alerts. Alert 5.1 is highlighted in yellow. A context menu is open over this alert, with the option "Kibana IP Lookup" selected. The menu also includes other options like "SrcIP", "DstIP", "Ver", "HL", "TOS", "len", "ID", "Flags", "Offset", "TTL", and "ChkSum". At the bottom of the interface, there are tabs for "IP Resolution", "Agent Status", "Snort Statistics", and "System Msg". The "System Msg" tab is currently active, showing a log entry related to a GPL ATTACK_RESPONSE.

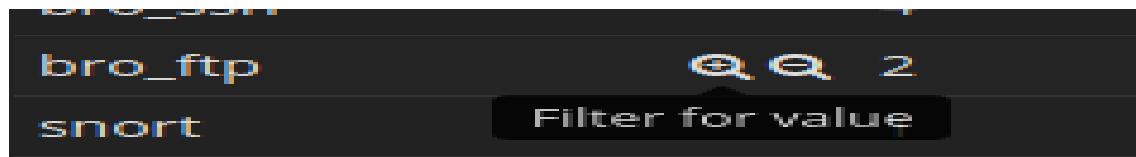
- Se l'intervallo di tempo è impostato sulle ultime 24 ore, cambia a Giugno 2020 in modo che l'11 giugno sia incluso nell'intervallo. Si usa la scheda Absolute per cambiare l'intervallo di tempo.

The screenshot shows the Kibana Overview dashboard. On the left, there is a sidebar with links to "Discover", "Visualize", "Dashboard", "Timeline", "Dev Tools", "Management", "Squert", and "Logout". The main area displays a "Time Range" section with three tabs: "Quick", "Relative", and "Absolute". The "Absolute" tab is selected, showing "From" and "To" fields. The "From" field is set to "2020-06-01 00:00:00.000" and the "To" field is set to "2020-07-01 23:59:59.999". Below these fields is a calendar for June and July 2020, with the date "01" highlighted in both months. At the bottom right of the dashboard, there are "Options" and "Update" buttons.

- Nei risultati visualizzati, c'è un elenco di diversi tipi di dati. Ti è stato detto che il file confidential.txt non è più accessibile. Nel grafico a torta "**Sensors - Sensors and Services**", sono presenti **ftp** e **ftp-data**. Determineremo se **FTP** è stato usato per rubare il file.



- d. Filtriamo per **bro_ftp**. Si passa il mouse sullo spazio vuoto accanto al conteggio dei tipi di dati **bro_ftp**. Si seleziona **+** per filtrare solo il traffico relativo a **FTP**



- e. Si scorre verso il basso fino a **All Logs**. Ci sono due voci elencate.

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	LDjqzXIB B6Cd_0 SbfqO	1-2 of 2
▶ June 11th 2020, 03:53:09.086	192.168.0.11	52776	209.165.200.235	21	LTjqzXIB B6Cd_0 SbfqO	1-2 of 2

