LAPORAN
PRAKTIKUM KEAMANAN INFORMASI 1
UNIT 7
EKSTRAK EXECUTABLE DARI PCAP DAN MENAFSIRKAN DATA HTTP DAN DNS UNTUK MENGISOLASI PELAKU ANCAMAN

DISUSUN OLEH:

Nama : Yana Dayinta Nesthi
Kelas : RI4AA
NIM : 21/478358/SV/19272
Dosen : Anni Karimatul Fauziyyah, S.Kom., M.Eng.

SARJANA TERAPAN TEKNOLOGI REKAYASA INTERNET
DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA
SEKOLAH VOKASI
UNIVERSITAS GADJAH MADA

2023

EKSTRAK EXECUTABLE DARI PCAP DAN MENAFSIRKAN DATA HTTP DAN DNS UNTUK MENGISOLASI PELAKU ANCAMAN

A. TUJUAN

- Investigasi SQL Injection Attack
- Analisis Pre-Captured Logs dan Traffic Captures
- Investigasi DNS Data Exfiltration

B. DASAR TEORI

1. SQL Injection Attack

SQL Injection Attack adalah serangan yang ditujukan pada situs web dan aplikasi web yang menggunakan database untuk menyimpan informasi. Dalam serangan ini, penyerang menyuntikkan kode SQL berbahaya ke dalam kueri database melalui input data yang disediakan oleh pengguna, yang memungkinkan penyerang untuk mengakses, memodifikasi, atau menghapus data yang tersimpan di dalam database. Selain itu, serangan ini dapat digunakan untuk mencuri data pengguna seperti kredensial login, informasi kartu kredit, dan informasi pribadi.

Untuk mencegah serangan SQL Injection, pengembang web harus mengimplementasikan teknik validasi dan sanitasi input yang sesuai, menggunakan *query* berparameter, dan menghindari pembentukan kueri SQL secara dinamis menggunakan input yang diberikan oleh pengguna.

2. Pre-Captured Logs dan Traffic Captures

Pre-Captured Logs adalah data log yang telah direkam dan disimpan sebelum sebuah insiden terjadi, yang dapat memberikan informasi penting untuk menganalisis dan menyelidiki insiden keamanan. Sementara itu, Traffic Captures adalah paket data yang ditangkap dari lalu lintas jaringan untuk menganalisis pola lalu lintas jaringan, menemukan masalah jaringan, dan menyelidiki insiden keamanan. Kedua jenis data ini dapat memberikan wawasan yang berharga tentang aktivitas dan perilaku pengguna dan sistem dalam sebuah jaringan.

3. DNS Data Exfiltration

DNS data exfiltration atau DNS tunneling merupakan teknik yang dimanfaatkan oleh penyerang untuk mencuri data dari jaringan target melalui protokol Domain Name System (DNS). Penyerang melakukan hal tersebut dengan mengkodekan data yang ingin dicuri ke dalam permintaan atau respons DNS, lalu mengirimkan data tersebut melalui permintaan DNS ke server eksternal yang dikendalikan oleh penyerang. Dengan cara ini, penyerang dapat menghindari tindakan keamanan seperti firewall yang mungkin tidak memantau DNS secara ketat.

C. ALAT DAN BAHAN

- PC
- Koneksi internet
- *CyberOps Workstation Virtual Machine*
- *Security Onion Virtual Machine*

D. HASIL DAN ANALISIS

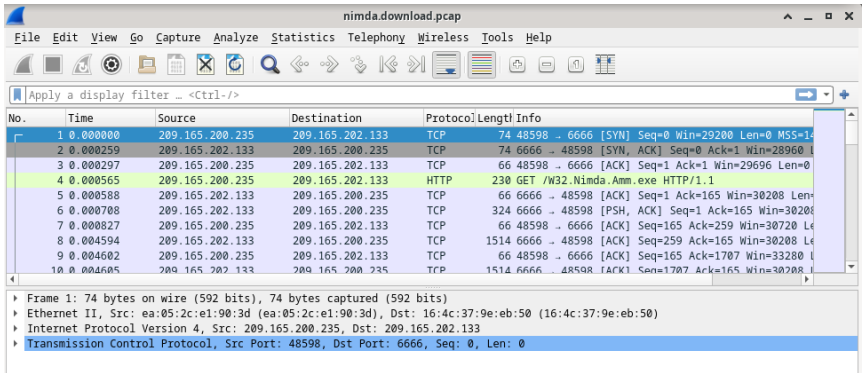
Langkah 1: Menganalisis Log yang Ditangkap sebelumnya dan Pengambilan Lalu Lintas

1. Ubah direktori ke folder lab.support.files/pcaps, dan dapatkan daftar file menggunakan perintah ls –l.
   [analyst@secOps ~]$ cd lab.support.files/pcaps
   [analyst@secOps pcaps]$ ls -l

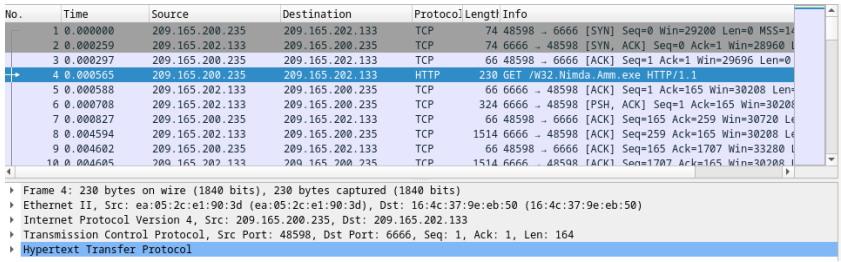
```
[analyst@secOps ~]$ cd lab.support.files/pcaps
[analyst@secOps pcaps]$ ls -l
total 4028
-rw-r--r-- 1 analyst analyst  371462 Mar 21  2018 nimda.download.pcap
-rw-r--r-- 1 analyst analyst 3750153 Mar 21  2018 wannacry_download_pcap.pcap
```

2. Keluarkan perintah di bawah ini untuk membuka file nimda.download.pcap di Wireshark.
   [analyst@secOps pcaps]$ wireshark nimda.download.pcap &

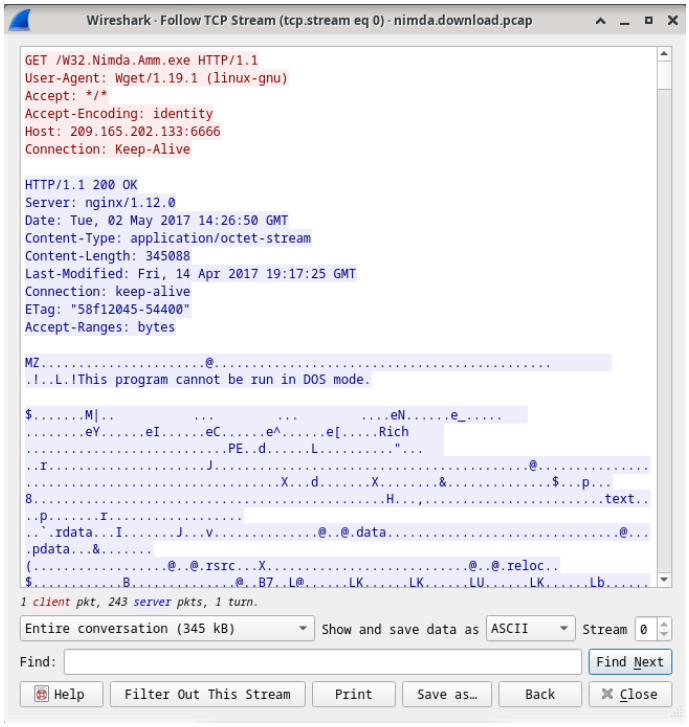
```
[analyst@secOps pcaps]$ wireshark nimda.download.pcap &
[1] 510
```



