**MANAJEMEN KEAMANAN INFORMASI  
“Scanning & Vulnerbility pada Website ”**



Oleh :

1. DERDI KURNIAWAN (09031181520026)

MATA KULIAH : Manajemen Keamanan Informasi  
Target Website : www.bagas31.com

**SISTEM INFORMASI FAKULTAS ILMU KOMPUTER**

**UNIVERSITAS SRIWIJAYA**

**2018**

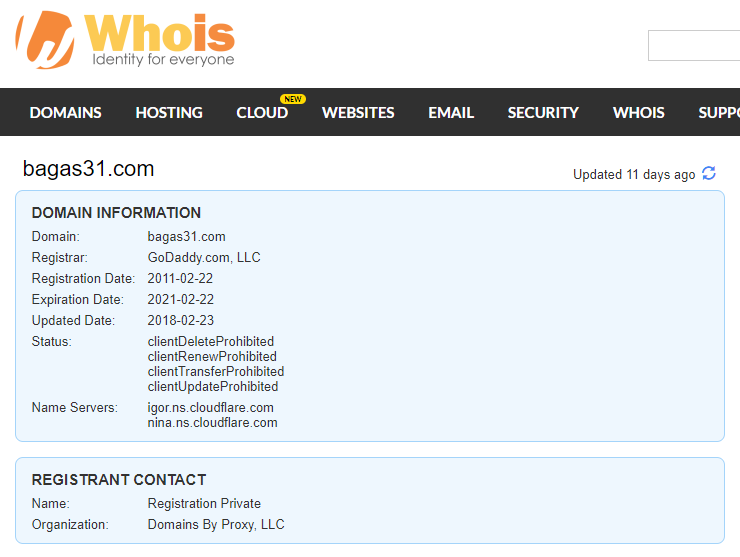
1. **LATAR BELAKANG**

Keamanan data merupakan hal yang sangat penting dalam menjaga kerahasiaan informasi terutama yang berisi informasi sensitif yang hanya boleh diketahui isinya oleh pihak yang berhak saja, apalagi jika website tersebut sering mengalami bug-bug yang tidak diinginkan, hal tersebut menjadi rentan untuk para hacker yang mencari celah dari sebuah website . Ketika para hacker telah memliki hak akses maka informasi yang ada pada situs tersebut kemungkinan besar bisa diretas oleh mereka.

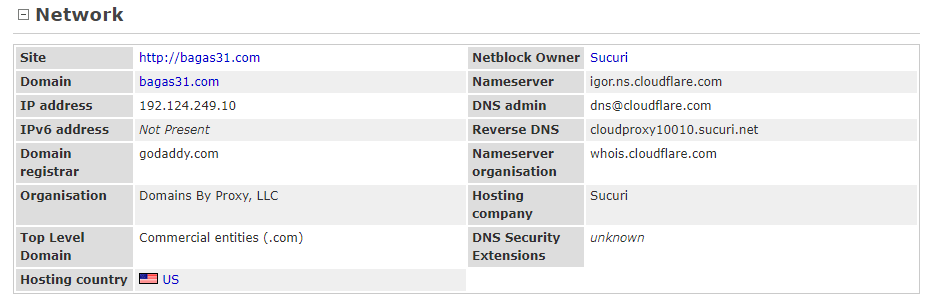
Pada penulisan ini saya mealukan scanning di bagas31.com. ini terjadi karena kepudulian saya terhadap website yang kurang memperhatikan keamanan datanya yang dimulai dari banyaknya masalah dari servernya. Dengan hal ini mungkin bisa sebagai solusi yang dihadapi saat ini.

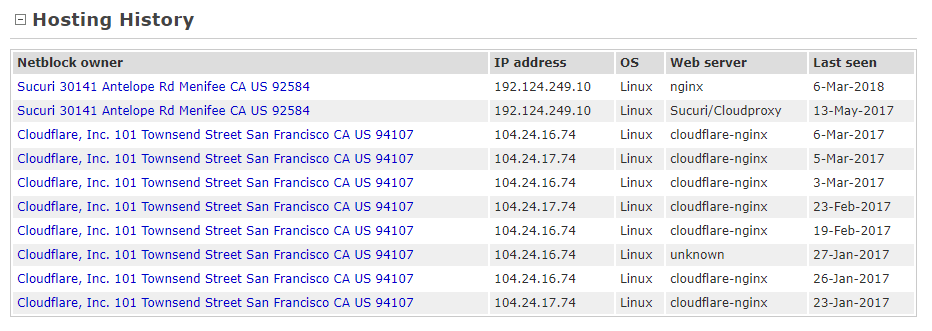
1. Data Collection

Proses pengumpulan data formal diperlukan untuk memastikan bahwa data yang dikumpulkan dapat didefinisikan dengan jelas dan akurat dan berdasarkan argumen dalam temuan yang valid. Proses ini menyediakan informasi dasar untuk mengukur dan menargetkan hal apa yang ingin diperbaiki. Dengan menggunkan tool who is, netcraft dan nmap.

