LAPORAN PRAKTIKUM

KEAMANAN INFORMASI 1

PERTEMUAN 5

IP & Enterprise Services Vullnerability

DISUSUN OLEH

Nama	: Muhamad Alan Dharma Saputro S
NIM	: 21/481348/SV/19761
Hari, Tanggal	: Selasa, 14 Maret 2023
Dosen Pengampu	: Anni Karimatul Fauziyyah, S.Kom., M.Eng.
Kelas	: RI4AA

SARJANA TERAPAN TEKNOLOGI REKAYASA INTERNET

DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA

SEKOLAH VOKASI

UNIVERSITAS GADJAH MADA

YOGYAKARTA

2023

A. Tujuan

1. Investigasi SQL Injection Attack
2. Analisis Pre-Captured Logs dan Traffic Capture
3. Investigasi DNS Data Exfiltration

B. Latar Belakang

Melihat log sangat penting, tetapi juga penting untuk memahami bagaimana transaksi jaringan terjadi pada tingkat paket. Di lab ini, Anda akan menganalisis lalu lintas dalam file pcap yang diambil sebelumnya dan mengekstrak file yang dapat dieksekusi dari file tersebut.

MySQL adalah database populer yang digunakan oleh banyak aplikasi web. Sayangnya, injeksi SQL adalah teknik peretasan web yang umum. Ini adalah teknik injeksi kode di mana penyerang mengeksekusi pernyataan SQL berbahaya untuk mengontrol server database aplikasi web.

Domain Server Name (DNS) adalah direktori nama domain, dan mereka menerjemahkan nama domain menjadi alamat IP. Layanan ini dapat digunakan untuk mengekstrak data.

Personel keamanan siber telah menentukan bahwa eksploitasi telah terjadi, dan data yang berisi PII mungkin telah diekspos ke pelaku ancaman. Di lab ini, Anda akan menggunakan Kibana untuk menyelidiki eksploitasi guna menentukan data yang dieksfiltrasi menggunakan HTTP dan DNS selama serangan.

Karena normalisasi file log itu penting, alat analisis log seringkali menyertakan fitur normalisasi log.Alat yang tidak menyertakan fitur tersebut sering mengandalkan plugin untuk normalisasi dan persiapan log. Tujuan dari plugin ini adalah untuk memungkinkan alat analisis log untuk menormalkan dan menyiapkan file log yang diterima untuk konsumsi alat.

Alat Security Onion bergantung pada sejumlah alat untuk menyediakan layanan analisis log. ELK, Zeek, Snortdan SGUIL bisa dibilang alat yang paling banyak digunakan. ELK (Elasticsearch Logstash dan Kibana) adalah solusi untuk mencapai hal berikut:

- Menormalkan,menyimpan, dan mengindeks log dengan volume dan tarif tak terbatas.
- Menyediakan antarmuka pencarian dan API yang sederhana dan bersih.

- Menyediakan infrastruktur untuk mengingatkan melaporkan,dan berbagi log. Sistem plugin untuk mengambil tindakan dengan log.
- Ada sebagai proyek sumber terbuka dan gratis sepenuhnya.

Zeek (sebelumnya disebut Bro) adalah kerangka kerja yang dirancang untuk menganalisis lalu lintas jaringan secara pasif dan menghasilkan log peristiwa berdasarkan itu. Setelah analisis lalu lintas jaringan, Zeek membuat log yang menjelaskan peristiwa seperti berikut:

- Koneksi jaringan TCP/UDP/ICMP
- Aktivitas DNS
- Aktivitas FTP
- Permintaan dan balasan HTTPS
- Jabat tangan SSL/TLS

Snort dan SGUIL

Snort adalah IDS yang bergantung pada aturan yang telah ditentukan sebelumnya untuk semua kejadian yang berbahaya. Snort melihat ke semua bagian dari paket jaringan (header dan payload), mencari pola yang ditentukan dalam aturannya. Saat, Snort mengambil tindakan yang ditentukan dalam aturan yang sama.

SGUIL menyediakan antarmuka grafis untuk log dan peringatan Snort, memungkinkan analisis keamanan untuk beralih dari SGUIL ke alat lain untuk informasi lebih lanjut. Misalnya, jika paket yang berpotensi berbahaya dikirim ke server web dan Snort memunculkan peringatan, SGUIL akan peringatan itu. Analis kemudian dapat mengklik kanan peringatan itu untuk mencari database ELSA atau Bro untuk pemahaman yang lebih baik tentang acara tersebut

C. Alat dan Bahan

- Mesin Virtual CyberOps Workstation
- Mesin Virtual CyberOps Security Onion

D. Intruksi Kerja

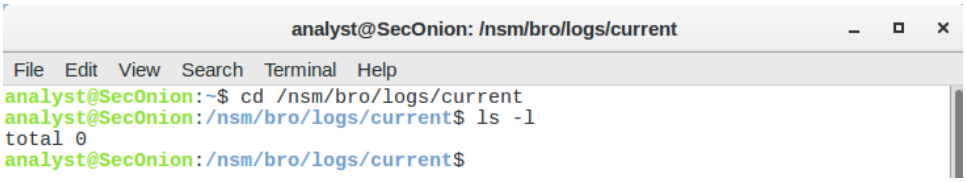
Persiapan Log File pada Security Onion Virtual Machine

i. Security Oion VM1

Luncurkan Security Onion VM dari Dasbor VirtualBox (username: analyst / password: cyberops).

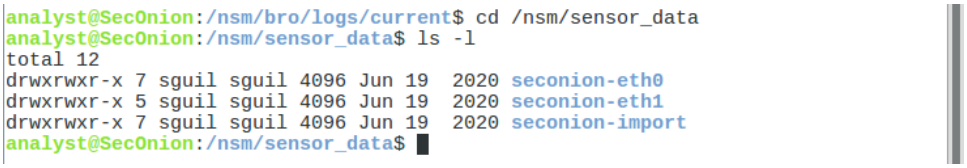
ii. Zeek Logs pada Security Onion

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.
3. Gunakan perintah ls -l untuk melihat file log yang dihasilkan oleh Zeek:

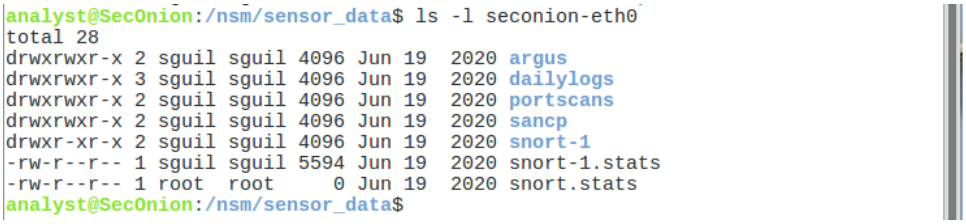


iii. Snort Logs

1. Log snort dapat ditemukan di /nsm/sensor_data/. Ubah direktori sebagai berikut.
2. Gunakan perintah ls -l untuk melihat semua file log yang dihasilkan oleh Snort



3. 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.



iv. Various Logs

1. Sementara direktori /nsm/ menyimpan beberapa file log, file log yang lebih spesifik dapat ditemukan di bawah /var/log/nsm/. Ubah direktori dan gunakan perintah ls untuk melihat semua file log di direktori.

```
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           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
analyst@SecOnion:/var/log/nsm$
```