3. File nimda.download.pcap berisi pengambilan paket yang terkait dengan unduhan malware

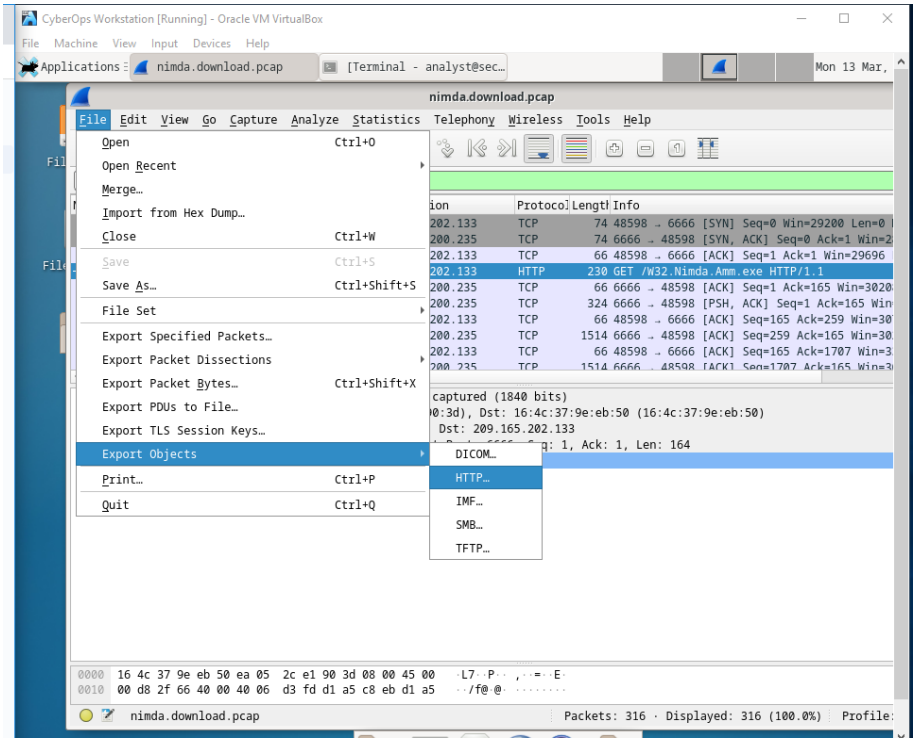


4. Karena HTTP berjalan di atas TCP, dimungkinkan untuk menggunakan fitur Follow TCP Stream Wireshark untuk membangun kembali transaksi TCP. Pilih paket TCP pertama yang di capture, paket SYN. Klik kanan dan pilih Ikuti > TCP Stream.
5. Wireshark menampilkan jendela lain yang berisi detail untuk seluruh aliran TCP yang dipilih.

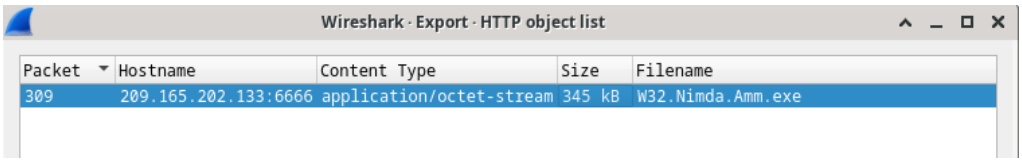


Part 2: Extract Files yang di unduh dari PCAP

6. Dalam paket keempat dalam file nimda.download.pcap, perhatikan bahwa permintaan HTTP GET dihasilkan dari 209.165.200.235 menjadi 209.165.202.133. Kolom Info juga menunjukkan bahwa ini sebenarnya adalah permintaan GET untuk file tersebut.
7. Dengan paket permintaan GET yang dipilih, navigasikan ke File > Export Objects > HTTP, dari menu Wireshark



8. Wireshark akan menampilkan semua objek HTTP yang ada dalam aliran TCP yang berisi permintaan GET. Dalam hal ini, hanya file W32.Nimda.Amm.exe yang ada dalam pengambilan. Ini akan memakan waktu beberapa detik sebelum file ditampilkan..



9. Di jendela daftar objek HTTP, pilih file W32.Nimda.Amm.exe dan klik Simpan Sebagai di bagian bawah layar.
10. Klik panah kiri hingga Anda melihat tombol Beranda. Klik Beranda lalu klik folder analis (bukan tab analis). Simpan file di sana.
11. Kembali ke jendela terminal Anda dan pastikan file telah disimpan. Ubah direktori ke folder /home/analyst dan daftarkan file di folder tersebut menggunakan perintah ls -l.

```
[analyst@secOps pcaps]$ cd /home/analyst
[analyst@secOps ~]$ ls -l
total 480
drwxr-xr-x 2 analyst analyst   4096 May 20  2020 Desktop
drwxr-xr-x 3 analyst analyst   4096 Feb 20 20:40 Downloads
-rw-r--r-- 1 root    root     80024 Mar  1 22:47 httpdump.pcap
-rw-r--r-- 1 root    root     36864 Feb 20 21:31 httpsdump.pcap
-rw-r--r-- 1 analyst analyst     51 Mar  6 21:18 lab.support
drwxr-xr-x 9 analyst analyst   4096 Jul 15  2020 lab.support.files
drwxr-xr-x 2 analyst analyst   4096 Mar 21  2018 second_drive
-rw-r--r-- 1 analyst analyst 345088 Mar 13 21:54 W32.Nimda.Amm.exe
```

12. Perintah file memberikan informasi tentang jenis file. Gunakan perintah file untuk mempelajari lebih lanjut tentang malware, seperti yang ditunjukkan di bawah ini:
[analyst@secOps ~]$ file W32.Nimda.Amm.exe

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

PEMBAHASAN:

Simbol-simbol yang ditampilkan pada jendela Follow FTP Stream mewakili konten asli dari file yang diunduh. Karena itu adalah file biner, Wireshark tidak tahu cara mempresentasikannya. Simbol-simbol yang ditampilkan adalah tebakan terbaik Wireshark untuk membuat makna dari data biner sambil mendekodekannya sebagai teks. Terdapat juga kata-kata yang tersebar di antara simbol-simbol tersebut, yang merupakan string yang terdapat dalam kode eksekutif. Biasanya, kata-kata ini adalah bagian dari pesan yang disediakan oleh program kepada pengguna saat program berjalan. Meskipun lebih bersifat seni daripada ilmu, seorang analis terampil dapat mengekstrak informasi berharga dengan membaca fragmen-fragmen tersebut.

