Tugas Manajemen keamanan informasi

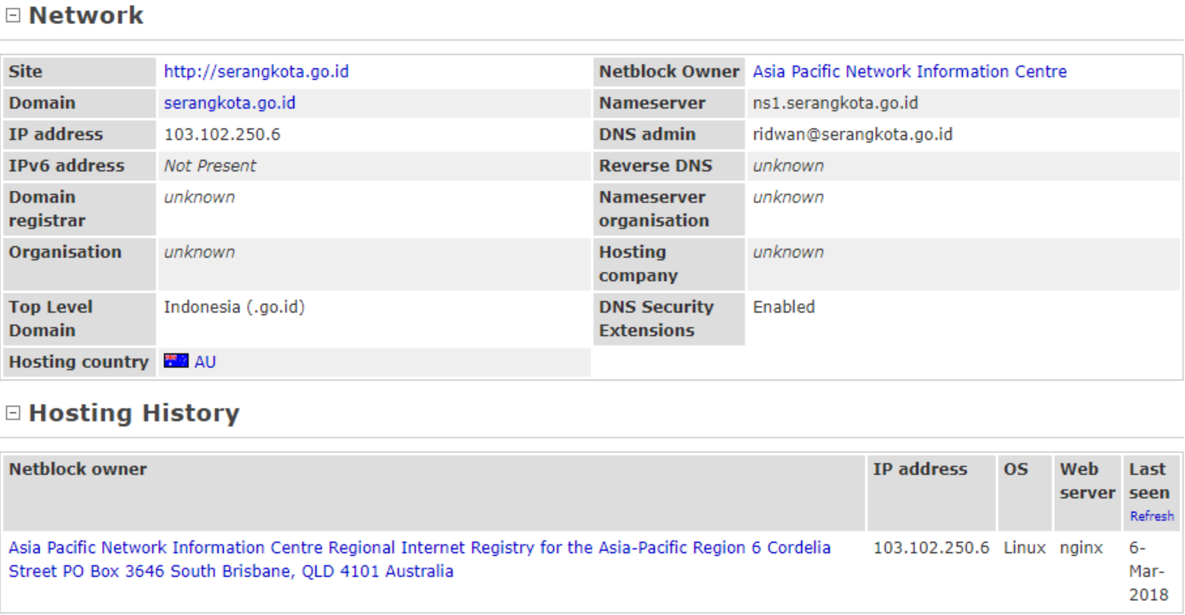
Nama : M Hengky Setiawan

NIM : 09031281520111

Target : serangkota.go.id

1. Scanning

Menggunakan Netcraft



⊟ Network

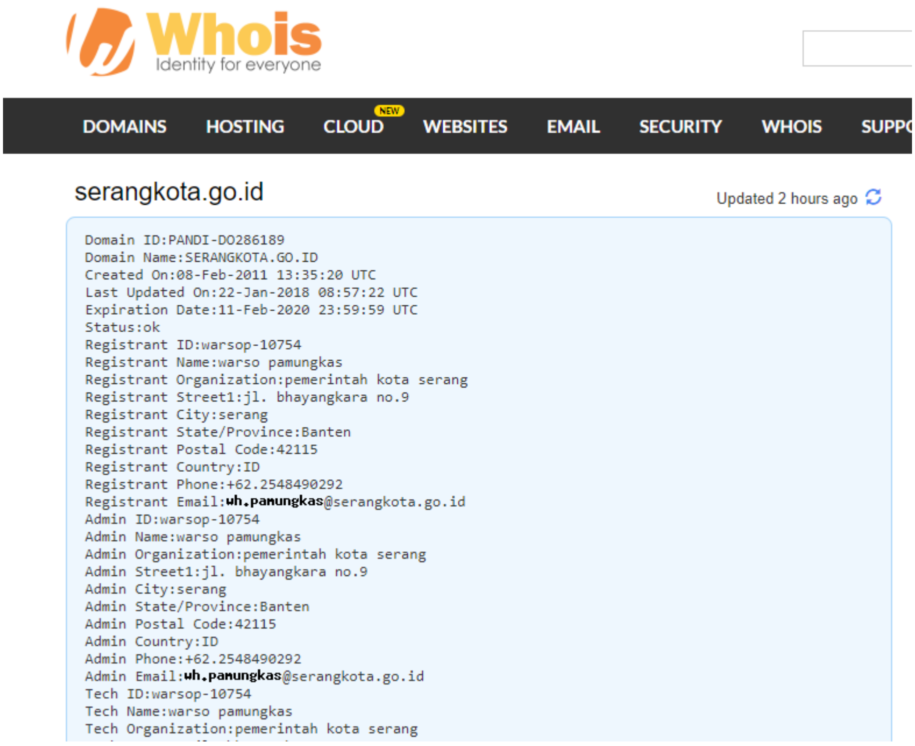
Site	http://serangkota.go.id	Netblock Owner	Asia Pacific Network Information Centre
Domain	serangkota.go.id	Nameserver	ns1.serangkota.go.id
IP address	103.102.250.6	DNS admin	ridwan@serangkota.go.id
IPv6 address	*Not Present*	Reverse DNS	*unknown*
Domain registrar	*unknown*	Nameserver organisation	*unknown*
Organisation	*unknown*	Hosting company	*unknown*
Top Level Domain	Indonesia (.go.id)	DNS Security Extensions	Enabled
Hosting country	AU		

