BONUS 2

Report di Analisi: Interpretazione del Traffico HTTP e DNS per Isolare un Attore Malevolo

---

Ambiente di Analisi: Cyber-Ops Onion
Strumenti utilizzati: Kibana, capME!
Obiettivo: Interpretare dati HTTP e DNS per isolare la minaccia

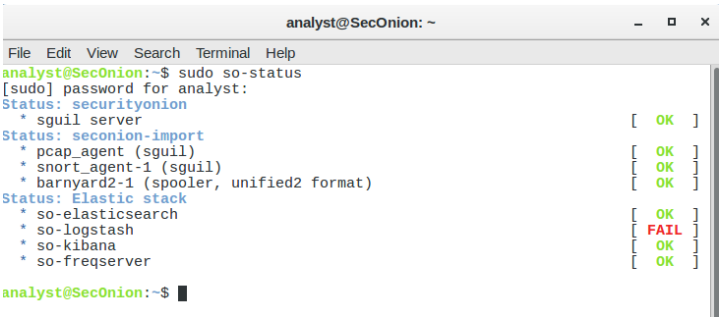
---

1. Obiettivo del Laboratorio

L'analisi dei log relativi allo sfruttamento delle vulnerabilità HTTP e DNS.

---

2. Procedura

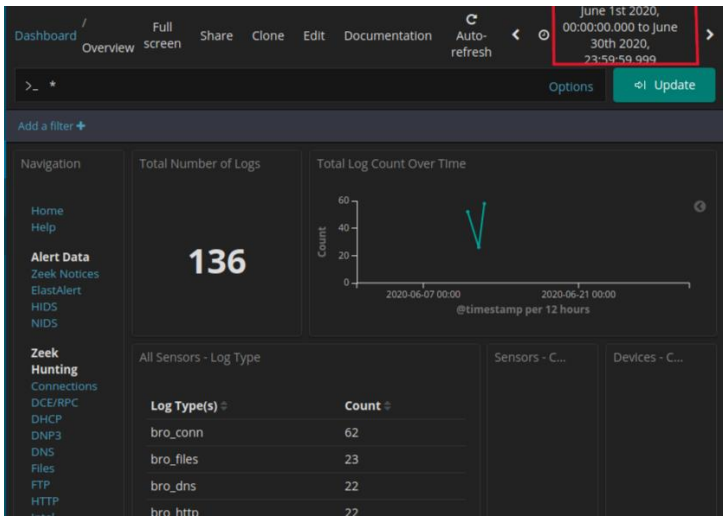


Parte 1: Esaminare un attacco SQL Injection

1. **Modificare il timeframe:**

   è consuetudine verificare lo stato dei servizi prima di accedervi ed utilizzarli.

   Si accede al servizio Kibana tramite lo shortcut sul desktop, si procede con la modifica del **Time Range** impostando un range assoluto al periodo nel quale l'attacco è avvenuto (tutto il mese di Giugno 2020).
   Si nota da subito il numero dei log.



2. **Filtrare il traffico HTTP**

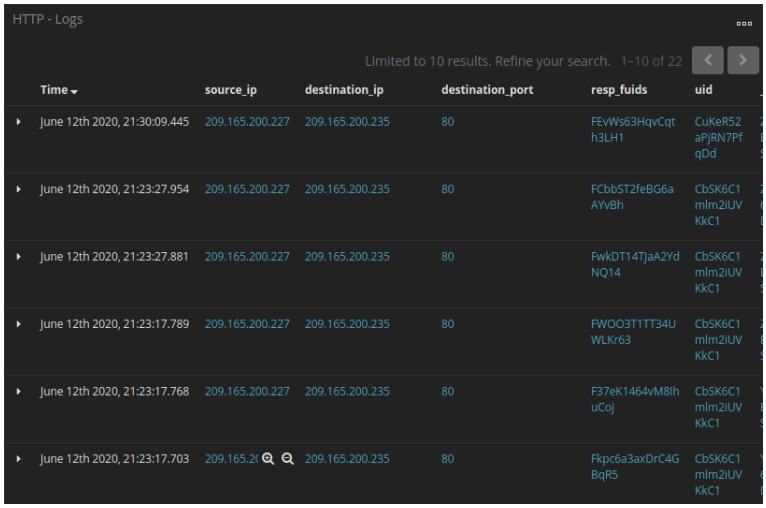
   Dal pannello di Navigazione a sinistra, si va a selezionare il filtro HTTP.