Meskipun dinamakan W32.Nimda.Amm.exe, file executable ini sebenarnya bukanlah worm yang terkenal. Untuk alasan keamanan, ini adalah file lain yang dapat dieksekusi yang diubah namanya menjadi W32.Nimda.Amm.exe. Dengan menggunakan fragmen kata yang ditampilkan oleh jendela Follow TCP Stream milik Wireshark, untuk mengetahui apakah executable ini sebenarnya dapat dilihat dengan menggulir ke bawah pada jendela tersebut, terungkap bahwa ini adalah file cmd.exe dari Microsoft Windows.

Apabila direktori diubah menjadi folder /home/analyst dan daftar file di dalam folder tersebut ditampilkan menggunakan ls -l, maka file telah disimpan. Dalam proses analisis malware, langkah selanjutnya yang mungkin diambil oleh seorang analis keamanan adalah memenuhi tujuannya. Tujuannya adalah untuk mengidentifikasi jenis malware dan menganalisis perilakunya. Oleh karena itu, file malware harus dipindahkan ke lingkungan yang terkendali dan dieksekusi untuk mengamati perilakunya. Lingkungan analisis malware sering bergantung pada mesin virtual dan disimpan dalam sandbox untuk menghindari kerusakan

pada sistem non-tes. Lingkungan tersebut biasanya berisi alat-alat yang memfasilitasi pemantauan eksekusi malware; penggunaan sumber daya, koneksi jaringan, dan perubahan sistem operasi adalah aspek pemantauan yang umum.

Terdapat juga beberapa alat analisis malware berbasis internet. VirusTotal (virustotal.com) adalah salah satu contohnya. Analis mengunggah malware ke VirusTotal, yang pada gilirannya mengeksekusi kode berbahaya. Setelah eksekusi dan beberapa pemeriksaan lainnya, VirusTotal mengembalikan laporan kepada analis.

E. KESIMPULAN

Dalam jendela Follow FTP Stream, simbol-simbol yang ditampilkan merupakan konten sebenarnya dari file yang diunduh, dan Wireshark melakukan tebakan terbaik dalam mengkonversinya menjadi teks. String-string dalam executable code yang ditampilkan bisa menjadi bagian dari pesan program kepada pengguna. W32.Nimda.Amm.exe bukanlah worm terkenal, melainkan executable yang namanya diubah. Untuk melakukan analisis malware, langkah selanjutnya adalah memindahkan file ke lingkungan terkendali seperti lingkungan virtual yang terisolasi dan mengamati perilakunya. Selain itu, ada alat analisis malware online seperti VirusTotal yang dapat mengeksekusi malware dan menghasilkan laporan hasil analisis.

F. DAFTAR PUSTAKA

Endance. (n.d.). *What is Network Packet Capture?* Endace. Diakses pada Maret 19, 2023, dari https://www.endace.com/learn/what-is-network-packet-capture

Infoblox. (n.d.). *DNS Data Exfiltration*. Infoblox. Diakses pada Maret 19, 2023, dari https://www.infoblox.com/dns-security-resource-center/dns-security-issues-threats/dns-security-threats-data-exfiltration/

PortSwigger. (n.d.). *What is SQL Injection? Tutorial & Examples | Web Security Academy*. PortSwigger. Diakses pada Maret 19, 2023, dari https://portswigger.net/web-security/sql-injection

LAPORAN
PRAKTIKUM KEAMANAN INFORMASI 1
UNIT 7 BAGIAN 2
PERSIAPAN LOG FILE PADA SECURITY ONION VIRTUAL MACHINE

DISUSUN OLEH:

Nama : Yana Dayinta Nesthi
Kelas : RI4AA
NIM : 21/478358/SV/19272
Dosen : Anni Karimatul Fauziyyah, S.Kom., M.Eng.

SARJANA TERAPAN TEKNOLOGI REKAYASA INTERNET
DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA
SEKOLAH VOKASI
UNIVERSITAS GADJAH MADA
2023

PERSIAPAN LOG FILE PADA SECURITY ONION VIRTUAL MACHINE

A. TUJUAN

Tujuan dari plugin ini adalah untuk memungkinkan alat analisis log untuk menormalkan dan menyiapkan file log yang diterima untuk konsumsi alat.

B. ALAT BAHAN

- PC
- Koneksi internet
- *Security Onion Virtual Machine*

C. DASAR TEORI

1. Log File

Sebuah file log adalah file data yang dihasilkan oleh komputer yang berisi informasi tentang pola penggunaan, aktivitas, dan operasi dalam sistem operasi, aplikasi, server, atau perangkat lainnya. File log menunjukkan apakah sumber daya berfungsi dengan baik dan optimal.

File log adalah catatan sejarah tentang semua hal yang terjadi dalam sebuah sistem, termasuk kejadian seperti transaksi, kesalahan, dan data lain dari aplikasi, sistem operasi. Mereka memberikan cara bagi administrator sistem untuk melacak operasi sistem komputasi.

File log dapat digunakan untuk menyelesaikan masalah dengan perangkat lunak atau perangkat keras dengan memberikan informasi terperinci tentang apa yang terjadi sebelum kesalahan terjadi. Mereka juga dapat digunakan untuk memantau kinerja sistem dan mengidentifikasi ancaman keamanan yang potensial.

Untuk membuka file log di Windows, Anda dapat menggunakan alat Viewer Acara bawaan. Pada sistem berbasis Linux, file log biasanya disimpan di direktori /var/log dan dapat dilihat menggunakan baris perintah atau editor teks.
Secara ringkas, file log adalah catatan penting tentang kejadian yang terjadi dalam sistem komputasi. Mereka menyediakan informasi berharga untuk menyelesaikan masalah dengan perangkat lunak atau perangkat keras dan memantau kinerja sistem.

2. Security Onion Virtual Machine

Security Onion merupakan distribusi Linux bebas dan sumber terbuka yang dirancang khusus untuk threat hunting, enterprise security monitoring, dan log management. Pengguna dapat menginstalnya sebagai mesin virtual pada VMware Workstation Pro atau VMware Fusion, atau pada VirtualBox.

Untuk menggunakan Security Onion sebagai mesin virtual, diperlukan perangkat keras yang mampu mendukungnya, termasuk ruang penyimpanan SSD

sebesar 200 GB, RAM 16GB, dan 4 CPU Cores. Pengguna harus mengunduh file ISO terbaru dari situs web resmi atau repositori GitHub.

Setelah mendapatkan file ISO, buatlah mesin virtual baru di VMware dengan memilih "File" > "New Virtual Machine" dan ikuti instruksinya.

