Tugas Manajemen keamanan informasi

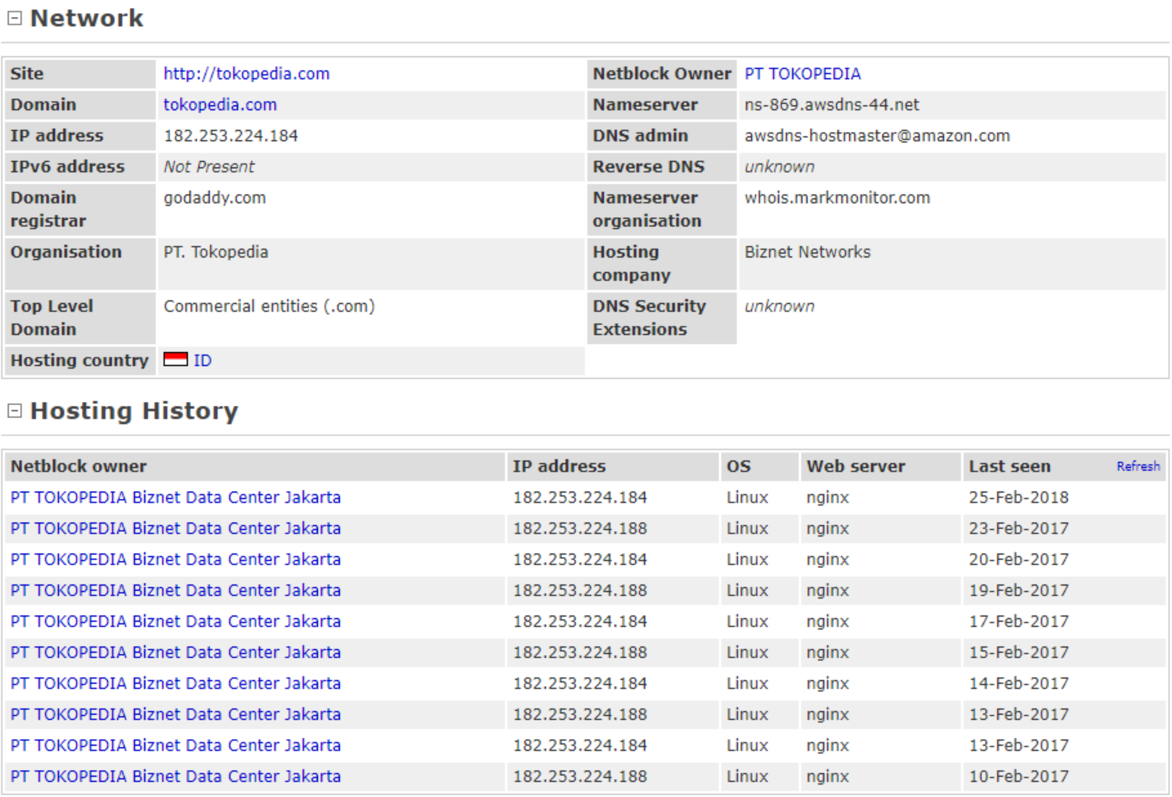
Nama : M Hengky Setiawan

NIM : 09031281520111

Target : tokopedia.com

1. Scanning

Menggunakan Netcraft



⊟ Network

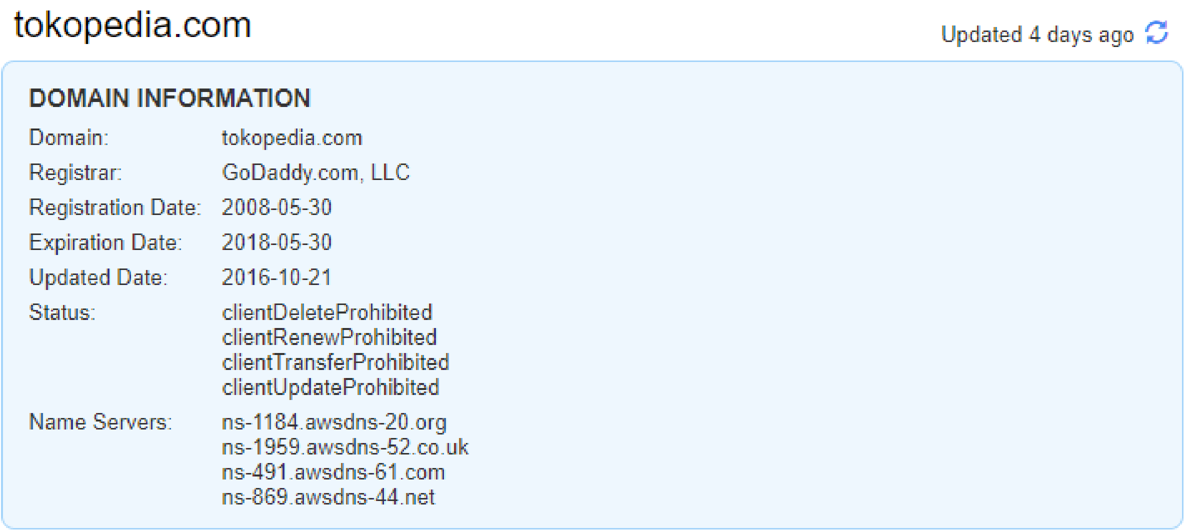
Site	http://tokopedia.com	**Netblock Owner**	PT TOKOPEDIA
Domain	tokopedia.com	**Nameserver**	ns-869.awsdns-44.net
IP address	182.253.224.184	**DNS admin**	awsdns-hostmaster@amazon.com
IPv6 address	*Not Present*	**Reverse DNS**	*unknown*
Domain registrar	godaddy.com	**Nameserver organisation**	whois.markmonitor.com
Organisation	PT. Tokopedia	**Hosting company**	Biznet Networks
Top Level Domain	Commercial entities (.com)	**DNS Security Extensions**	*unknown*
Hosting country	ID		

⊟ Hosting History

Netblock owner	IP address	OS	Web server	Last seen Refresh
PT TOKOPEDIA Biznet Data Center Jakarta	182.253.224.184	Linux	nginx	25-Feb-2018
PT TOKOPEDIA Biznet Data Center Jakarta	182.253.224.188	Linux	nginx	23-Feb-2017
PT TOKOPEDIA Biznet Data Center Jakarta	182.253.224.184	Linux	nginx	20-Feb-2017
PT TOKOPEDIA Biznet Data Center Jakarta	182.253.224.188	Linux	nginx	19-Feb-2017
PT TOKOPEDIA Biznet Data Center Jakarta	182.253.224.184	Linux	nginx	17-Feb-2017
PT TOKOPEDIA Biznet Data Center Jakarta	182.253.224.188	Linux	nginx	15-Feb-2017
PT TOKOPEDIA Biznet Data Center Jakarta	182.253.224.184	Linux	nginx	14-Feb-2017
PT TOKOPEDIA Biznet Data Center Jakarta	182.253.224.188	Linux	nginx	13-Feb-2017
PT TOKOPEDIA Biznet Data Center Jakarta	182.253.224.184	Linux	nginx	13-Feb-2017
PT TOKOPEDIA Biznet Data Center Jakarta	182.253.224.188	Linux	nginx	10-Feb-2017

Data diatas merupakan data yang di dapat dari netcraft. Dan pada hosting history ada 10 kali.