In questa pagina otteniamo le seguenti informazioni:

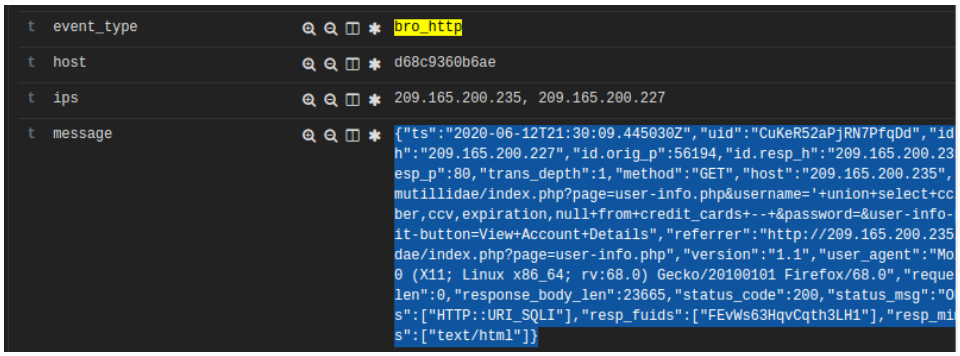
- Indirizzo IP Sorgente: **209.165.200.227**
- Indirizzo IP Destinatario: **209.165.200.235**
- Porta di destinazione: **80**
- Lista dei **log HTTP**.

Andiamo ad analizzare il primo log:

- Timestamp: 12 Giugno 2020, 21:30:09.445
- Tipo di evento: **bro_http** (bro perchè è il vecchio nome ma kibana fa riferimento a Zeek)
- Messaggio: si capisce che è stata fatta una richiesta GET dal client verso il server. Informazioni richieste: username, ccid, ccnumber, cvv, expiration e password.

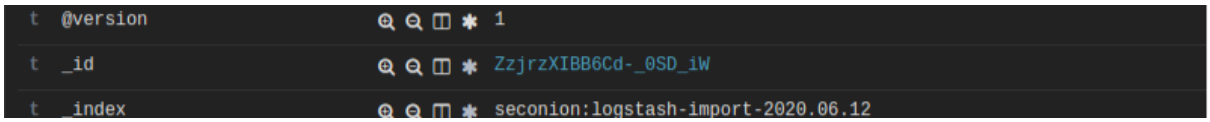


Stringhe come **union, select,** quando appaiono nei campi username e password fanno capire che il sistema ha subito un attacco di tipo **SQL Injection.**.

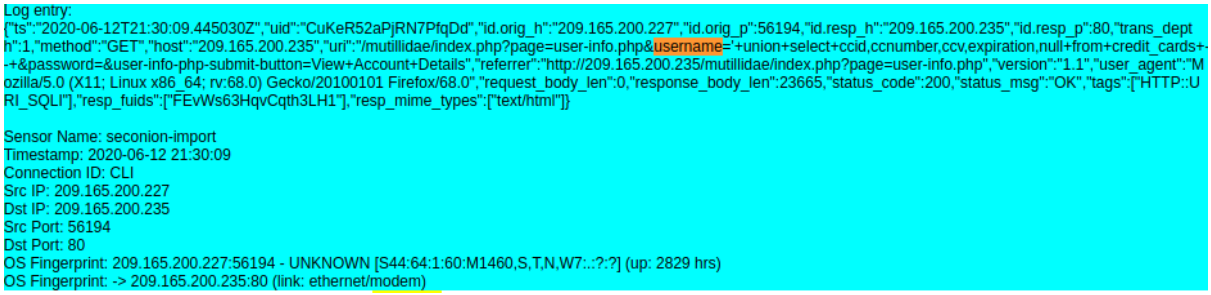


3. Analisi dettagliata del Log

Aprendo il link nel alert “_id” si apre una scheda con le informazioni di “**capME!**”.



