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

> A cura di Iris Canole, Federico Giannini, Daniele Castello, Luca Pani, Rosario Papa, Yari Olmi, Alessandro Salerno

Obiettivi

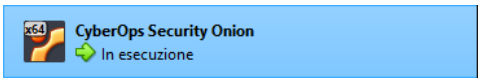
In questo laboratorio, esaminerai i log raccolti durante lo sfruttamento di una vulnerabilità documentata per determinare gli host e il file compromessi.

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

Dopo l'attacco, gli utenti non hanno più accesso al file chiamato `confidential.txt`.
Ora esamineremo i log per determinare come il file è stato compromesso.

Parte 1: Esaminare gli Alert in Sguil

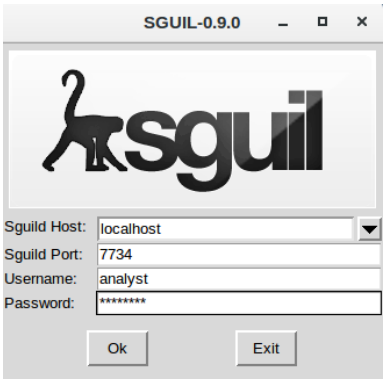
1. Abbiamo avviato la VM Security Onion ed effettuato il login.
   Credenziali:
   - UTENTE: `analyst`
   - PASSWORD: `cyberops`



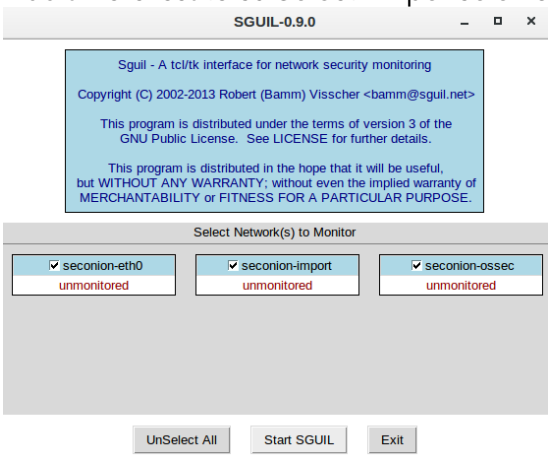
2. Abbiamo aperto Sguil e poi effettuato il login.

Credenziali:

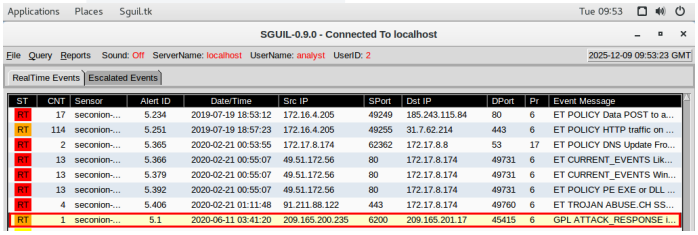
- USERNAME: `analyst`
- PASSWORD: `cyberops`



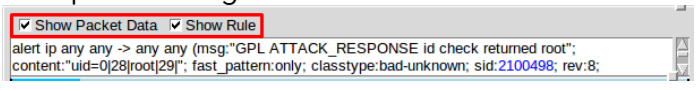
Abbiamo cliccato su Select All per selezionare le interfacce e poi su Start SGUIL.



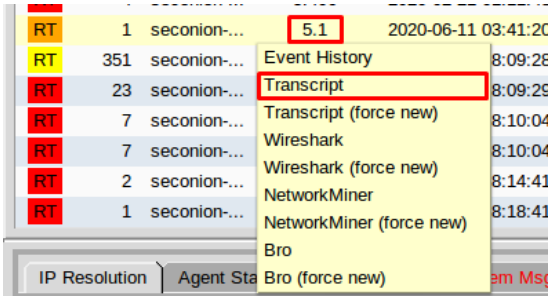
3. Abbiamo esaminato gli eventi elencati nella colonna `Event Message`.
   Uno di questi messaggi è `GPL ATTACK_RESPONSE id check returned root`, ed indica che potrebbe essere stato ottenuto l'accesso root durante un attacco.
   L'host `209.165.200.235` ha restituito l'accesso root a `209.165.201.17`.