Menggunakan Whois



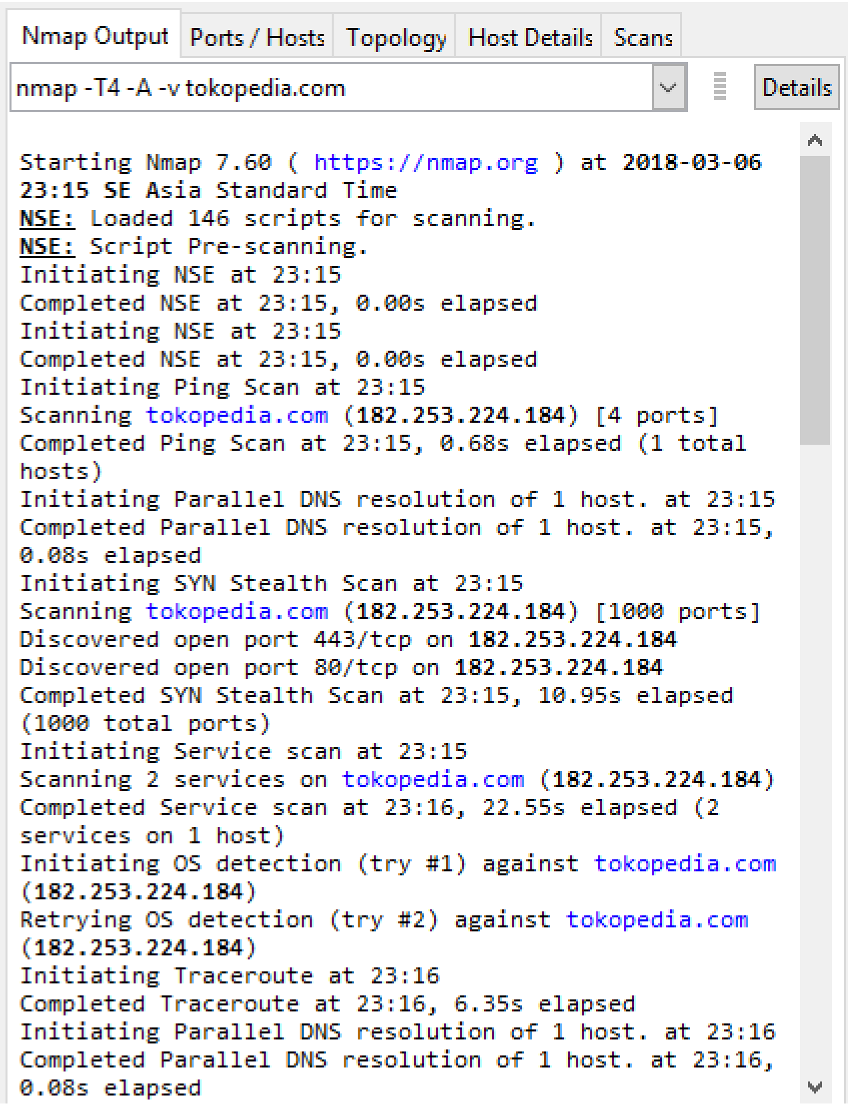
tokopedia.com

Updated 4 days ago

DOMAIN INFORMATION

Domain:	tokopedia.com
Registrar:	GoDaddy.com, LLC
Registration Date:	2008-05-30
Expiration Date:	2018-05-30
Updated Date:	2016-10-21
Status:	clientDeleteProhibited clientRenewProhibited clientTransferProhibited clientUpdateProhibited
Name Servers:	ns-1184.awsdns-20.org ns-1959.awsdns-52.co.uk ns-491.awsdns-61.com ns-869.awsdns-44.net

Menggunakan aplikasi nmap



nmap -T4 -A -v tokopedia.com

```
Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-06
23:15 SE Asia Standard Time
NSE: Loaded 146 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 23:15
Completed NSE at 23:15, 0.00s elapsed
Initiating NSE at 23:15
Completed NSE at 23:15, 0.00s elapsed
Initiating Ping Scan at 23:15
Scanning tokopedia.com (182.253.224.184) [4 ports]
Completed Ping Scan at 23:15, 0.68s elapsed (1 total
hosts)
Initiating Parallel DNS resolution of 1 host. at 23:15
Completed Parallel DNS resolution of 1 host. at 23:15,
0.08s elapsed
Initiating SYN Stealth Scan at 23:15
Scanning tokopedia.com (182.253.224.184) [1000 ports]
Discovered open port 443/tcp on 182.253.224.184
Discovered open port 80/tcp on 182.253.224.184
Completed SYN Stealth Scan at 23:15, 10.95s elapsed
(1000 total ports)
Initiating Service scan at 23:15
Scanning 2 services on tokopedia.com (182.253.224.184)
Completed Service scan at 23:16, 22.55s elapsed (2
services on 1 host)
Initiating OS detection (try #1) against tokopedia.com
(182.253.224.184)
Retrying OS detection (try #2) against tokopedia.com
(182.253.224.184)
Initiating Traceroute at 23:16
Completed Traceroute at 23:16, 6.35s elapsed
Initiating Parallel DNS resolution of 1 host. at 23:16
Completed Parallel DNS resolution of 1 host. at 23:16,
0.08s elapsed
```

