Tugas

Manajemen Keamanan Informasi

“Data Collection and Vulnerability Assesment”

Dahlia 09031181520117

Dosen Pengampuh

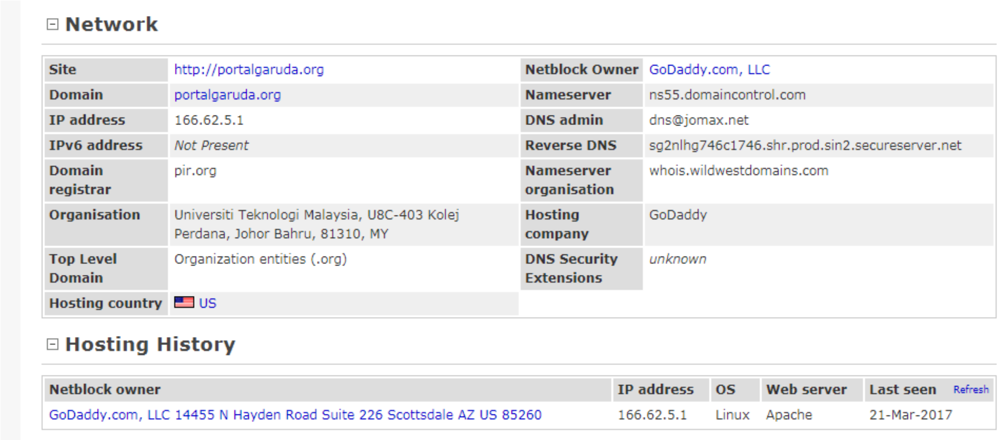
Deris Setiawan, M.T., Ph.D.

Jurusan Sitem Informasi
Fakultas Ilmu Komputer
Universitas Sriwijaya
2018

Webstite : portalgaruda.org

1. Data Collection
   Proses mengumpulkan data yang diperlukan pada target.
   Data dikumpulkan dari situs Whois, Nmap dan Netcraft dan domain yang dijadikan target yaitu portalgaruda.org
   Berikut data yang didapat dari situs tersebut

   Menggunakan Netcraft



⊟ **Network**

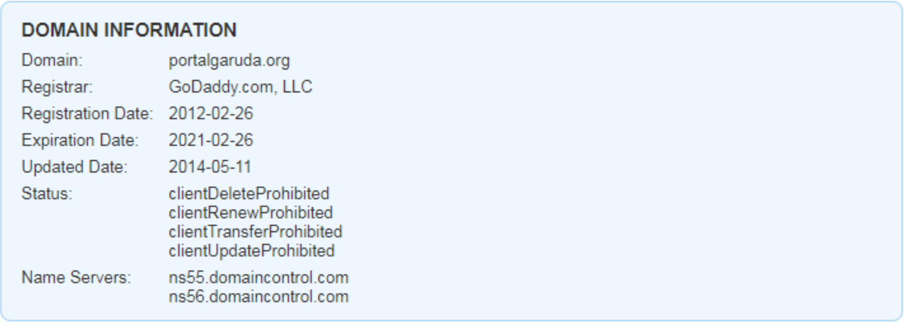
Site	http://portalgaruda.org	**Netblock Owner**	GoDaddy.com, LLC
Domain	portalgaruda.org	**Nameserver**	ns55.domaincontrol.com
IP address	166.62.5.1	**DNS admin**	dns@jomax.net
IPv6 address	*Not Present*	**Reverse DNS**	sg2nlhg746c1746.shr.prod.sin2.secureserver.net
Domain registrar	pir.org	**Nameserver organisation**	whois.wildwestdomains.com
Organisation	Universiti Teknologi Malaysia, U8C-403 Kolej Perdana, Johor Bahru, 81310, MY	**Hosting company**	GoDaddy
Top Level Domain	Organization entities (.org)	**DNS Security Extensions**	*unknown*
Hosting country	US		

⊟ **Hosting History**

Netblock owner	IP address	OS	Web server	Last seen Refresh
GoDaddy.com, LLC 14455 N Hayden Road Suite 226 Scottsdale AZ US 85260	166.62.5.1	Linux	Apache	21-Mar-2017

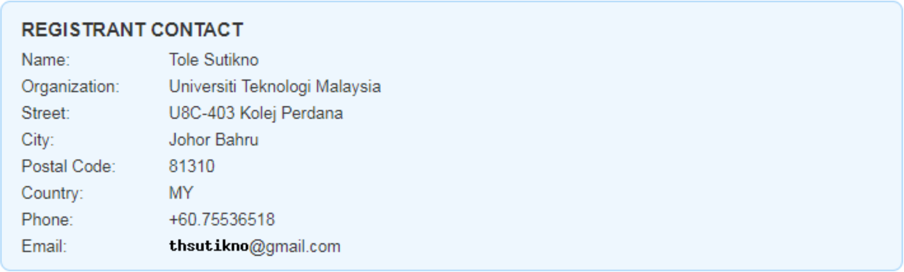
Tampilan diatas merupakan hasil scanning yang menghasilkan data Network dan Hosting History (IP Address, Web Server, Waktu Terakhir di Update)

