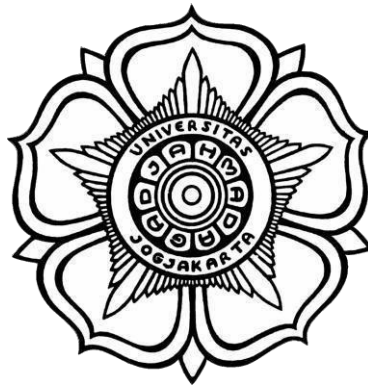


LAPORAN PRAKTIKUM
KEAMANAN INFORMASI 1
UNIT 5

“IP dan Enterprise Service Vulnerability”



Disusun Oleh:

| | |
|-------------------|---|
| Nama | : Saadah Mardatillah |
| NIM | : 21/473000/SV/18792 |
| Kelas | : Teknologi Rekayasa Internet A |
| Hari, Tanggal | : Selasa, 21 Maret 2023 |
| Dosen Pengampu | : Anni Karimatul Fauziyyah, S.Kom.,M.Eng. |
| Asisten Praktikum | : 1. Annisa Nurul Ramadhani Novelika 2. Gabriella Alvera Chaterine |

PROGRAM STUDI DIPLOMA IV TEKNOLOGI REKAYASA INTERNET

DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA

SEKOLAH VOKASI

UNIVERSITAS GADJAH MADA

2023

Unit 5

Ekstrak Executable dari PCAP, Menafsirkan Data HTTP dan DNS

I. Tujuan

1. Mahasiswa dapat melakukan investigasi SQL injection attack
2. Mahasiswa dapat melakukan analisis Pre-Captured logs dan traffic captures
3. Mahasiswa dapat melakukan investigasi DNS data exfiltration

II. Alat dan Bahan

1. Laptop
2. Mesin virtual CyberOps Workstation
3. Jaringan Internet

III. Latar Belakang

Wireshark merupakan *tool* yang digunakan dalam penganalisisan paket data jaringan. *Wireshark* melakukan pengawasan paket dengan cara *real time* dan menangkap data lalu menampilkannya secara *detail*. Untuk memulai penggunaan aplikasi *wreshark* membutuhkan aplikasi pelengkap seperti Pcap dalam melihat lalu lintas jaringan internet yang sedang kita gunakan. Cuplikan pada gambar jaringan yang menunjukkan protokol yang sedang berjalan dan dapat dicuplikan. Protokol yang biasanya terdapat dalam cuplikan seperti TCP, UDP, HTTP, dsb. *Wireshark* dapat membaca data secara langsung dari ethernet, token-ring, FDDI, serial (PPP dan SLIP), 802.11 wireless LAN, dan koneksi ATM. Semua jenis paket informasi yang terdiri dari berbagai format protokol mudah ditangkap dan dianalisa. Karena *tool* ini dapat dipakai untuk memperoleh informasi penting seperti *password* email atau akun lainnya (*sniffing*) dengan metode menangkap paket yang berjalan di dalam jaringan.

Kibana merupakan platform visualisasi dan manajemen data, pencarian, kueri, dan analisis, yang terdedikasi untuk data yang tersimpan dalam index

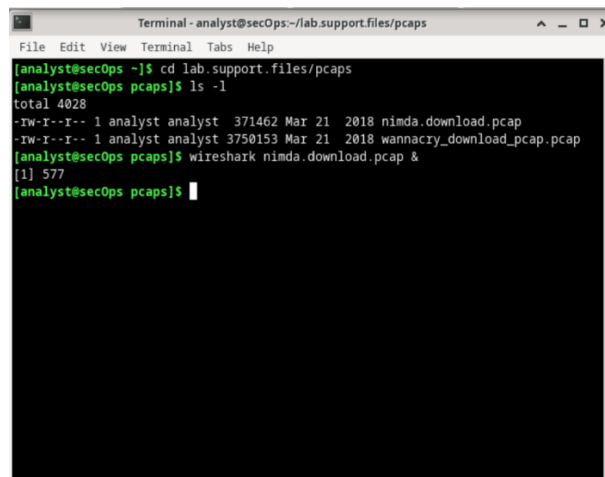
Elasticsearch. Kibana menyediakan *interface* berbasis web. Bagian utama kibana terbagi menjadi empat bagian utama:

1. *Management*: tempat dalam mencari index dibanding mencari teks secara langsung. Index terdiri dari *document* yang berisi *fields*, atau pasangan *key-value* dan *document* harus di definisikan melalui *mapping*.
2. *Discover*: bagian yang memungkinkan untuk menelusuri dan menganalisis entri data murni secara interaktif dan dapat dengan mudah dicari dan difilter menurut waktu atau property *document* menggunakan Bahasa kueri yang Bernama Kibana Querying Language (KBL).
3. *Visualize*: bagian ini memberikan kemungkinan dalam memvisualisasikan data dalam bentuk tabel, grafik, peta, histogram dan lainnya. Visualisasi Kibana dibangun berdasarkan kueri Elasticsearch menggunakan KBL Berbagai tindakan pemrosesan dapat tren dalam data. Setiap visualisasi hanya dapat bekerja pada single index pattern.
4. *Canvas*: bagian ini menggabungkan beberapa kueri *discover* dan hasil visualisasi *dashboards* yang telah disimpan menjadi sebuah tampilan visualisasi.

IV. Data Instruksi Kerja

Lab I

1. Mengubah direktori ke folder lab.support.files/pcaps untuk mendapatkan daftar file dengan menggunakan perintah `ls -l`

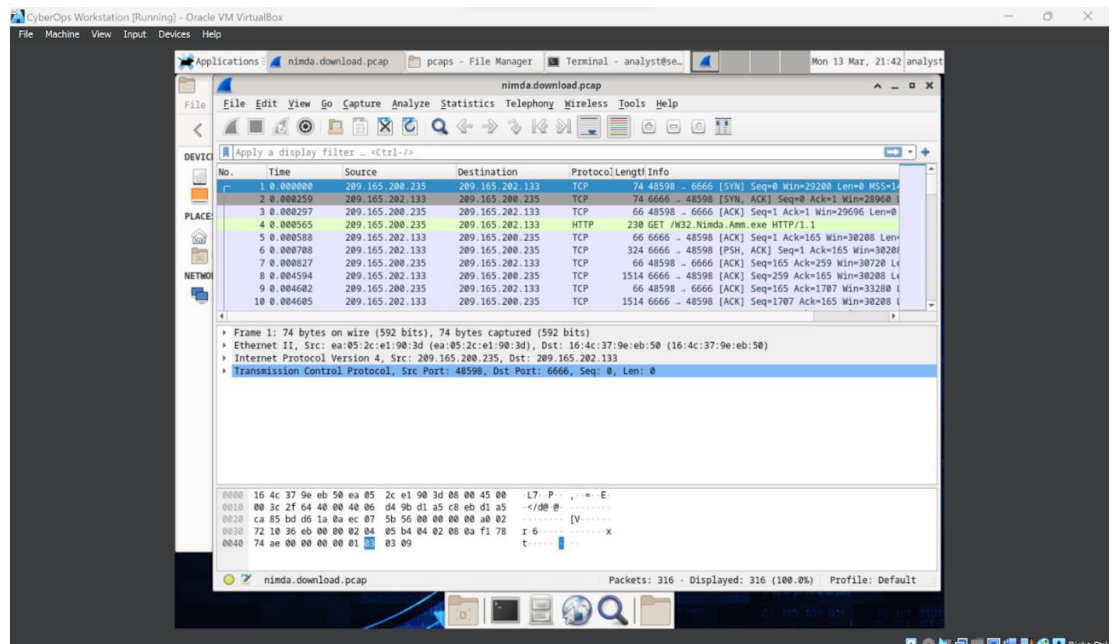


```
Terminal - analyst@secOps:~/lab.support.files/pcaps
File Edit View Terminal Tabs Help
[analyst@secOps ~]$ cd lab.support.files/pcaps
[analyst@secOps pcaps]$ ls -l
total 4028
-rw-r--r-- 1 analyst analyst 371462 Mar 21 2018 nimda.download.pcap
-rw-r--r-- 1 analyst analyst 3750153 Mar 21 2018 wannacry_download_pcap.pcap
[analyst@secOps pcaps]$ wireshark nimda.download.pcap &
[1] 577
[analyst@secOps pcaps]$
```