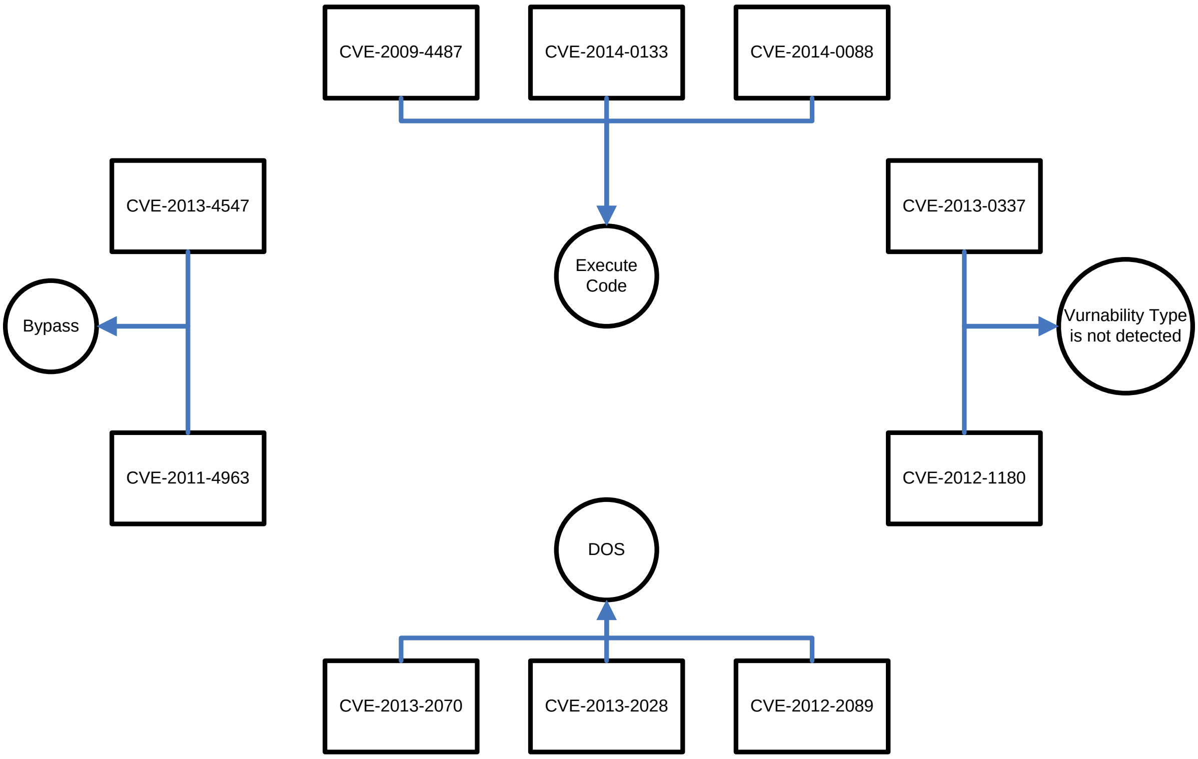
Pada hasil scanning ini. Dapat membuka 2 port yaitu:

Discovered open port 443/tcp on 182.253.224.184

Discovered open port 80/tcp on 182.253.224.184

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

Referensi :

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