Menggunakan Whois



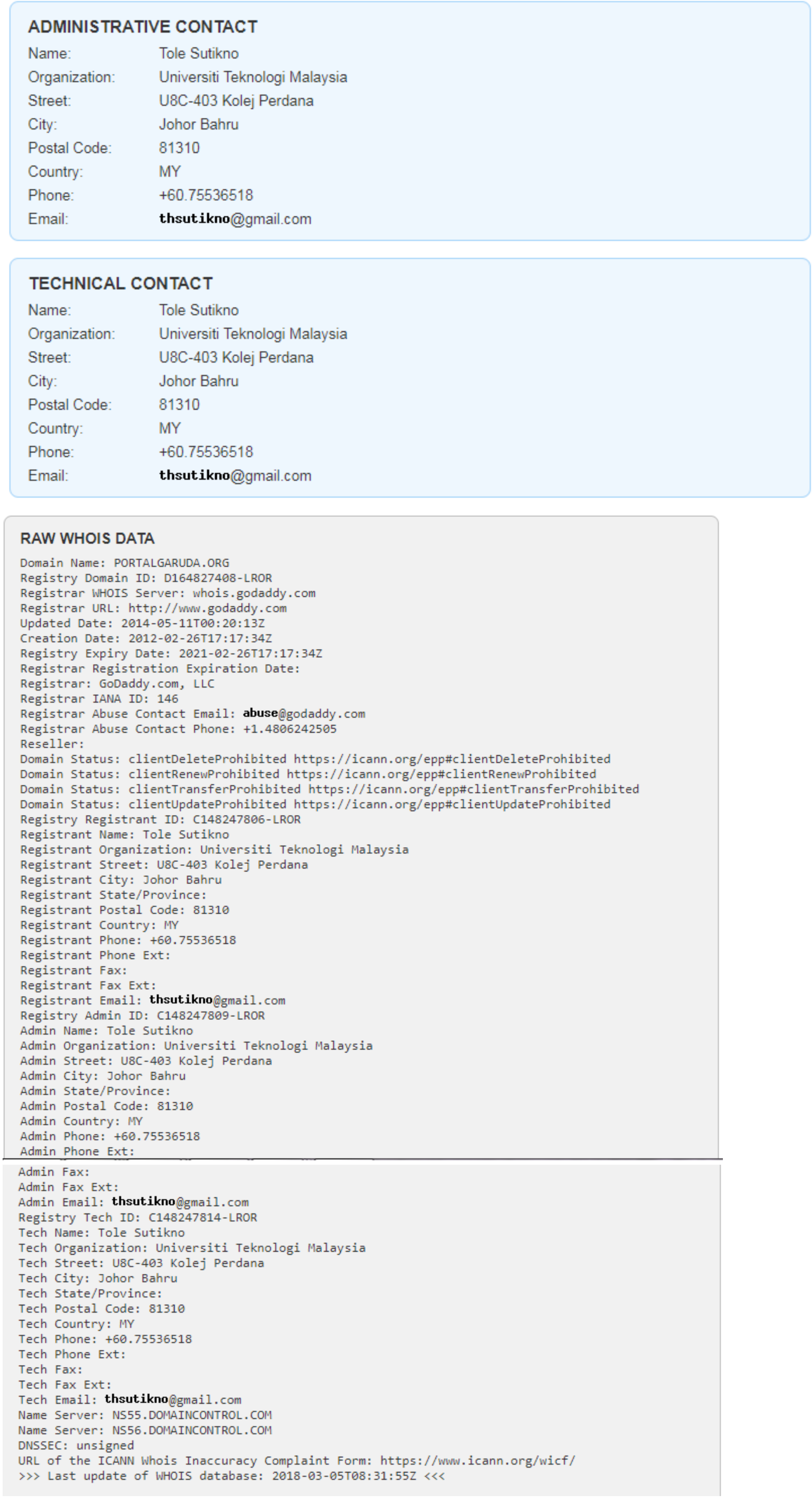
DOMAIN INFORMATION

Domain:	portalgaruda.org
Registrar:	GoDaddy.com, LLC
Registration Date:	2012-02-26
Expiration Date:	2021-02-26
Updated Date:	2014-05-11
Status:	clientDeleteProhibited clientRenewProhibited clientTransferProhibited clientUpdateProhibited
Name Servers:	ns55.domaincontrol.com ns56.domaincontrol.com



REGISTRANT CONTACT

Name:	Tole Sutikno
Organization:	Universiti Teknologi Malaysia
Street:	U8C-403 Kolej Perdana
City:	Johor Bahru
Postal Code:	81310
Country:	MY
Phone:	+60.75536518
Email:	**thsutikno**@gmail.com



ADMINISTRATIVE CONTACT

Name:	Tole Sutikno
Organization:	Universiti Teknologi Malaysia
Street:	U8C-403 Kolej Perdana
City:	Johor Bahru
Postal Code:	81310
Country:	MY
Phone:	+60.75536518
Email:	**thsutikno**@gmail.com