4. Abbiamo selezionato le caselle di controllo Show Packet Data e Show Rule per visualizzare ogni alert più in dettaglio.



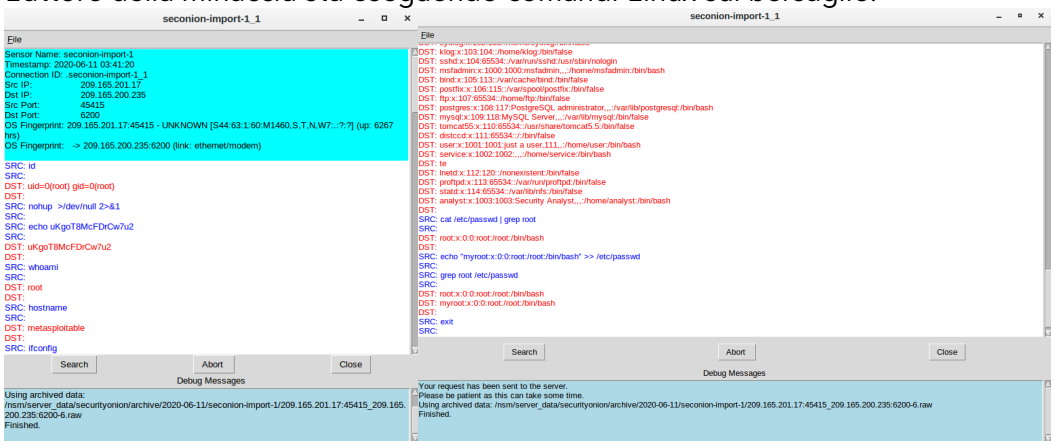
5. Abbiamo cliccato con il pulsante destro sull'ID dell'alert `5.1` e selezionato Transcript.



6. Abbiamo esaminato le trascrizioni per l'alert.

   Mostrano 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.



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

   In questo attacco, l'attaccante ha compromesso il server, ha confermato di essere root, ha rubato gli hash delle password e ha creato un account amministratore nascosto `myroot` per garantirsi l'accesso futuro.

Cronologia delle transazioni

Reconnaissance

- **Comando**: `id`

  Risposta: `uid=0(root) gid=0(root)`
- **Comando**: `whoami`

  Risposta: `root`

L'attaccante verifica i suoi privilegi.

La risposta conferma che ha accesso root sulla macchina.

—

- **Comando**: `hostname`

Risposta: `metasploitable`

L'attaccante identifica il nome della macchina.

—

- **Comando**: `ifconfig`

L'attaccante controlla la configurazione di rete.

Information Gathering

- **Comando**: `cat /etc/passwd`

L'attaccante legge il file che contiene la lista degli utenti del sistema

—

- **Comando**: `cat /etc/shadow`

L'attaccante legge il file che contiene gli hash delle password degli utenti.
Con questi hash, l'attaccante può tentare di decifrare le password offline.

Creating a Backdoor User

- **Comando**: `echo "myroot:x:0:0:root:/root:/bin/bash" >> /etc/passwd`
- **Comando**: `echo "myroot::14747:0:99999:7:::" >> /etc/shadow`

L'attaccante ha modificato il sistema per assicurarsi di poter rientrare anche se la vulnerabilità originale venisse corretta.

