LAPORAN ANALISIS

MANAJEMEN KEAMANAN INFORMASI

KOMINFO.GO.ID

OLEH :

YOPIS SAPUTRA (09031181520119)

SISTEM INFORMASI

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA 2018

- **Lakukan scanning pada website pemerintahan?**

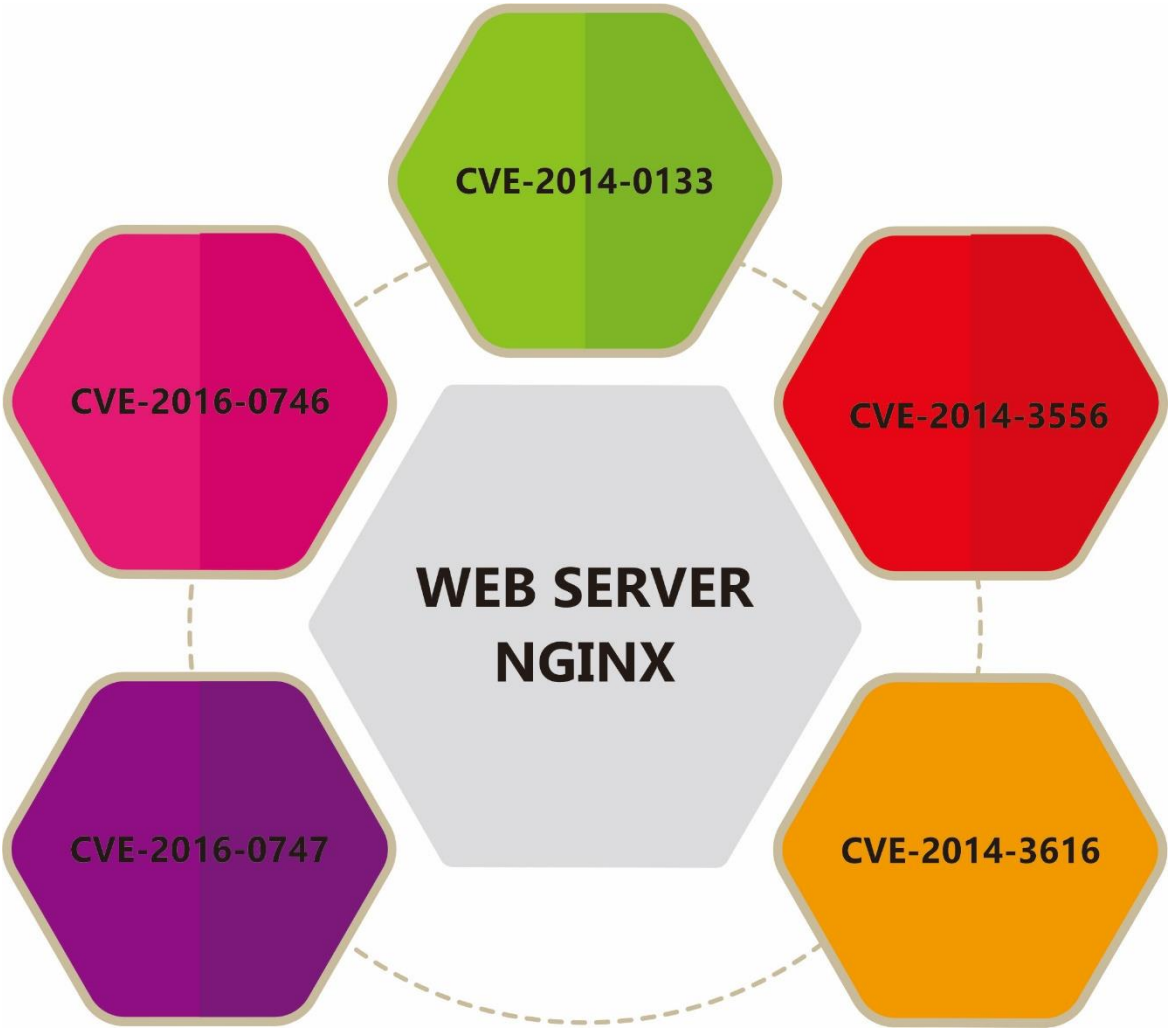
Gambar 1. Hasil Website Kominfo.go.id

Dari gambar di atas saya menganalisis website kominfo.go.id menggunakan netcraft dan di dapatlah beberapa bagian-bagian yang ada di website tersebut seperti :

- Domain : kominfo.go.id
- IP : 202.89.117.69
- Netblock Owner : Kementrian Komunikasi dan Informasi Republik Indonesia
- Namesever : ns1.kominfo.go.id
- DNS admin : postmaster@kominfo.go.id
- Hosting company : Kementrian Komunikasi dan Informasi Republik Indonesia
- OS : linux

- Web server : nginx
- Alamat : Direct Member IDNIC Jl. Medan Merdeka Barat no. 9 Jakarta Pusat, 10110.

Kemudian saya melakukan analisis selanjutnya menggunakan CVE guna melihat kelemahan dari web server dan OS yang digunakan oleh kominfo.go.id, web server yang digunakan yaitu nginx dan OS nya linux, sehingga di dapat sebagai berikut :



Gambar 2. Scanning Web server

1	CVE-2014-0133	Heap berbasis buffer overflow dalam implementasi SPDY di nginx 1.3.15 sebelum 1.4.7 dan 1.5.x sebelum 1.5.12 memungkinkan penyerang remote untuk mengeksekusi kode yang sewenang-wenang melalui permintaan yang dibuat.

2	CVE-2014-3556	Implementasi STARTTLS di surat / ngx_mail_smtp_handler.c di proxy SMTP di nginx 1.5.x dan 1.6.x sebelum 1.6.1 dan 1.7.x sebelum 1.7.4 tidak membatasi pemblokiran I / O dengan benar, yang memungkinkan Penyerang man-in-the-middle untuk memasukkan perintah ke sesi SMTP terenkripsi dengan mengirimkan perintah cleartext yang diproses setelah TLS ada, terkait dengan serangan "perintah injeksi plaintext", sebuah isu serupa pada CVE-2011-0411.
3	CVE-2014-3616	nginx 0.5.6 sampai 1.7.4, saat menggunakan shared ssl_session_cache atau ssl_session_ticket_key yang sama untuk beberapa server, dapat menggunakan kembali sesi SSL cache untuk konteks yang tidak terkait, yang memungkinkan penyerang jarak jauh dengan hak istimewa tertentu untuk melakukan "kebingungan host virtual "serangan.
4	CVE-2016-0747	Resolver di nginx sebelum 1.8.1 dan 1.9.x sebelum 1.9.10 tidak membatasi resolusi CNAME dengan benar, yang memungkinkan penyerang jarak jauh menyebabkan penolakan layanan (konsumsi bahan proses pekerja) melalui vektor yang terkait dengan nama yang sewenang-wenang.
5	CVE-2016-0746	Kerentanan penggunaan setelah penggunaan di penyelesai di nginx sebelum 1.8.1 dan 1.9.x sebelum 1.9.10 memungkinkan penyerang jarak jauh menyebabkan penyangkalan layanan (proses pekerja mogok) atau kemungkinan dampak lain yang tidak ditentukan melalui respon DNS yang dibuat terkait dengan pemrosesan respons CNAME, dan lain-lain.