TECHNICAL CONTACT

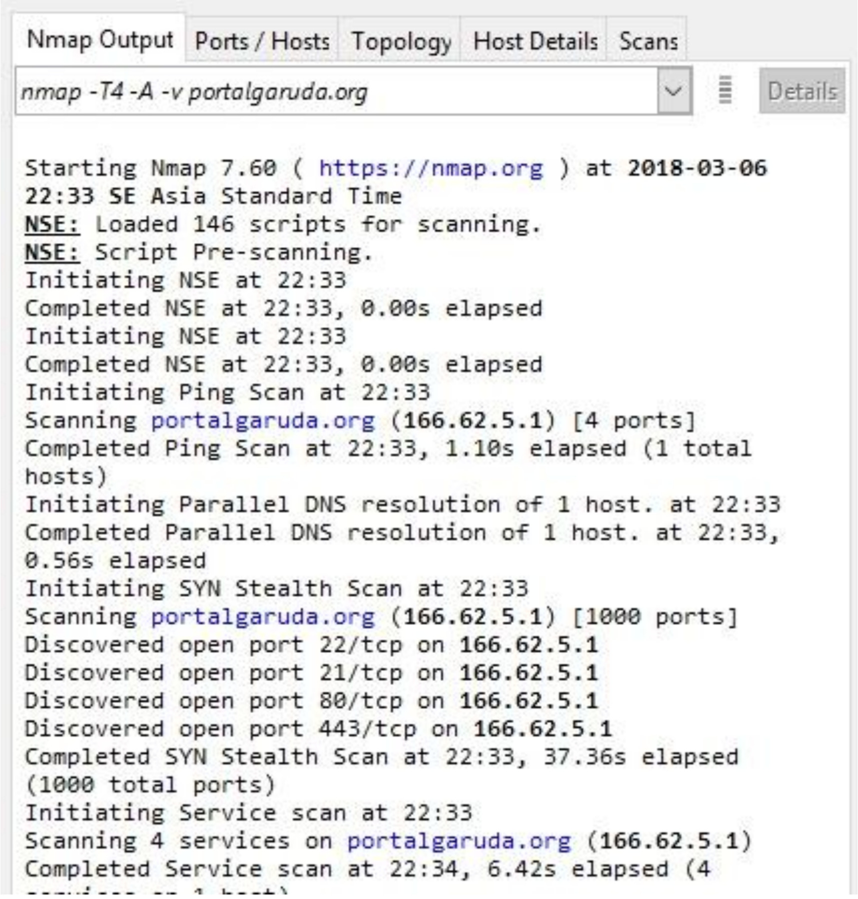
Name:	Tole Sutikno
Organization:	Universiti Teknologi Malaysia
Street:	U8C-403 Kolej Perdana
City:	Johor Bahru
Postal Code:	81310
Country:	MY
Phone:	+60.75536518
Email:	**thsutikno**@gmail.com

RAW WHOIS DATA

```
Domain Name: PORTALGARUDA.ORG
Registry Domain ID: D164827408-LROR
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Updated Date: 2014-05-11T00:20:13Z
Creation Date: 2012-02-26T17:17:34Z
Registry Expiry Date: 2021-02-26T17:17:34Z
Registrar Registration Expiration Date:
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Reseller:
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Registry Registrant ID: C148247806-LROR
Registrant Name: Tole Sutikno
Registrant Organization: Universiti Teknologi Malaysia
Registrant Street: U8C-403 Kolej Perdana
Registrant City: Johor Bahru
Registrant State/Province:
Registrant Postal Code: 81310
Registrant Country: MY
Registrant Phone: +60.75536518
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: thsutikno@gmail.com
Registry Admin ID: C148247809-LROR
Admin Name: Tole Sutikno
Admin Organization: Universiti Teknologi Malaysia
Admin Street: U8C-403 Kolej Perdana
Admin City: Johor Bahru
Admin State/Province:
Admin Postal Code: 81310
Admin Country: MY
Admin Phone: +60.75536518
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: thsutikno@gmail.com
Registry Tech ID: C148247814-LROR
Tech Name: Tole Sutikno
Tech Organization: Universiti Teknologi Malaysia
Tech Street: U8C-403 Kolej Perdana
Tech City: Johor Bahru
Tech State/Province:
Tech Postal Code: 81310
Tech Country: MY
Tech Phone: +60.75536518
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: thsutikno@gmail.com
Name Server: NS55.DOMAINCONTROL.COM
Name Server: NS56.DOMAINCONTROL.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2018-03-05T08:31:55Z <<<
```

Tampilan diatas hasil scanning pada Whois, yang menampilkan data-data target mulai dari register sampai lokasi.