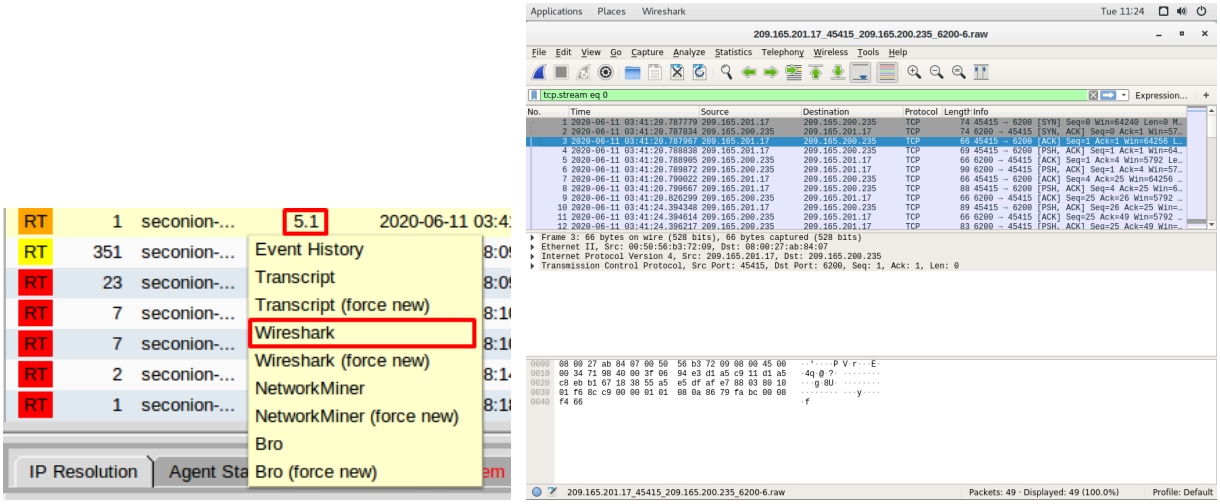
Verifica della persistenza

- **Comando**: `grep root /etc/passwd`
- **Risposta**: gli ha mostrato sia l'utente `root` originale sia il nuovo utente `myroot`.

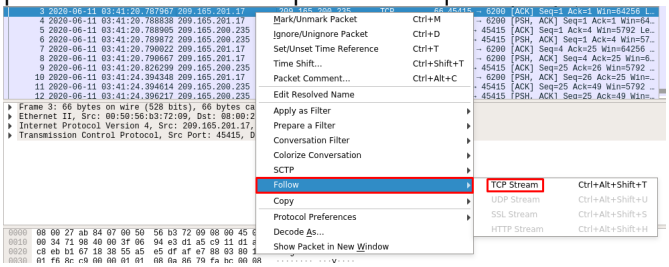
L'attaccante ha confermato che la modifica al file è andata a buon fine.

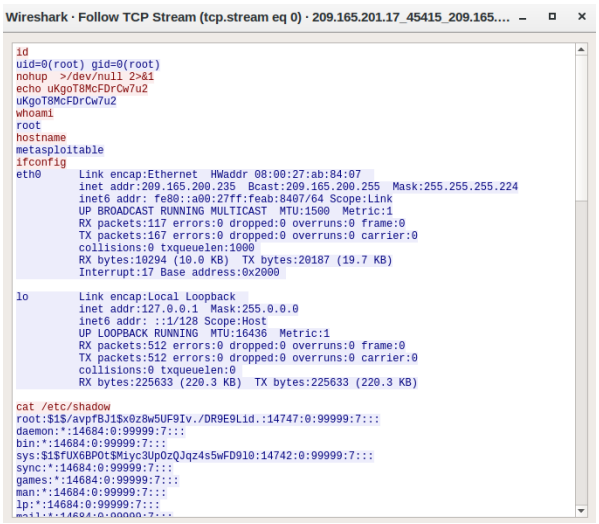
Parte 2: Passare a Wireshark

1. Abbiamo selezionato l'alert che ci ha fornito la trascrizione nel passo precedente. Abbiamo cliccato con il pulsante destro sull'ID dell'alert `5.1` e selezionato **Wireshark**.



2. Per visualizzare tutti i pacchetti assemblati in una conversazione TCP, Abbiamo cliccato con il pulsante destro su un pacchetto qualsiasi e abbiamo selezionato `Follow > TCP Stream`.





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

RISPOSTA: Si è aperta una finestra che mostra l'interazione tra l'attaccante e il server Target. In rosso vediamo ciò che scrive l'attaccante, quindi i comandi, mentre in blu è ciò che il server nella console risponde.