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

Ip di origine (**source_ip**) **192.168.0.11**, porta **52776**

Ip di destinazione (**destination_ip**) **209.165.200.225**, porta **21**

- f. Si espande e si esaminano 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**. Si esamina anche il messaggio nella voce di log per saperne di più su questo evento

```

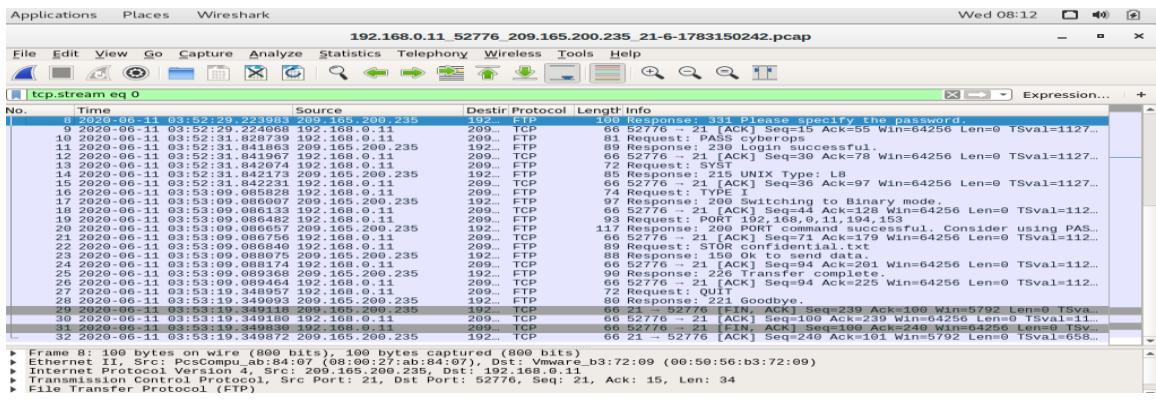
192.168.0.11:52776_209.165.200.235:21->476111494.pcap
Log entry:
{
  "ts": "2020-06-11T03:53:09.086840Z", "uid": "C5GkeA4t8oXzdWTPr6", "id.orig_h": "192.168.0.11", "id.orig_p": 52776, "id.resp_h": "209.165.200.235", "id.resp_p": 21, "user": "analyst", "password": "chiddenz", "command": "STOR", "arg": "ftp://209.165.200.235/.confidential.txt", "mime_type": "text/plain", "reply_code": 226, "reply_msg": "Transfer complete.", "fuid": "F-X1IV63eSMAEIN1652" }

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:
DST: 230 Login successful.
DST:
SRC: SYST
SRC:
DST: 215 UNIX Type: L8
DST:
SRC: TYPE I
SRC:
DST: 200 Switching to Binary mode.
  
```

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

	Table	JSON		
@timestamp	Q Q D * June 11th 2020, 03:53:09.086		View surrounding documents	View single document
@version	Q Q D * 1			
_id	Q Q D * LTjqzXIBB6Cd_0SbfqO			
_index	Q Q D * seconion:logstash-import-2020.06.11			
_score	Q Q D * -			
_type	Q Q D * doc			
destination_geo.city_name	Q Q D * Monterey			
destination_geo.country_name	Q Q D * United States			

- h. Si esamina la trascrizione per le transazioni tra l'attaccante e il bersaglio. Si scarica il pcap per esaminare il traffico usando **Wireshark**.



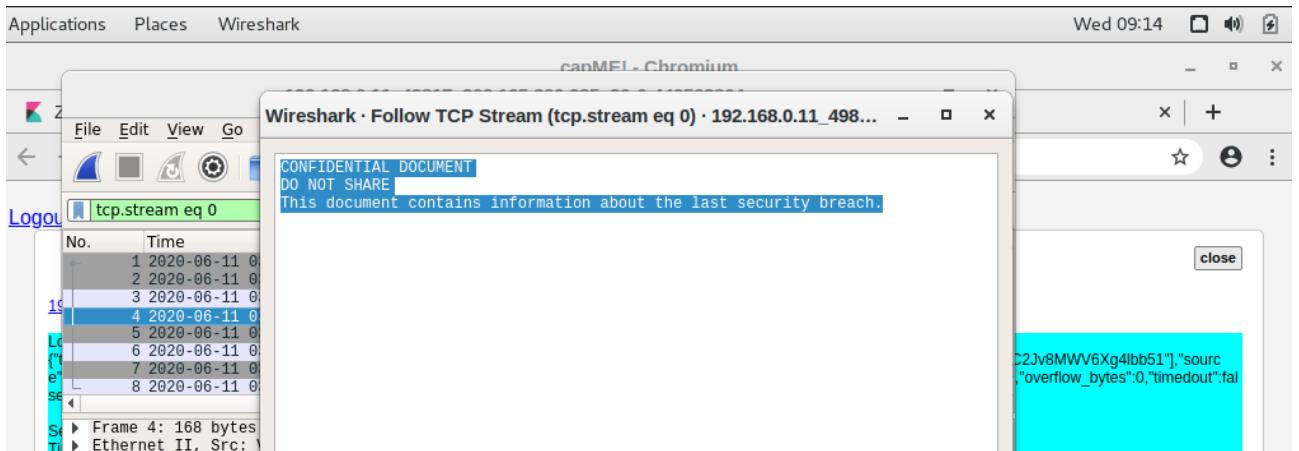
Quali sono le credenziali utente per accedere al sito FTP?