2. 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
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
daemon.log              fsck              salt
analyst@SecOnion:/var/log$
```

Ekstrak Executable dari PCAP dan Menafsirkan Data HTTP dan DNS untuk Mengisolasi Pelaku Ancaman

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

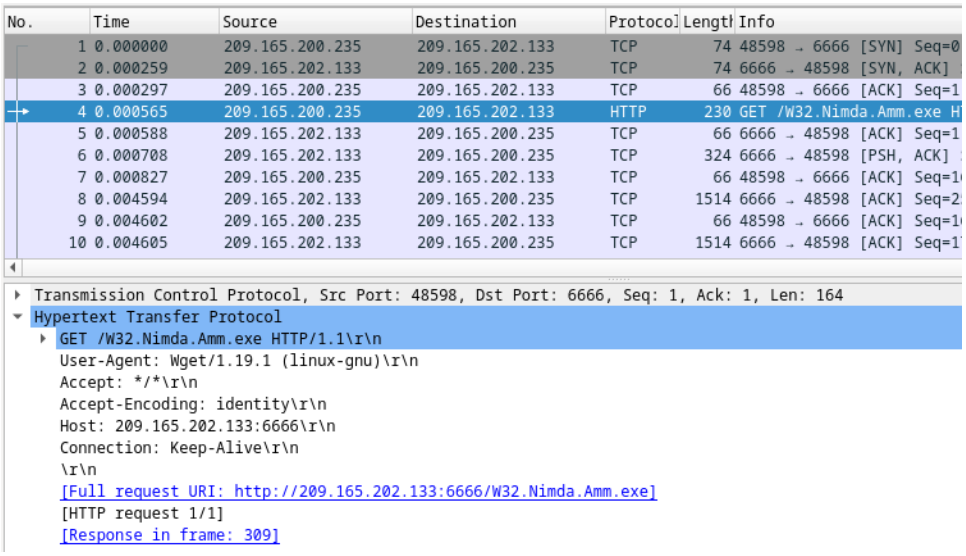
1. Ubah direktori ke folder lab.support.files/pcaps, dan dapatkan daftar file menggunakan perintah ls –l.

```
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]$
```

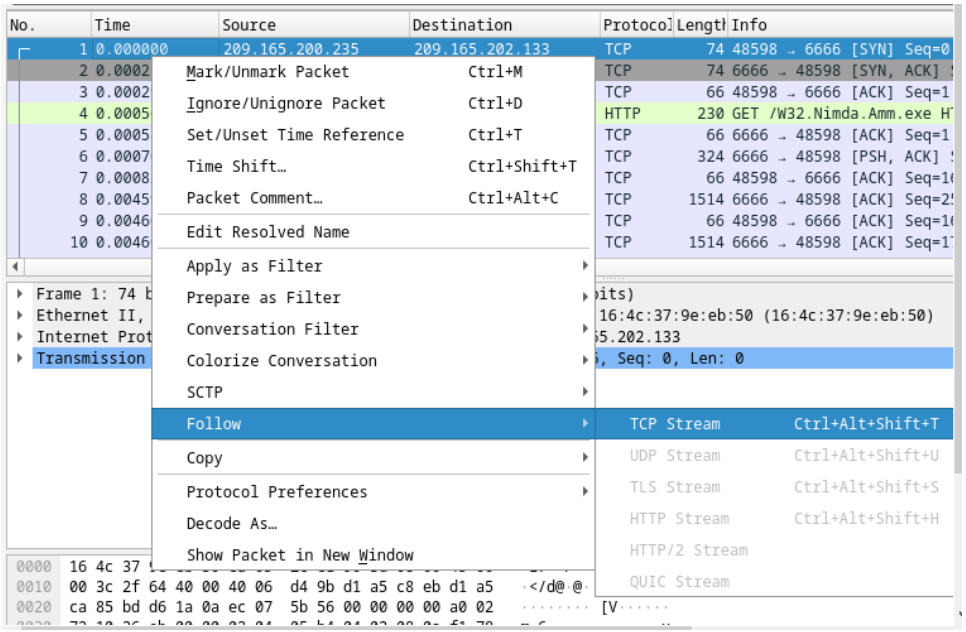
2. Keluarkan perintah di bawah ini untuk membuka file nimda.download.pcap di Wireshark.

