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



Oleh :

1. DERDI KURNIAWAN (09031181520026)

MATA KULIAH : Manajemen Keamanan Informasi  
Target Website : www. jatengprov.go.id

**SISTEM INFORMASI FAKULTAS ILMU KOMPUTER**

**UNIVERSITAS SRIWIJAYA**

**2018**

1. **LATAR BELAKANG**

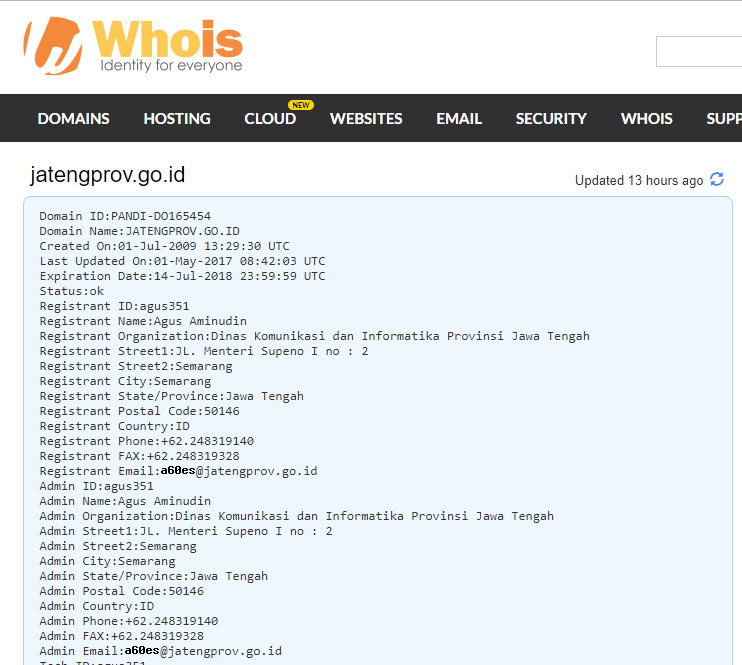
Keamanan data merupakan hal yang sangat penting dalam menjaga kerahasiaan informasi terutama yang berisi informasi sensitif yang hanya boleh diketahui isinya oleh pihak yang berhak saja, apalagi jika website tersebut sering mengalami bug-bug yang tidak diinginkan, hal tersebut menjadi rentan untuk para 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 jatengprov.go.id. 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.

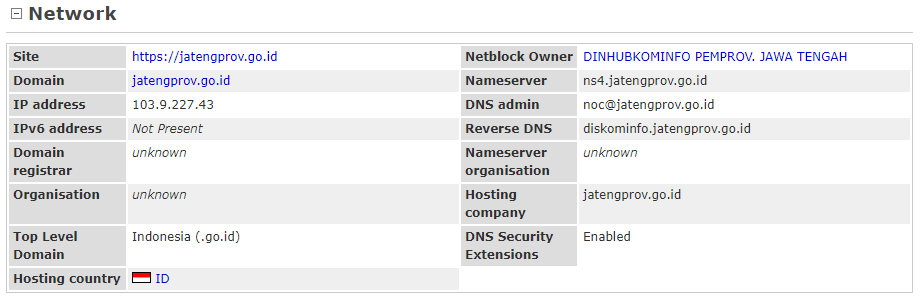
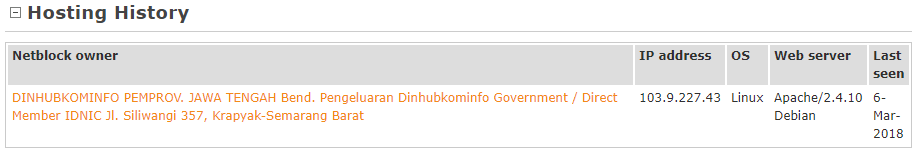
1. Data Collection

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.