Nmap



nmap -T4 -A -v portalgaruda.org

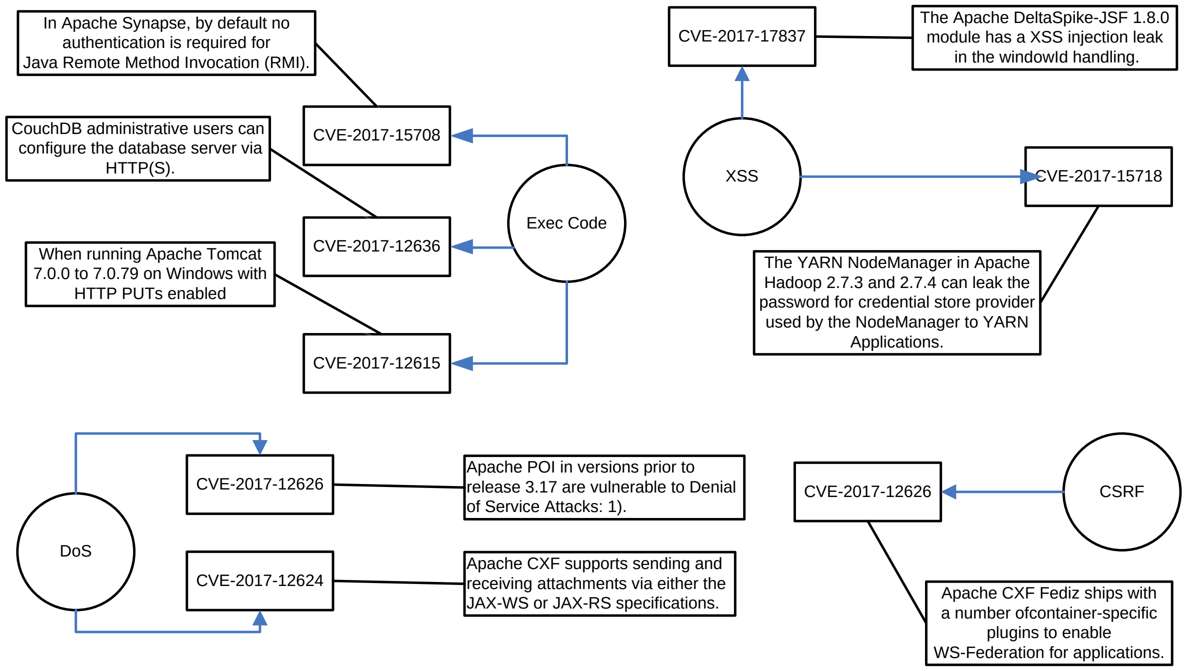
```
Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-06
22:33 SE Asia Standard Time
NSE: Loaded 146 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 22:33
Completed NSE at 22:33, 0.00s elapsed
Initiating NSE at 22:33
Completed NSE at 22:33, 0.00s elapsed
Initiating Ping Scan at 22:33
Scanning portalgaruda.org (166.62.5.1) [4 ports]
Completed Ping Scan at 22:33, 1.10s elapsed (1 total
hosts)
Initiating Parallel DNS resolution of 1 host. at 22:33
Completed Parallel DNS resolution of 1 host. at 22:33,
0.56s elapsed
Initiating SYN Stealth Scan at 22:33
Scanning portalgaruda.org (166.62.5.1) [1000 ports]
Discovered open port 22/tcp on 166.62.5.1
Discovered open port 21/tcp on 166.62.5.1
Discovered open port 80/tcp on 166.62.5.1
Discovered open port 443/tcp on 166.62.5.1
Completed SYN Stealth Scan at 22:33, 37.36s elapsed
(1000 total ports)
Initiating Service scan at 22:33
Scanning 4 services on portalgaruda.org (166.62.5.1)
Completed Service scan at 22:34, 6.42s elapsed (4
```

Pada hasil scanning ini. Dapat membuka 4 port (Open Port) yaitu:

Discovered open port 22/tcp on 166.62.5.1
Discovered open port 443/tcp on 166.62.5.1
Discovered open port 21/tcp on 166.62.5.1
Discovered open port 80/tcp on 166.62.5.1

2. Vulnerability Assesment
   Berikut ini beberapa Vulnerability yang ada. Pencarian vurnability dilakukan pada https://www.cvedetails.com

   Webserver Apache :
   Gambar berikut merupakan beberapa vurnability yang didapat pada CVE



In Apache Synapse, by default no authentication is required for Java Remote Method Invocation (RMI).

CouchDB administrative users can configure the database server via HTTP(S).

When running Apache Tomcat 7.0.0 to 7.0.79 on Windows with HTTP PUTs enabled

The Apache DeltaSpike-JSF 1.8.0 module has a XSS injection leak in the windowId handling.

The YARN NodeManager in Apache Hadoop 2.7.3 and 2.7.4 can leak the password for credential store provider used by the NodeManager to YARN Applications.

Apache POI in versions prior to release 3.17 are vulnerable to Denial of Service Attacks: 1).

Apache CXF supports sending and receiving attachments via either the JAX-WS or JAX-RS specifications.

Apache CXF Fediz ships with a number ofcontainer-specific plugins to enable WS-Federation for applications.

