


NASKAH UJIAN

<input type="checkbox"/> UTS	<input checked="" type="checkbox"/> UAS	<input type="checkbox"/> LAIN-LAIN	Ganjil / Genap / Pendek TA : 2023/2024
Program Studi	: Sistem Informasi	NIM	: 6101121004
Kode - Mata Kuliah	: Keamanan Informasi dan Internet		
Nama Dosen	: Erick Dazki, M.Kom & Refgiufi Patria, S.Kom., M.Kom	Nama Mahasiswa	: Qaulan Sakila Usman
Hari / Tanggal	: Rabu, 20 Desember 2023		
Waktu Ujian	: 13.00 sd 15.30	Tanda Tangan	: 
Sifat Ujian	: Buka Buku / Tutup Buku		
Lembar Jawaban	: Ya / Tidak		
Kalkulator	: Ya / Tidak		

Naskah ujian dikumpulkan bersama kertas jawaban ujian !

- Perhatian : 1. Taatilah segala peraturan ujian yang telah ditetapkan
2. Pelanggaran terhadap peraturan ujian dikenakan Sanksi Akademik

Kajilah sebuah kasus berikut ini:

- Seorang hacker dari Nigeria melakukan serangan dari airport Changi (Singapore) terhadap server yang berada di Australia dimana seluruh transaksi e-commerce yang berasal dari Indonesia dengan menggunakan kartu kredit Amerika diubah datanya sehingga menyebabkan bank kustodian dari Swiss yang menyimpan dana transaksi tersebut mengalami gangguan. Pertanyaannya adalah:
 - Hukum negara mana yang dipergunakan/diberlakukan terhadap pelaku kejahatan ini? Apa alasannya?
 - Bukti-bukti apa saja yang dibutuhkan oleh pengadilan agar dapat mengambil keputusan yang adil?
 - Ruang lingkup forensik apa saja yang harus dilakukan untuk menggali fakta yang ada untuk dipergunakan sebagai bukti?
- Lakukanlah Pemantauan Langsung / Real Monitoring pada serangan cyber di 2 situs ini
 - Kaspersky Real Time Attack, lakukan pengamatan pada suatu negara 1 minggu terakhir ditanggal berapa terjadi hit detection tertinggi dari Mail Anti-virus, Web Anti-Virus dan Ransome ware (sertakan SS) kemudian jelaskanlah ancaman No. 1 dari ketiga Deteksi tersebut
 - Livethreatmap.radware.com, lakukan pengamatan pada website tersebut analisislah tipe serangan yang terjadi dan top application violations yang sering di serang serta 5 top attacker dan 5 top attacked country, adakah Indonesia?
- Jelaskan apa fungsi dari Nmap dan Netcat? Berikanlah masing-masing 3 Command utama dari Nmap dan Netcat dan coba lakukan commandnya di virtual lab berita ova?

Diperiksa dan Disetujui, 04-12-2023



0507231343001

JAWABAN SOAL UAS

1. a. Hukum negara mana yang dipergunakan/diberlakukan terhadap pelaku kejahatan ini? Apa alasannya?

Dalam kasus ini, hukum yang dipergunakan adalah hukum dari negara di mana pelaku terlibat dalam serangan tersebut. Namun, karena serangan melibatkan lintas negara, hukum internasional juga mungkin diberlakukan. Berikut adalah beberapa hukum yang mungkin berlaku:

- Hukum Indonesia: Pelaku kejahatan ini mungkin berlaku terhadap Undang-Undang Nomor 11 Tahun 2008 yang menghalangi hacking dan cracking
- Hukum Australia: Serangan ini mungkin berlaku terhadap undang-undang australia yang menghalangi hacking dan pencurian data.
- Hukum Internasional: Serangan ini mungkin berlaku terhadap perjanjian penyuruh dan konvensi antarnegara yang menghalangi hacking dan pencurian data.

Alasannya adalah untuk melindungi kepentingan negara-negara yang terlibat, serta menjaga ketertiban dan keamanan data pribadi.