Setelah berhasil menginstal Security Onion sebagai mesin virtual, Anda bisa menggunakannya untuk memonitor lalu lintas jaringan perusahaan dan mendeteksi ancaman keamanan potensial. Dengan menggunakan Setup wizard yang mudah digunakan, pengguna dapat membuat jaringan sensor yang terdistribusi untuk perusahaan pengguna dalam waktu singkat.

D. HASIL DAN ANALISIS

1. Buka jendela terminal di Security Onion VM. Klik kanan Desktop. Di menu pop-up, pilih Buka Terminal.
2. Log Zeek disimpan di /nsm/bro/logs/. Seperti biasa dengan sistem Linux, file log diputar berdasarkan tanggal, diganti namanya dan disimpan di disk. File log saat ini dapat ditemukan di bawah direktori saat ini. Dari jendela terminal, ubah direktori menggunakan perintah berikut.
   analyst@SecOnion:~$ cd /nsm/bro/logs/current
3. Gunakan perintah ls -l untuk melihat file log yang dihasilkan oleh Zeek:

```
analyst@SecOnion:~$ cd /nsm/bro/logs/current
analyst@SecOnion:/nsm/bro/logs/current$ ls -l
total 0
analyst@SecOnion:/nsm/bro/logs/current$
```

4. Log snort dapat ditemukan di /nsm/sensor_data/. Ubah direktori sebagai berikut.
   analyst@SecOnion:/nsm/bro/logs/current$ cd /nsm/sensor_data

```
analyst@SecOnion:/nsm/bro/logs/current$ cd /nsm/sensor_data
analyst@SecOnion:/nsm/sensor_data$
```

5. Gunakan perintah ls -l untuk melihat semua file log yang dihasilkan oleh Snort

```
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
analyst@SecOnion:/nsm/sensor_data$
```

6. Perhatikan bahwa Security Onion memisahkan file berdasarkan antarmuka. Karena image Security Onion VM memiliki dua antarmuka yang dikonfigurasi sebagai sensor dan folder khusus untuk data yang diimpor, tiga direktori disimpan. Gunakan perintah ls –l seconion-eth0 untuk 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
```

7. Sementara direktori /nsm/ menyimpan beberapa file log, file log yang lebih spesifik dapat ditemukan di bawah /var/log/nsm/. Ubah direktori menggunakan perintah ls untuk melihat semua file log di direktori.
   analyst@SecOnion:/nsm/sensor_data$ cd /var/log/nsm/
   analyst@SecOnion:/var/log/nsm$ ls

```
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           sosetup.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
```

8. 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        fsck              salt
alternatives.log.1      daemon.log.1      gpu-manager.log   samba
alternatives.log.2.gz   daemon.log.2.gz   installer         sguild
alternatives.log.3.gz   daemon.log.3.gz   kern.log          so-boot.log
alternatives.log.4.gz   daemon.log.4.gz   kern.log.1        syslog
alternatives.log.5.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
btmp                    error             messages.1        user.log.3.gz
btmp.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
```

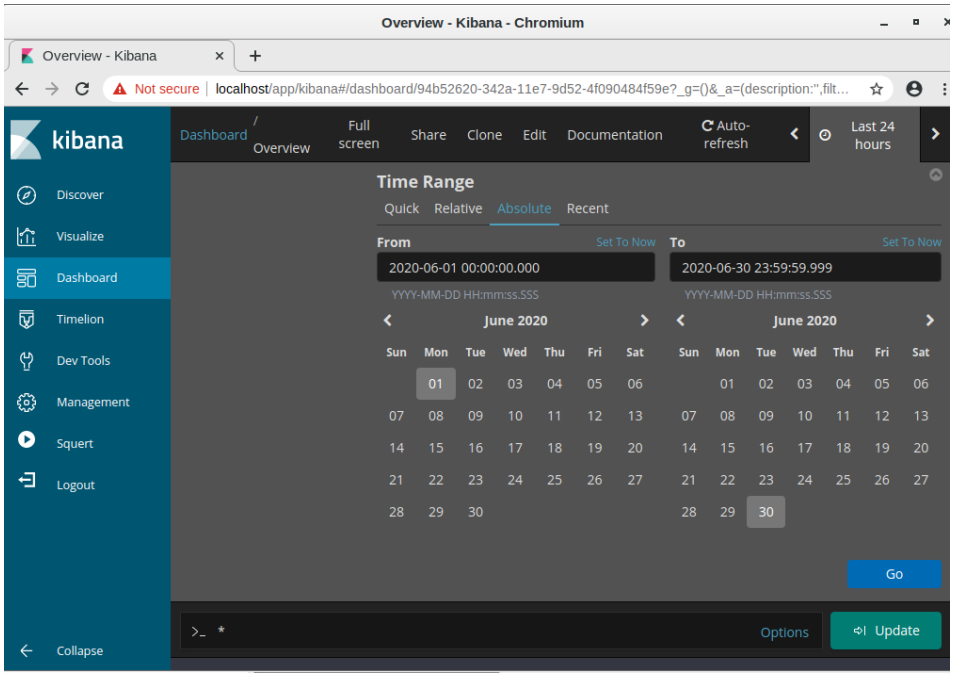
Part 3: Langkah 1: Investigasi SQL Injection Attack

1. Mulai Security Onion VM dan masuk dengan username analyst and the password cyberops.

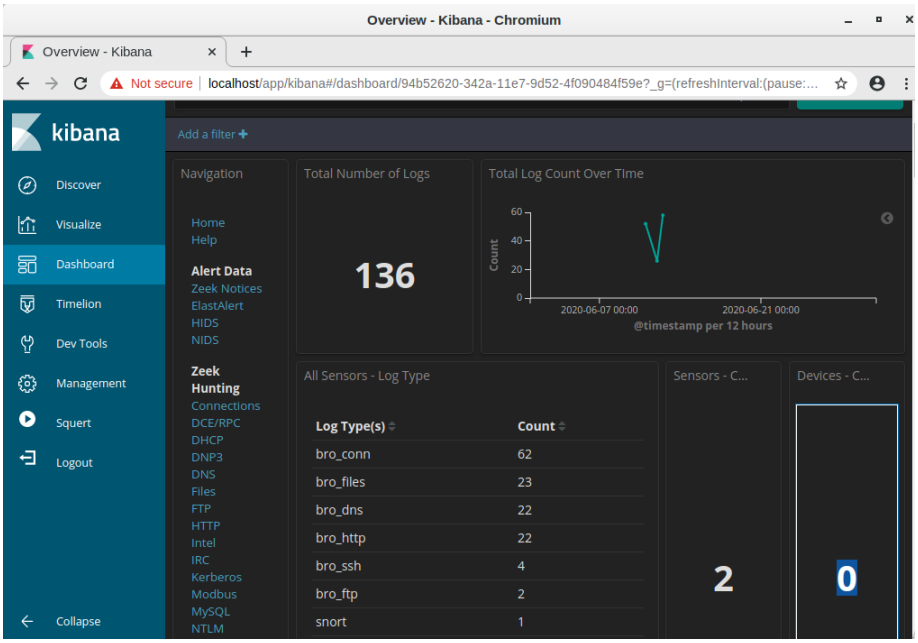
2. Masukkan perintah sudo so-status untuk memeriksa status layanan. Status untuk semua layanan harus OK sebelum memulai analisis . Ini bisa memakan waktu beberapa menit.
   analyst@SecOnion:~$ sudo so-status

```
analyst@SecOnion:/$ sudo so-status
[sudo] password for analyst:
Status: securityonion
  * sguil server                                                [  OK  ]
Status: seconion-import
  * pcap_agent (sguil)                                          [  OK  ]
  * snort_agent-1 (sguil)                                       [  OK  ]
  * barnyard2-1 (spooler, unified2 format)                      [  OK  ]
Status: Elastic stack
  * so-elasticsearch                                            [  OK  ]
  * so-logstash                                                 [  OK  ]
  * so-kibana                                                   [  OK  ]
  * so-freqserver                                               [  OK  ]
```