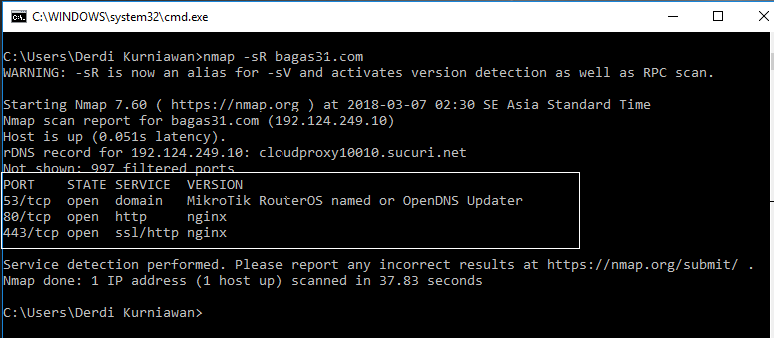
* Who is

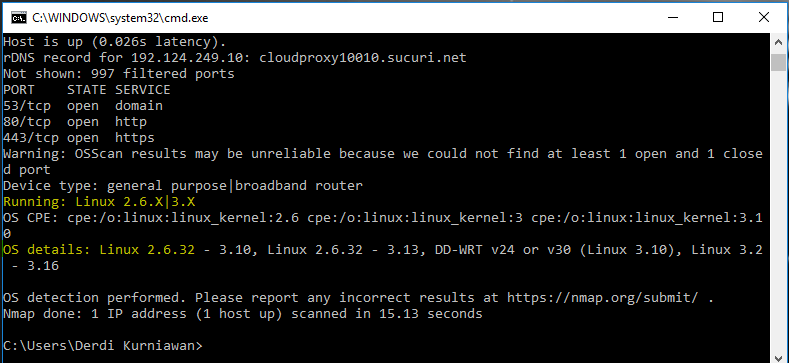
Gambar 1 ( Hasil Scanning menggunkan whois.com )

* Netcraft



Gambar 2 ( Hasil Scanning menggunkan netcraft.com )

* Nmap



Gambar 3 ( Hasil Scanning menggunkan tool nmap )

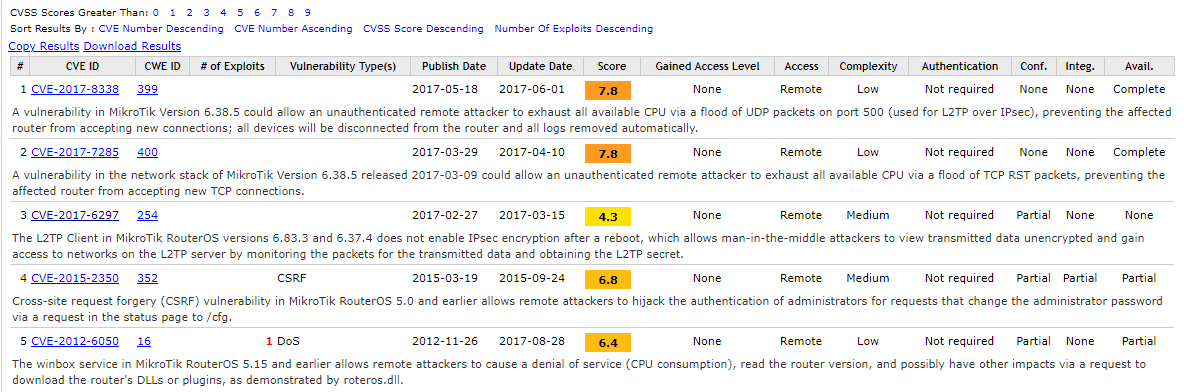
Hasil dari data collection sebagai berikut :

|  |  |
| --- | --- |
| Data Collection | |
| Domain | bagas31.com |
| IP address | 192.124.249.10 |
| Registrar URL | <http://www.godaddy.com> |
| Registration Date | 2011-02-22 |
| Expiration Date | 2021-02-23 |
| Updated Date | 2018-02-23 |
| Registrant | Scottsdale |
| Registrant Province | Arizona |
| Registrant Country | US |
| OS Running | Linux 2.6.32 |
| Name Servers | igor.ns.cloudflare.com |
| Web Server | Nginx |
| Port | 53/tcp, State = Open , Service = domain  80/tcp, State = Open, Service = http  443/tcp, State = Open, Service = https |