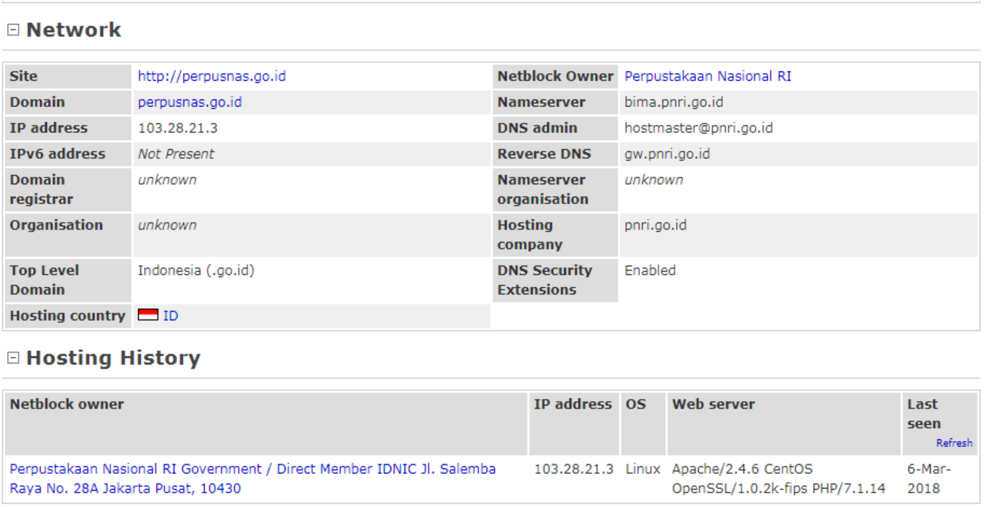
Pada Apache ini dari vurnability yang ada, memiliki tingkat kompleksitas yang beragam mulai dari low, medium dan high.

Website Perpusnas.go.id

1. Data Collection

   Data dikumpulkan dari situs Whois, Nmap dan Netcraft dan domain yang dijadikan target yaitu perpusnas.go.id

   Berikut data yang didapat dari situs tersebut



⊟ Network

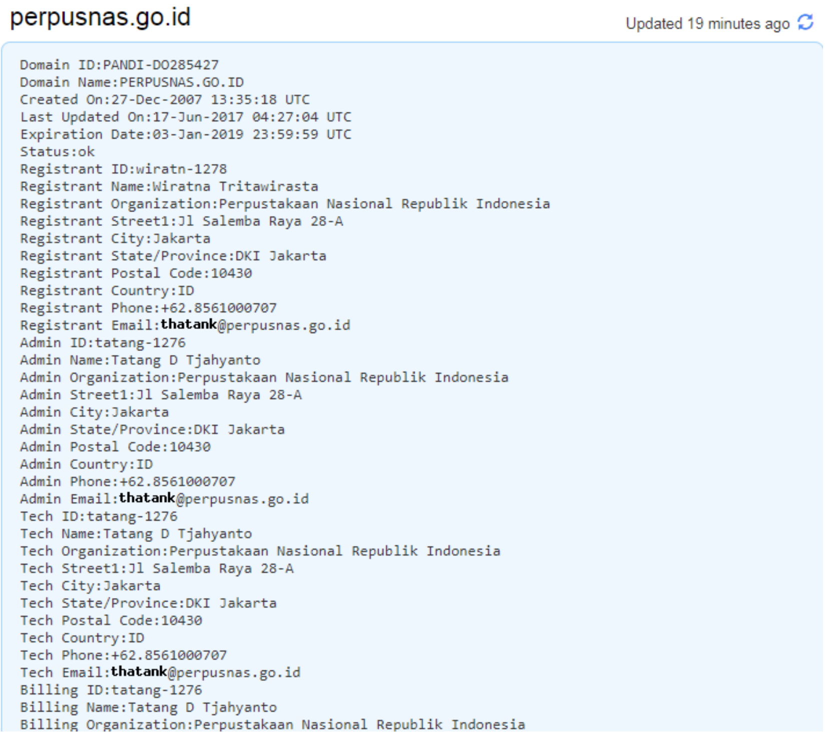
Site	http://perpusnas.go.id	Netblock Owner	Perpustakaan Nasional RI
Domain	perpusnas.go.id	Nameserver	bima.pnri.go.id
IP address	103.28.21.3	DNS admin	hostmaster@pnri.go.id
IPv6 address	*Not Present*	Reverse DNS	gw.pnri.go.id
Domain registrar	*unknown*	Nameserver organisation	*unknown*
Organisation	*unknown*	Hosting company	pnri.go.id
Top Level Domain	Indonesia (.go.id)	DNS Security Extensions	Enabled
Hosting country	ID		

⊟ Hosting History

Netblock owner	IP address	OS	Web server	Last seen Refresh
Perpustakaan Nasional RI Government / Direct Member IDNIC Jl. Salemba Raya No. 28A Jakarta Pusat, 10430	103.28.21.3	Linux	Apache/2.4.6 CentOS OpenSSL/1.0.2k-fips PHP/7.1.14	6-Mar-2018

Tampilan diatas merupakan hasil scanning yang menghasilkan data Network dan Hosting History (IP Address, Web Server, Waktu Terakhir di Update)