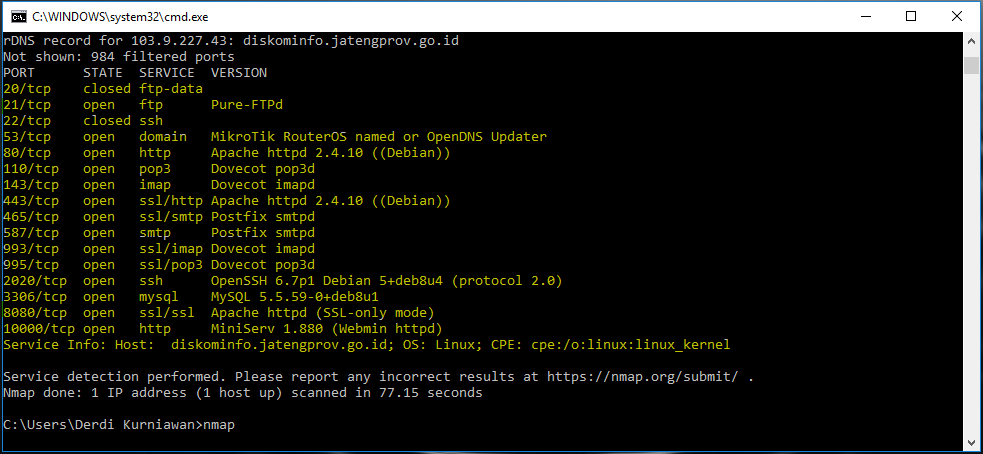
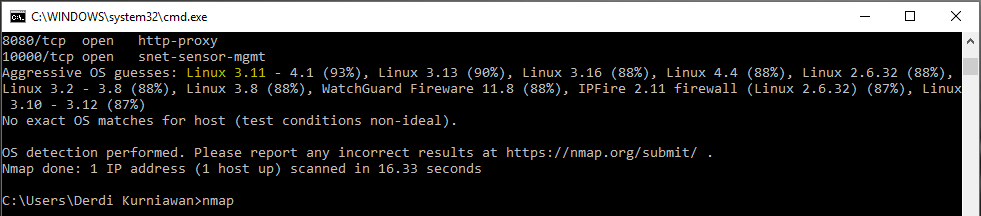
* Who is



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 | Jatengprov.go.id |
| IP address | 103.9.227.43 |
| Created On | 01 – Jul – 2009 13:29:30 utc |
| EXPIRATION DATE | 14 – Jul – 2018 23:59:59 utc |
| last updated On | 01 – May – 2017 08:42:03 utc |
| Registrant city | Semarang |
| Registrant Province | Jawa Tengah |
| Registrant Country | ID |
| OS Running | Linux 3.11 |
| Name Servers | NS1.JATENGPROV.GO.ID |
| Web Server | Apache/2.4.10 Debian |
| Port | 20/tcp, State = Closed , Service = ftp-data  21/tcp, State = Open, Service = ftp  22/tcp, State = Closed, Service = ssh  53/tcp, State = Open, Service = domain  80/tcp, State = Open, Service = http  110/tcp, State = Open, Service = pop3  143/tcp, State = Open, Service = imap  443/tcp, State = Open, Service = ssl/http  465/tcp, State = Open, Service = ssl/smtp  587/tcp, State = Open, Service = smtp  993/tcp, State = Open, Service = ssl/pop3  2020/tcp, State = Open, Service = ssh  3306/tcp, State = Open, Service = mysql  8080/tcp, State = Open, Service = ssl  10000/tcp, State = Open, Service = http |