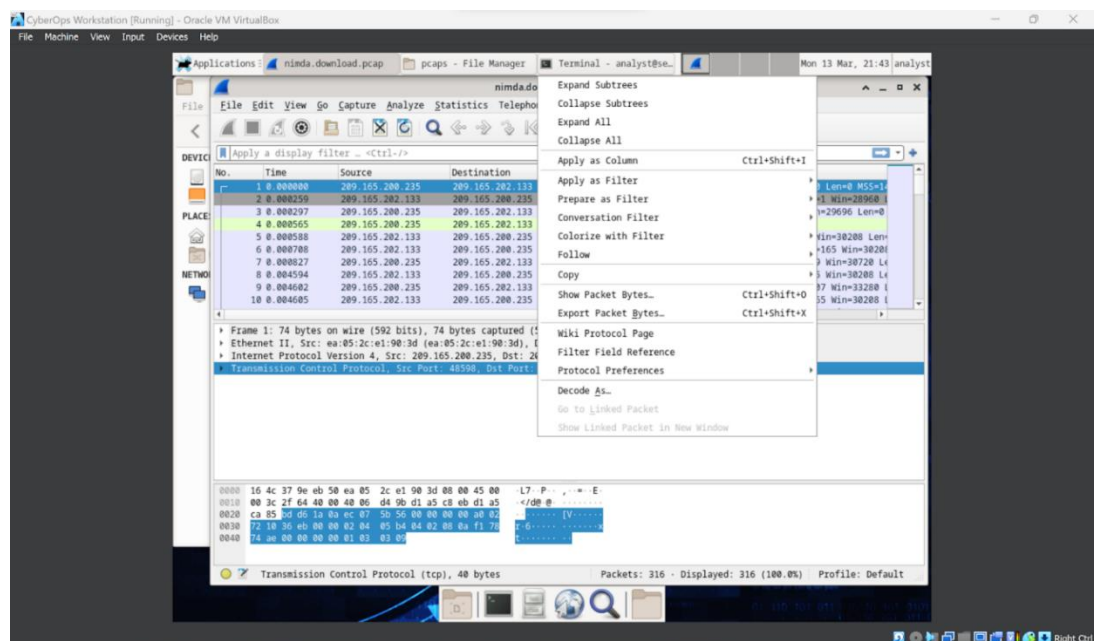
2. Membuka file nimda.download.pcap di Wireshark

```
[analyst@secOps pcaps]$ wireshark nimda.download.pcap &
[1] 577
[analyst@secOps pcaps]$
```

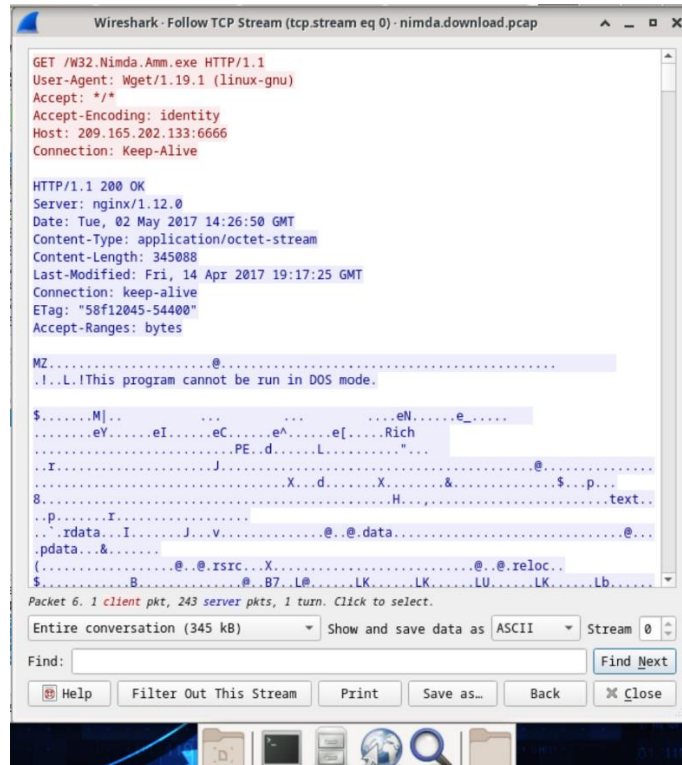
3. Mengambil paket yang terkait dengan unduhan malware sebelumnya, dengan memiliki paker keempat seperti dibawah ini:



4. Memilih paket TCP pertama dan klik ikuti seperti gambar dibawah:

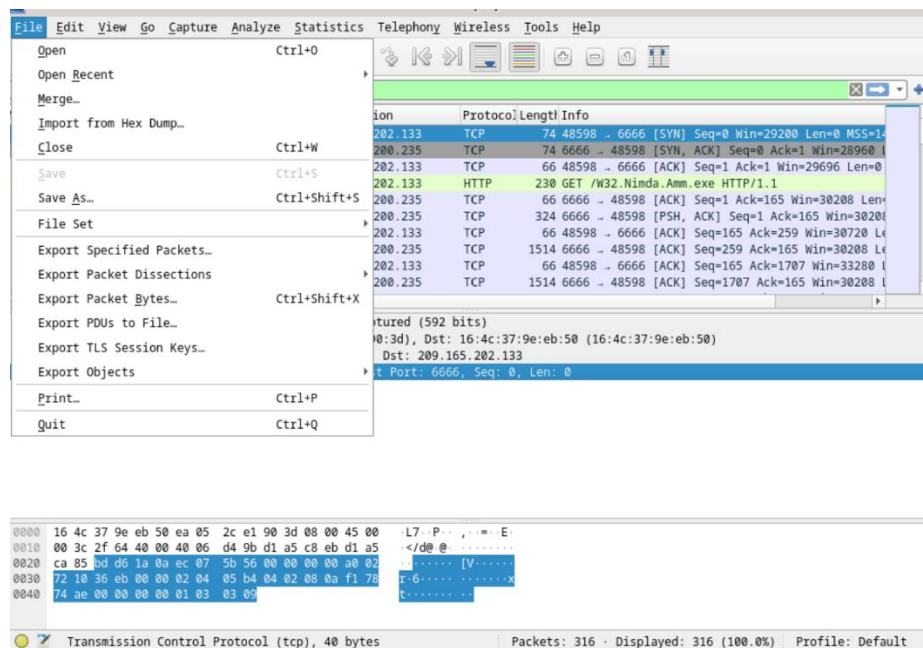


5. Menampilkan jendela wireshark yang berisi detail untuk seluruh aliran TCP yang dipilih seperti dibawah ini:

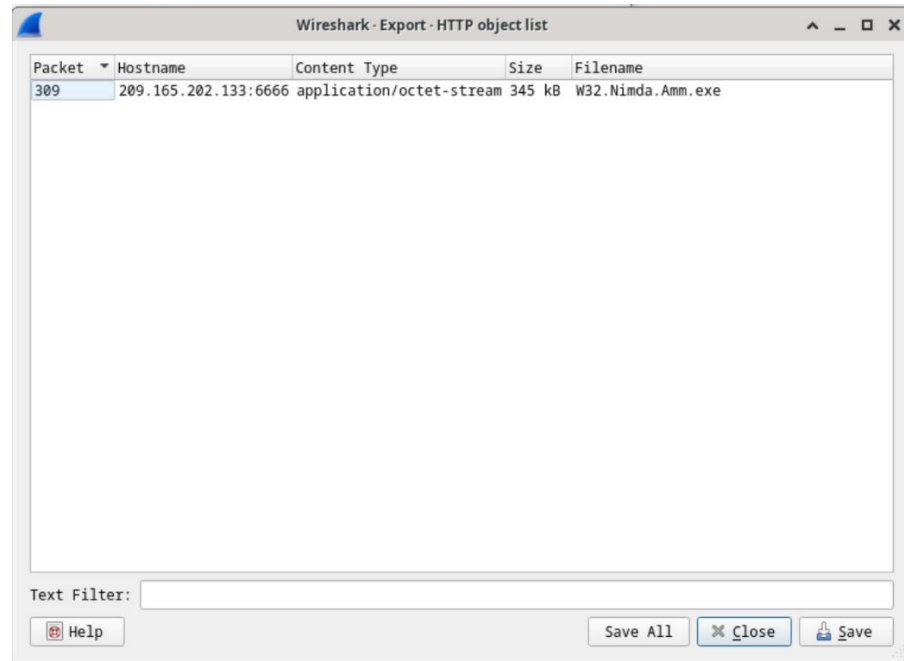


Lab II

1. Extract file



2. Menampilkan semua objek HTTP dalam aliran TCP yang berisi permintaan GET



3. Simpan file di analyst

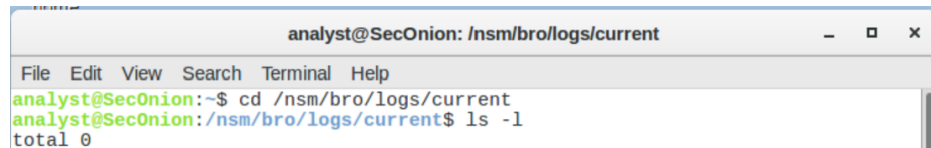
```
[analyst@secOps ~]$ cd /home/analyst
[analyst@secOps ~]$ ls -l
total 9064
drwxr-xr-x 2 analyst analyst 4096 May 20 2020 Desktop
drwxr-xr-x 3 analyst analyst 4096 Apr 2 2020 Downloads
-rw-r--r-- 1 root root 229695 Feb 27 08:15 httpdump.pcap
-rw-r--r-- 1 root root 8677167 Feb 27 08:30 httpsdump.pcap
drwxr-xr-x 9 analyst analyst 4096 Mar 13 22:01 lab.support.files
drwxr-xr-x 2 analyst analyst 4096 Mar 21 2018 second_drive
drwxr-xr-x 2 analyst analyst 4096 Feb 27 08:37 Tugas_Unit3_SaadahM
-rw-r--r-- 1 analyst analyst 345088 Mar 13 21:58 W32.Nimda.Amm.exe
[analyst@secOps ~]$
```

4. Perintah file untuk malware

```
[analyst@secOps ~]$ file W32.Nimda.Amm.exe
W32.Nimda.Amm.exe: PE32+ executable (console) x86-64, for MS Windows
[analyst@secOps ~]$
```

Lab II (Persiapan Log File pada Security Onion Virtual Machine)

1. Zeek Logs pada Security Onion



```
analyst@SecOnion: /nsm/bro/logs/current
File Edit View Search Terminal Help
analyst@SecOnion:~$ cd /nsm/bro/logs/current
analyst@SecOnion:/nsm/bro/logs/current$ ls -l
total 0
```

2. Snort Logs (sensor data)

```
analyst@SecOnion:/nsm/bro/logs/current$ cd /nsm/sensor_data
analyst@SecOnion:/nsm/sensor_data$ ls -l
total 12
drwxrwxr-x 7 sguil sguil 4096 Jun 19 2020 seconion-eth0
drwxrwxr-x 5 sguil sguil 4096 Jun 19 2020 seconion-eth1
drwxrwxr-x 7 sguil sguil 4096 Jun 19 2020 seconion-import
```

- Melihat file yang dihasilkan oleh antarmuka eth0

```
analyst@SecOnion:/nsm/sensor_data$ ls -l seconion-eth0
total 28
drwxrwxr-x 2 sguil sguil 4096 Jun 19 2020 argus
drwxrwxr-x 3 sguil sguil 4096 Jun 19 2020 dailylogs
drwxrwxr-x 2 sguil sguil 4096 Jun 19 2020 portscans
drwxrwxr-x 2 sguil sguil 4096 Jun 19 2020 sancp
drwxr-xr-x 2 sguil sguil 4096 Jun 19 2020 snort-1
-rw-r--r-- 1 sguil sguil 5594 Jun 19 2020 snort-1.stats
-rw-r--r-- 1 root root 0 Jun 19 2020 snort.stats
analyst@SecOnion:/nsm/sensor_data$
```

3. Various logs

- Direktori /nsm/menyimpan beberapa file log

```
analyst@SecOnion:/nsm/sensor_data$ cd /var/log/nsm/
analyst@SecOnion:/var/log/nsm$ ls
eth0-packets.log          sensor-newday-argus.log
netsniff-sync.log        sensor-newday-http-agent.log
ossec_agent.log           sensor-newday-pcap.log
seconion-eth0             so-elastic-configure-kibana-dashboards.log
seconion-import           so-elasticsearch-pipelines.log
securityonion             so-setup.log
sensor-clean.log          so-zeek-cron.log
sensor-clean.log.1.gz     squert-ip2c-5min.log
sensor-clean.log.2.gz     squert-ip2c.log
sensor-clean.log.3.gz     squert_update.log
sensor-clean.log.4.gz     watchdog.log
sensor-clean.log.5.gz     watchdog.log.1.gz
sensor-clean.log.6.gz     watchdog.log.2.gz
sensor-clean.log.7.gz
```

- Log ELK dapat ditemukan di direktori /var/log. Ubah direktori dan gunakan perintah ls untuk membuat daftar file dan direktori


```

analyst@SecOnion:/var/log/nsm$ cd ..
analyst@SecOnion:/var/log$ ls
alternatives.log      daemon.log.1         gpu-manager.log      samba
alternatives.log.1    daemon.log.2.gz      installer            sguild
alternatives.log.2.gz daemon.log.3.gz      kern.log             so-boot.log
alternatives.log.3.gz daemon.log.4.gz      kern.log.1           syslog
alternatives.log.4.gz debug               kern.log.2.gz        syslog.1
apache2               debug.1              Kibana               syslog.2.gz
apt                  debug.2.gz           lastlog              syslog.3.gz
auth.log              debug.3.gz           lightdm              syslog.4.gz
auth.log.1            debug.4.gz           logstash             syslog.5.gz
auth.log.2.gz          dmesg                lpr.log              syslog.6.gz
auth.log.3.gz          domain_stats         mail.err             syslog.7.gz
auth.log.4.gz          dpkg.log             mail.info            unattended-upgrades
boot                 dpkg.log.1           mail.log             user.log
boot.log             elastalert            mail.warn            user.log.1
bootstrap.log        elasticsearch         messages             user.log.2.gz
btmtp                error                messages.1           user.log.3.gz
btmtp.1              error.1              messages.2.gz        user.log.4.gz
cron.log              error.2.gz           messages.3.gz        wtmp
cron.log.1            error.3.gz           messages.4.gz        wtmp.1
cron.log.2.gz          error.4.gz           mysql                Xorg.0.log
cron.log.3.gz          faillog              nsm                  Xorg.0.log.old
cron.log.4.gz          freq_server           ntpstats             Xorg.1.log
curator              freq_server_dns      redis
daemon.log           fsck                  salt
analyst@SecOnion:/var/log$

```

Lab III

Langkah 1: Investigasi SQL Injection Attack

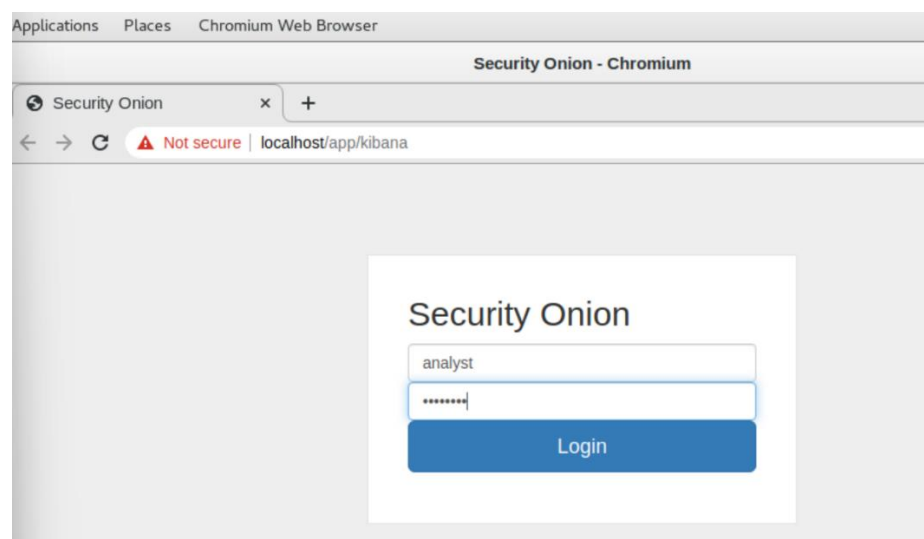
1. Perintah sudo

```

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 [ OK ]
* so-kibana [ OK ]
* so-freqserver [ OK ]
analyst@SecOnion:~$

