

# Isolamento di un Attore di Minaccia tramite HTTP e DNS

## Isolamento di un Attore di Minaccia tramite HTTP e DNS

### Obiettivo

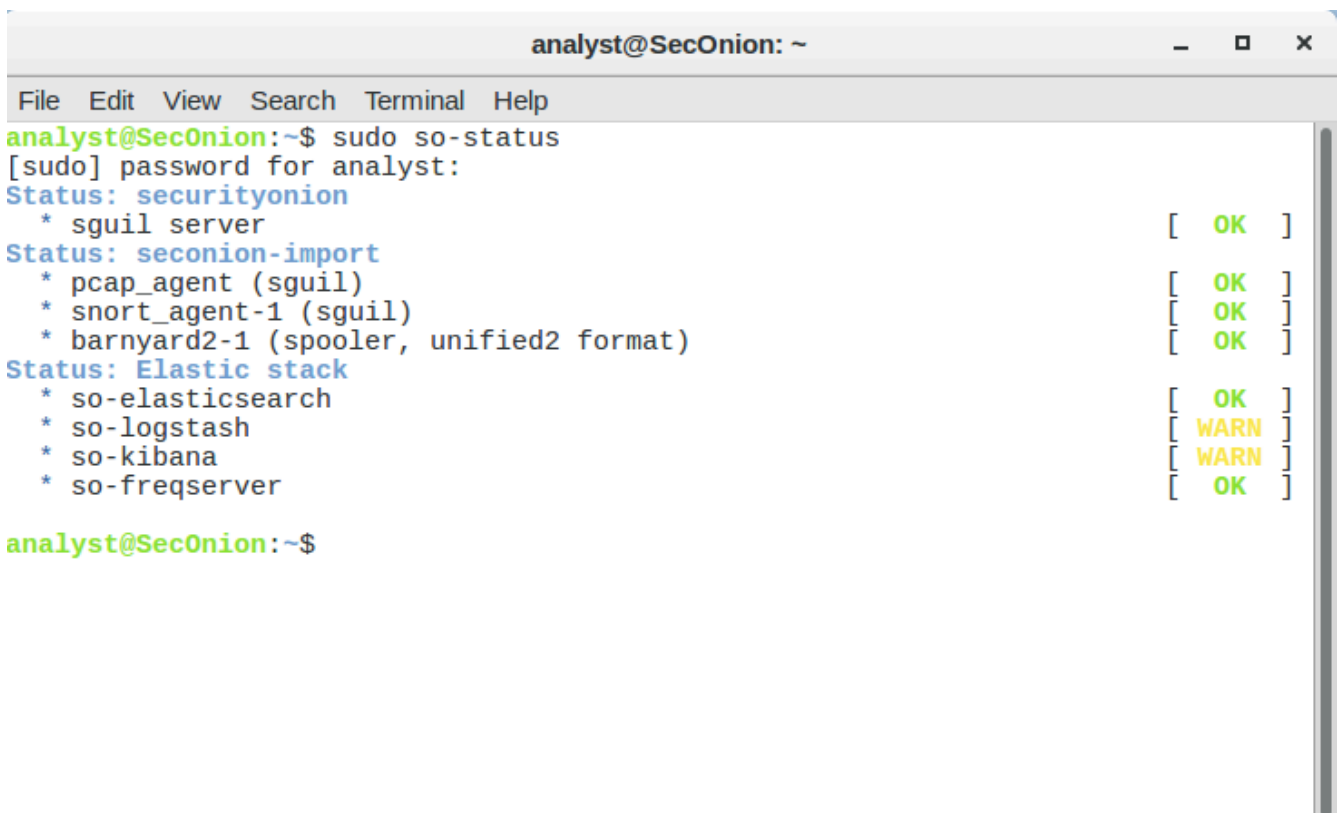
In questo esercizio, ho analizzato i log raccolti durante lo sfruttamento di vulnerabilità HTTP e DNS per identificare gli host compromessi e i dati esfiltrati. Ho dettagliato ogni passaggio affinché chiunque possa replicare il processo, anche senza esperienza pregressa.