Le credenziali utente sono username **analyst** e password **cyberops**

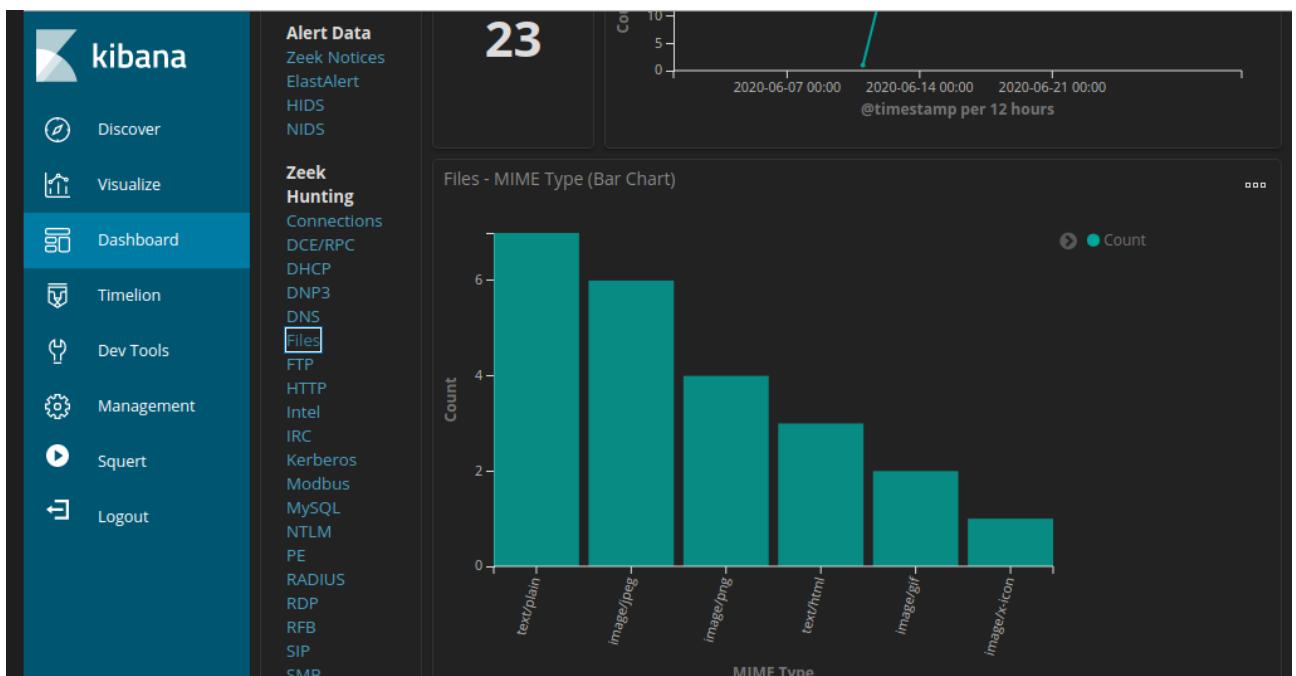
- Verificato che l'attaccante ha usato **FTP** per copiare il contenuto del file **confidential.txt** per poi cancellarlo dal bersaglio.

Qual è il contenuto del file?

Il contenuto del file è “CONFIDENTIAL DOCUMENT DO NOT SHARE
[...]"



- Si naviga in cima alla dashboard. Si seleziona **Files** sotto l'intestazione **Zeek Hunting** nel pannello di sinistra



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?

I diversi tipi di file sono **text/plain**, **image/jpeg**, **image/png**, **text/html**, **image/gif**, **image/x-icon**.

Dashboard

Timelion

Dev Tools

Management

Squert

Logout

Files - MIME Type

MIME Type	Count
text/plain	7
Image/jpeg	6
Image/png	4
text/html	3
Image/gif	2
Image/x-icon	1

Files - Source IP Address

File IP Address	Count
209.165.200.235	22
192.168.0.11	1

Files - Destination IP Address

IP Address	Count
209.165.200.227	22
209.165.200.235	1

Le sorgenti (File -Source) sono HTTP e FTP_DATA

Files - Source		Files - Files By Size (Bytes)	
Source	Count	Bytes Seen	Count
HTTP	22	99.685KB	1
FTP_DATA	1	70.19KB	1
		55.912KB	1
		50.438KB	1
		38.326KB	1
		23.687KB	1
		23.11KB	1
		22.569KB	1
		12.137KB	1
		10.032KB	1

k. Si filtra per **FTP_DATA** passando il mouse sullo spazio vuoto accanto al conteggio per **FTP_DATA** e si fa clic su +

l. Si scorre 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?**
Il tipo **MIME** è **text/plain**, l'indirizzo ip di origine è **192.168.0.11** e indirizzo ip di destinazione è **209.165.200.235**

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

Quando si è verificato questo trasferimento?