```

2. Akses ke Kibana



3. Tampilkan dashboard kibana

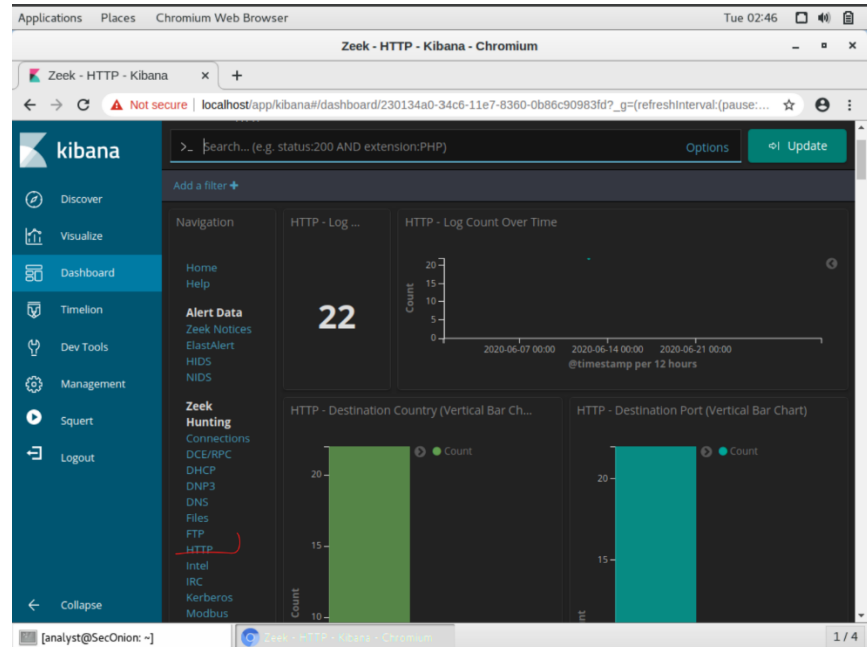
The top screenshot shows the Kibana 'Time Range' configuration page. The interface includes a sidebar with navigation options like Discover, Visualize, Dashboard, and Timelion. The main area is titled 'Time Range' and shows a calendar for June 2020. The 'From' date is set to 2020-06-01 00:00:00.000 and the 'To' date is 2020-06-30 23:59:59.999. A 'Go' button is visible at the bottom right of the calendar.

The bottom screenshot shows the Kibana dashboard. The main area displays several visualizations: 'Total Number of Logs' showing a count of 136, 'Total Log Count Over Time' showing a line graph, and 'All Sensors - Log Type' showing a table of log types and their counts.

| Log Type(s) | Count |
|-------------|-------|
| bro_conn | 62 |
| bro_files | 23 |
| bro_dns | 22 |
| bro_http | 22 |

Langkah 2: Filter dari HTTP traffic

1. Pilih filter HTTP



Alamat IP sumber dan tujuan

The screenshot shows the Kibana dashboard for Zeek - HTTP. The left sidebar contains navigation links: Timelion, Dev Tools, Management, Squert, and Logout. The main panel displays two visualizations: 'HTTP - Source IP Address' and 'HTTP - Destination IP Address'. Both visualizations show a table with IP addresses and their corresponding counts.

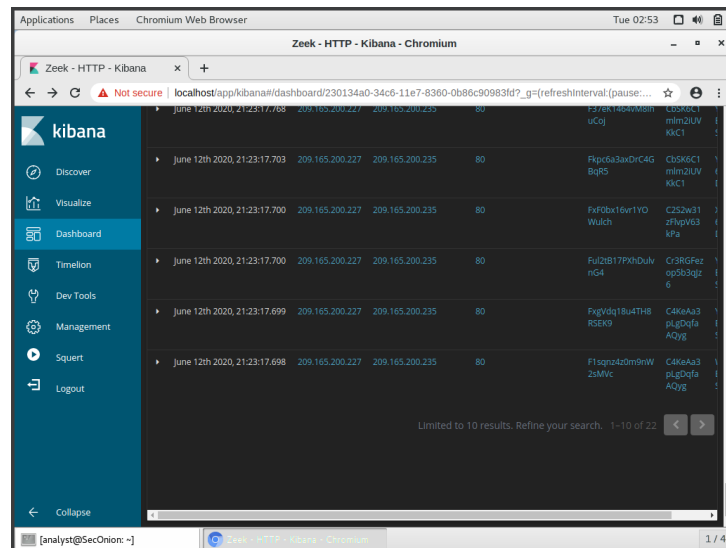
| IP Address | Count |
|-----------------|-------|
| 209.165.200.227 | 22 |

| IP Address | Count |
|-----------------|-------|
| 209.165.200.235 | 22 |

10 log hasil pertama:

The screenshot shows the Kibana dashboard for Zeek - HTTP. The left sidebar contains navigation links: Discover, Visualize, Dashboard, Timelion, Dev Tools, Management, Squert, and Logout. The main panel displays a table titled 'HTTP - Logs' showing the first 10 log results. The table has columns for Time, source_ip, destination_ip, destination_port, resp_fuids, and uid.

| 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 | FEWw63HqCgt h3LH1 | CukaR52 apJRN7PF qdd |
| June 12th 2020, 21:23:27.954 | 209.165.200.227 | 209.165.200.235 | 80 | FCbb5T2feB6Ga AYVBh | Cb5K6C1 mim2UUV KK1 |
| June 12th 2020, 21:23:27.881 | 209.165.200.227 | 209.165.200.235 | 80 | FwkdT14TjaAZYd NQ14 | Cb5K6C1 mim2UUV KK1 |
| June 12th 2020, 21:23:17.789 | 209.165.200.227 | 209.165.200.235 | 80 | FWOO3T1TT34U WLK63 | Cb5K6C1 mim2UUV KK1 |
| June 12th 2020, 21:23:17.768 | 209.165.200.227 | 209.165.200.235 | 80 | F37ek1464vM8th uCQj | Cb5K6C1 mim2UUV KK1 |
| June 12th 2020, 21:23:17.703 | 209.165.200.227 | 209.165.200.235 | 80 | Flp6da3axDrC4G BqR5 | Cb5K6C1 mim2UUV KK1 |
| June 12th 2020, 21:23:17.700 | 209.165.200.227 | 209.165.200.235 | 80 | FvR0bx16w1YO Wulch | C252wR1 zFwpw63 s63 |



Timestamp pertama:

| 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 |

Jenis event:

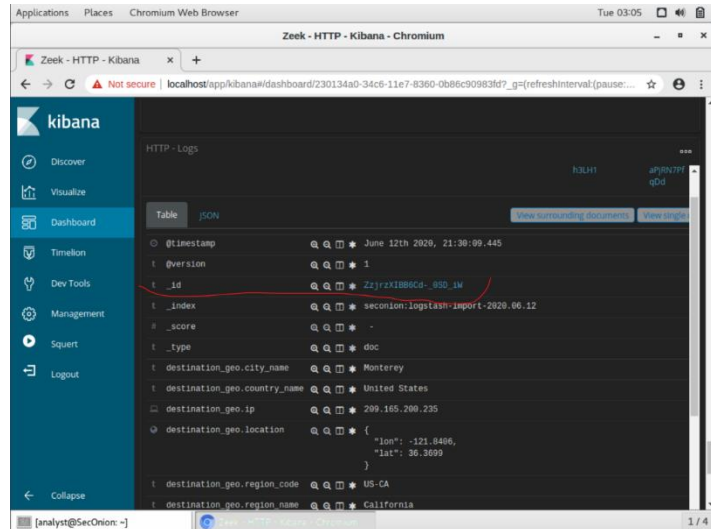
t event_type * bro_http

Termasuk dalam pesan:

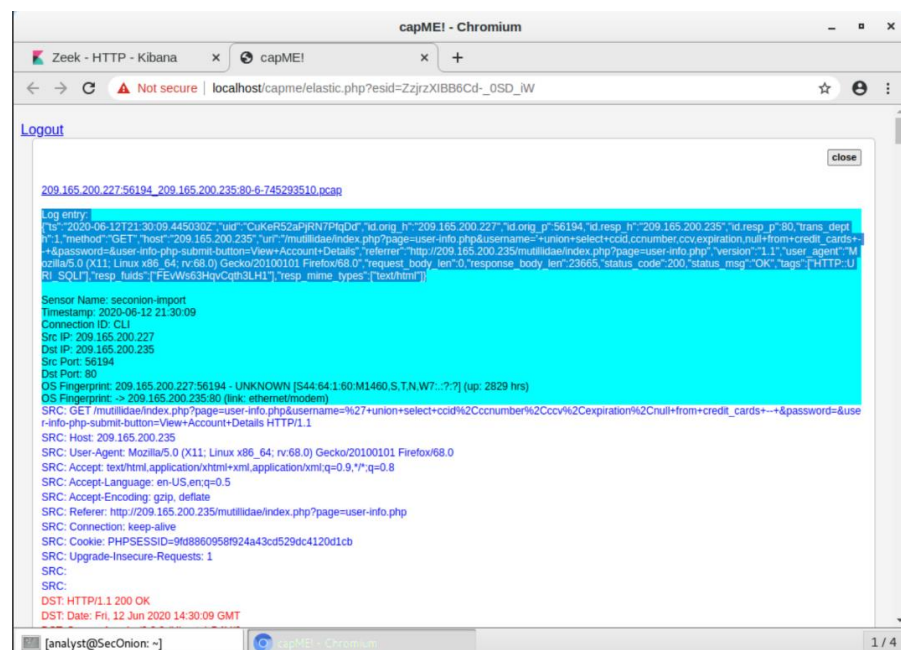
```
t message {"ts":"2020-06-12T21:30:09.445030Z","uid":"CuKeR52aPjRN7PfQdD","id":
h":"209.165.200.227","id.orig_p":56194,"id.resp_h":"209.165.200.235",
esp_p":80,"trans_depth":1,"method":"GET","host":"209.165.200.235",
mutillidae/index.php?page=user-info.php&username='+union+select+cc
ber,ccv,expiration,null+from+credit_cards+--+&password=&user-info-
it-button=View+Account+Details","referrer":"http://209.165.200.235
dae/index.php?page=user-info.php","version":"1.1","user_agent":"Mo
0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0","reque
len":0,"response_body_len":23665,"status_code":200,"status_msg":"0
s":["HTTP::URI_Sqli"],"resp_fuids":["FEVWs63HqvCqth3LH1"],"resp_mi
s":["text/html"]}
```

Langkah 2: Review Hasil

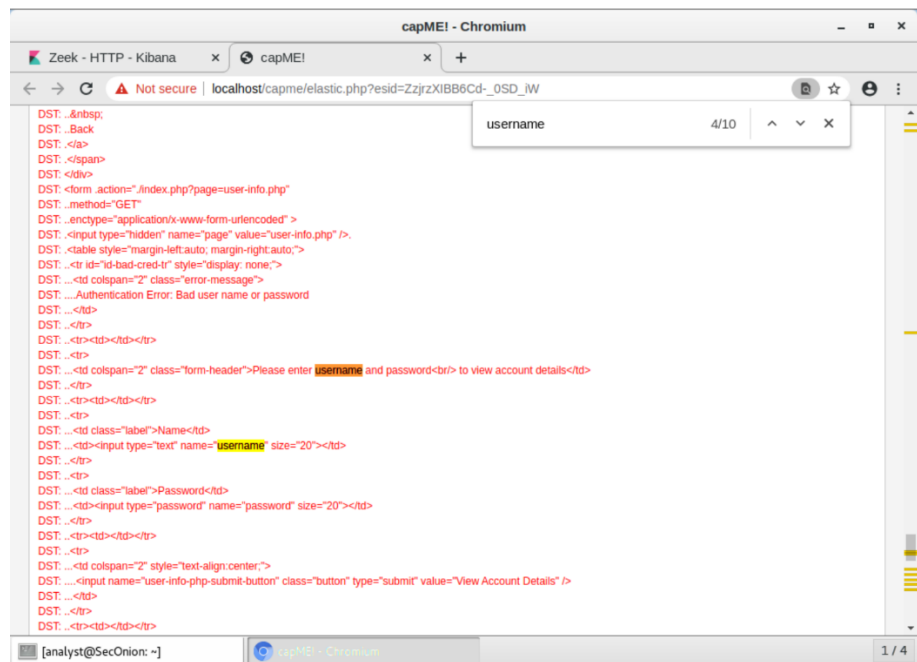
1. Klik nilai di bidang alert_id



2. Informasi CAPME *perhatikan entri log*



3. Menemukan username



Terlihat dalam transkrip username:

```
Log entry:
[{"ts":2020-06-12T21:30:09.445030Z,"uid":"CuKeR52aPJRN7PtQd","id.orig_h":"209.165.200.227","id.orig_p":56194,"id.resp_h":"209.165.200.235","id.resp_p":80,"trans_dept":1,"method":"GET","host":"209.165.200.235","uri":"/multilidae/index.php?page=user-info.php&username=%27+union+select+ccid%2Cccnumber%2Cccv%2Cexpiration%2Cnull+from+credit_cards+&password=&user-info-submit-button=View+Account+Details","referrer":"http://209.165.200.235/multilidae/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_huids":["FEVW563HqvCqth3LH1"],"resp_mime_types":["text/html"]}].
Sensor Name: seconion-import
Timestamp: 2020-06-12 21:30:09
Connection ID: CL1
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...7?] (up: 2829 hrs)
OS Fingerprint: -> 209.165.200.235:80 (link: ethernet/modem)
SRC: GET /multilidae/index.php?page=user-info.php&username=%27+union+select+ccid%2Cccnumber%2Cccv%2Cexpiration%2Cnull+from+credit_cards+&password=&user-info-submit-button=View+Account+Details HTTP/1.1
```

Contoh username, password dan signature yang telah di eksfiltrasi:

```
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
```

```

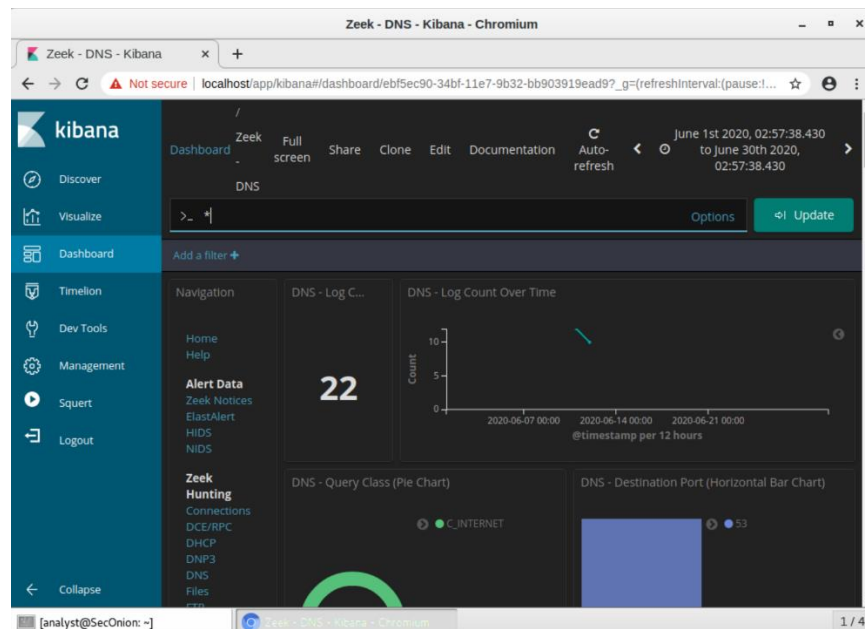
DST: <b>Username=</b>8242325748474749<br>
DST:
DST: 17
DST: <b>Password=</b>461<br>
DST:
DST: 22
DST: <b>Signature=</b>2016-03-01<br><p>
DST:
DST: 24

-----
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:
DST: 3

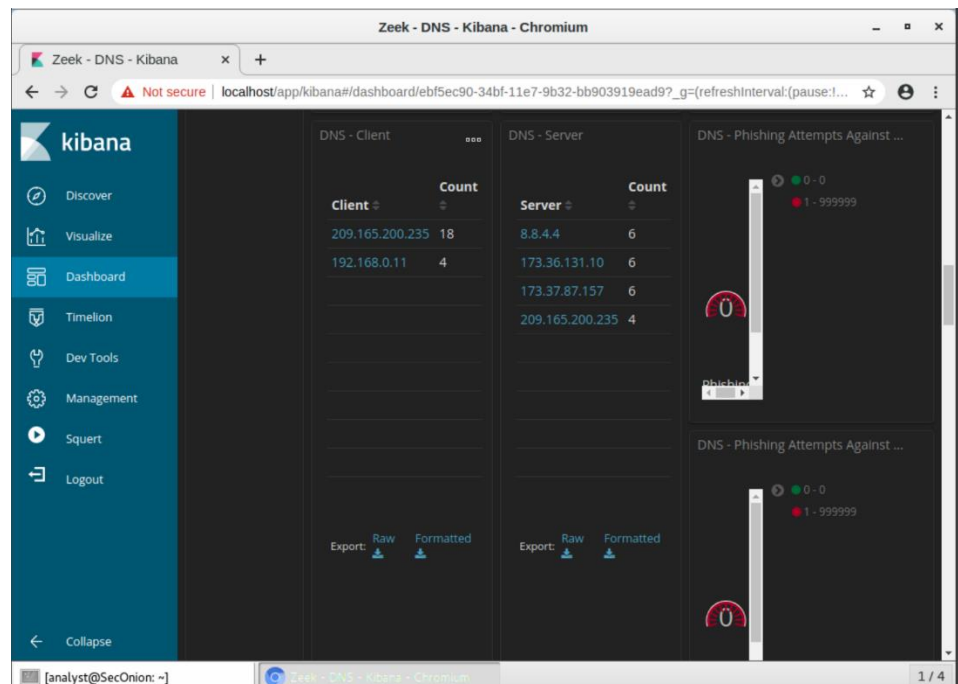
```

