LAPORAN

SECURITY ASSESSMENT

DNS SERVER

KEMENTERIAN KOMUNIKASI DAN INFORMATIKA

KOMINFO.GO.ID

2020-RELEASED

Oleh:

Tim Pondok Siber

Keterangan Dokumen

Title	*Security Assessment DNS Server*
Version	*2020-RELEASED*
Author	*Tim Pondok Siber*
Auditor	*Muhammad Ilyas*
Reviewed By	*Aiman Alauddin*
Approved By	
Document Classification	***Confidential/Sangat Rahasia***

Catatan Revisi

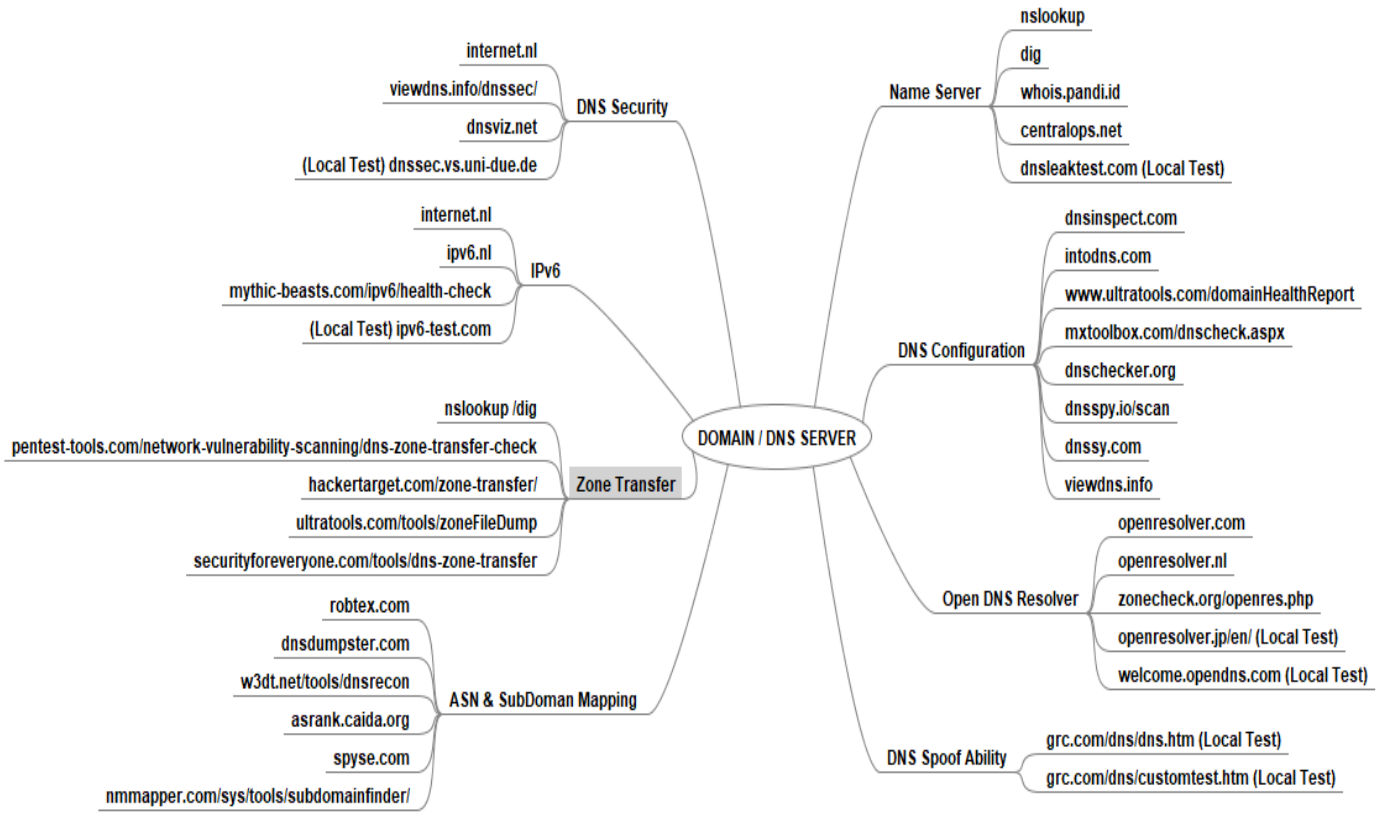
Version	***Date***	***Author***	***Description***

Daftar Isi

A. Executive Summary

Tim Indeks Kerentanan Internet Domain Indonesia (KIDI) telah melakukan Penilaian terhadap konfigurasi dasar DNS Server pada domain kominfo.go.id sesuai dengan standar Internet Engineering Task Force (IETF) RFC 1035 https://www.ietf.org/rfc/rfc1035.txt

Berikut adalah bagan proses pengujian DNS Server dengan menggunakan INDONESE Assessment Framework 2020-RELEASED