```
[analyst@secOps pcaps]$ wireshark nimda.download.pcap &
[1] 527
[analyst@secOps pcaps]$
```

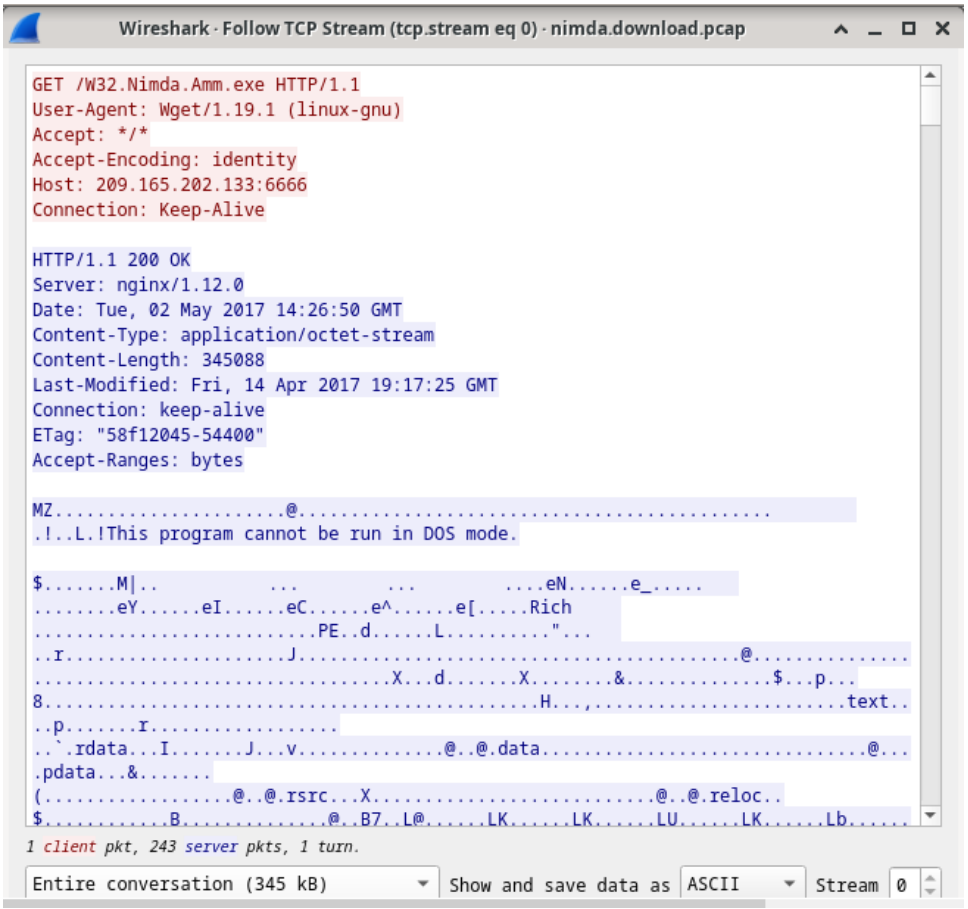
3. File nimda.download.pcap berisi pengambilan paket yang terkait dengan unduhan malware yang dilakukan di lab sebelumnya. Pcap berisi semua paket yang dikirim dan diterima saat tcpdump sedang berjalan. Pilih paket keempat dalam tangkapan dan perluas Protokol Transfer Hypertext untuk ditampilkan seperti yang ditunjukkan di bawah ini.



4. Paket satu sampai tiga adalah jabat tangan TCP. Paket keempat menunjukkan permintaan file malware. Mengonfirmasi apa yang sudah diketahui, permintaan dilakukan melalui HTTP, dikirim sebagai permintaan GET.
5. 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.



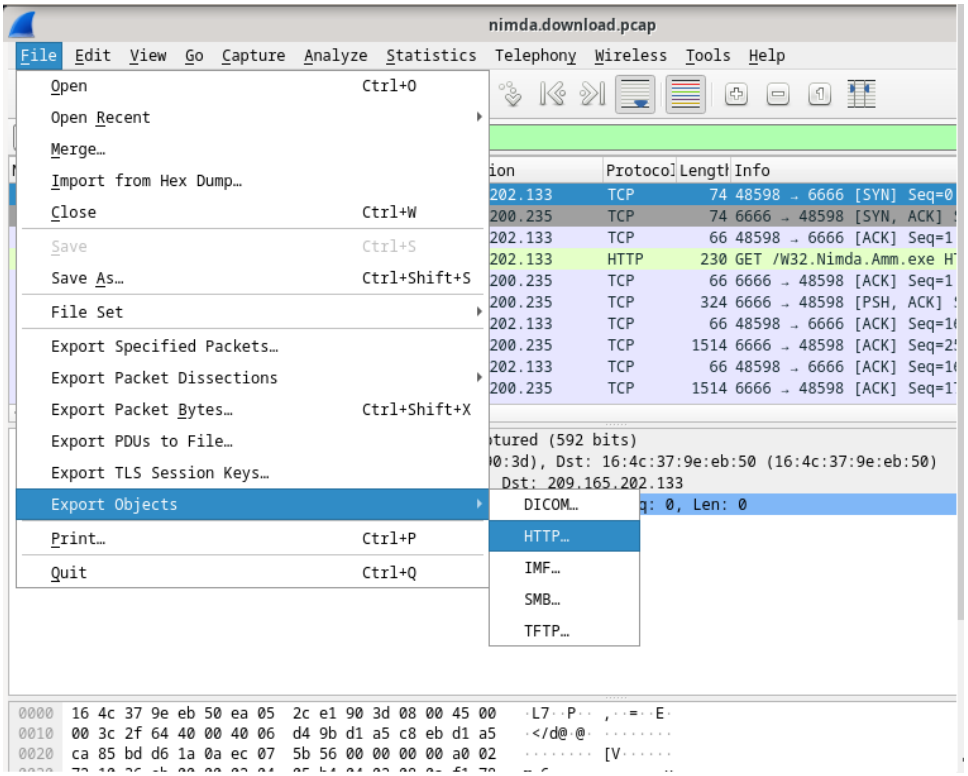
6. Wireshark menampilkan jendela lain yang berisi detail untuk seluruh aliran TCP yang dipilih.



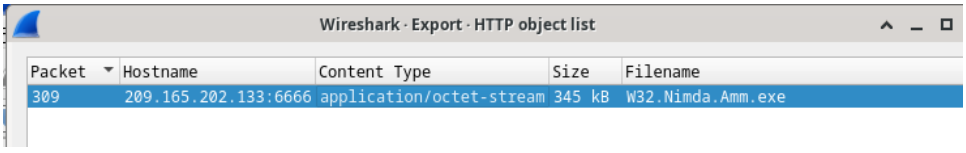
Apa semua simbol yang ditampilkan di jendela Ikuti TCP Stream? Jelaskan.

Part 2 : Extract Files yang di unduh dari PCAP

1. 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.
2. Dengan paket permintaan GET yang dipilih, navigasikan ke File > Export Objects > HTTP, dari menu Wireshark.

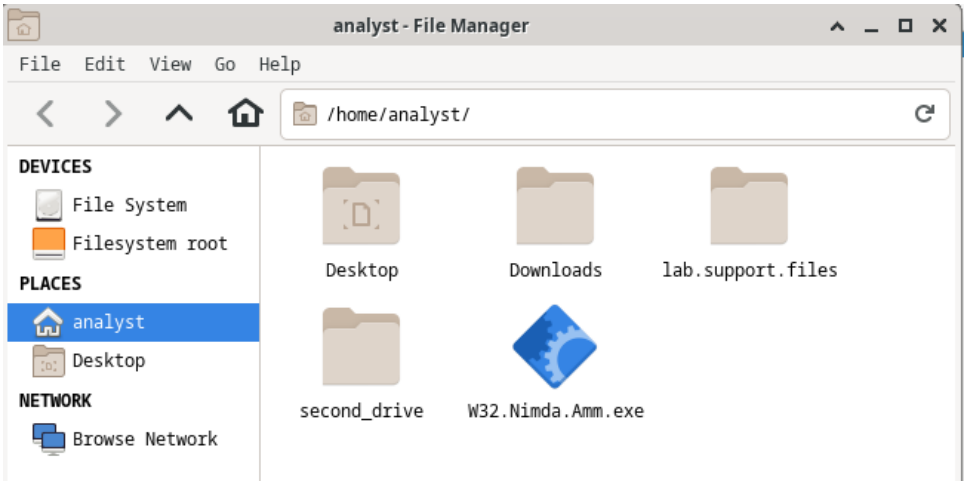


3. Wireshark akan menampilkan semua objek HTTP yang ada dalam aliran TCP yang berisi permintaan GET. Dalam hal ini, hanya file W32.Nimda.Amm.exe yang ada dalam pengambilan. Ini akan memakan waktu beberapa detik sebelum file ditampilkan.



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

4. Di jendela daftar objek HTTP, pilih file W32.Nimda.Amm.exe dan klik Simpan Sebagai di bagian bawah layer.
5. Klik panah kiri hingga Anda melihat tombol Beranda. Klik Beranda lalu klik folder analis (bukan tab analis). Simpan file di sana.



6. 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 356
drwxr-xr-x 2 analyst analyst   4096 May 20  2020 Desktop
drwxr-xr-x 3 analyst analyst   4096 Apr  2  2020 Downloads
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 19 15:16 W32.Nimda.Amm.exe
[analyst@secOps ~]$
```