⊟ Hosting History

Netblock owner	IP address	OS	Web server	Last seen Refresh
Asia Pacific Network Information Centre Regional Internet Registry for the Asia-Pacific Region 6 Cordelia Street PO Box 3646 South Brisbane, QLD 4101 Australia	103.102.250.6	Linux	nginx	6-Mar-2018

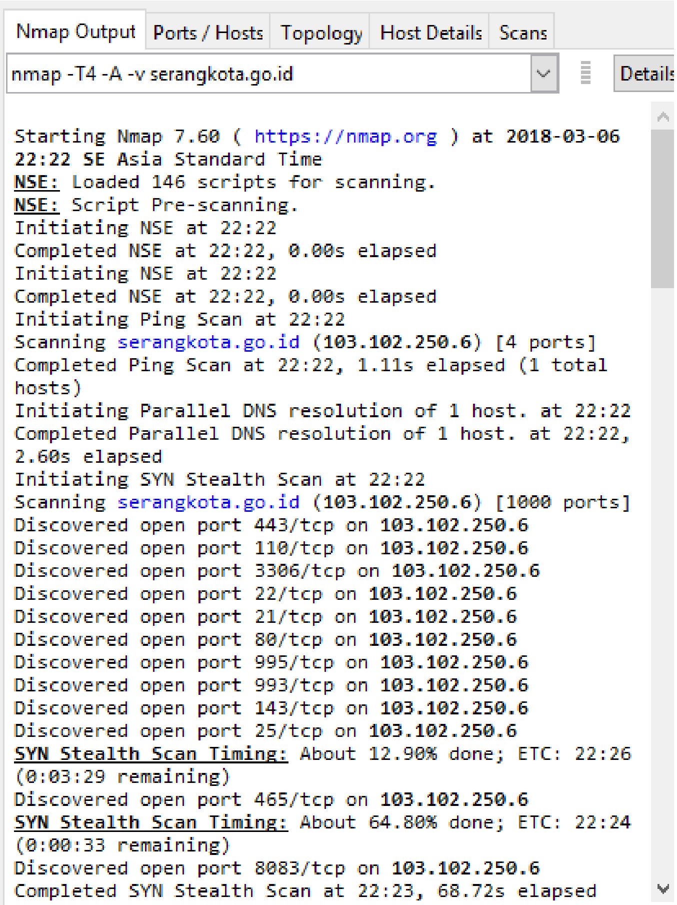
Data diatas merupakan data yang di dapat dari netcraft. Dan pada hosting history ada 1 kali.

Menggunakan Whois



```
Domain ID:PANDI-DO286189
Domain Name:SERANGKOTA.GO.ID
Created On:08-Feb-2011 13:35:20 UTC
Last Updated On:22-Jan-2018 08:57:22 UTC
Expiration Date:11-Feb-2020 23:59:59 UTC
Status:ok
Registrant ID:warsop-10754
Registrant Name:warso pamungkas
Registrant Organization:pemerintah kota serang
Registrant Street1:jl. bhayangkara no.9
Registrant City:serang
Registrant State/Province:Banten
Registrant Postal Code:42115
Registrant Country:ID
Registrant Phone:+62.2548490292
Registrant Email:wh.pamungkas@serangkota.go.id
Admin ID:warsop-10754
Admin Name:warso pamungkas
Admin Organization:pemerintah kota serang
Admin Street1:jl. bhayangkara no.9
Admin City:serang
Admin State/Province:Banten
Admin Postal Code:42115
Admin Country:ID
Admin Phone:+62.2548490292
Admin Email:wh.pamungkas@serangkota.go.id
Tech ID:warsop-10754
Tech Name:warso pamungkas
Tech Organization:pemerintah kota serang
```