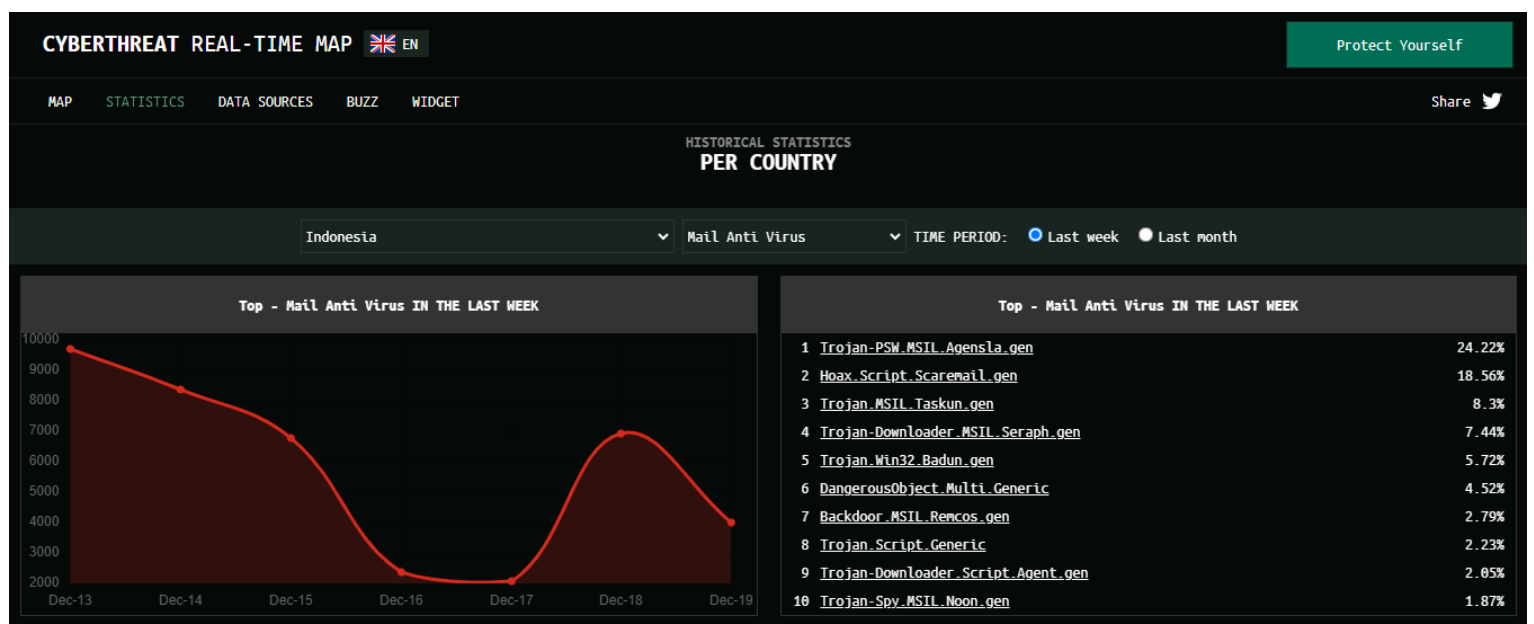
b. Bukti-bukti apa saja yang dibutuhkan oleh pengadilan agar dapat mengambil keputusan yang adil?

- Bukti digital: Daftar perubahan data, transaksi, dan komunikasi yang terjadi sebelum dan setelah serangan.
- Bukti fisik: Perangkat keras komputer, perangkat penyimpanan data, dan jaringan yang terlibat dalam serangan.
- Analisis forensik: Hasil analisis forensik yang menunjukkan perubahan data dan akses yang tidak sah.

c. Ruang lingkup forensik apa saja yang harus dilakukan untuk menggali fakta yang ada untuk dipergunakan sebagai bukti?