7. 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
W32.Nimda.Amm.exe: PE32+ executable (console) x86-64, for MS Windows
[analyst@secOps ~]$
```

Part 3 : Investigasi SQL Injection Attack

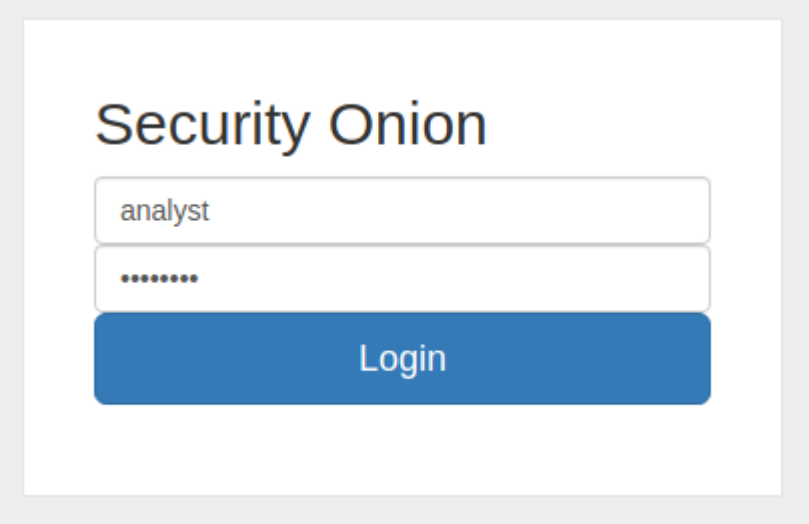
Langkah 1 : Ubah jangka waktu/timeframe

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.

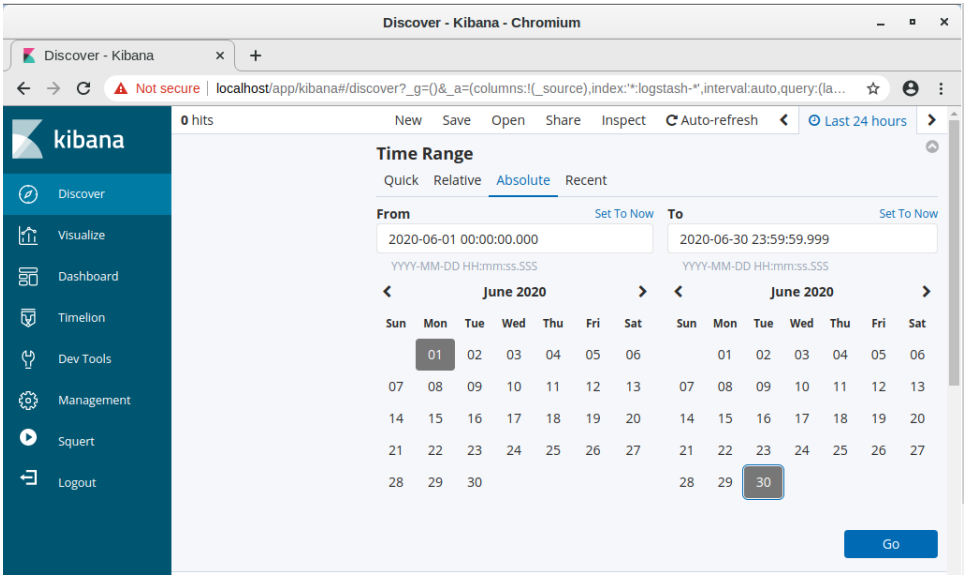
```
analyst@SecOnion:/var/log$ sudo so-status
[sudo] password for analyst:
Status: securityonion
  * sguil server                                                    [  OK  ]
Status: seconion-import
  * pcap_agent (sguil)                                              [  OK  ]
  * snort_agent-1 (sguil)                                           [  OK  ]
  * barnyard2-1 (spooler, unified2 format)                          [  OK  ]
Status: Elastic stack
  * so-elasticsearch                                                [  OK  ]
  * so-logstash
    Logstash API/stats not yet available...still initializing.      [ WARN ]
  * so-kibana                                                       [  OK  ]
  * so-freqserver                                                   [  OK  ]