Cosa è capME! ?
Uno strumento sviluppato per semplificare l’analisi dei file PCAP, rendendo più accessibile l’estrazione e la visualizzazione dei dati catturati durante il monitoraggio del traffico di rete.
Viene utilizzato per analisi forense di incidenti di sicurezza, monitoraggio delle reti azienda.
Il testo in blu contiene richieste HTTP inviate dal source,mentre la parte in rosso rappresenta la risposta del server di destinazione.



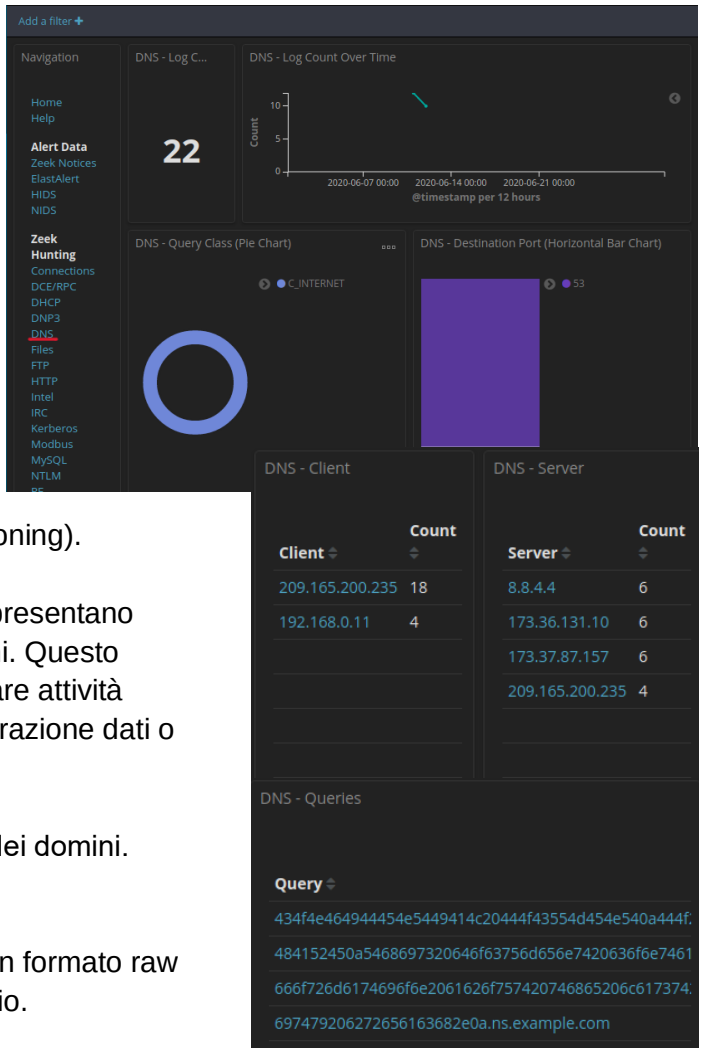
nella sezione **Log Entry** si nota la porzione **username=’union+select+ccid,ccnumber,cvv,expiration,null+from+credit_cards+--+&password=**
che indica un tentato attacco al sito, utilizzando una SQL Injection per bypassare l’autenticazione. Le stringhe **UNION** e **SELECT** sono dei comandi utilizzati per interrogare i database SQL.