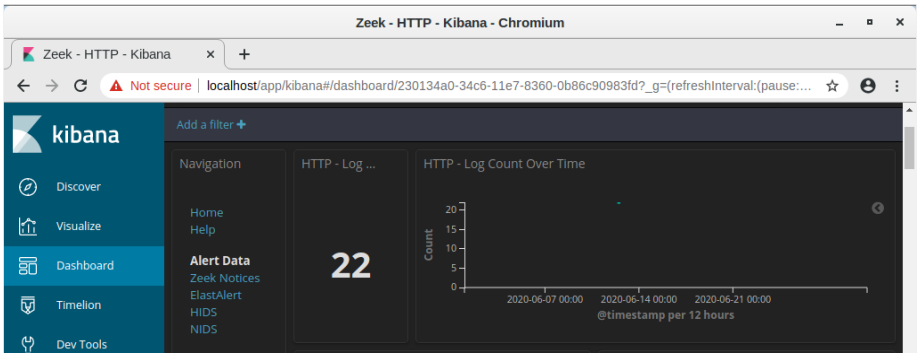
3. Setelah Anda masuk, buka Kibana menggunakan pintasan di Desktop. Masuk dengan username analyst dan password cyberops.
   Di Security Onion, Kibana memiliki banyak dasbor dan visualisasi bawaan untuk pemantauan dan analisis. Anda juga dapat membuat dasbor dan visualisasi khusus Anda sendiri untuk memantau lingkungan jaringan khusus Anda. Catatan: Dasbor Anda mungkin tidak memiliki hasil apa pun dalam 24 jam terakhir.
4. Di sudut kanan atas jendela, klik 24 jam terakhir untuk mengubah ukuran Rentang Waktu sampel. Perluas rentang waktu untuk menyertakan peringatan yang menarik. Serangan injeksi SQL terjadi pada Juni 2020 jadi itulah yang perlu Anda targetkan. Pilih Absolute di bawah Rentang Waktu dan edit waktu Dari dan Ke untuk memasukkan seluruh bulan Juni di 2020. Klik Pergi untuk melanjutkan.



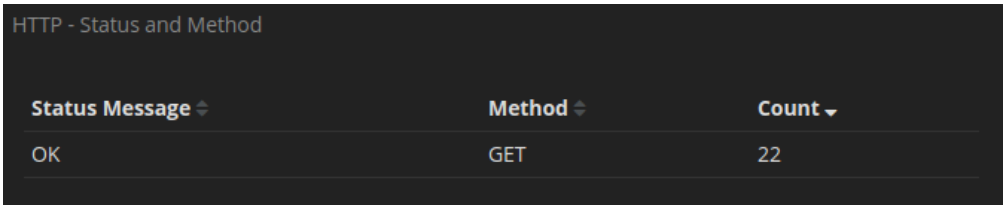
5. Perhatikan jumlah total log untuk seluruh bulan Juni 2020. Dasbor Anda harus serupa dengan yang ditunjukkan pada gambar. Luangkan waktu sejenak untuk menjelajahi informasi yang disediakan oleh antarmuka Kibana.

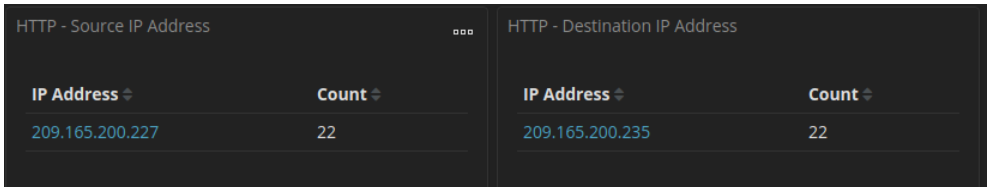


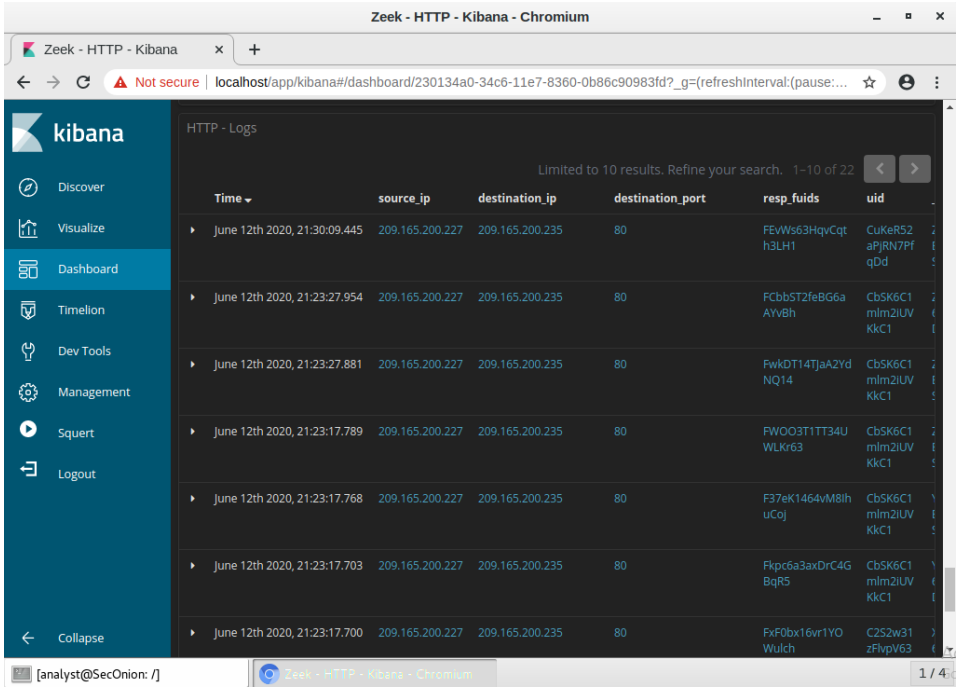
6. Karena aktor ancaman menilai data yang disimpan di server web, filter HTTP digunakan untuk memilih log yang terkait dengan lalu lintas HTTP. Pilih HTTP di bawah judul Zeek Hunting, seperti yang ditunjukkan pada gambar.