analyst@SecOnion:/var/log$
```

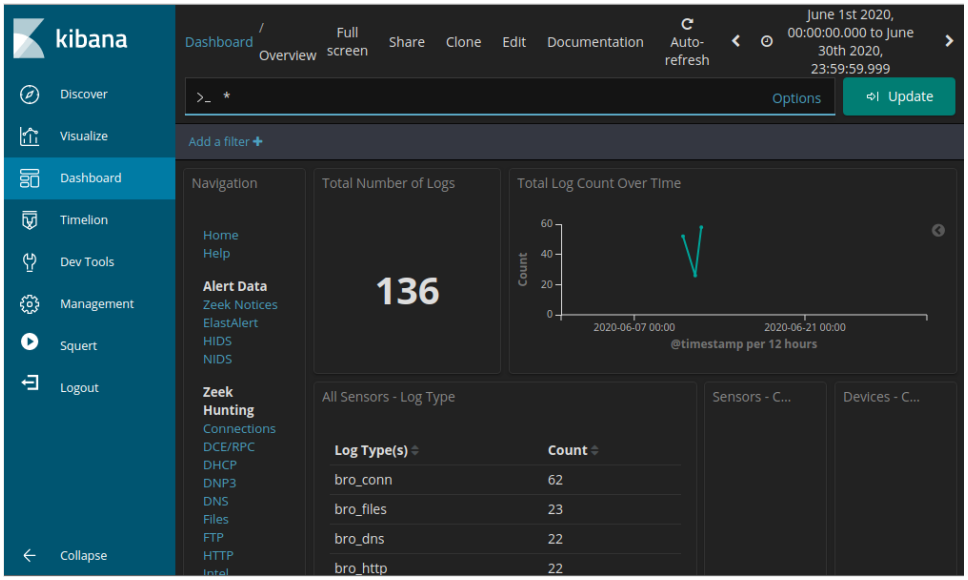
3. Setelah Anda masuk, buka Kibana menggunakan pintasan di Desktop. Masuk dengan username analyst dan password cyberops.



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.

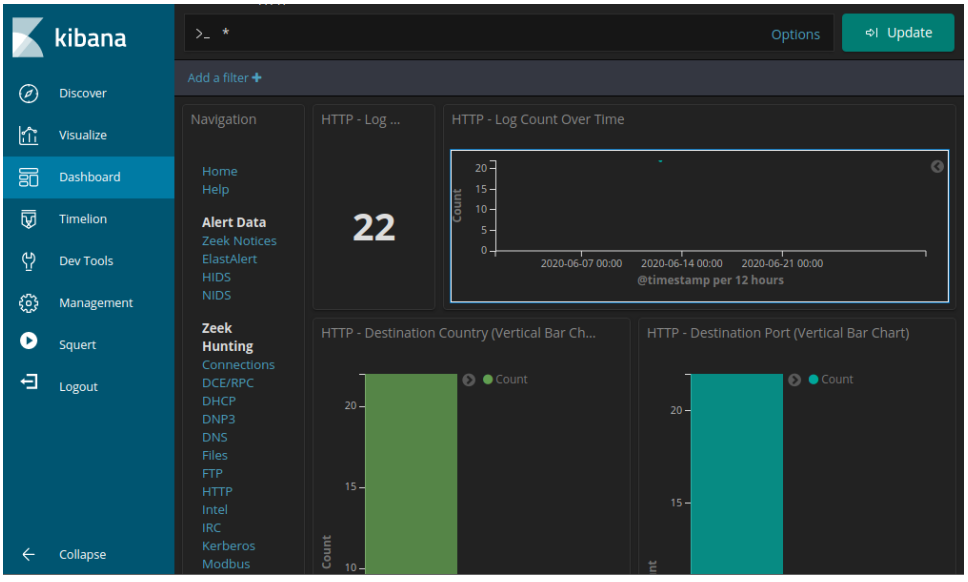


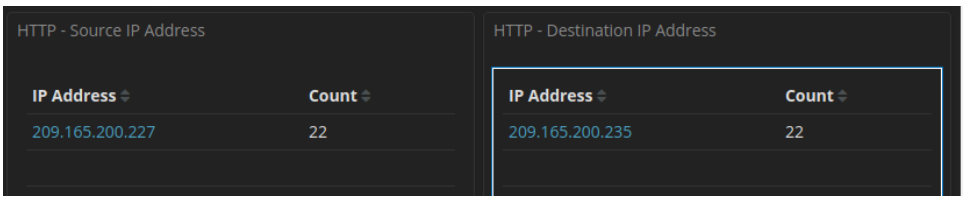
5. Perhatikan jumlah total log untuk seluruh bulan Juni 2020. Dasbor Anda harus serupa dengan yang ditunjukkan pada gambar. Luangkan waktu sejenak untuk menjelajahi informasi yang disediakan oleh antarmuka Kibana.



Langkah 2 : Filter dari HTTP traffic

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.





Apa alamat IP sumber?

209.165.200.227

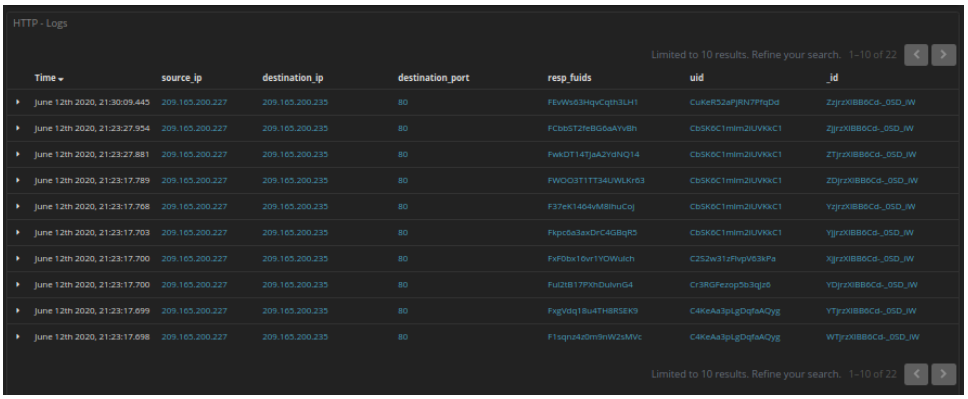
Apa alamat IP tujuan?

209.165.200.235

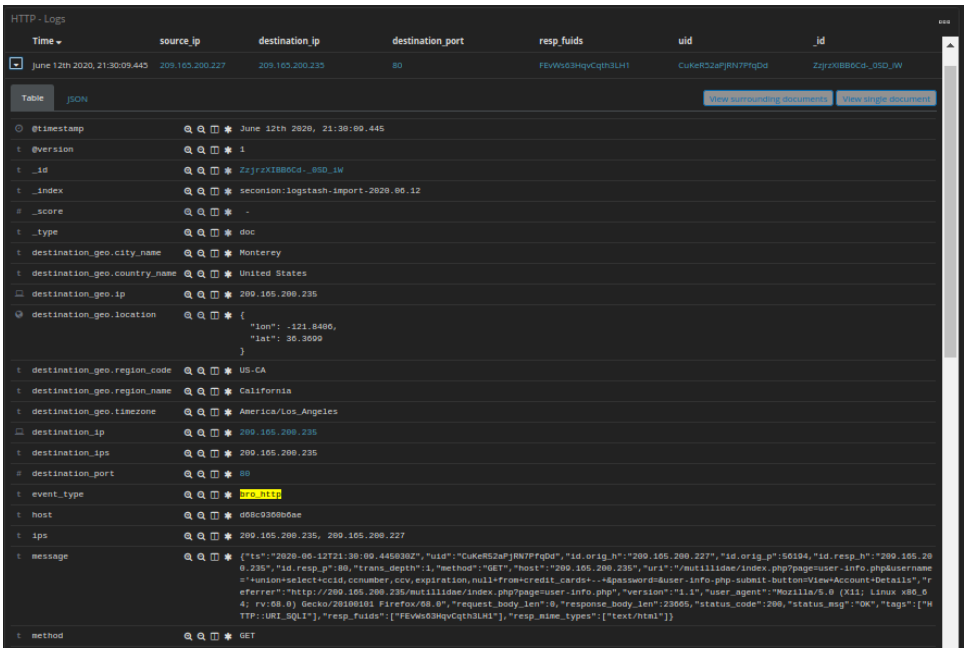
Berapa nomor port tujuan?

80

7. Gulir ke bawah ke Log HTTP. daftar 10 hasil pertama.



8. Klik detail hasil pertama dengan mengklik panah yang ada di sebelah timestamp entri log. Perhatikan informasi yang tersedia.



Apa timestamp dari hasil pertama?

June 12th 2020, 21:30:09.445

Apa jenis event?

bro_http

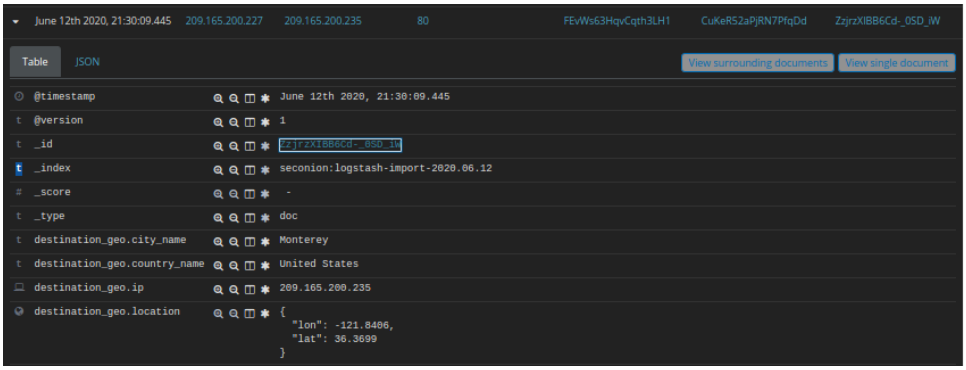
Apa yang termasuk dalam kolom pesan?

Apa pentingnya informasi ini?

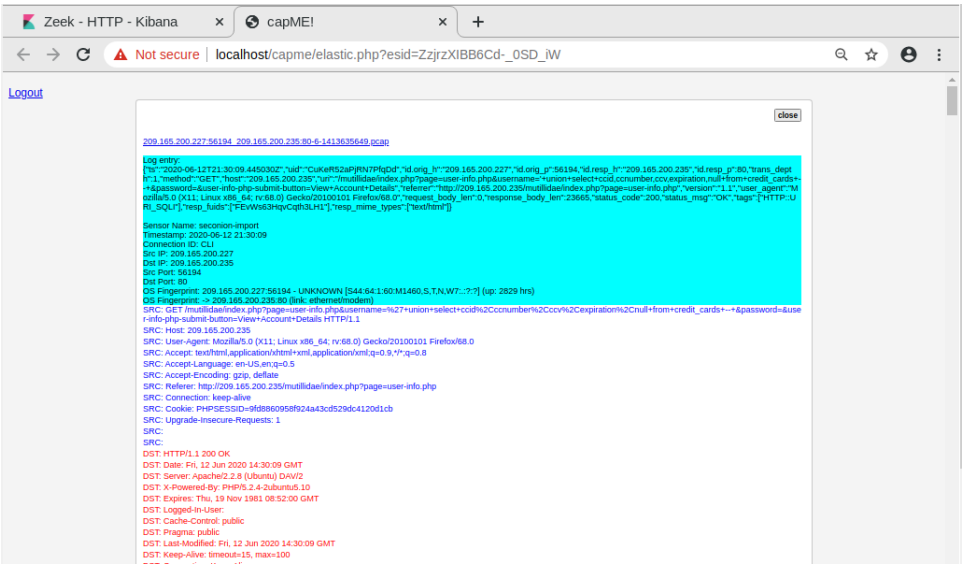
Informasi ini dapat digunakan untuk mengetahui identitas, location, ataupun port dari HTTP log.

Langkah 3 : Review hasil

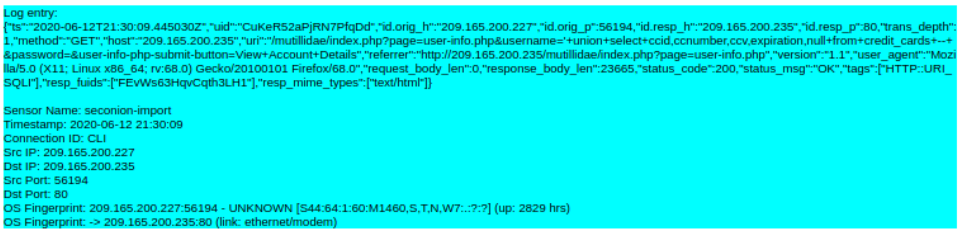