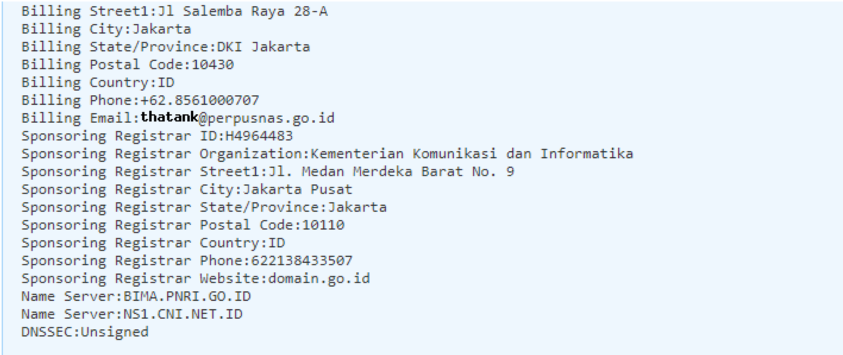
Who is



perpusnas.go.id

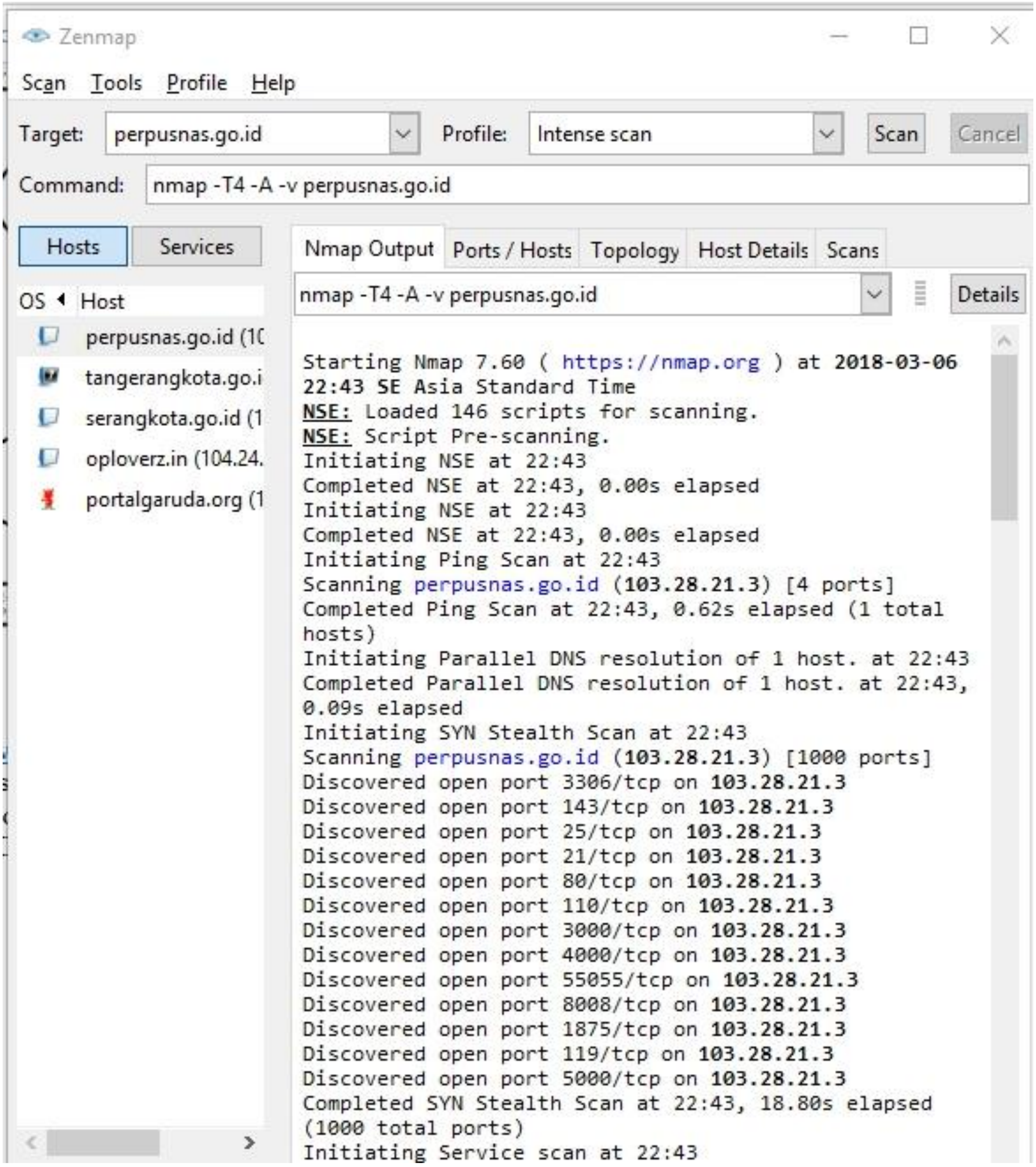
Updated 19 minutes ago

```
Domain ID:PANDI-DO285427
Domain Name:PERPUSNAS.GO.ID
Created On:27-Dec-2007 13:35:18 UTC
Last Updated On:17-Jun-2017 04:27:04 UTC
Expiration Date:03-Jan-2019 23:59:59 UTC
Status:ok
Registrant ID:wiratn-1278
Registrant Name:Wiratna Tritawirasta
Registrant Organization:Perpustakaan Nasional Republik Indonesia
Registrant Street1:Jl Salemba Raya 28-A
Registrant City:Jakarta
Registrant State/Province:DKI Jakarta
Registrant Postal Code:10430
Registrant Country:ID
Registrant Phone:+62.8561000707
Registrant Email:thatank@perpusnas.go.id
Admin ID:tatang-1276
Admin Name:Tatang D Tjahyanto
Admin Organization:Perpustakaan Nasional Republik Indonesia
Admin Street1:Jl Salemba Raya 28-A
Admin City:Jakarta
Admin State/Province:DKI Jakarta
Admin Postal Code:10430
Admin Country:ID
Admin Phone:+62.8561000707
Admin Email:thatank@perpusnas.go.id
Tech ID:tatang-1276
Tech Name:Tatang D Tjahyanto
Tech Organization:Perpustakaan Nasional Republik Indonesia
Tech Street1:Jl Salemba Raya 28-A
Tech City:Jakarta
Tech State/Province:DKI Jakarta
Tech Postal Code:10430
Tech Country:ID
Tech Phone:+62.8561000707
Tech Email:thatank@perpusnas.go.id
Billing ID:tatang-1276
Billing Name:Tatang D Tjahyanto
Billing Organization:Perpustakaan Nasional Republik Indonesia
```



```
Billing Street1:Jl Salemba Raya 28-A
Billing City:Jakarta
Billing State/Province:DKI Jakarta
Billing Postal Code:10430
Billing Country:ID
Billing Phone:+62.8561000707
Billing Email:thatank@perpusnas.go.id
Sponsoring Registrar ID:H4964483
Sponsoring Registrar Organization:Kementerian Komunikasi dan Informatika
Sponsoring Registrar Street1:Jl. Medan Merdeka Barat No. 9
Sponsoring Registrar City:Jakarta Pusat
Sponsoring Registrar State/Province:Jakarta
Sponsoring Registrar Postal Code:10110
Sponsoring Registrar Country:ID
Sponsoring Registrar Phone:622138433507
Sponsoring Registrar Website:domain.go.id
Name Server:BIMA.PNRI.GO.ID
Name Server:NS1.CNI.NET.ID
DNSSEC:Unsigned
```