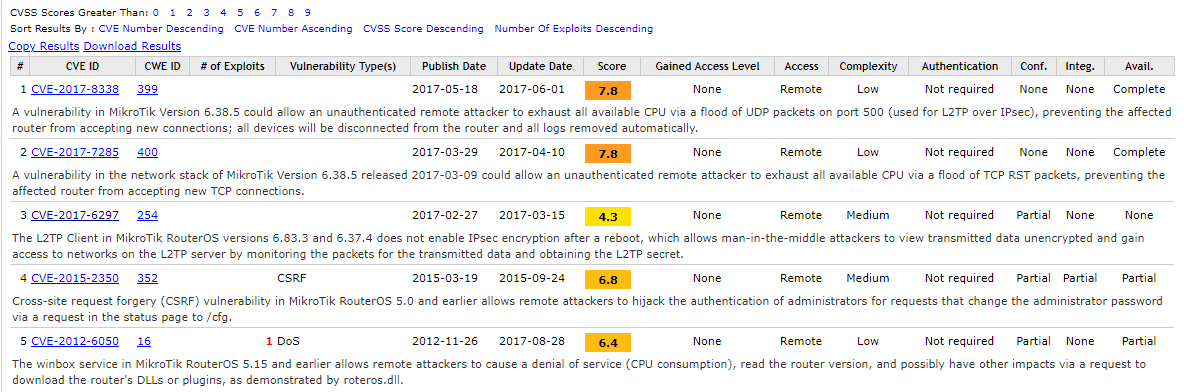
1. Vulnerbility

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

* Aplikasi Running beserta Holenya
* Pada Port 20

Pada Port ini berstate colosed, jadi tidak bisa dianalisa.

* Pada Port 21 menggunkan aplikasi ftp dengan versi Pure-FTPd

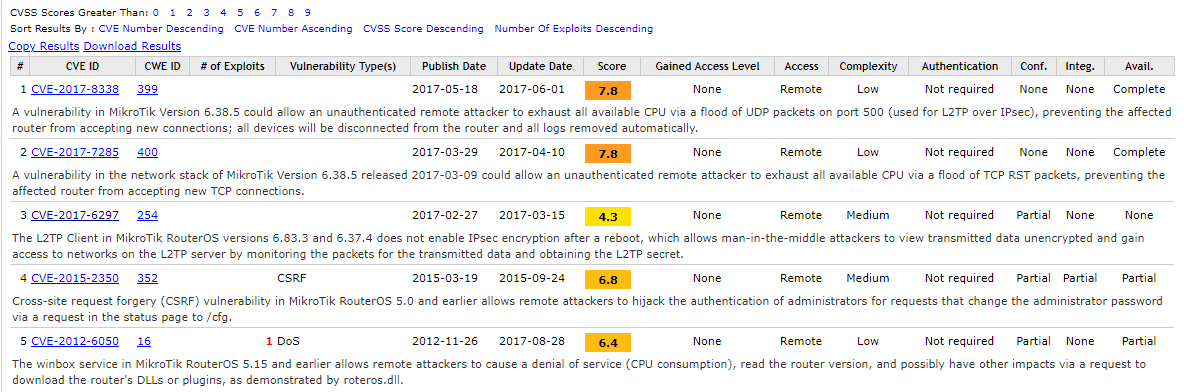
Pada port tesebut aplikasi yang running yaitu ftp, dimana apliksi tersebut setelah dianalisis dan terdapat celah dimana para hecker dapat masuk dengan memanfaatkan celah tersebut. Celah tersebut sebagai berikut:

Gambar 4 ( cvedetails.com. Hole pada port 21 )

* Pada Port 23

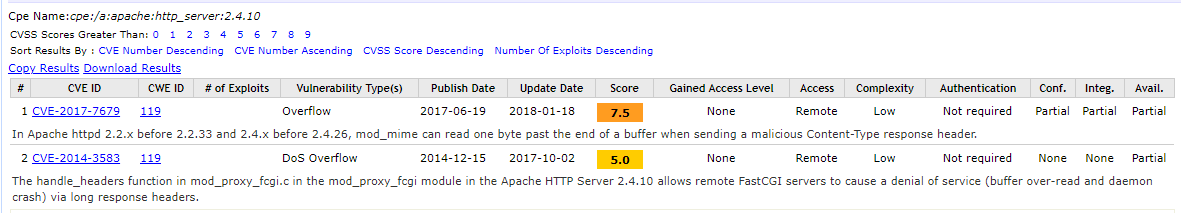
Pada Port ini berstate colosed, jadi tidak bisa dianalisa.