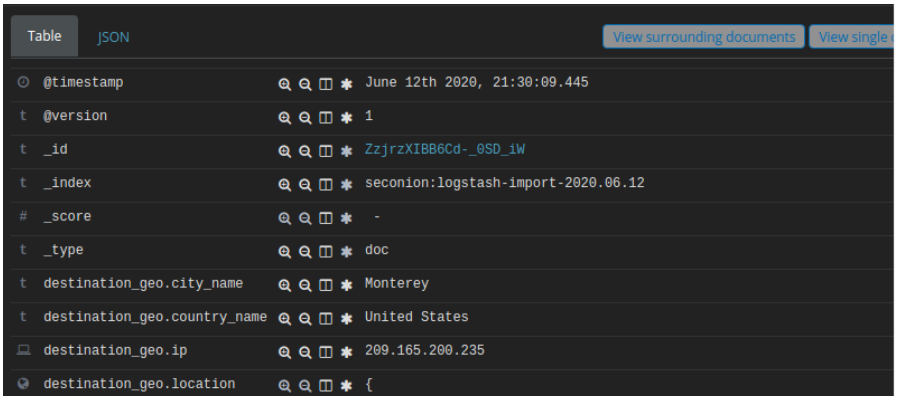


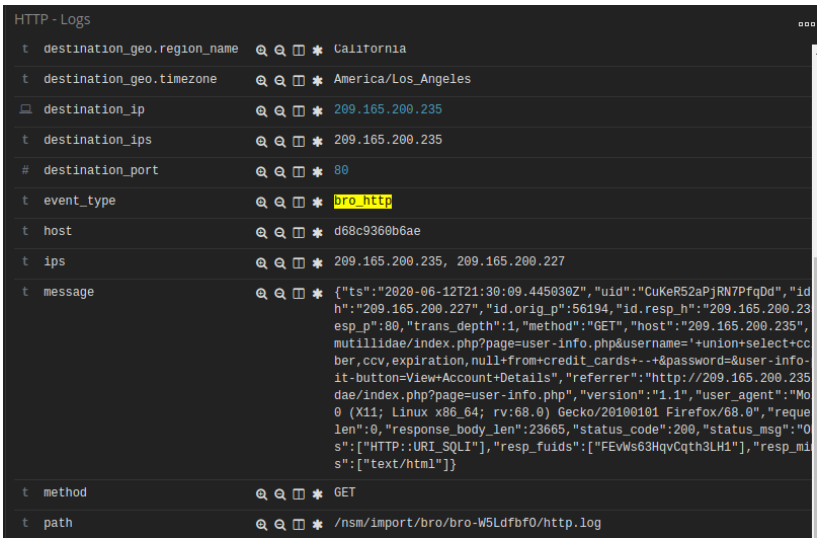

Zeek - HTTP - Kibana - Chromium
Zeek - HTTP - Kibana
Not secure
localhost/app/kibana#/dashboard/230134a0-34c6-11e7-8360-0b86c90983fd?_g=(refreshInterval:(pause:...
kibana
Discover
Visualize
Dashboard
Timelion
Dev Tools
Management
Squert
Logout
Zeek Hunting
Connections
DCE/RPC
DHCP
DNP3
DNS
Files
FTP
HTTP
Intel
IRC
Kerberos
Modbus
MySQL
NTLM
PE
RADIUS
RDP
RFB
SIP
SMB
SMTP
SNMP
Software
SSH
SSL
Syslog
Tunnels
HTTP - Destination Country (Vertical Bar Ch...
Count
United States
Country
HTTP - Destination Port (Vertical Bar Chart)
Count
80
Port


HTTP - Status and Method
Status Message
Method
Count
OK
GET
22


HTTP - Source IP Address
IP Address
Count
209.165.200.227
22
HTTP - Destination IP Address
IP Address
Count
209.165.200.235
22

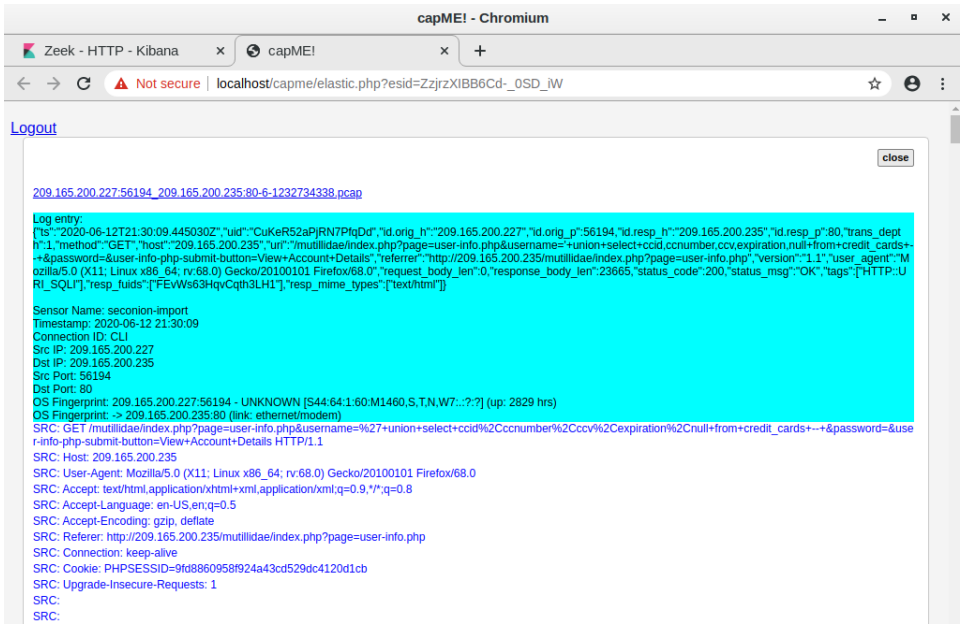

Zeek - HTTP - Kibana - Chromium
Zeek - HTTP - Kibana
Not secure
localhost/app/kibana#/dashboard/230134a0-34c6-11e7-8360-0b86c90983fd?_g=(refreshInterval:(pause:...
kibana
Discover
Visualize
Dashboard
Timelion
Dev Tools
Management
Squert
Logout
Collapse
HTTP - Logs
Limited to 10 results. Refine your search. 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 FEvWs63HqvCqth3LH1 CuKeR52aPjRN7PfqDd
June 12th 2020, 21:23:27.954 209.165.200.227 209.165.200.235 80 FCbbST2feBG6aAYvBh CbSK6C1mlm2IUVKkC1
June 12th 2020, 21:23:27.881 209.165.200.227 209.165.200.235 80 FwkDT14TjaA2YdNQ14 CbSK6C1mlm2IUVKkC1
June 12th 2020, 21:23:17.789 209.165.200.227 209.165.200.235 80 FWOO3T1TT34UWLKr63 CbSK6C1mlm2IUVKkC1
June 12th 2020, 21:23:17.768 209.165.200.227 209.165.200.235 80 F37eK1464vM8IhuCoj CbSK6C1mlm2IUVKkC1
June 12th 2020, 21:23:17.703 209.165.200.227 209.165.200.235 80 Fkpc6a3axDrC4GBqR5 CbSK6C1mlm2IUVKkC1
June 12th 2020, 21:23:17.700 209.165.200.227 209.165.200.235 80 FxF0bx16vr1YOWulch C2S2w31zFlvpV63
[analyst@SecOnion: /]
Zeek - HTTP - Kibana - Chromium
1 / 4



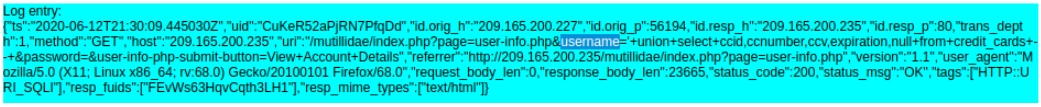


7. Beberapa informasi untuk entri log ditautkan ke alat lain. Klik nilai di bidang alert _id dari entri log untuk mendapatkan tampilan yang berbeda pada event tersebut.