Lab IV: Analisis DNS Exfiltration

Langkah 2: filter DNS traffic



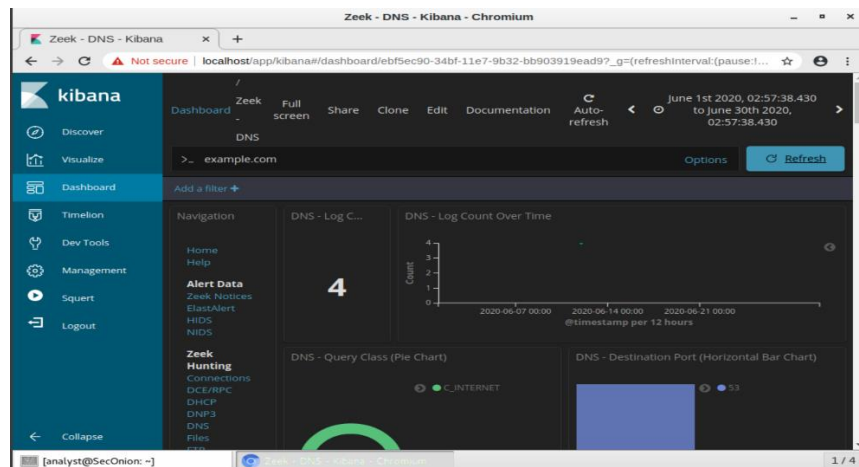
Langkah 2: tinjau entri terkait DNS



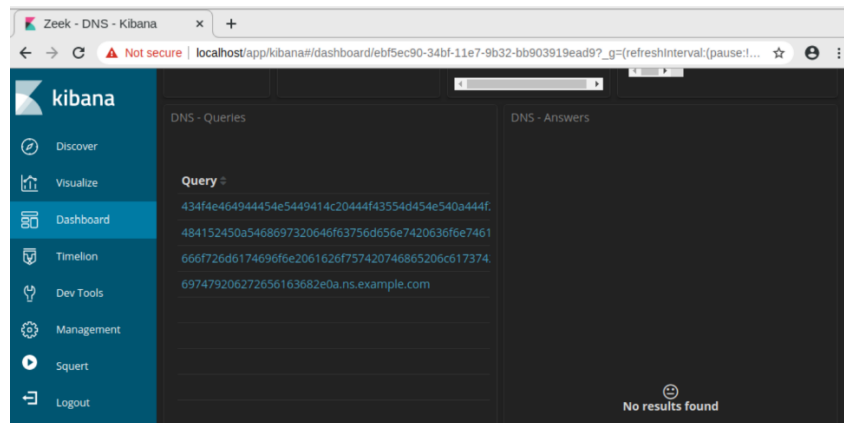
Daftar queri DNS teratas:

| DNS - Queries | DNS - Answers |
|--|-----------------------------|
| <div>Query</div> <div>17.201.165.209.in-addr.arpa</div> <div>434f4e464944454e5449414c20444f43554d454e540a444f.</div> <div>484152450a5468697320646f63756d656e7420636f6e7461</div> <div>666f726d6174696f6e2061626f757420746865206c617374.</div> <div>697479206272656163682e0a.ns.example.com</div> | <div>No results found</div> |

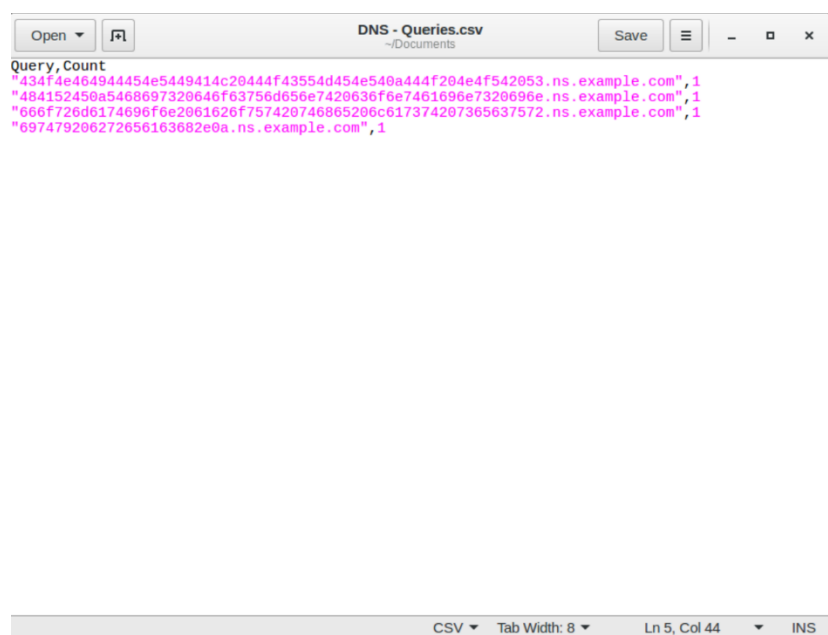
Filter example.com:



Data ekstraksi:



1. File teks



2. Menggunakan perintah xxd

```
analyst@Sec0nion:~$ cd /home/analyst/Downloads/  
analyst@Sec0nion:~/Downloads$ xxd -r -p "DNS - Queries.csv" > secret.txt  
analyst@Sec0nion:~/Downloads$ catsecret.txt  
catsecret.txt: command not found  
analyst@Sec0nion:~/Downloads$ cat secret.txt  
CONFIDENTIAL DOCUMENT  
DO NOT SHARE  
This document contains information about the last security breach.  
analyst@Sec0nion:~/Downloads$
```

V. Analisis

Analisis untuk pembahasan praktikum ini adalah dengan menjawab pertanyaan yang diberikan pada soal praktikum. Pada bagian 1, kita menyelesaikan pada permasalahan analisis log yang telah *capture* dan sebelum *capture* lalu lintas log. Disini kita menggunakan file *nimda.download.pcap*, berisikan paket-paket yang memiliki kaitan dengan unduhan malware Nimda. Penggunaan TCP dump untuk menganalisis file yang diambil, *interface* grafis wireshark dalam menyelesaikan permasalahan. Penyelesaian soal bagian pertama yaitu:

Soal 1:

Apa semua simbol yang ditampilkan di jendela Ikuti TCP Stream? jelaskan.