Menggunakan aplikasi nmap



```
nmap -T4 -A -v serangkota.go.id
```

```
Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-06
22:22 SE Asia Standard Time
NSE: Loaded 146 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 22:22
Completed NSE at 22:22, 0.00s elapsed
Initiating NSE at 22:22
Completed NSE at 22:22, 0.00s elapsed
Initiating Ping Scan at 22:22
Scanning serangkota.go.id (103.102.250.6) [4 ports]
Completed Ping Scan at 22:22, 1.11s elapsed (1 total
hosts)
Initiating Parallel DNS resolution of 1 host. at 22:22
Completed Parallel DNS resolution of 1 host. at 22:22,
2.60s elapsed
Initiating SYN Stealth Scan at 22:22
Scanning serangkota.go.id (103.102.250.6) [1000 ports]
Discovered open port 443/tcp on 103.102.250.6
Discovered open port 110/tcp on 103.102.250.6
Discovered open port 3306/tcp on 103.102.250.6
Discovered open port 22/tcp on 103.102.250.6
Discovered open port 21/tcp on 103.102.250.6
Discovered open port 80/tcp on 103.102.250.6
Discovered open port 995/tcp on 103.102.250.6
Discovered open port 993/tcp on 103.102.250.6
Discovered open port 143/tcp on 103.102.250.6
Discovered open port 25/tcp on 103.102.250.6
SYN Stealth Scan Timing: About 12.90% done; ETC: 22:26
(0:03:29 remaining)
Discovered open port 465/tcp on 103.102.250.6
SYN Stealth Scan Timing: About 64.80% done; ETC: 22:24
(0:00:33 remaining)
Discovered open port 8083/tcp on 103.102.250.6
Completed SYN Stealth Scan at 22:23, 68.72s elapsed
```

Pada hasil scanning ini. Dapat membuka 10 port yaitu:

Discovered open port 443/tcp on 103.102.250.6

Discovered open port 110/tcp on 103.102.250.6

Discovered open port 3306/tcp on 103.102.250.6

Discovered open port 22/tcp on 103.102.250.6

Discovered open port 21/tcp on 103.102.250.6

Discovered open port 80/tcp on 103.102.250.6

Discovered open port 995/tcp on 103.102.250.6

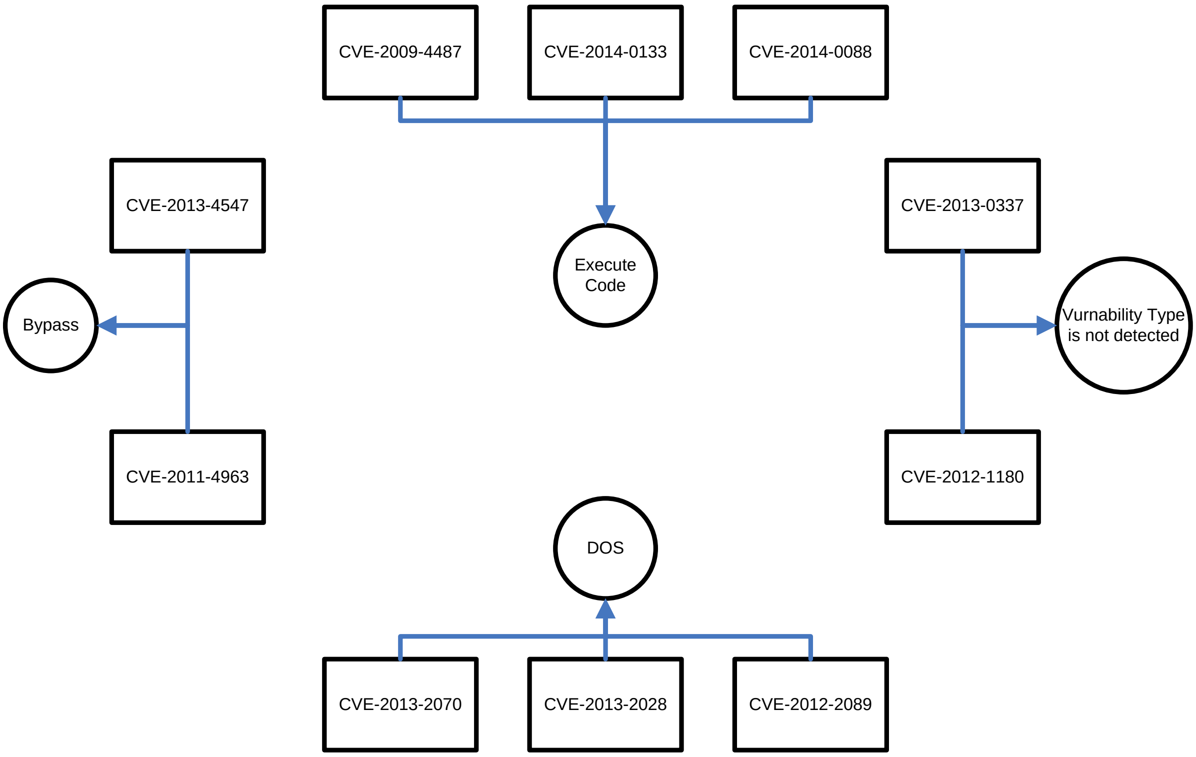
Discovered open port 993/tcp on 103.102.250.6