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

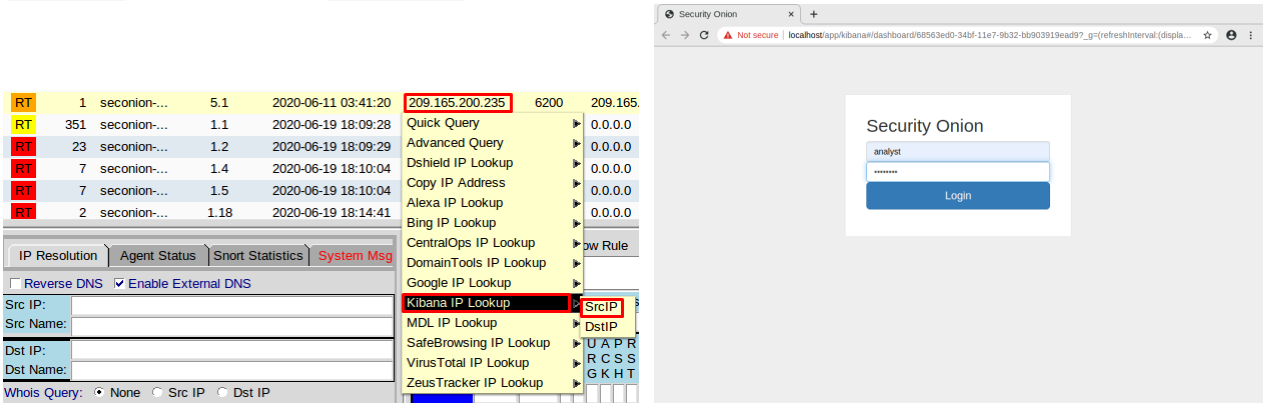
RISPOSTA: Questo comando rivela all'attaccante che ha accesso root sul Target.

DOMANDA: Scorri il flusso TCP. Che tipo di dati ha letto l'attore della minaccia?
RISPOSTA: L'attaccante ha letto dati come, la configurazione di rete, la lista degli utenti del sistema e il file che contiene gli hash delle password degli utenti

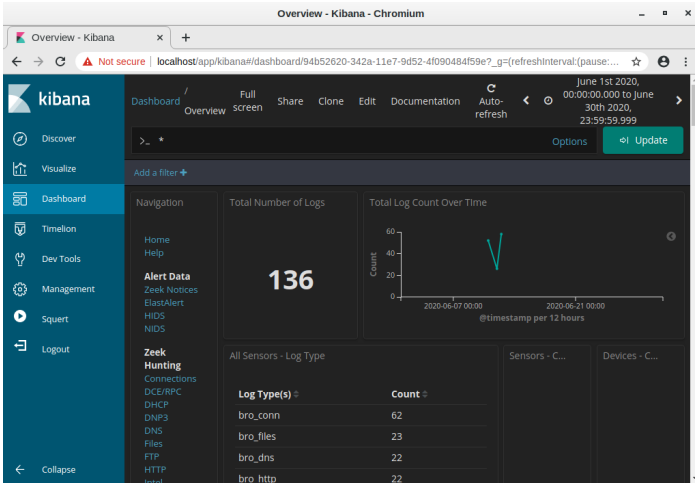
3. Siamo usciti dalla finestra del flusso TCP. E infine abbiamo chiuso Wireshark quando abbiamo finito di esaminare le informazioni fornite.

Parte 3: Passare a Kibana

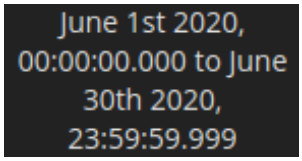
1. Su Sguil abbiamo fatto click con il pulsante destro sull'indirizzo IP di origine per l'ID dell'alert `5.1` e abbiamo selezionato Kibana `IP Lookup > SrcIP`. Abbiamo poi inserito il nome utente `analyst` e la password `cyberops` in quanto richiesto da Kibana.