## Parte 1: Investigazione di un Attacco SQL Injection

### 1. Avvio della VM Security Onion

- Ho avviato la macchina virtuale Security Onion.
- Ho effettuato l'accesso con:
  - **Username:** `analyst`
  - **Password:** `cyberops`
- Ho verificato lo stato dei servizi con il comando:

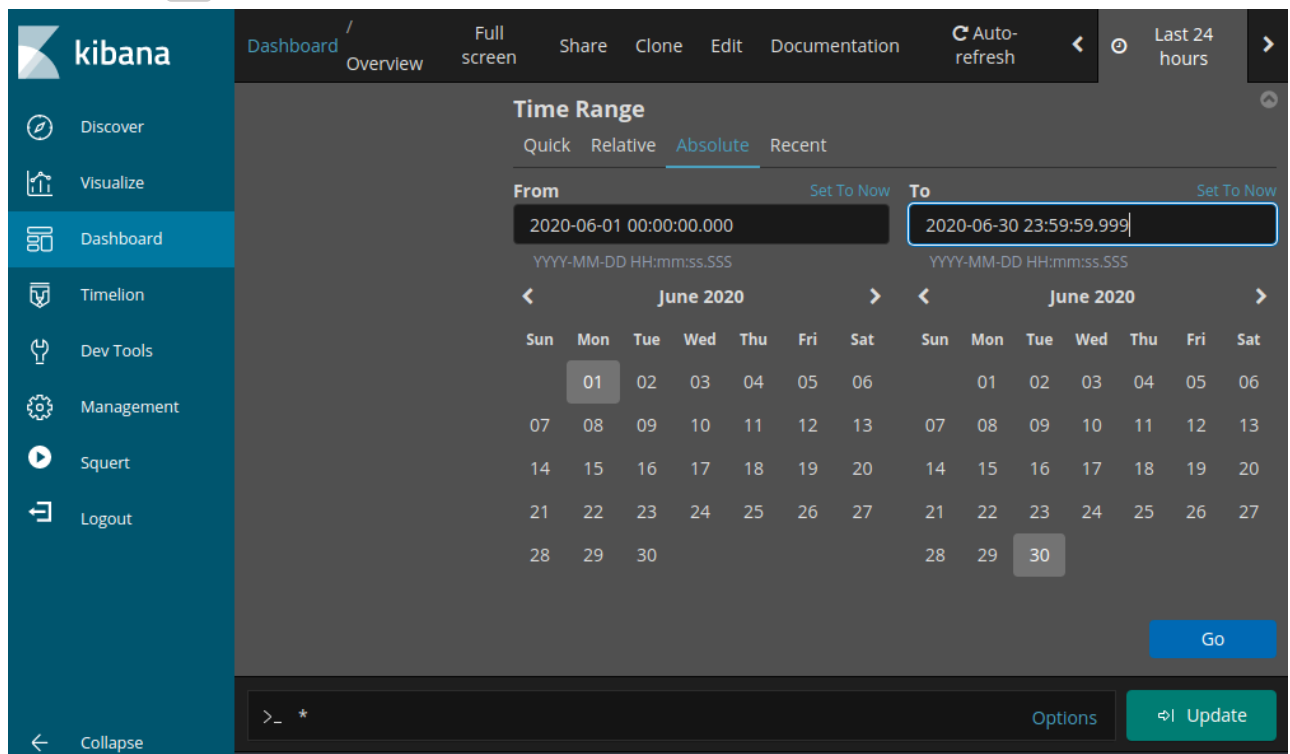
```
sudo so-status
```



```
analyst@SecOnion: ~  
File Edit View Search Terminal Help  
analyst@SecOnion:~$ sudo so-status  
[sudo] password for analyst:  
Status: securityonion  
* sgul server [ OK ]  
Status: seconion-import  
* pcap_agent (sgul) [ OK ]  
* snort_agent-1 (sgul) [ OK ]  
* barnyard2-1 (spooler, unified2 format) [ OK ]  
Status: Elastic stack  
* so-elasticsearch [ OK ]  
* so-logstash [ WARN ]  
* so-kibana [ WARN ]  
* so-freqserver [ OK ]  
analyst@SecOnion:~$
```