Menggunakan Nmap



Target: perpusnas.go.id

Profile: Intense scan

Command: nmap -T4 -A -v perpusnas.go.id

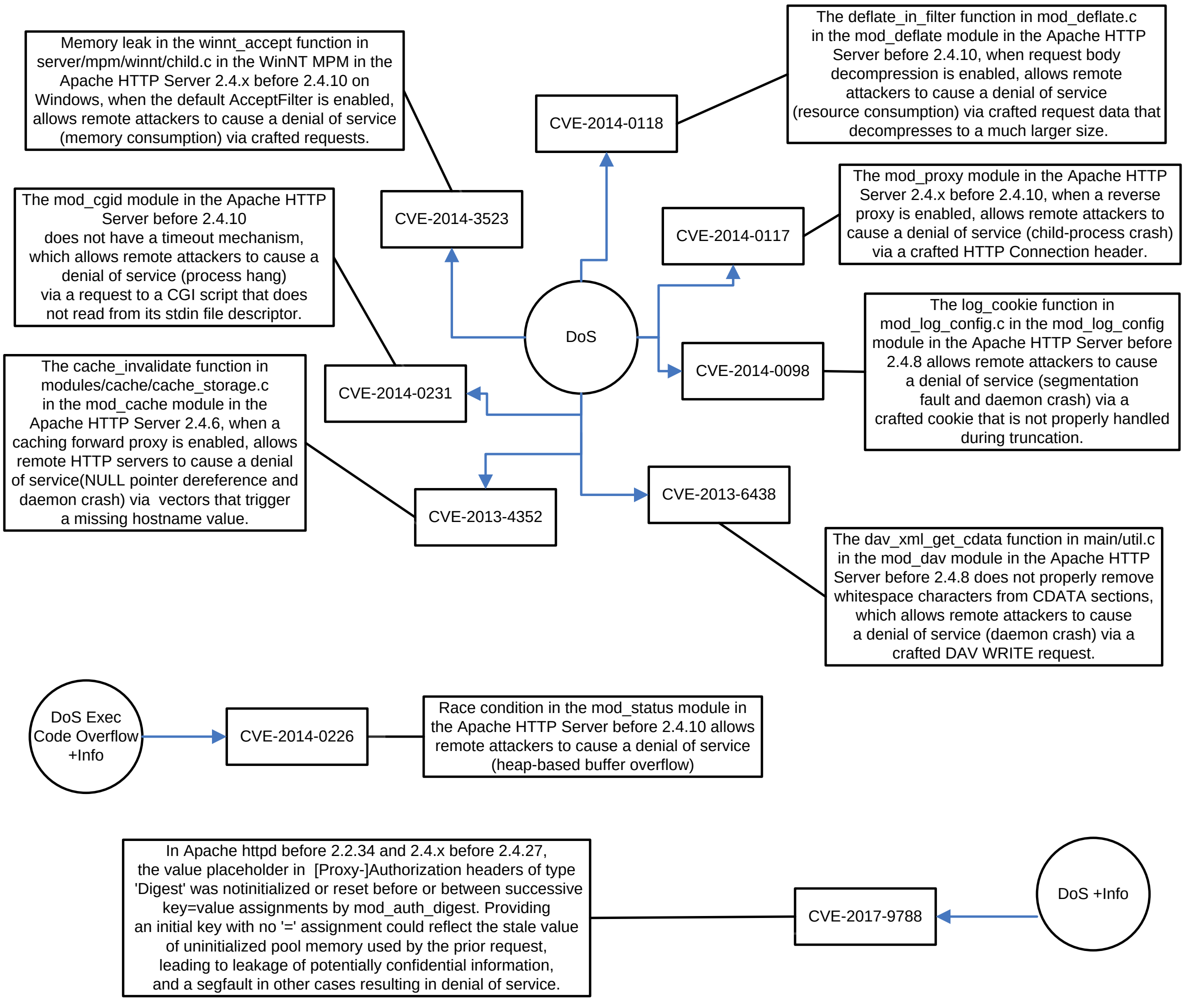
perpusnas.go.id (10
tangerangkota.go.i
serangkota.go.id (1
oploverz.in (104.24.
portalgaruda.org (1