9. Beberapa informasi untuk entri log ditautkan ke alat lain. Klik nilai di bidang alert _id dari entri log untuk mendapatkan tampilan yang berbeda pada event tersebut.



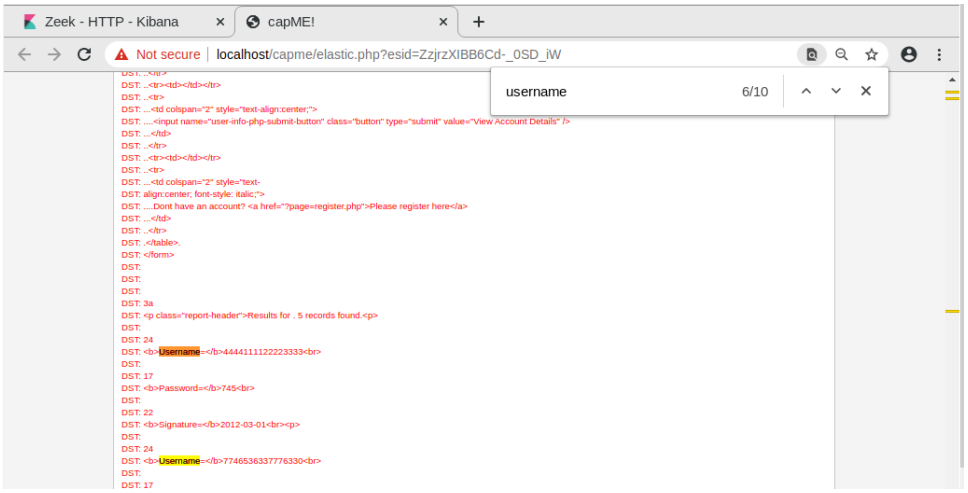
10. Hasilnya terbuka di tab browser web baru dengan informasi dari capME!. capME! tab adalah antarmuka web yang memungkinkan Anda melihat transkrip pcap. Teks biru berisi permintaan HTTP yang dikirim dari sumber (SRC). Teks merah adalah tanggapan dari server web tujuan (DST).



11. 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.



12. 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.



Apa yang Anda lihat nanti dalam transkrip tentang nama pengguna?

Terdapat beberapa username dan password dari source ip pada entry log tersebut

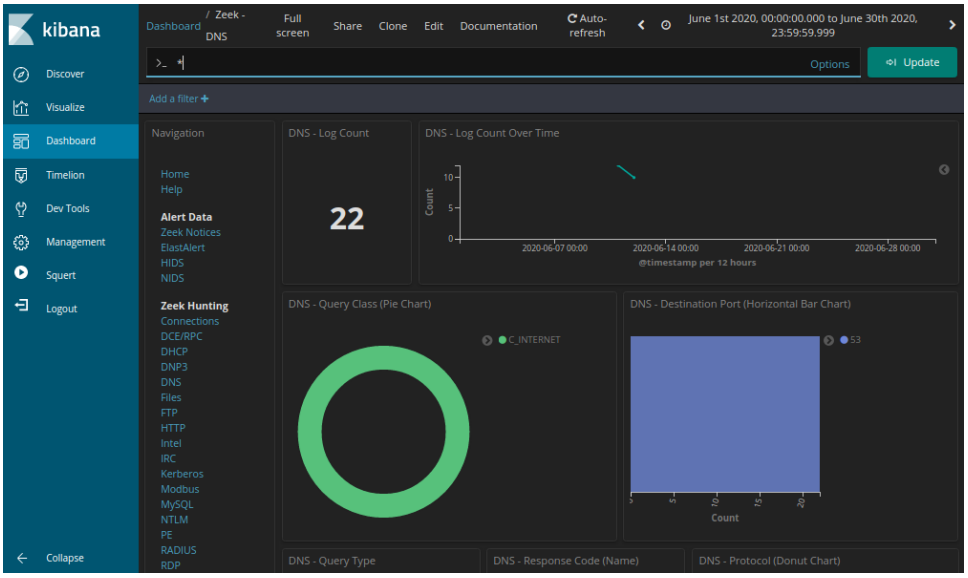
Berikan beberapa contoh username, password, dan signature yang telah dieksfiltrasi.Ty.

Username	Password	Signature
444111122223333	745	2012-03-01
7746536337776330	722	2015-04-01
8242325748474749	461	2016-03-01
7725653200487633	230	2017-06-01
1234567812345678	627	2018-11-01

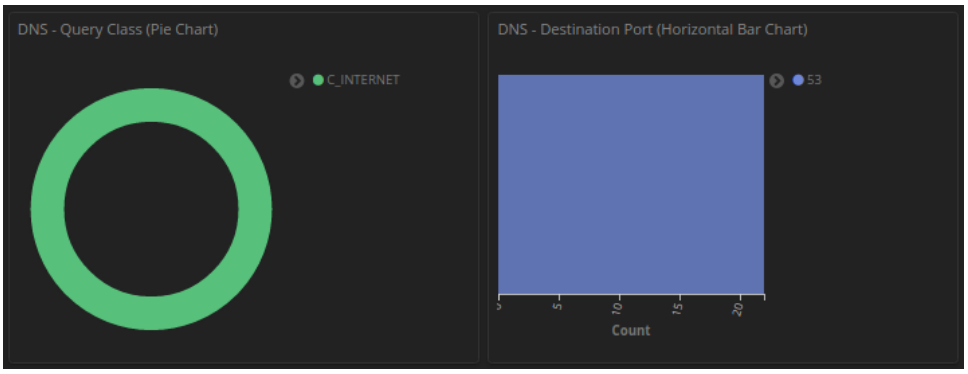
Part 4 : Analisis DNS exfiltration.

Langkah 1 : Filter DNS traffic.

1. Dari bagian atas Dasbor Kibana, hapus semua filter dan istilah pencarian dan klik Beranda di bawah bagian Navigasi Dasbor. Periode Waktu masih harus mencakup Juni 2020.

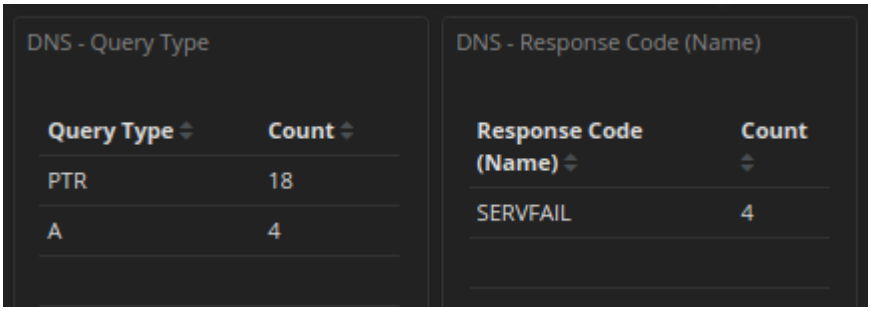


