LAPORAN

TUGAS MANAJEMEN KEAMANAN INFORMASI

OLEH :

YOPIS SAPUTRA (09031181520119)

SISTEM INFORMASI

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA 2018

- Lakukan scanning network dan scanning system?

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

- Domain : detik.com
- IP : 203.190.242.211
- Netblock Owner : PT. Detik ini juga
- Namesever : ns.detik.com
- DNS admin : sysnet@detik.com
- Hosting company : Detikcom
- OS : linux
- Web server : nginx/id25
- Alamat : Lantai 2 Jl. Warung Buncit Raya No.75 Jakarta Selatan 12740.

Kemudian saya melakukan analisis selanjutnya menggunakan CVE guna melihat kelemahan dari web server dan OS yang digunakan oleh detik.com, sebagai berikut :

- Di Apache Allura sebelum 1.8.0, penyerang yang tidak diautentikasi dapat mengambil file yang sewenang-wenang melalui aplikasi web Allura. Beberapa webserver yang digunakan dengan Allura, seperti Nginx, Apache / mod_wsgi atau paster dapat mencegah serangan dari berhasil. Yang lainnya, seperti gunicorn tidak mencegahnya dan membiarkan Allura rentan.
- Versi Nginx sejak 0.5.6 sampai dengan dan termasuk 1.13.2 rentan terhadap kerentanan overflow integer dalam modul filter rentang nginx yang mengakibatkan bocornya informasi sensitif yang dipicu oleh permintaan yang dibuat secara khusus.
- os / unix / ngx_files.c di nginx sebelum 1.10.1 dan 1.11.x sebelum 1.11.1 memungkinkan penyerang jarak jauh menyebabkan penolakan layanan (NULL pointer dereference dan proses pekerja crash) melalui permintaan yang dibuat, melibatkan menulis sebuah permintaan klien ke file sementara.
- 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 resolusi.
- 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 resolusi, Dan lain-lain.

Hasil dari netcraft

- **Gambar 1**

Network

Site	http://www.detik.com	**Netblock Owner**	PT. Detik Ini Juga
Domain	detik.com	**Nameserver**	ns.detik.com
IP address	103.49.221.211	**DNS admin**	sysnet@detik.com
IPv6 address	*Not Present*	**Reverse DNS**	*unknown*
Domain registrar	networksolutions.com	**Nameserver organisation**	whois.networksolutions.com
Organisation	Aldevco Octagon Building lt 2, Jakarta, 12740, IN	**Hosting company**	Detikcom
Top Level Domain	Commercial entities (.com)	**DNS Security Extensions**	*unknown*
Hosting country	ID		

- **Gambar 2**

Hosting History

Netblock owner	IP address	OS	Web server	Last seen Refresh
PT. Detik Ini Juga Internet Service Provider Aldevco Octagon Building - Lantai 2 Jl. Warung Buncit Raya No.75 Jakarta Selatan 12740	203.190.242.211	Linux	nginx/id25	5-Mar-2018
PT. Detik Ini Juga Internet Service Provider Aldevco Octagon Building - Lantai 2 Jl. Warung Buncit Raya No.75 Jakarta Selatan 12740	203.190.242.211	Linux	nginx/id29	28-Feb-2018
PT. Detik Ini Juga Internet Service Provider Aldevco Octagon Building - Lantai 2 Jl. Warung Buncit Raya No.75 Jakarta Selatan 12740	203.190.242.211	Linux	nginx/id28	20-Feb-2018
PT. Detik Ini Juga Internet Service Provider Aldevco Octagon Building - Lantai 2 Jl. Warung Buncit Raya No.75 Jakarta Selatan 12740	203.190.242.211	Linux	nginx/id27	18-Dec-2017
PT. Detik Ini Juga Internet Service Provider Aldevco Octagon Building - Lantai 2 Jl. Warung Buncit Raya No.75 Jakarta Selatan 12740	203.190.242.211	Linux	nginx/id25	30-Oct-2017
PT. Detik Ini Juga Internet Service Provider Aldevco Octagon Building - Lantai 2 Jl. Warung Buncit Raya No.75 Jakarta Selatan 12740	203.190.242.211	Linux	nginx/id12	26-Sep-2017
PT. Detik Ini Juga Internet Service Provider Aldevco Octagon Building - Lantai 2 Jl. Warung Buncit Raya No.75 Jakarta Selatan 12740	203.190.242.211	Linux	nginx/id17	13-Sep-2017
PT. Detik Ini Juga Internet Service Provider Aldevco Octagon Building - Lantai 2 Jl. Warung Buncit Raya No.75 Jakarta Selatan 12740	203.190.242.211	Linux	nginx/id14	29-Aug-2017
PT. Detik Ini Juga Internet Service Provider Aldevco Octagon Building - Lantai 2 Jl. Warung Buncit Raya No.75 Jakarta Selatan 12740	203.190.242.211	Linux	nginx/1.10.3	16-Aug-2017
PT. Detik Ini Juga Internet Service Provider Aldevco Octagon Building - Lantai 2 Jl. Warung Buncit Raya No.75 Jakarta Selatan 12740	203.190.242.211	Linux	nginx/id23	26-Jul-2017