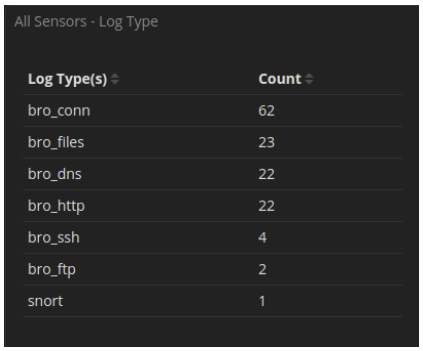
2. Ci siamo ritrovati nella Dashboard di Kibana.



E abbiamo cambiato l'intervallo di tempo in modo tale che l'11 giugno fosse incluso nell'intervallo.



3. Nella schermata è presente un elenco di diverso tipo di dati.

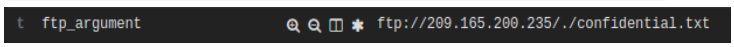


4. Abbiamo filtrato per `bro_ftp` selezionando il `+` nel Filter for value.

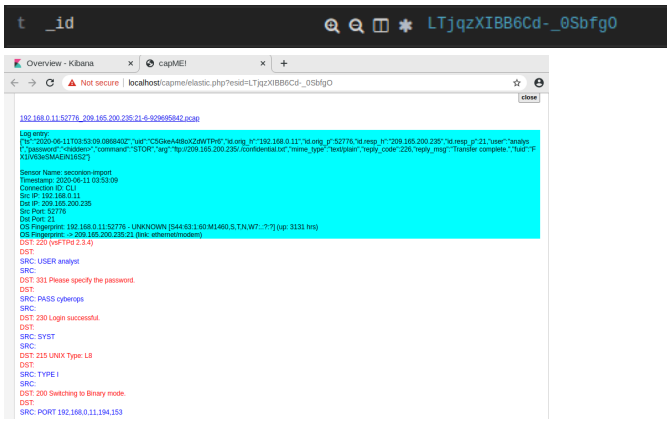
5. Siamo andati fino in fondo alla Dashboard e abbiamo trovato `All Logs`, le voci elencate erano quelle nello Screenshot sotto:

DOMANDA: Quali sono gli indirizzi IP e i numeri di porta di origine e destinazione per il traffico FTP?
RISPOSTA: L'indirizzo IP e la porta di origine è `192.168.0.11` e `52776`, mentre quello di destinazione è `209.165.200.235` e `21`.

6. Espandendo la seconda voce di Log, nel campo `ftp_argument` abbiamo trovato la voce `ftp://209.165.200.235/./confidential.txt`



7. Abbiamo aperto poi il campo `_id` schiacciando sul link e abbiamo trovato le transazioni tra l'attaccante e il server Target.



DOMANDA: Quali sono le credenziali utente per accedere al sito FTP?

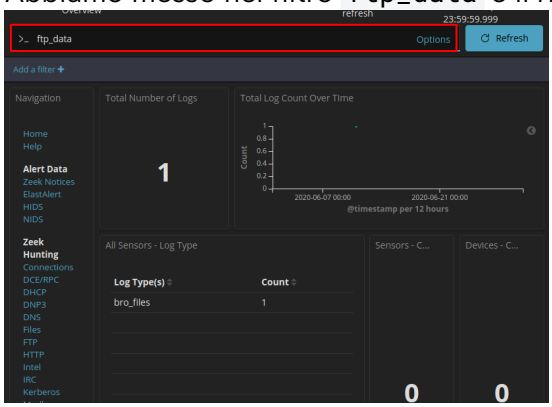
RISPOSTA: Le credenziali utente per accedere al sito FTP sono:

- **USER**: `analyst`
- **PASS**: `cyberops`

8. Ora che sappiamo che l'attaccante ha usato FTP per copiare il contenuto del file `confidential.txt` e poi cancellarlo dal bersaglio.

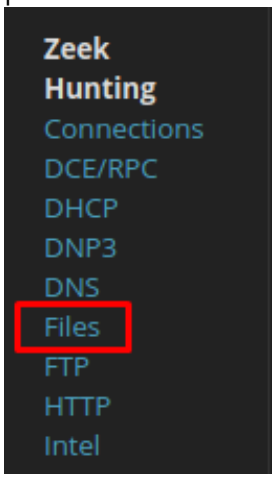
DOMANDA: Qual è il contenuto del file? Ricorda che uno dei servizi elencati nel grafico a torta è `ftp_data`.