Penyelesaian:

Simbol-simbol yang ditampilkan pada jendela yang diikuti oleh TCP stream merupakan isi sebenarnya dari file yang telah di *download* atau diunduh. File yang diunduh merupakan file biner, dimana wireshark tidak dapat merepresentasikannya, sehingga simbol yang ditampilkan merupakan tebakan terbaik wireshark dalam memahami data biner yang dikerjakan bersamaan dengan mendekodekan file tersebut sebagai teks.

Bagian 2 yaitu melakukan extract file yang telah diunduh dari PCAP. Disini tetap menggunakan wireshark dalam mengambil malware nimda dan wireshark akan menampilkan semua objek HTTP yang terdapat dalam aliran TCP yang berisi permintaan GET. Penyelesaian soal bagian kedua yaitu:

Soal 2:

Mengapa W32.Nimda.Amm.exe setu-satunya file yang di *capture*?

Penyelesaian:

W32.Nimda.Amm.exe menjadi satu-satunya file yang di *capture*, karena proses *capture* dimulai tepat sebelum dilakukannya pengunduhan dan berhenti setelahnya. Sehingga tidak ada lalu lintas lain yang ter *capture* saat proses *capture* sedang aktif.

Tahap terakhir adalah memastikan file telah disimpan dan berhasil dimasukan pada folder seperti gambar dibawah ini:

Nama file: Tugas_Unit3_SaadahM

```
[analyst@secOps ~]$ cd /home/analyst
[analyst@secOps ~]$ ls -l
total 9064
drwxr-xr-x 2 analyst analyst 4096 May 20 2020 Desktop
drwxr-xr-x 3 analyst analyst 4096 Apr 2 2020 Downloads
-rw-r--r-- 1 root root 229695 Feb 27 08:15 httpdump.pcap
-rw-r--r-- 1 root root 8677167 Feb 27 08:30 httpsdump.pcap
drwxr-xr-x 9 analyst analyst 4096 Mar 13 22:01 lab.support.files
drwxr-xr-x 2 analyst analyst 4096 Mar 21 2018 second_drive
drwxr-xr-x 2 analyst analyst 4096 Feb 27 08:37 Tugas_Unit3_SaadahM
-rw-r--r-- 1 analyst analyst 345088 Mar 13 21:58 W32.Nimda.Amm.exe
[analyst@secOps ~]$
```

Sehingga Terlihat W32.Nimda.Amm.exe memanf file executable windows:

```
[analyst@secOps ~]$ file W32.Nimda.Amm.exe
W32.Nimda.Amm.exe: PE32+ executable (console) x86-64, for MS Windows
[analyst@secOps ~]$
```

Pada bagian 3 yaitu investigasi SQL dengan analisis log pada Kibana. Akan tetapi sebelum melakukan praktikum bagian 3, mahasiswa melakukan persiapan log file pada security onion VM. Pada bagian sebelumnya mahasiswa melakukan pengambilan data dengan menggunakan CyberOps Workstation VM. Melakukan normalisasi file log penting karena memungkinkan tools analisis log dalam menormalkan dan menyiapkan file log untuk menyediakan layanan analisis log seperti ELK. Pada bagian ini kita melakukan Log ELK untuk dapat kita temukan pada direktori /var/log dengan menggunakan perintah ls dalam membuat daftar file dan direktori seperti yang ditunjukkan pada gambar dibawah ini:

```

analyst@SecOnion: /var/log/nsm$ cd ..
analyst@SecOnion: /var/log$ ls
alternatives.log      daemon.log.1          gpu-manager.log       samba
alternatives.log.1    daemon.log.2.gz       installer             sguild
alternatives.log.2.gz daemon.log.3.gz       kern.log              so-boot.log
alternatives.log.3.gz daemon.log.4.gz       kern.log.1            syslog
alternatives.log.4.gz debug                kern.log.2.gz         syslog.1
apache2               debug.1              Kibana               syslog.2.gz
apt                  debug.2.gz           lastlog              syslog.3.gz
auth.log             debug.3.gz           lightdm              syslog.4.gz
auth.log.1           debug.4.gz           logstash             syslog.5.gz
auth.log.2.gz        dmesg               lpr.log             syslog.6.gz
auth.log.3.gz        dpkg.log            mail.err            syslog.7.gz
auth.log.4.gz        dpkg.log.1          mail.info           unattended-upgrades
boot                domain_stats        mail.log            user.log
boot.log            elastalert          mail.warn           user.log.1
bootstrap.log        elasticsearch       messages            user.log.2.gz
btmtp               error              messages.1          user.log.3.gz
btmtp.1             error.1            messages.2.gz       user.log.4.gz
cron.log            error.2.gz         messages.3.gz       wtmp
cron.log.1          error.3.gz         messages.4.gz       wtmp.1
cron.log.2.gz       error.4.gz         mysql              Xorg.0.log
cron.log.3.gz       faillog            nsm                Xorg.0.log.old
cron.log.4.gz       freq_server        ntpstats           Xorg.1.log
curator             freq_server_dns    redis
daemon.log          fsck               salt
analyst@SecOnion: /var/log$

```

Pada bagian 3 kita akan melakukan penyelidikan dengan eksploitasi akses yang tidak sah dibuat ke informasi sensitive yang disimpan pada server web. Disini dengan menggunakan kibana dalam menentukan sumber serangan dan informasi yang dikases oleh penyerang. Kibana berperan dalam visualisasi data dan alat penjelajahan untuk meninjau log dan kejadian. Kibana memungkinkan pengguna untuk mengeksplorasi dan memantau seluruh ELK Stack. Langkah pertama yaitu mengubah *timeframe*, dimana kibana akan melakukan default data selama 24 jam terakhir dengan menggunakan perintah `sudo so-status`. Terlihat pada data instruksi kerja terdapat 136 jumlah total log pada seluruh bulan juni 2020. Pada langkah 2 yaitu melakukan filter dari HTTP traffic, filter HTTP digunakan untuk memilih log yang terkait dengan lalu lintas HTTP. Pada proses filter ini ada pertanyaan soal yang harus diselesaikan. Berikut pertanyaan pada bagian 3:

Soal 3:

Apa alamat IP sumber?

Penyelesaian :

Alamat IP sumber adalah = 209.165.200.227. Penyelesaian ini telah dibuktikan dari pengambilan data pada instruksi kerja.

Soal 4:

Apa alamat IP tujuan?

Penyelesaian :

Alamat IP sumber adalah = 209.165.200.235. Penyelesaian ini telah dibuktikan dari pengambilan data pada instruksi kerja.

Soal 5:

Berapa nomor port tujuan?

Penyelesaian :

Port tujuan adalah 80. Penyelesaian ini telah dibuktikan dari pengambilan data pada instruksi kerja.

daftar 10 hasil pertama telah telampir pada data instruksi kerja

Soal 6:

Apa timestamp dari hasil pertama?

Penyelesaian :

Timestamp pertama adalah June 12th 2020, 21:30:09.445.

Soal 7:

Apa jenis event?

Penyelesaian :

Jenis event adalah bro_http.

Soal 8:

Apa yang termasuk dalam kolom pesan?

Penyelesaian :

Dalam kolom pesan berisikan rincian mengenai permintaan HTTP GET yang dibuat oleh klien ke server. Fokus utama pada bidang uri dalam teks pesan.

pesan yang termasuk adalah: *username*, *ccid*, *ccnumber*, *ccv*, *expiration* dan *password*.

Soal 9:

Apa pentingnya informasi ini?

Penyelesaian :

Informasi ini sepertinya adalah permintaan informasi mengenai kartu kredit.

Langkah 2 pada bagian 3 adalah review hasil, dengan beberapa informasi untuk entri log di tautkan ke tools lainnya. Untuk mendapatkan tampilan entri log dengan klik pada nilai bidang alert *_id*. Dimana nanti hasil yang akan terbuka pada tab browser web baru dengan informasi dari CAPME. CAPME merupakan *interface* web yang dapat memungkinkan *user* melihat transkrip PCAP. Seperti yang terlihat dari data instruksi kerja pada CAPME menampilkan **teks biru: berisi permintaan HTTP yang dikirimkan dari sumber (SRC)** dan **teks merah: tanggapan dari server web tujuan (DST)**. Disini kita akan menemukan *username* dalam transkrip seperti penyelesaian soal seperti dibawah ini:

Soal 10:

Apa yang anda lihat nanti dalam transkrip tentang nama pengguna?