* 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 5 ( cvedetails.com. Hole pada port 53 )

* Pada Port 80, 433 dan 8080

Pada port tesebut aplikasi yang running yaitu http/ssl dengan versi Apache httpd 2.4.10 ((Debian)), dimana apliksi tersebut setelah dianalisi terdapat celah dimana para hecker dapat masuk dengan memanfaatkan celah dari tersebut. Celah tersebut sebagai berikut:

Gambar 6 ( cvedetails.com. Hole pada port 80, 433 dan 8080)

* Pada Port 110 dan 995 menggunkan aplikasi pop3 dengan versi Dovecot pop3d

Pada port tesebut aplikasi yang running yaitu pop3n, dimana apliksi tersebut setelah dianalisi terdapat celah dimana para hecker dapat masuk dengan memanfaatkan celah dari tersebut. Celah tersebut sebagai berikut:

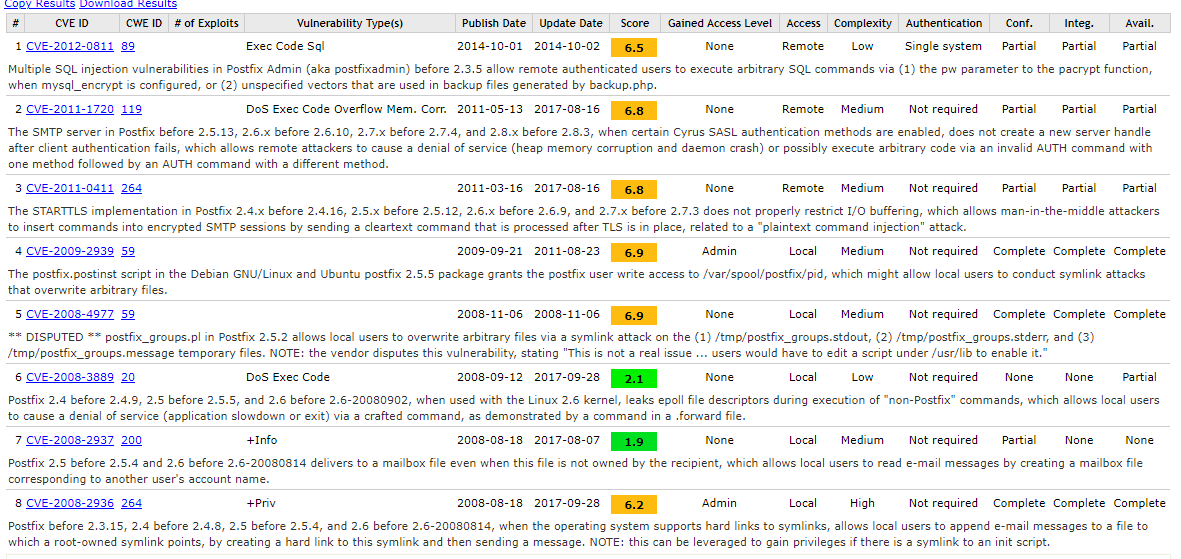
Gambar7 ( cvedetails.com. Hole pada port 110 dan 995 )