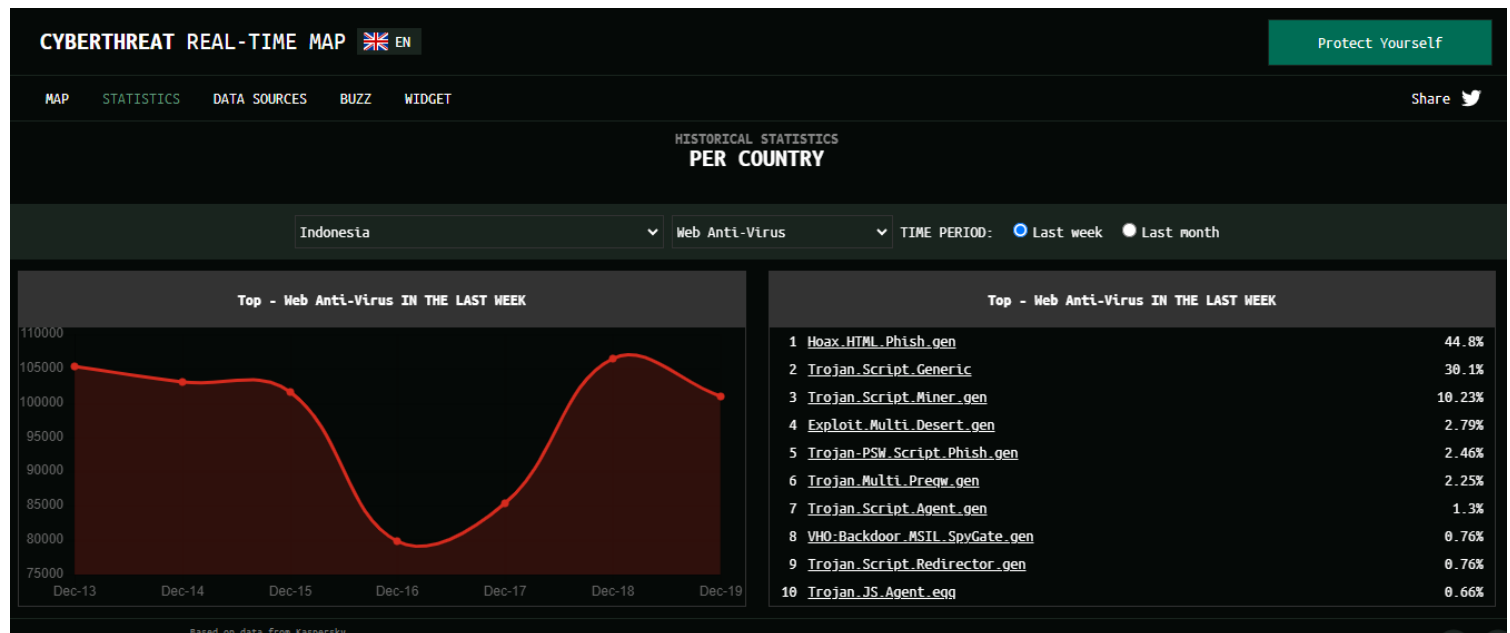
- Mengidentifikasi sumber dan tujuan serangan, serta metode yang digunakan.
- Menganalisis perubahan data, transaksi, dan komunikasi yang terjadi sebelum dan setelah serangan.
- Menganalisis log sistem dan jaringan yang terlibat dalam serangan.
- Mengumpulkan bukti-bukti fisik seperti perangkat keras komputer dan perangkat penyimpanan data yang terlibat dalam serangan.

2. a. Mail Anti-Virus



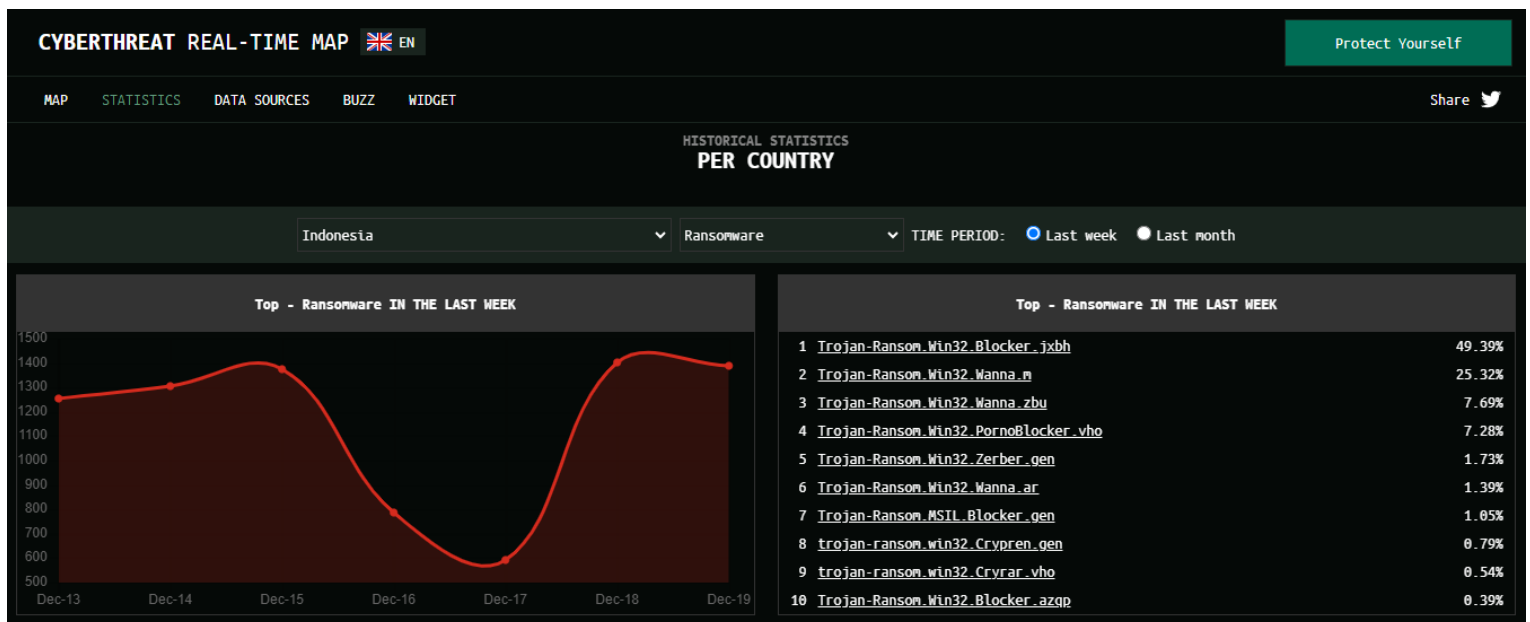
Pada negara Indonesia Hit detection tertinggi dari Mail Anti-Virus terjadi pada tanggal 13 Desember 2023 dengan angka 9688.