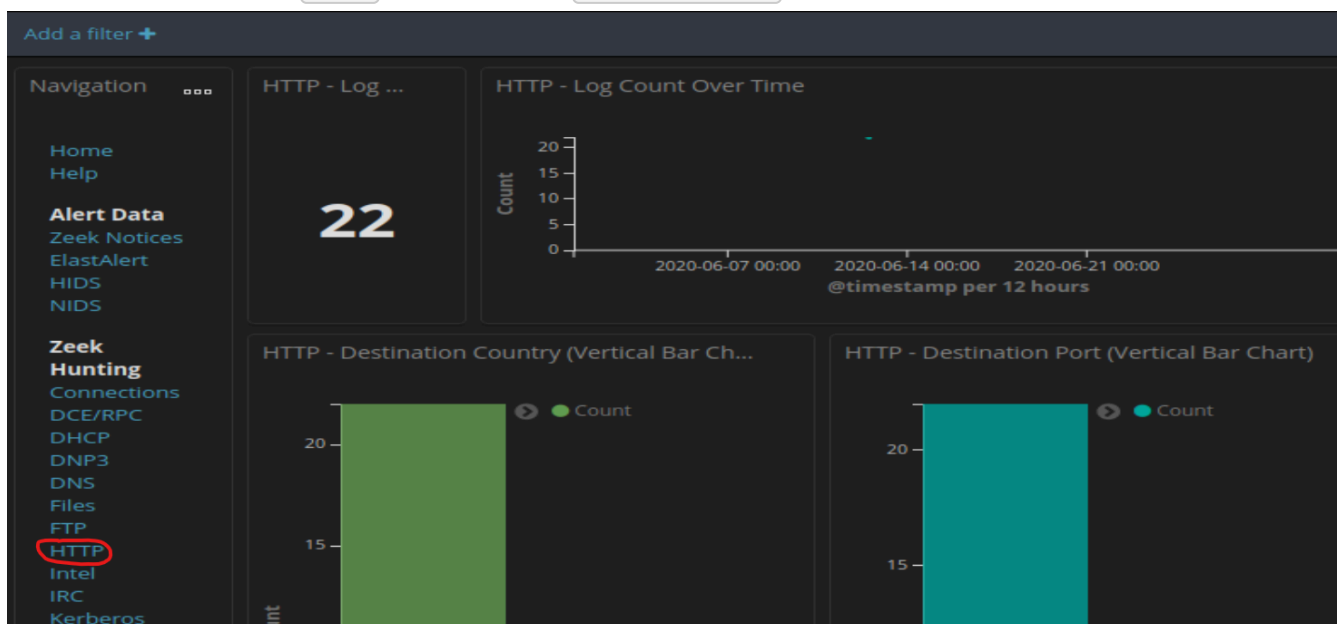
## 2. Accesso a Kibana e Impostazione dell'Intervallo Temporale

- Ho aperto Kibana tramite il collegamento sul desktop.
- Ho effettuato l'accesso con le credenziali fornite.
- Ho impostato il range temporale su **Giugno 2020**:
  1. Cliccare su `Last 24 hours` nell'angolo in alto a destra.
  2. Selezionare `Absolute`.
  3. Impostare **From** e **To** per coprire l'intero mese di giugno 2020.
  4. Cliccare su `Go` per applicare il filtro.



## 3. Filtraggio del Traffico HTTP

- Ho selezionato il filtro `HTTP` nella sezione `Zeek Hunting`.