* Pada Port 143 dan 993 menggunkan aplikasi imap dengan versi Dovecot imapd

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

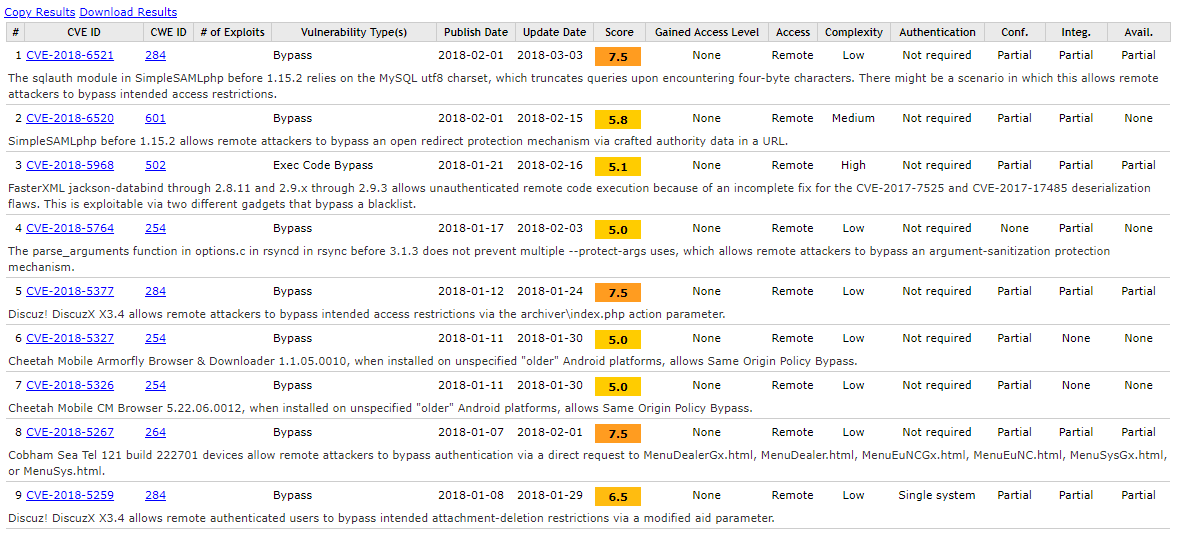
Gambar8 ( cvedetails.com. Hole pada port 143 dan 993)

* Pada Port 587 menggunkan aplikasi smtp dengan versi Postfix smtpd

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

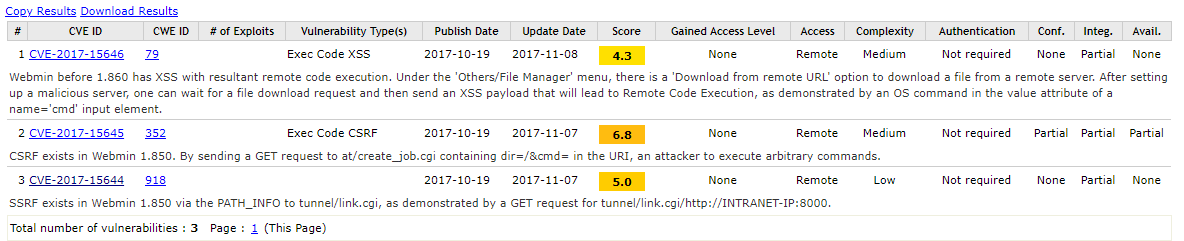
Gambar9 ( cvedetails.com. Hole pada port 587)

* ada Port 3306 menggunkan aplikasi myql dengan versi MySQL 5.5.59-0+deb8u1

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

Gambar10 ( cvedetails.com. Hole pada port 3306)

* ada Port 10000 menggunkan aplikasi http dengan versi MiniServ 1.880 (Webmin httpd)

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

Gambar11 ( cvedetails.com. Hole pada port 10000)

1. Kesimpulan

Pada analisa dan hasil tersebut dapat kita simpulkan bahwa:

* Target tersebut memiliki 15 port.
* Target tersebut menggunkan OS Linuk 3.11
* Dengan 15 port yang dimiliki setidaknya terdapat 47 serangan dengan complexity 34 Low, 2 Hight dan 11 Medium
* Serangan terjadi salah satunya diakibatkan kurang updatenya webserver yang digunkan

1. Referensi

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