Web Anti-Virus



Pada negara Indonesia Hit detection tertinggi dari Web Anti-Virus terjadi pada tanggal 18 Desember dengan angka 106430.

Ransomware



Pada negara Indonesia Hit detection tertinggi dari Ransomware terjadi pada tanggal 18 Desember dengan angka 1401.

- Ancaman No. 1 dari ketiga deteksi tersebut adalah sebagai berikut:
 - Mail Anti-virus: Ancaman utama yang dihadapi oleh Mail Anti-virus adalah malware yang menyebar melalui email, seperti skorang, spam, dan virus yang disertakan melalui email. Malware ini dapat merusak data dalam komputer dan mengganggu kinerja sistem pengguna
 - Web Anti-virus: Ancaman utama yang dihadapi oleh Web Anti-virus adalah malware yang menyebar melalui surfing web, seperti skorang, malware, dan virus yang disertakan melalui situs web yang berkelanjutan atau berbahaya. Virus yang berasal dari website atau spam e-mail dapat merusak data dalam komputer sehingga tidak bisa diakses oleh pengguna.

- c) Ransomware: Ancaman utama yang dihadapi oleh Ransomware adalah virus yang mengenkripsi data di dalam komputer dan meminta tebusan agar data tersebut dapat diakses kembali. Ransomware merupakan ancaman serius yang dapat menyebabkan kerugian finansial dan merusak integritas data pengguna.

Dengan demikian, ancaman No. 1 dari ketiga deteksi tersebut adalah malware yang menyebar melalui email dan web, serta ransomware yang mengenkripsi data pengguna. Melalui penggunaan Mail Anti-virus, Web Anti-virus, dan perlindungan terhadap Ransomware, pengguna dapat mengurangi risiko terkena ancaman-ancaman tersebut dan menjaga keamanan sistem dan data mereka.

b. Setelah melakukan pengamatan dan menganalisa pada website livethreatmap.radware.com diperoleh hasil sebagai berikut :

- Tipe Serangan Yang Terjadi : Web Attackers, Scanners dan Anonymizers.
- Top Application Violations yang sering di serang : Access Violations
- 5 Top Attacker Country : US(68%), UK(10%), UNITED ARAB EMIRATES(10%), GERMANY(7%), CHINA(5%).
- 5 Top Attacked Country : US(35%), INDIA(18%), JAPAN(17%), INDONESIA(17%), HONGKONG(13%).



3. Fungsi dari Nmap dan Netcat:

- a. Nmap (Network Mapper): Nmap adalah alat pemetaan jaringan yang digunakan untuk menemukan host dan layanan di jaringan komputer, sehingga membuat peta jaringan. Nmap juga digunakan untuk memeriksa keamanan jaringan dan memeriksa ketersediaan layanan jaringan.
- b. Netcat: Netcat, juga dikenal sebagai "nc," adalah alat serbaguna dalam Kali Linux yang dapat digunakan untuk melakukan port scanning. Selain itu, Netcat juga dapat berfungsi sebagai alat pengiriman dan penerimaan data melalui jaringan.

- Tiga Command Utama dari Nmap:
 - a. `nmap [target]`: Melakukan pemindaian port pada target yang ditentukan dan menampilkan hasilnya, termasuk port yang terbuka, status port, dan informasi tambahan.
 - b. `nmap -sV [target]`: Melakukan pemindaian port dan mendeteksi versi layanan yang berjalan di port yang terbuka.
 - c. `nmap -A [target]`: Melakukan pemindaian yang lengkap, termasuk deteksi versi, script scanning, dan menunjukkan rute yang dilewati sebuah paket data.
- Tiga Command Utama dari Netcat:
 - a. `nc -z [target] [port]`: Mencoba terhubung ke port yang ditentukan pada target dan menampilkan apakah port tersebut terbuka atau tidak.
 - b. `nc -l -p [port]`: Mendengarkan koneksi pada port yang ditentukan.
 - c. `nc -v [target] [port]`: Membuka koneksi ke target pada port yang ditentukan dan menampilkan informasi verbose tentang proses koneksi.