2. Di area Dashboard yang sama, klik DNS di bagian Zeek Hunting. Perhatikan metrik Jumlah Log DNS dan diagram batang horizontal Port Tujuan.



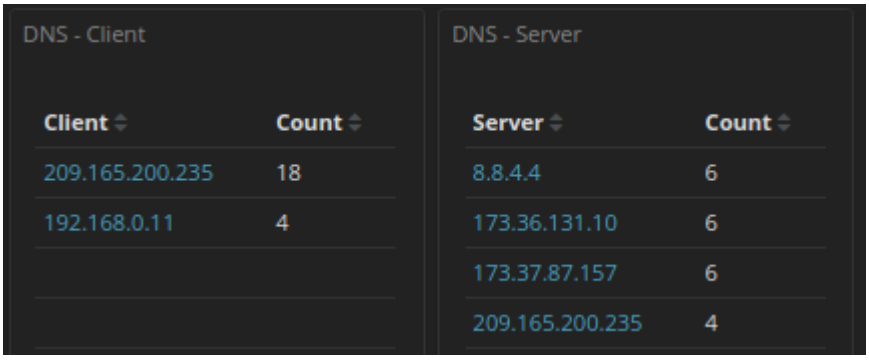
Langkah 2 : Tinjau entri terkait DNS.

3. Gulir ke bawah jendela. Anda dapat melihat jenis kueri 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.

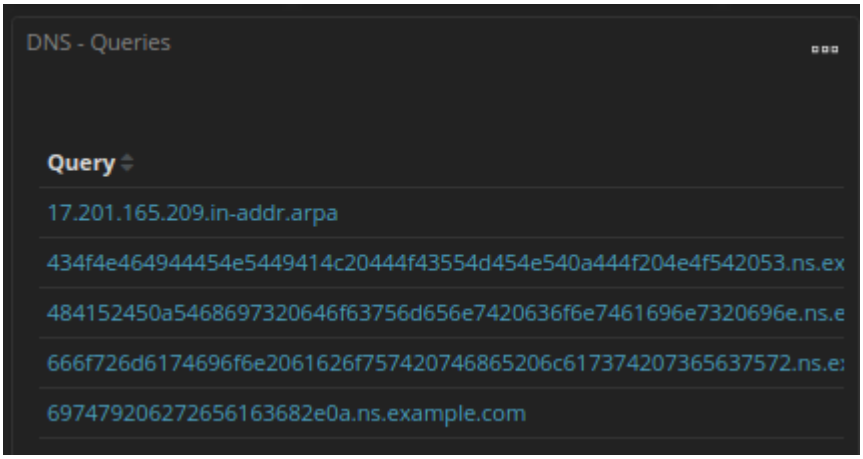


4. Dengan Menggulir lebih jauh ke bawah, Anda dapat melihat daftar klien DNS dan Server DNS teratas berdasarkan jumlah permintaan dan respons mereka. Ada juga

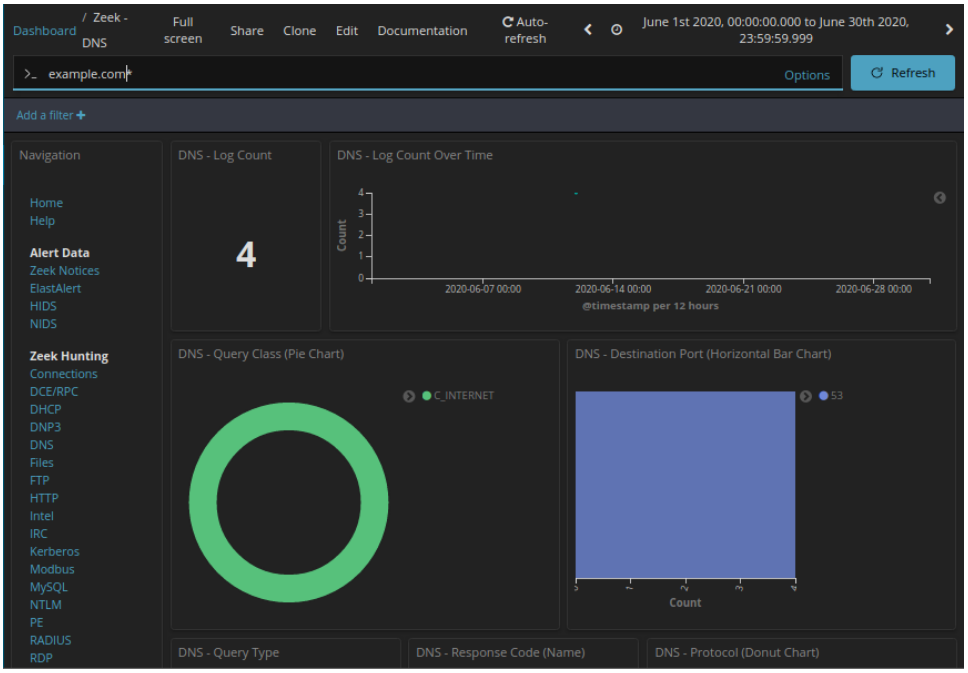
metrik untuk jumlah upaya DNS Phishing, yang juga dikenal sebagai pharming DNS, spoofing, atau poisoning.



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.



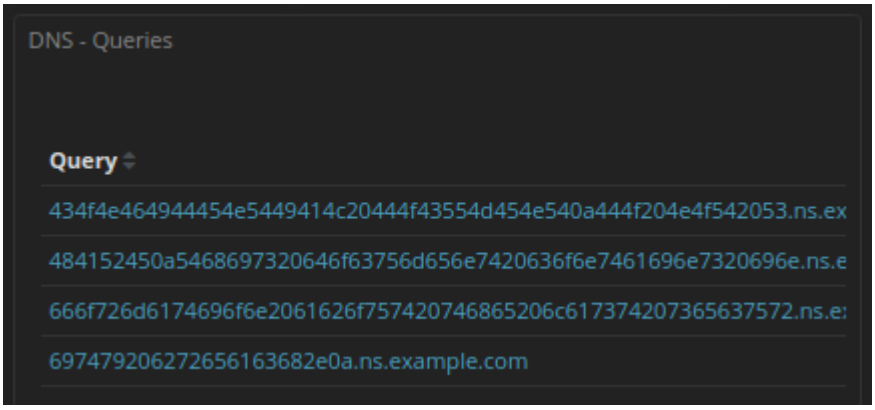
Sebutkan alamat IP klien dan server DNS.

IP Client : 192.168.0.11

Server DNS : 209.165.200.235

Langkah 3 : Tentukan data yang diekstraksi.

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. Arahkan ke folder /home/analyst/Downloads. Buka file menggunakan editor teks, seperti gedit. Edit file dengan menghapus teks di sekitar bagian heksadesimal dari subdomain, hanya menyisakan karakter heksadesimal. Pastikan untuk menghapus

tanda kutip juga. Isi file Anda akan terlihat seperti informasi di bawah ini. Simpan file teks yang diedit dengan nama file asli.

9. 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:~/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$
```