nmap -T4 -A -v perpusnas.go.id

```
Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-06
22:43 SE Asia Standard Time
NSE: Loaded 146 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 22:43
Completed NSE at 22:43, 0.00s elapsed
Initiating NSE at 22:43
Completed NSE at 22:43, 0.00s elapsed
Initiating Ping Scan at 22:43
Scanning perpusnas.go.id (103.28.21.3) [4 ports]
Completed Ping Scan at 22:43, 0.62s elapsed (1 total
hosts)
Initiating Parallel DNS resolution of 1 host. at 22:43
Completed Parallel DNS resolution of 1 host. at 22:43,
0.09s elapsed
Initiating SYN Stealth Scan at 22:43
Scanning perpusnas.go.id (103.28.21.3) [1000 ports]
Discovered open port 3306/tcp on 103.28.21.3
Discovered open port 143/tcp on 103.28.21.3
Discovered open port 25/tcp on 103.28.21.3
Discovered open port 21/tcp on 103.28.21.3
Discovered open port 80/tcp on 103.28.21.3
Discovered open port 110/tcp on 103.28.21.3
Discovered open port 3000/tcp on 103.28.21.3
Discovered open port 4000/tcp on 103.28.21.3
Discovered open port 55055/tcp on 103.28.21.3
Discovered open port 8008/tcp on 103.28.21.3
Discovered open port 1875/tcp on 103.28.21.3
Discovered open port 119/tcp on 103.28.21.3
Discovered open port 5000/tcp on 103.28.21.3
Completed SYN Stealth Scan at 22:43, 18.80s elapsed
(1000 total ports)
Initiating Service scan at 22:43
```

Terdapat 4 port pada situs perpurnas.go.id

2. Vulnerability Assesment
   Berikut ini Vulnerability yang ada. Pencarian vurnability dilakukan pada https://www.cvedetails.com.
   Berikut ini beberapa Vulnerability yang ada pada Apache 2.4.6, terdapat 9 vurnability



Memory leak in the winnt_accept function in server/mpm/winnt/child.c in the WinNT MPM in the Apache HTTP Server 2.4.x before 2.4.10 on Windows, when the default AcceptFilter is enabled, allows remote attackers to cause a denial of service (memory consumption) via crafted requests.

The deflate_in_filter function in mod_deflate.c in the mod_deflate module in the Apache HTTP Server before 2.4.10, when request body decompression is enabled, allows remote attackers to cause a denial of service (resource consumption) via crafted request data that decompresses to a much larger size.

The mod_cgid module in the Apache HTTP Server before 2.4.10 does not have a timeout mechanism, which allows remote attackers to cause a denial of service (process hang) via a request to a CGI script that does not read from its stdin file descriptor.

The mod_proxy module in the Apache HTTP Server 2.4.x before 2.4.10, when a reverse proxy is enabled, allows remote attackers to cause a denial of service (child-process crash) via a crafted HTTP Connection header.

The log_cookie function in mod_log_config.c in the mod_log_config module in the Apache HTTP Server before 2.4.8 allows remote attackers to cause a denial of service (segmentation fault and daemon crash) via a crafted cookie that is not properly handled during truncation.

The cache_invalidate function in modules/cache/cache_storage.c in the mod_cache module in the Apache HTTP Server 2.4.6, when a caching forward proxy is enabled, allows remote HTTP servers to cause a denial of service(NULL pointer dereference and daemon crash) via vectors that trigger a missing hostname value.

The dav_xml_get_cdata function in main/util.c in the mod_dav module in the Apache HTTP Server before 2.4.8 does not properly remove whitespace characters from CDATA sections, which allows remote attackers to cause a denial of service (daemon crash) via a crafted DAV WRITE request.

Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow)

In Apache httpd before 2.2.34 and 2.4.x before 2.4.27, the value placeholder in [Proxy-]Authorization headers of type 'Digest' was notinitialized or reset before or between successive key=value assignments by mod_auth_digest. Providing an initial key with no '=' assignment could reflect the stale value of uninitialized pool memory used by the prior request, leading to leakage of potentially confidential information, and a segfault in other cases resulting in denial of service.

Pada Apache 2.4.6 ini dari 9 vurnability yang ada, memiliki tingkat kompleksitas low dan medium tidak ada high (6 low dan 3 medium).