- Ho identificato i seguenti dettagli dell'attacco:

- **IP sorgente:** 209.165.200.227
- **IP destinazione:** 209.165.200.235
- **Porta di destinazione:** 80
- **Timestamp primo evento:** 12 giugno 2020, 21:30:09.445
- **Tipo di evento:** bro\_http (Zeek HTTP log)

Time ▾	source_ip	destination_ip	destination_port	resp_fuids	uid	_id
▶ June 12th 2020, 21:30:09.445	209.165.200.227	209.165.200.235	80	FEvWs63HqvCqth3LH1	CuKeR52aPjRN7PfqDd	ZzjrZXIBB6Cd-_0SD_IW
▶ June 12th 2020, 21:23:27.954	209.165.200.227	209.165.200.235	80	FCbbST2feBG6aAYvBh	CbSK6C1mlm2iUVKkC1	ZjrzXIBB6Cd-_0SD_IW
▶ June 12th 2020, 21:23:27.881	209.165.200.227	209.165.200.235	80	FwkDT14TjaA2YdNQ14	CbSK6C1mlm2iUVKkC1	ZTjrZXIBB6Cd-_0SD_IW
▶ June 12th 2020, 21:23:17.789	209.165.200.227	209.165.200.235	80	FWOO3T1TT34UWLKr63	CbSK6C1mlm2iUVKkC1	ZDjrZXIBB6Cd-_0SD_IW
▶ June 12th 2020, 21:23:17.768	209.165.200.227	209.165.200.235	80	F37eK1464vM8ihuCoj	CbSK6C1mlm2iUVKkC1	YzjrZXIBB6Cd-_0SD_IW
▶ June 12th 2020, 21:23:17.703	209.165.200.227	209.165.200.235	80	Fkpc6a3axDrC4GBqR5	CbSK6C1mlm2iUVKkC1	YjrzXIBB6Cd-_0SD_IW
▶ June 12th 2020, 21:23:17.700	209.165.200.227	209.165.200.235	80	FxF0bx16vr1YOWulch	C252w31zFlvpV63kPa	XjrzXIBB6Cd-_0SD_IW
▶ June 12th 2020, 21:23:17.700	209.165.200.227	209.165.200.235	80	Ful2tB17PXhDulvnG4	Cr3RGFezop5b3qjz6	YDjrZXIBB6Cd-_0SD_IW
▶ June 12th 2020, 21:23:17.699	209.165.200.227	209.165.200.235	80	FxgVdq18u4TH8RSEK9	C4KeAa3pLgDqfaAQyg	YTjrZXIBB6Cd-_0SD_IW
▶ June 12th 2020, 21:23:17.698	209.165.200.227	209.165.200.235	80	F1sqnz4z0m9nW2sMVC	C4KeAa3pLgDqfaAQyg	WTjrZXIBB6Cd-_0SD_IW

event\_type bro\_http

## 4. Analisi del Traffico HTTP con capME!

- Ho individuato un attacco SQL Injection nel campo message della richiesta HTTP GET:

```
username=' +union+ select+ ccid, ccnumber, ccv, expiration, null from
credit_cards -- &password=
```

- Ho trovato dati sensibili esfiltrati, inclusi numeri di carte di credito e password:

Username	Password	Data di Scadenza
4444111122223333	745	2012-03-01
7746536337776330	722	2015-04-01
8242325748474749	461	2016-03-01
7725653200487633	230	2017-06-01
1234567812345678627	627	2018-11-01

DST: 24  
DST: <b>Username=</b>4444111122223333<br>  
DST:  
DST: 17  
DST: <b>Password=</b>745<br>  
DST:  
DST: 22  
DST: <b>Signature=</b>2012-03-01<br><p>  
DST:  
DST: 24  
DST: <b>Username=</b>7746536337776330<br>  
DST:  
DST: 17  
DST: <b>Password=</b>722<br>  
DST:  
DST: 22  
DST: <b>Signature=</b>2015-04-01<br><p>  
DST:  
DST: 24  
DST: <b>Username=</b>8242325748474749<br>  
DST:  
DST: 17  
DST: <b>Password=</b>461<br>  
DST:  
DST: 22  
DST: <b>Signature=</b>2016-03-01<br><p>  
DST:  
DST: 24  
DST: <b>Username=</b>7725653200487633<br>  
DST:  
DST: 17  
DST: <b>Password=</b>230<br>  
DST:  
DST: 22  
DST: <b>Signature=</b>2017-06-01<br><p>  
DST:  
DST: 24  
DST: <b>Username=</b>1234567812345678<br>  
DST:  
DST: 17  
DST: <b>Password=</b>627<br>  
DST:  
DST: 22  
DST: <b>Signature=</b>2018-11-01<br><p>  
DST:

---

## Parte 2: Analisi dell'Esfiltrazione di Dati tramite DNS

### 1. Filtraggio del Traffico DNS

- Ho ripulito i filtri precedenti in Kibana.