E. Pembahasan

Pada praktikum ini kita melakukan melakukan 2 percobaan yaitu menganalisis File Log dan navigasi SQL Injection pada Kibana menggunakan VM CyberOps Security Onion dan analisis File Log pada Wireshark menggunakan VM CyberOps Workstation. Pertam kita menggunakan VM CyberOps Security Onion, masuk ke terminal lalu masuk ke direktori /nsm/bro/logs/current. Selanjutnya masukkan perintah ls -l untuk melihat file log pada direktori tersebut secara default dari total file. Selajutnya pindah ke direktori /nsm/sensor_data lakukan perintah yang sama, dapat dlihat bahwa terdapat total 12 file log pada diretori tersebut. Masih pada direktori yang sama masukkan perintah ls –l seconion-eth0 untuk melihat file yang dihasilkan interface eth0, terdapat total 28 file. Pindah direktori lagi yaitu pada var/log/nsm, masukkan perintah ls untuk melihat semua file yang terdapat pada direktori tersebut. Keluar satu folder dengan memasukkan perintah cd .. lalu berikan perintah yang sama, dapat dilihat terdapat folder nsm yang dimasukkan peritah sebelumnya.

Percobaan selanjutnya pindah menggunakan VM CyberOps Workstation untuk melihat file log yang ada pada wireshark. Perintah wireshark nimda.download.pcap & digunakan untuk melihat file tersebut dari wireshark. File pcap berisi semua paket yang dikirim dan diterima saat tcpdump sedang berjalan yang dapat dilihat melalui wireshark. Paket satu sampai tiga adalah jabat tangan TCP. Paket keempat menunjukkan permintaan file malware. Mengonfirmasi apa yang sudah diketahui, permintaan dilakukan melalui HTTP, dikirim sebagai permintaan GET. Karena HTTP berjalan di atas TCP, dimungkinkan untuk menggunakan fitur Follow TCP Stream

Wireshark untuk membangun kembali transaksi TCP. Wireshark menampilkan jendela lain yang berisi detail untuk seluruh aliran TCP yang dipilih.

Selanjutnya berganti lagi menggunakan VM CyberOps Security Onion, masuk pada terminal lalu masukkan perintah sudo so-status, perintah sudo berfungsi untuk melakukan tugas yang memerlukan izin admin, lalu perintah so-status berfungsi untuk melihat status dari administrasi tersebut. Lalu masuk pada Kibana yang berfungsi untuk memonitoring dan analisis dari aktifitas data log. Ubah terlebih dahulu time range pada Kibana dengan bulan Juni 2020 untuk melihat serangan injeksi SQL terjadi pada Juni 2020. Yang perlu dilakukan selanjutnya yaitu memfilter traffic dari HTTP. Pada HTTP tersebut terdapat 2 IP yaitu sebagai sumber dan tujuan untuk masing-masingnya adalah 209.165.200.227/27 dan 209.165.200.235/27 dengan port 80. Pada entri log terdapat 10 log, yang kita gunakan yaitu pada log yang pertama dengan timestamp June 12th 2020, 21:30:09.445, jenis event bro_http, informasi ini dapat digunakan untuk mengetahui identitas, location, ataupun port dari HTTP log. Langkah selanjutnya yaitu mereview hasil dengan mengklik nilai di bidang alert_id dari entri log tadi untuk mendapatkan tampilan yang berbeda pada event tersebut. Nantinya akan terbuka di web baru dengan informasi dari capME yang merupakan antarmuka web yang memungkinkan kita melihat transkip pcap. Teks biru berisi permintaan HTTP yang dikirim dari sumber (SRC). Teks merah adalah tanggapan dari server web tujuan (DST). 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. Langkah selanjutnya yaitu melakukan filter DNS. Dapat filihat dari tipe kueri DNS antara lain 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. Kita dapat melihat daftar client DNS dan server DNS teratas berdasarkan jummlah permintaan dan respon mereka. Dikethui alamat IP client yairu 209.165.200.235 dengan jumlah permintaan 18 dan 192.168.0.11 dengan jumlah permintaan 4. Sementara server DNS yaitu 8.8.4.4, 173.36.131.10, 173.37.87.157 dengan masing-masing jumlah permintaan 6 dan 209.165.200.235 jumlah permiintaan 4. Filter lagi menggunakan example.com perhatikan bahwa jumlah entri dalam Hitungan Log lebih kecil karena tampilan sekarang terbatas pada permintaan ke server example.com. IP client yang digunakan yaitu 192.168.0.11 dan server DNS nya yaitu 209.165.200.235. Pada kueri DNS setelah didownlaod Hasil yang disiratkan tentang

permintaan DNS khusus ini menunjukkan bahwa permintaan DNS terpisah, permintaan terkoordinasi yang berisi konten tersembunyi. Dapat dilihat jika memsukkan perintah seperti diatas pada direktori download akan menampilkan output CONFIDENTIAL DOCUMENT ; DO NOT SHARE. Yang membuktikan bahwa file tersebut berifat rahasia. Terdapat kemungkinan yang membuat queri DNS yang disandikan dan DNS dipilih sebagai sarana untuk mengekstrak data bahwa malware membuat ini dengan menelusuri dokumen di host dan menyandikan kontennya dalam heksadesimal dan kemudian membuat kueri DNS yang menggunakan string heksadesimal sebagai subdomain DNS.

F. Kesimpulan

Kesimpulan yang didapatkan dari praktikum kali ini yaitu:

1. Snort adalah IDS yang bergantung pada aturan yang telah ditentukan sebelumnya untuk semua kejadian yang berbahaya.
2. Domain Server Name (DNS) adalah direktori nama domain, dan mereka menerjemahkan nama domain menjadi alamat IP. Layanan ini dapat digunakan untuk mengekstrak data.
3. Saat menormalkan dan menyiapkan file log secara manual, periksa ulang skrip untuk memastikan hasil yang diinginkan tercapai. Skrip normalisasi yang ditulis dengan buruk dapat mengubah data, secara langsung berdampak pada pekerjaan analis.
4. alamat IPv6 catatan Quad A (AAAA), catatan NetBIOS (NB) dan catatan pointer untuk menyelesaikan nama host (PTR). Anda juga dapat melihat kode respons DNS.

G. Daftar Pustaka

F, A. (2021) 4 feature Keren Kibana Untuk Visualisasi Dan Eksplorasi data - halovina, halovina.com. Available at: https://halovina.com/4-feature-keren-kibana-untuk-visualisasi-dan-eksplorasi-data/ (Accessed: March 20, 2023).

C., A. (2023) 40 Perintah Dasar Linux Yang Perlu Anda Tahu, Hostinger Tutorial. Available at: https://www.hostinger.co.id/tutorial/perintah-dasar-linux (Accessed: March 20, 2023).

Maulana, M. (2019) Gunakan perintah ls L seconion eth0 untuk melihat file Yang Dihasilkan Oleh: Course hero, file yang dihasilkan oleh | Course Hero. Available at: https://www.coursehero.com/file/p6tpicfe/Gunakan-perintah-ls-l-seconion-eth0-untuk-melihat-file-yang-dihasilkan-oleh/ (Accessed: March 20, 2023).

Tatang, T. (2017) Web server dengan debian etch 4.0, Academia.edu. Available at: https://www.academia.edu/31510223/WEB_SERVER_DENGAN_DEBIAN_ETCH_4_0 (Accessed: March 20, 2023).