Abbiamo messo nel filtro `ftp_data` e il risultato è stato `1`.

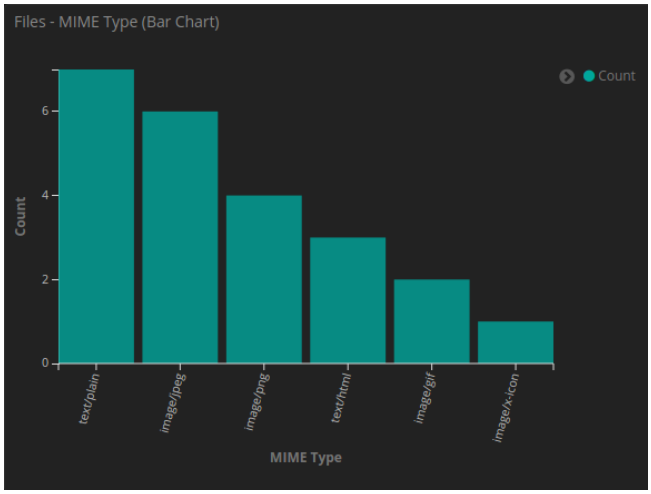


RISPOSTA: Il contenuto del file è stato il seguente:

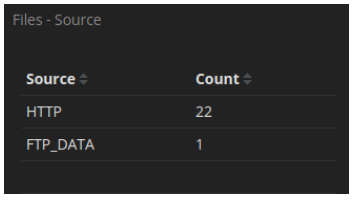
9. Abbiamo selezionato Files sotto l'intestazione Zeek Hunting nel pannello di sinistra. Questo permette di esaminare i tipi di file che sono stati registrati.



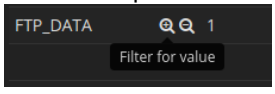
DOMANDA: Quali sono i diversi tipi di file? Guarda la sezione `MIME Type` dello schermo.
RISPOSTA: Sono presenti diversi tipi di file tra cui `text/plain`, `image/jpeg`, etc.



DOMANDA: Scorri fino all'intestazione Files - Source. Quali sono le sorgenti dei file elencate?
RISPOSTA: Le sorgenti dei file elencate sono `HTTP` e `FTP_DATA`.



10. Abbiamo poi filtrato per `FTP_DATA` cliccando sul `+` di `Filter for value`.



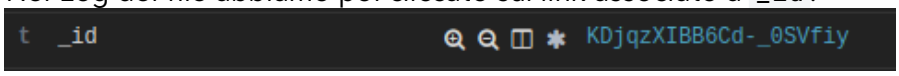
11. Abbiamo esaminato i risultati filtrati in fondo alla pagina.

DOMANDA: 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?

RISPOSTA:

- Il MIME type è `FTP_DATA`
- L'indirizzo IP di origine e di destinazione sono `192.168.0.11` e `209.165.200.235`
- Il trasferimento si è verificato l'`11th June 2020 alle ore 03:53:09`

12. Nei Log dei file abbiamo poi cliccato sul link associato a `_id`.



DOMANDA: Qual è il contenuto testuale del file trasferito tramite FTP?

RISPOSTA: Il contenuto del file è riportato nello Screenshot seguente:

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

RISPOSTA: È fondamentale scollegare dalla rete il sistema `192.168.0.11` per consentire l'indagine forense. È necessario effettuare un audit delle regole FTP restringendo l'invio di dati verso l'esterno e verificare l'eventuale presenza di attività di esfiltrazione analoghe. Applicare subito una regola di blocco sul firewall per l'IP `209.165.200.235`.

Conclusioni

Grazie a strumenti come Sguil, Wireshark e Kibana, siamo riusciti a ricostruire completamente l'evento di sicurezza.

L'analisi ha confermato che l'attaccante è riuscito a diventare `root` su una macchina non sicura, utilizzandola poi per trasferire all'esterno il documento `confidential.txt` mediante una connessione FTP.