1. Vulnerbility

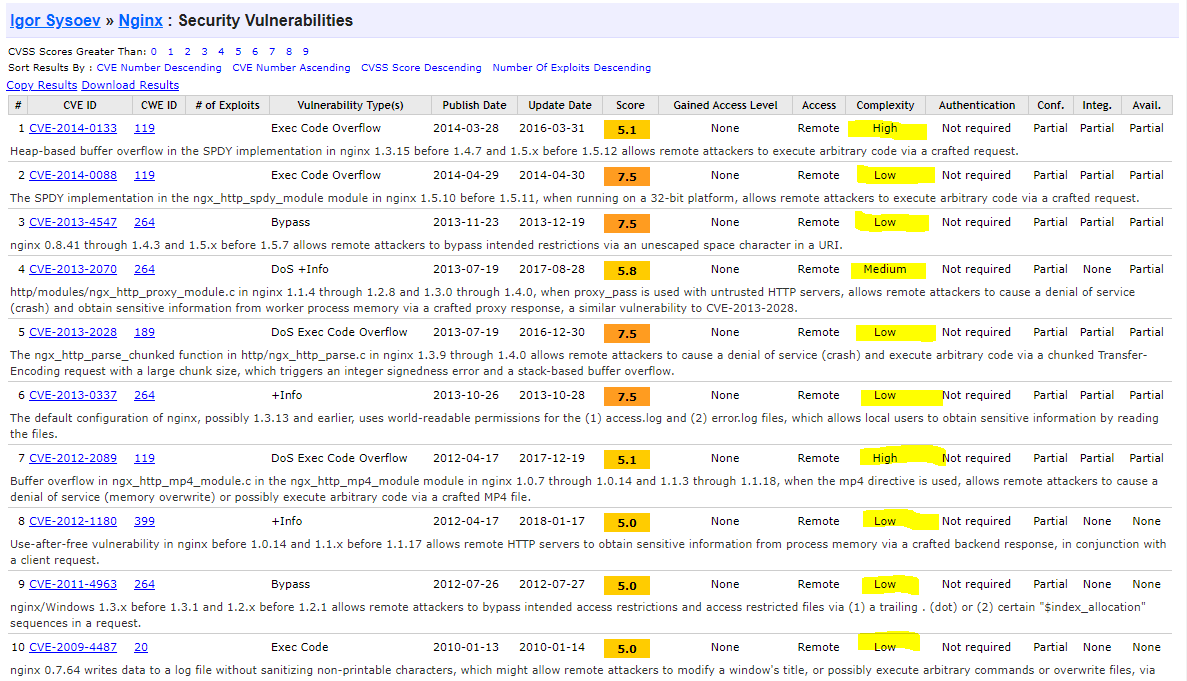
Berikut hasil Vulnerbility dari hasil Data Collection dengan bantuan **cvedetails.com**

* Aplikasi Running beserta Holenya
* Pada Port 53 menggunkan aplikasi OpenDomain dengan versi MikroTik RouterOS named or OpenDNS Updater

Pada port tesebut aplikasi yang running yaitu OpenDomain, dimana apliksi tersebut setelah dianalisi terdapat celah dimana para hecker dapat masuk dengan memanfaatkan celah dari tersebut. Celah tersebut sebagai berikut:

Gambar 4 ( cvedetails.com. Hole pada port 53 )

* Pada Port 80 dan 433

Pada port tesebut aplikasi yang running yaitu Nginx, dimana apliksi tersebut setelah dianalisi terdapat celah dimana para hecker dapat masuk dengan memanfaatkan celah dari tersebut. Celah tersebut sebagai berikut:

Gambar 5 ( cvedetails.com. Hole pada port 80 dan 433 )

1. Kesimpulan

Pada analisa dan hasil tersebut dapat kita simpulkan bahwa:

* Target tersebut memiliki 3 port.
* Target tersebut menggunkan OS Linuk 2.6.32
* Pada port 80 dan 433 terdapat 10 serangan dengan complexity 7 Low, 2 Hight dan 1 Medium
* Pada port 53 terdapat 5 seranagn dengan complexity 3 Low dan 2 Hight
* Serangan terjadi salah satunya diakibatkan kurang updatenya webserver yang digunkan

1. Referensi

* whois.com
* netcraft.com
* Nmap
* CveDetail.com
* CVE