8. Hasilnya terbuka di tab browser web baru dengan informasi dari capME!. capME! tab adalah antarmuka web yang memungkinkan Anda melihat transkrip pcap. Teks biru berisi permintaan HTTP yang dikirim dari sumber (SRC). Teks merah adalah tanggapan dari server web tujuan (DST).



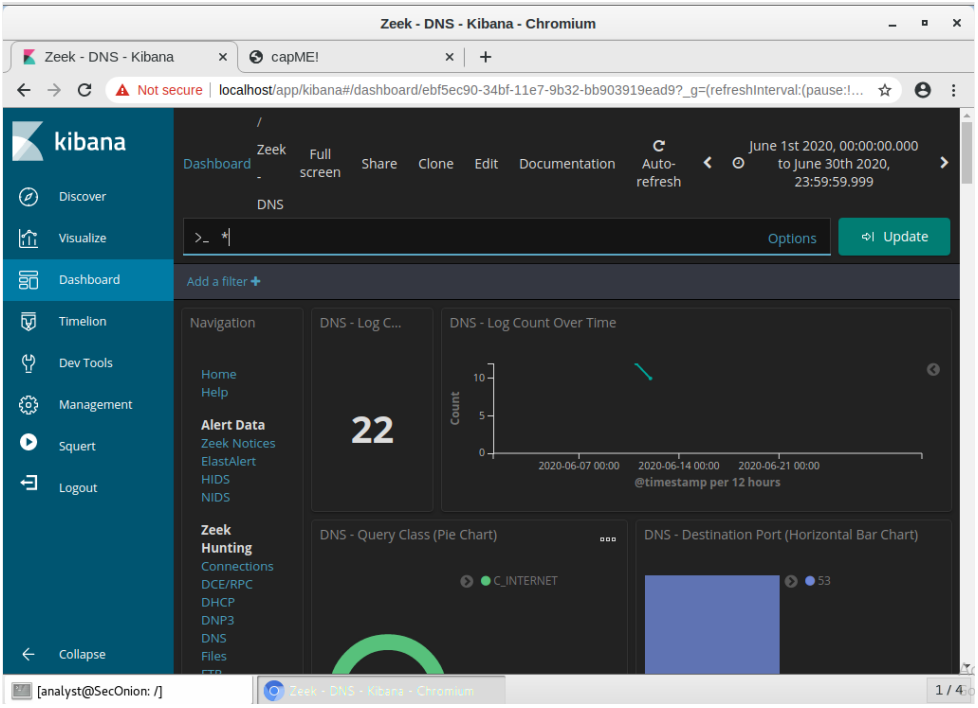
9. Di bagian entri Log, yang ada di awal transkrip, perhatikan bagian username='+union+select+ccid,ccnumber,ccv,expiration,null+from+credit_cards+-- +&password= menunjukkan bahwa seseorang mungkin telah mencoba untuk menyerang browser web menggunakan injeksi SQL untuk melewati otentikasi. Kata kunci, union dan select, adalah perintah yang digunakan dalam mencari informasi dalam database SQL. Jika kotak input pada halaman web tidak terlindungi dengan baik dari input ilegal, pelaku ancaman dapat menyuntikkan string pencarian SQL atau kode lain yang dapat mengakses data yang terdapat dalam database yang ditautkan ke halaman web.



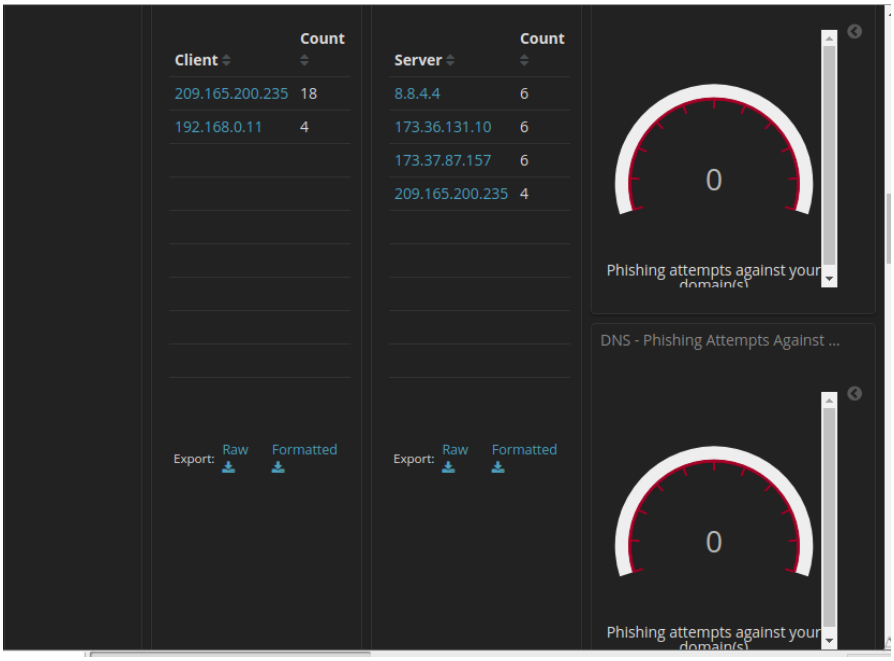
10. Temukan keyword nama pengguna dalam transkrip. Gunakan Ctrl-F untuk membuka kotak pencarian. Gunakan tombol panah bawah di kotak pencarian untuk menelusuri kejadian yang ditemukan

Bagian 4: Analisis DNS exfiltration.