- Dashboard

Zeek - DNS

Full screen

Share

Clone

Edit

Documentation

Auto-refresh

◀

🔄

June 1st 2020, 00:00:00.000 to June 30th 2020, 23:59:59.999

▶

>\_ |

Options

🔄 Update

Add a filter +

Navigation

Home

Help

Alert Data

Zeek Notices

ElastAlert

HIDS

NIDS

Zeek Hunting

Connections

DCE/RPC

DHCP

DNP3

**DNS**

Files

FTP

HTTP

Intel

IRC

Kerberos

Modbus

MySQL

NTLM

PE

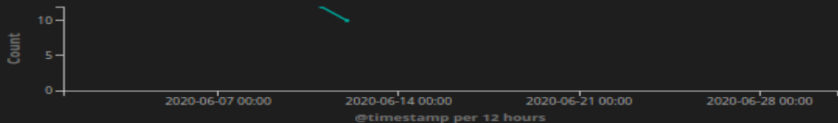
RADIUS

RDP


DNS - Log Count

22

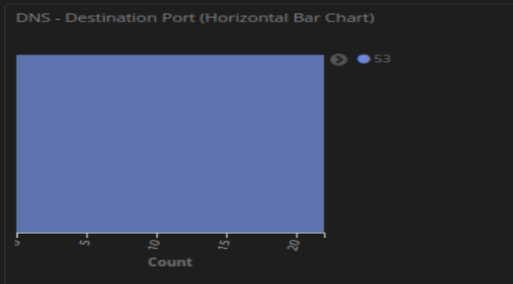
DNS - Log Count Over Time



DNS - Query Class (Pie Chart)



DNS - Destination Port (Horizontal Bar Chart)



DNS - Query Type

DNS - Response Code (Name)