Penyelesaian :

Seperti ada daftar nama pengguna dan kata sandi yang merupakan bagian dari informasi yang dikembalikan sebagai respons terhadap permintaan HTTP GET.

Soal 11:

Berikan beberapa contoh username, password, dan signature yang telah dieksfiltrasi

Penyelesaian :

| Username | Password | Signature |
|------------------|----------|------------|
| 4444111122223333 | 745 | 2012-03-01 |
| 7746536337776330 | 722 | 2015-04-01 |
| 8242325748474749 | 461 | 2016-03-01 |
| 7725653200487633 | 230 | 2017-06-01 |
| 1234567812345678 | 627 | 2018-11-01 |

Bagian selanjutnya adalah analisis DNS exfiltration. Pada bagian DNS kita akan memperhatikan permintaan DNS yang panjangnya tidak sesuai dengan domain dan tampak aneh. Tugas kita disini adalah menyelidiki anomali. Langkah pertama adalah dengan menghapus semua filter dan istilah bagian pencarian. Pada bagian area dashboard yang sama ketika klik DNS bagian zeek hunting, terlihat metrik jumlah log DNS yang itu 22 dan diagram batang dari horizontal port tujuan. Pada peninjauan entri terakit DNS terlihat jenis kueri DNS teratas, catatan IP address, IPv6, catatan Quad A (AAAA), catatan NetBIOS (NB) dan catatan pointer yang akan digunakan dalam menyelesaikan nama host (PTR) dan dapat melihat kode respons dari DNS. Disini kita juga dapat melihat daftar klien DNS dan server DNS teratas berdasarkan jumlah permintaan dan respon. Terdapat metrik untuk jumlah upaya DNS phishing yang dikenal dengan pharminf DNS, spoofing atau poisoning. Terlihat daftar kueri DNS teratas berdasarkan nama domain. Disini terdapat kueri memiliki subdomain yang sangat panjang dilampirkan ke ns.example.com dan pada saat inilah kita melakukan penyelidikan pada domain example.com. Sesuai dengan apa ditampilkan terlihat jumlah entri dalam hitungan log yaitu 4 atau lebih kecil dikarenakan tampilan terbatas pada permintaan ke server example.com.

Soal 12:

Sebutkan alamat IP klien dan server DNS?

Penyelesaian :

Alamat IP klien adalah 192.168.0.11 dan server adalah 209.165.200.235.

Terbukti dari data instruksi kerja tinjau entri terkait DNS.

Percobaan terakhir adalah menentukan data yang diekstraksi. Dengan melihat empat log unik untuk kueri DNS ke example.com. Disini kita memperhatikan bagaimana kueri ke subdomain panjang yang mencurigakan dilampirkan ke ns.example.com. Selanjutnya adalah dengan melakukan ekspor tautan dan mengunduh kueri ke file eksternal. File CSV yang diunduh ke folder /home/analys/Downloads. Lalu membuka file menggunakan editor teks. Pada terminal kita menggunakan perintah xxd untuk memecahkan kode teks dalam file CSV dan menyimpan ke file bernama secret.text. Kita menggunakan cat untuk menampilkan konten secret.text. ke konsol. Langkah ini telah dilakukan dan data dimasukkan pada bagian data instruksi kerja.

Soal 13:

Apakah subdomain dari subdomain kueri DNS? Jika tidak, apa teksnya?

Penyelesaian :

DOKUMEN RAHASIA

JANGAN BERBAGI

Dokumen ini berisi informasi tentang pelanggaran keamanan terakhir.

Soal 14:

Apa yang disiratkan hasil ini tentang permintaan DNS khusus ini? Apa signifikansi yang lebih besar?

Penyelesaian :

Hasilnya menunjukkan bahwa permintaan DNS terpisah, permintaan terkoordinasi yang berisi konten tersembunyi. Signifikansi yang lebih besar dari hasilnya adalah bahwa permintaan DNS dapat digunakan untuk menyembunyikan pengiriman file dan melewati keamanan jaringan.

Soal 15:

Apa yang mungkin membuat kueri DNS yang disandikan ini dan mengapa DNS dipilih sebagai sarana untuk mengekstrak data?

Penyelesaian :

Ada kemungkinan bahwa malware membuat permintaan ini dengan menelusuri dokumen di host dan menyandikan kontennya dalam heksadesimal dan kemudian membuat kueri DNS yang menggunakan string heksadesimal sebagai subdomain DNS. Permintaan DNS sangat umum dikirim dari jaringan ke internet, sehingga permintaan DNS mungkin tidak dipantau

VI. Kesimpulan

1. Menafsirkan data HTTP dan DNS merupakan keahlian penting dalam analisis ancaman. Melalui analisis tangkapan paket menggunakan alat seperti Wireshark, analis dapat mengekstrak informasi berharga seperti alamat IP, nama domain, dan nama pengguna yang dapat membantu mengidentifikasi potensi aktivitas berbahaya. Dengan menganalisis pola komunikasi dan mengidentifikasi anomali atau lalu lintas yang mencurigakan dapat mengisolasi sumber ancaman dan mengambil tindakan yang tepat untuk mengurangi risiko
2. Mengekstrak file yang dapat dieksekusi dari file PCAP menjadi teknik bagi analis keamanan. Dengan menganalisis tangkapan paket menggunakan alat seperti Wireshark dan memeriksa isi lalu lintas jaringan dapat mengidentifikasi file yang berpotensi berbahaya dan mengekstraknya untuk analisis lebih lanjut. Setelah file yang dapat dieksekusi diekstrak dapat menggunakan tools tambahan dalam melakukan analisis statis dan dinamis untuk mendapatkan pemahaman yang lebih baik tentang perilaku file dan potensi dampaknya terhadap sistem. Mengesktraksi dan menganalisis file executable membutuhkan

keterampilan teknis dan pengetahuan tentang tren dan teknik ancaman terbaru.

DAFTAR PUSTAKA

- [1] Amazon Web Services. (n.d.). What is the ELK Stack? from <https://aws.amazon.com/id/what-is/elk-stack/>
- [2] Binus University. (2020). Mengenal Aplikasi Wireshark. from <https://binus.ac.id/bandung/2020/06/mengenal-aplikasi-wireshark/>
- [3] Eduparx. (2021). Mengenal ELK Stack untuk Monitoring Server. from <https://eduparx.id/blog/insight/mengenal-elk-stack-untuk-monitoring-server/>
- [4] Hidayatullah, A., & Firmansyah, M. R. (2020). Implementasi Log Management Server Menggunakan ELK (Elastic Search, Logstash, dan Kibana) Stack pada Server Web Snort di PT.XYZ. Jurnal Teknologi dan Sistem Komputer, 8(4), 153-160. doi: 10.14710/jtsiskom.2020.12369
- [5] Kurniawan, A. R., & Setiawan, E. A. (2018). Implementasi SIEM (Security Information and Event Management) menggunakan ELK (Elasticsearch, Logstash, Kibana) pada Jaringan Komputer. Jurnal Informatika dan Teknologi Informasi, 4(2), 43-51. doi: 10.30743/jiti.v4i2.366
- [6] Kusuma, F. H., & Febriyanto, A. (2015). Analisa Hasil Capture Wireshark. From https://www.academia.edu/14830081/Analisa_Hasil_Capture_Wireshark
- [7] Mappesona, M. (2015). Praktikum Analisis File Pcap. from <https://mappesona.me/2015/08/05/praktikum-analisis-file-pcap/>
- [8] Microsoft. (n.d.). Cluster Logging Kibana. from <https://learn.microsoft.com/id-id/sql/big-data-cluster/cluster-logging-kibana?view=sql-server-ver15>

- [9] Mustofa, K., & Cahyani, D. P. (2016). Analisis Protokol VoIP Menggunakan Wireshark. Jurnal Ilmiah Teknik Informatika, 9(2), 167-174. doi: 10.28932/jutisi.v9i2.95
- [10] Nesaba Media. (n.d.). Pengertian Wireshark. from <https://www.nesabamedia.com/pengertian-wireshark/>

LINK GITHUB

<https://github.com/saadahmardatillah/Unit-4.2-Keamanan-Informasi-1>