Il trasferimento si è verificato in data 11/06/2020 alle 03:53

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	C2Jv8MWV6Xg4Ibb51	FX1IV63eSMAEiN16S2	KDjqzXIBB6Cd-0SVfly

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?

Tramite la dashboard **Files** (nella suite **Zeek Hunting di Kibana**), l'indagine è stata ristretta alla categoria di traffico **FTP_DATA**. Accedendo alla trascrizione del singolo evento di trasferimento, è stato possibile visualizzare il dump testuale del payload di rete.

Il contenuto del file è “CONFIDENTIAL DOCUMENT DO NOT SHARE [...]”

```
192.168.0.11:49817_209.165.200.235:20-6-370252123.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": ["C2Jv8MWV6Xg4Ibb51"],
  "source": "FTP_DATA",
  "depth": 0,
  "analyzers": [
    {
      "name": "SHA1",
      "value": "MD5"
    }
  ],
  "mime_type": "text/plain",
  "duration": 0.0,
  "is_orig": false,
  "seen_bytes": 102,
  "missing_bytes": 0,
  "overflow_bytes": 0,
  "timedout": false,
  "mid": "e7bc9c20bd5666365379c91294d536b",
  "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:

DEBUG: Using archived data: /hsm/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 0.28 seconds: 0.05 0.12 0.00 0.10 0.00

192.168.0.11:49817_209.165.200.235:20-6-370252123.pcap
```

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

Conclusioni e Protocollo di Rimediazione (Incident Response)

L'indagine ha permesso la ricostruzione integrale dell'incidente: l'attaccante ha violato il perimetro (Ottenimento Accesso), ha innalzato i privilegi al livello di sistema (Privilege Escalation), ha impiantato una backdoor in **/etc/passwd** (Persistenza), ha compromesso le credenziali FTP legittime e ha completato l'obiettivo esfiltrando documenti riservati prima di attuare tattiche di sabotaggio (Data Wiping/Evasion).

Per il contenimento e l'eradicazione della minaccia, si impone il seguente piano d'azione immediato:

- Quarantena dell'Asset:** Disconnessione fisica e logica (tramite regole switch/VLAN quarantine) dell'host 209.165.200.235 dalla rete aziendale di produzione.

2. **Mitigazione Perimetrale:** Implementazione di regole di blocco (Drop/Deny) sull'infrastruttura Firewall/IPS per interdire ogni comunicazione bidirezionale con l'indirizzo IP malevolo 209.165.201.17.
3. **Eradicazione della Backdoor:** Pulizia manuale del sistema infetto, procedendo alla cancellazione della riga associata all'account **myroot** sia dal file **/etc/passwd** che dal file crittografato **/etc/shadow**.
4. **Bonifica delle Credenziali e Hardening:** **Invalidare e forzare** il reset delle password per tutti gli account di sistema (in particolare l'utente **analyst** e l'amministratore **root**). Infine, **deprecare** l'utilizzo del protocollo FTP in favore di alternative sicure basate su cifratura asimmetrica, quali SFTP o FTPS.
5. **Identificazione dello host interno:** L'indirizzo **192.168.0.11** appartiene ad una classe di indirizzi privati, ciò significa che rappresenta un dispositivo all'interno della rete locale LAN. Attraverso Kibana, questo IP risulta essere la sorgente (**Source IP**) della sessione **FTP** che ha prelevato il file **confidential.txt** del server compromesso. L'attaccante dopo aver preso il controllo del server potrebbe aver utilizzato lo host **192.168.0.11** come pivoting (movimento laterale) per prelevare i dati sensibili. poiché **Wireshark** ha mostrato che l'attaccante ha rubato i file delle password (**/etc/shadow**), è molto probabile che abbia usato quelle credenziali per autenticarsi tramite FTP da questo host interno e scaricare il documento. **L'host 192.168.0.11** quindi, deve essere oggetto di analisi. Risulta necessario verificare se all'interno del dispositivo associato a questo host sono stati installati Malware e che tipo di violazione ha subito.