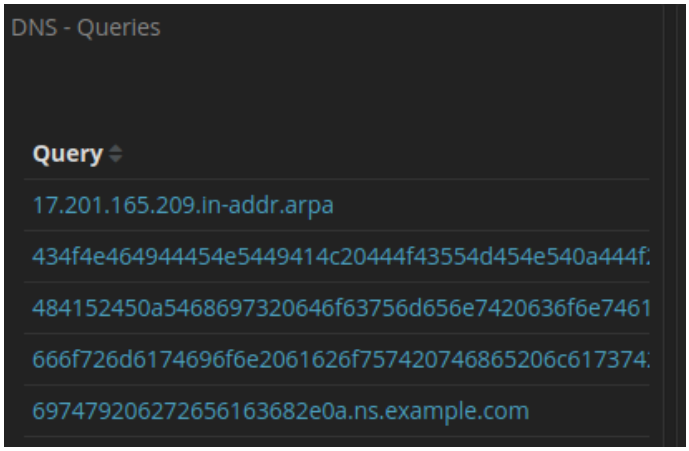
1. Dari bagian atas Dashboard Kibana, hapus semua filter dan istilah pencarian dan klik Beranda di bawah bagian Navigasi Dasbor. Periode Waktu masih harus mencakup Juni 2020.
2. Di area Dashboard yang sama, klik DNS di bagian Zeek Hunting. Perhatikan metrik Jumlah Log DNS dan diagram batang horizontal Port Tujuan.



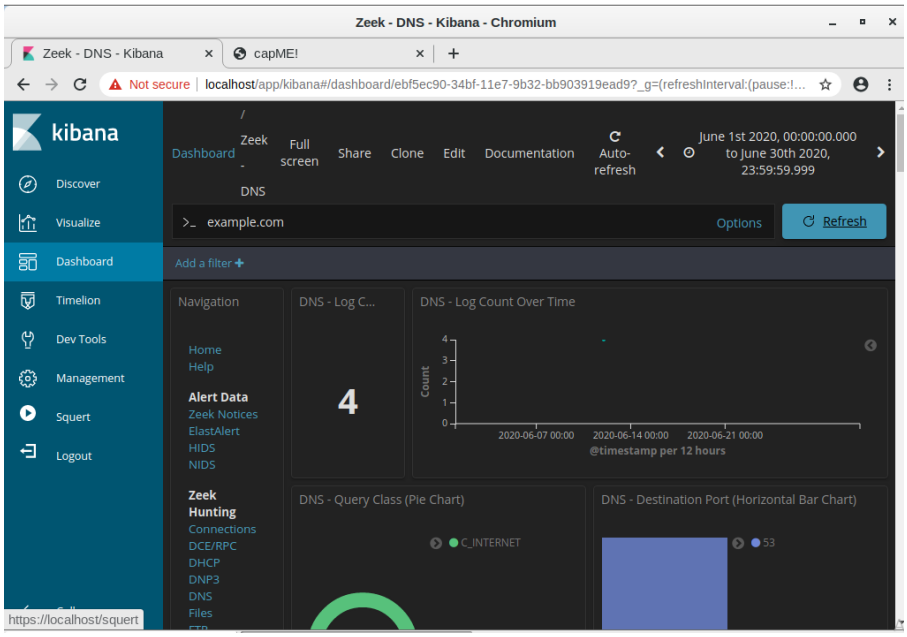
3. Gulir ke bawah jendela. Anda dapat melihat jenis query DNS teratas. Anda mungkin melihat catatan alamat (catatan A), alamat IPv6 catatan Quad A (AAAA), catatan NetBIOS (NB) dan catatan pointer untuk menyelesaikan nama host (PTR). Anda juga dapat melihat kode respons DNS.
4. Dengan Menggulir lebih jauh ke bawah, Anda dapat melihat daftar klien DNS dan Server DNS teratas berdasarkan jumlah permintaan dan respons mereka. Ada juga metrik untuk jumlah upaya DNS Phishing, yang juga dikenal sebagai pharming DNS, spoofing, atau poisoning.



5. Menggulir lebih jauh ke bawah jendela, Anda dapat melihat daftar kueri DNS teratas berdasarkan nama domain. Perhatikan bagaimana beberapa kueri memiliki subdomain yang sangat panjang yang dilampirkan ke ns.example.com. Domain example.com harus diselidiki lebih lanjut.



6. Gulir kembali ke bagian atas jendela dan masukkan example.com di bilah pencarian untuk memfilter example.com dan klik Perbarui. Perhatikan bahwa jumlah entri dalam Hitungan Log lebih kecil karena tampilan sekarang terbatas pada permintaan ke server example.com.



7. Lanjutkan untuk menggulir lebih jauh ke bawah untuk melihat empat entri log unik untuk kueri DNS ke example.com. Perhatikan bagaimana kueri ke subdomain panjang yang mencurigakan yang dilampirkan ke ns.example.com. String panjang angka dan huruf di subdomain terlihat seperti teks yang dikodekan ke dalam heksadesimal (0-9, a-f) daripada nama subdomain yang sah. Klik tautan

Ekspor: Unduh untuk mengunduh kueri ke file eksternal. File CSV diunduh ke folder /home/analyst/Downloads.

8. Di terminal, gunakan perintah xxd untuk memecahkan kode teks dalam file CSV dan menyimpannya ke file bernama secret.txt. Gunakan cat untuk menampilkan konten secret.txt ke konsol.

```
analyst@SecOnion:/$ cd /home/analyst/Downloads
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.
```

PEMBAHASAN:

Pulledpork adalah sebuah sistem yang digunakan untuk mengelola aturan-aturan Snort. Sistem ini mempermudah proses pembaruan aturan Snort. Aturan Snort yang sudah tidak terpakai lagi dapat membuat seluruh sistem tidak berguna. Namun pada praktikum kali ini log file Pulledpork tidak muncul pada output.

OSSEC adalah sebuah sistem yang digunakan untuk menormalisasi dan memusatkan log sistem lokal. Ketika sistem ini diterapkan di seluruh organisasi, seorang analis dapat memiliki gambaran yang jelas mengenai apa yang terjadi di sistem.

Squert adalah sebuah alat visual yang berusaha memberikan konteks tambahan pada peristiwa dengan menggunakan metadata, representasi seri waktu, serta kelompok hasil yang terberat dan logis.

Elasticsearch adalah mesin pencari dan analitik yang terdistribusi. Data disimpan secara sentral untuk memberikan pencarian yang cepat dan memungkinkan penyesuaian halus.

Logstash mengumpulkan data dari berbagai sumber dan mengirimkannya ke ElasticSearch.

Kibana adalah visualisasi data untuk ELK stack yang digunakan untuk memberikan wawasan cepat mengenai data.

E. KESIMPULAN

- Saat menormalkan dan menyiapkan file log secara manual, pastikan untuk memeriksa skrip untuk mendapatkan hasil yang diinginkan.
- Skrip normalisasi yang buruk dapat mendistorsi data dan secara langsung memengaruhi pekerjaan analis.

F. DAFTAR PUSTAKA

Gavin, B. (2018, July 27). *What Is a Log File (and How Do I Open One)?* How-To Geek. Diakses pada March 20, 2023, dari https://www.howtogeek.com/359463/what-is-a-log-file/

SecurityOnion. (n.d.). *Security Onion Solutions*. Security Onion Solutions. Diakses pada March 20, 2023, dari https://securityonionsolutions.com/software/

SecurityOnion. (n.d.). *VMware — Security Onion 2.3 documentation*. Security Onion Documentation. Diakses pada March 20, 2023, dari https://docs.securityonion.net/en/2.3/vmware.html