Discovered open port 143/tcp on 103.102.250.6

Discovered open port 25/tcp on 103.102.250.6

2. Vurnabilities

Melakukan cve mapping



Gambar diatas merupakan cve mapping yang ada pada website serangkota.go.id terdapat tipe serangan Bypass, DOS, Execute Code, dan ada yang tidak teridentifikasi.

Keterangan :

- CVE-2014-0133 →Heap-based buffer overflow in the SPDY implementation in nginx 1.3.15 before 1.4.7 and 1.5.x before 1.5.12 allows remote attackers to execute arbitrary code via a crafted request.
- CVE-2014-0088 → The SPDY implementation in the ngx_http_spdy_module module in nginx 1.5.10 before 1.5.11, when running on a 32-bit platform, allows remote attackers to execute arbitrary code via a crafted request.
- CVE-2013-4547 → nginx 0.8.41 through 1.4.3 and 1.5.x before 1.5.7 allows remote attackers to bypass intended restrictions via an unescaped space character in a URI.
- CVE-2013-2070 → http/modules/ngx_http_proxy_module.c in nginx 1.1.4 through 1.2.8 and 1.3.0 through 1.4.0, when proxy_pass is used with untrusted HTTP servers, allows remote attackers to cause a denial of service (crash) and obtain sensitive information from worker process memory via a crafted proxy response, a similar vulnerability to CVE-2013-2028.
- CVE-2013-2028 → The ngx_http_parse_chunked function in http/ngx_http_parse.c in nginx 1.3.9 through 1.4.0 allows remote attackers to cause a denial of service (crash) and execute arbitrary code via a chunked Transfer-Encoding request with a large chunk size, which triggers an integer signedness error and a stack-based buffer overflow.
- CVE-2013-0337 → The default configuration of nginx, possibly 1.3.13 and earlier, uses world-readable permissions for the (1) access.log and (2) error.log files, which allows local users to obtain sensitive information by reading the files.
- CVE-2012-2089 → Buffer overflow in ngx_http_mp4_module.c in the ngx_http_mp4_module module in nginx 1.0.7 through 1.0.14 and 1.1.3 through 1.1.18, when the mp4 directive is used, allows remote attackers to cause a denial of service (memory overwrite) or possibly execute arbitrary code via a crafted MP4 file.
- CVE-2012-1180 → Use-after-free vulnerability in nginx before 1.0.14 and 1.1.x before 1.1.17 allows remote HTTP servers to obtain sensitive information from process memory via a crafted backend response, in conjunction with a client request.
- CVE-2011-4963 → nginx/Windows 1.3.x before 1.3.1 and 1.2.x before 1.2.1 allows remote attackers to bypass intended access restrictions and access restricted files via (1) a trailing . (dot) or (2) certain "$index_allocation" sequences in a request.
- CVE-2009-4487 → nginx 0.7.64 writes data to a log file without sanitizing non-printable characters, which might allow remote attackers to modify a window's title, or possibly execute arbitrary commands or overwrite files, via an HTTP request containing an escape sequence for a terminal emulator.

Kesimpulan :

- Target memiliki 10 port
- Target tersebut menggunakan os linux
- Target memiliki 4 jenis serangan melalui cve

Referensi :

- Whois.com
- Netcraft.com
- Cvedetails.com
- Nmap
- cve