Se i campi di input di una pagina web non sono opportunamente protetti da input malevoli, gli attaccanti possono iniettare le stringhe o codici per tentare un accesso ai dati nei database.Nella parte rossa andiamo a ricercare la stringa **username**, si nota che il server rispondendo alla richiesta HTTP GET ha inviato una lista di username e password **DATI ESFILTRATI.**

Username	Password
4444111122223333	745
7746536337776330	722
8242325748474749	461
7725653200487633	230

Parte 2: Analisi traffico DNS esfiltrato

1. **Filtrare il traffico DNS**
   Nella dashboard principale, sezione **Zeek Hunting,** andiamo a selezionare il filtro **DNS.**



2. **Revisione voci DNS**
   Scorrendo la pagina in basso si trovano i principali **Client** e **Server,** con i relativi tentativi di phishing DNS (DNS Pharming, Spoofing, DNS Poisoning).

   Nota come alcune delle query presentano sottodomini insolitamente lunghi. Questo comportamento potrebbe indicare attività sospette, come tentativi di esfiltrazione dati o DNS tunneling.

   Quindi si procede con l'analisi dei domini.

3. **Determinare i dati esfiltrati**
   La query DNS viene esportata in formato raw per essere analizzata in dettaglio.

Il file esportato **"DNS - Queries.csv"** contenente le query, si pulisce manualmente lasciando solo i caratteri esadecimali e si salva in fromato **.txt**.

```
analyst@SecOnion:~/Downloads$ ls -l
total 4
-rw-rw-r-- 1 analyst analyst 304 Feb  3 13:57 DNS - Queries.csv
```

Dal terminale si procede alla conversione inversa del file con il tool **xxd,** ottenendo un'informazione che non ci si dovrebbe aspettare, ovvero un breach di sistema.

```
analyst@SecOnion:~/Downloads$ xxd -r -p "DNS - Queries.csv" > secret.txt
analyst@SecOnion:~/Downloads$ cat secret.txt
CONFIDENTIAL DOCUMENT
DO NOT SHARE
This document contains information about the last security breach.
```

Se gli output fossero stati sottodomini legittimi l'output atteso sarebbe dovuto essere di tipo: **login.example.com, mail.example.com, ftp.example.com, vpn.example.com .**

---

3. Risultati e Conclusioni

- I risultati indicano che le richieste DNS erano separate e coordinate, contenenti dati nascosti. Il significato più ampio di questo risultato è che le query DNS possono essere utilizzate per nascondere l'invio di file e aggirare le misure di sicurezza della rete.
- È possibile che un malware abbia generato queste richieste, scorrendo i documenti presenti sull'host, codificando il contenuto in esadecimale e creando query DNS che utilizzano queste stringhe esadecimali come sottodomini. Poiché le richieste DNS vengono inviate regolarmente da una rete verso l'esterno, spesso non sono monitorate in modo rigoroso, rendendole un canale efficace per l'esfiltrazione dei dati.

---

4. Mitigazione e Contromisure

HTTP

- Validare e Sanificare l'Input
  - Validazione lato Server
  - Whitelist degli Input
  - Filtrare o Rimuovere i caratteri speciali
- Query Parametrizzate e Prepared Statements
- Applicare il Principio del Minimo Privilegio
- Configurazioni di Sicurezza dei Databse
  - Gestione degli errori
  - Limitare tempo di esecuzione di una query
- Implementare l'uso di Strumenti di Monitoraggio e Prevenzione
  - Web Application Firewall (WAF)
  - Database Activity Monitoring (DAM)
  - Analisi dei log
- Installare Aggiornamenti e Patch non appena disponibili
- Test di Sicurezza
- Formazione

DNS

- Monitorare ed Analizzare il traffico DNS
  - DNS Anomaly Detection

    - DNS Logging Completo
- Limitare e Controllare il traffico DNS
    - Whitelist dei domini consentiti
    - Firewall DNS
    - Bloccare TLD (Top-Level Domains) inutilizzati
- Configurazioni Sicurezza Avanzate
    - Implementare DNS over HTTPS/TLS (DoH, DoT) interno
    - Isolare Server DNS Interni
    - Limitare i Privilegi degli Utenti
- Rilevamento Avanzato
    - Frequency Analysis & Thresholding
    - Entropy Analysis
- Formazione e Policy Aziendali
- Risposta agli incidenti