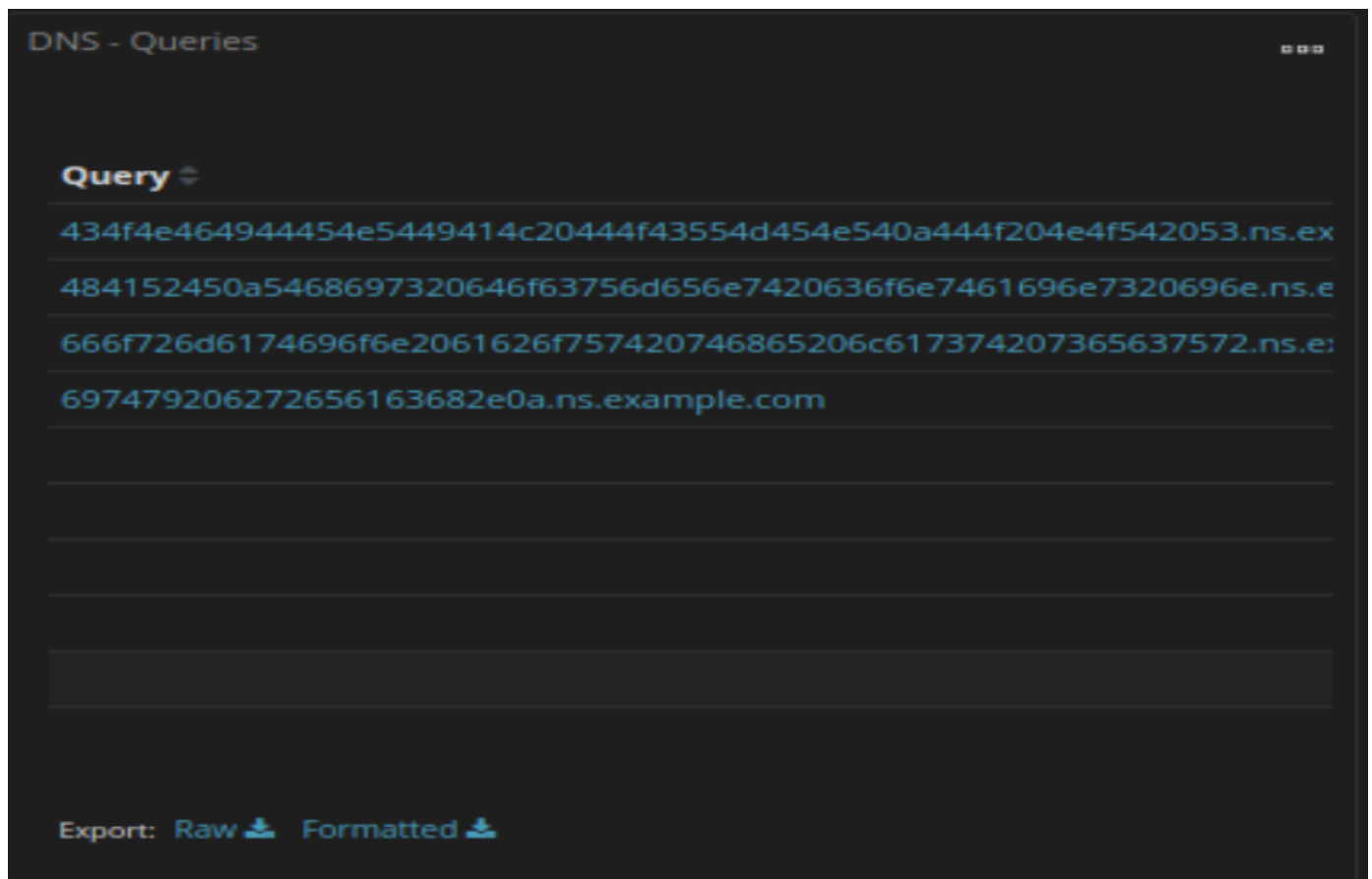
DNS - Protocol (Donut Chart)

- [illegible]

- Ho notato richieste DNS con sottodomini lunghi appartenenti a `ns.example.com`.
- Sembravano contenere dati codificati in esadecimale.
- Ho esportato i log in un file CSV, eliminando le parti superflue per mantenere solo le stringhe esadecimali:

```
434f4e464944454e5449414c204444f43554d454e540a444f204e4f542053
484152450a5468697320646f63756d656e7420636f6e7461696e7320696e
```

```
666f726d617469666e2061626f757420746865206c617374207365637572
697479206272656163682e0a
```



### 3. Decodifica e Analisi dei Dati

- Ho decodificato il testo con il comando:

```
xxd -r -p "DNS - Queries.csv" > secret.txt
cat secret.txt
```

- Il contenuto rivelato:

```
CONFIDENTIAL DOCUMENT
DO NOT SHARE
This document contains information about the last security breach.
```

- Questo conferma l'uso del DNS tunneling per esfiltrare dati.

```
File Edit View Search Terminal Help
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.
analyst@SecOnion:~/Downloads$
```

## Raccomandazioni per la Sicurezza

### 1. Cambio immediato delle credenziali

- Aggiornare la password dell'utente `analyst` su tutti i sistemi coinvolti.

### 2. Limitazione dell'accesso FTP e DNS

- Disabilitare FTP e monitorare le richieste DNS anomale.

### 3. Monitoraggio continuo dei log

- Implementare un sistema di rilevamento accessi sospetti.

### 4. Autenticazione a più fattori (MFA)

- Proteggere gli account critici con MFA.

### 5. Verifica dell'integrità dei file di sistema

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

---

## Conclusione

L'analisi ha confermato che l'attaccante ha sfruttato una SQL Injection per ottenere dati sensibili e ha utilizzato il DNS tunneling per esfiltrare ulteriori informazioni. Le contromisure suggerite aiuteranno a prevenire attacchi simili in futuro.