Hasil Penilaian		
No	**Kondisi eksisting Konfigurasi DNS Server**	**Hasil**
1	Name Server	✓
2	DNS Configuration	✓
3	DNS Security Test	✓
4	IPv6 Test	✗
5	Open DNS Resolver Test	✓
6	Zone Transfer DNS Server Test	✓
7	AS Number & Sub-Domain Mapping	✓ ✗
8	DNS Spoofability Test (Optional) – Tidak dilakukan pengujian	-

Keterangan :

✓ : Konfigurasi sudah bersesuaian dengan best practice

✗ : Terdapat ketidaksesuaian konfigurasi

Medan, 31 Desember 2021

Aiman Alauddin
Team Leader

B. Proses Audit Domain dan DNS Server

B.1. Name Server		
Tujuan : Untuk mengetahui informasi umum tentang Name Server pada domain kominfo.go.id , antara lain : • Name Server dan DNS Record • Grafik Route Domain		
Tools : http://centralops.net/ dan https://www.robtex.com/		
Hasil Penilaian dan Rekomendasi		
No	**Kondisi eksisting DNS dan Infrastruktur**	**Hasil**
2	Terdapat 2 atau lebih Name Server yang bersesuaian dengan domain dan atau Memiliki Backup Name Server pada network atau domain berbeda.	✓
	Rekomendasi :	
CVSS:3.0/		
Referensi: RFC 2182		

Keterangan :

✓ : Konfigurasi sudah bersesuaian dengan best practice

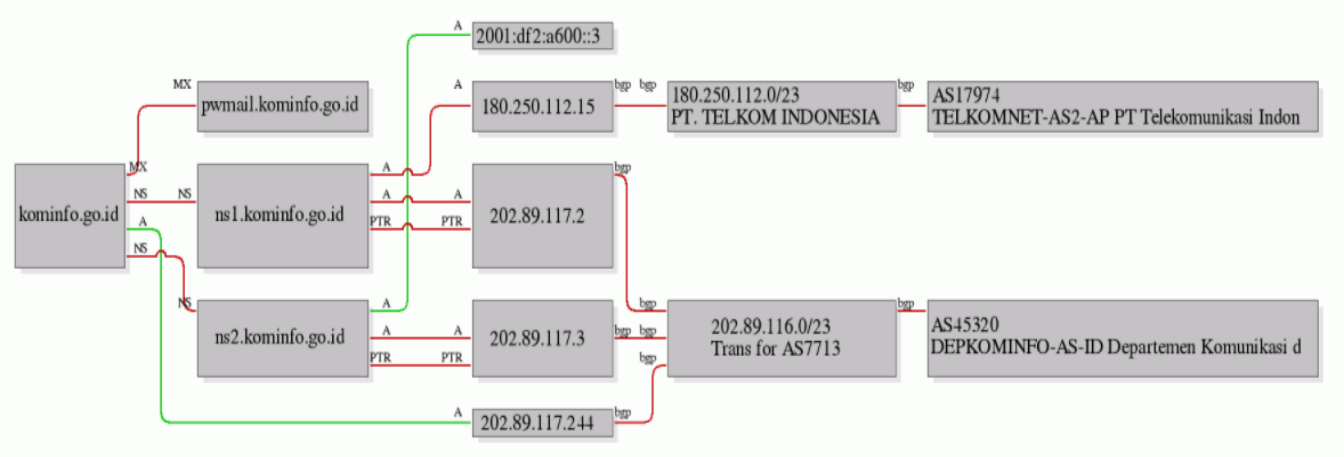
✗ : Terdapat ketidaksesuaian konfigurasi

Proses Pengujian :

1. ***https://centralops.net***

kominfo.go.id	IN	NS	ns1.kominfo.go.id	3600s (01:00:00)
kominfo.go.id	IN	NS	ns2.kominfo.go.id	3600s (01:00:00)
117.89.202.in-addr.arpa	IN	NS	ns2.kominfo.go.id	0s (00:00:00)
117.89.202.in-addr.arpa	IN	NS	ns5.kominfo.go.id	0s (00:00:00)
117.89.202.in-addr.arpa	IN	NS	ns7.kominfo.go.id	0s (00:00:00)

2. https://www.robtex.com/



B.2. DNS Configuration		
Tujuan : Untuk mengetahui dan menilai sejauh mana penerapan konfigurasi DNS Server dan implementasinya pada domain kominfo.go.id sesuai dengan standar Internet Engineering Task Force (IETF) RFC 1035 https://www.ietf.org/rfc/rfc1035.txt		
Tools : http://www.dnsinspect.com/		
Hasil Penilaian dan Rekomendasi		
No	**Konfigurasi yang tidak bersesuaian**	**Hasil**
1	mengalokasikan lebih dari satu ASN (Referensi: RFC 2182)	✓
CVSS:3.0/		

Keterangan :

✓ : Konfigurasi sudah bersesuaian dengan best practice

✗ : Terdapat ketidaksesuaian konfigurasi

Proses Pengujian :

1. http://dnsinspect.com

Input domain name ... Run Report »

Report created on: Fri, 31 Dec 2021 07:01:45 GMT

Share this report: | permalink

Parent	100
NS	100
SOA	88
MX	100
Mail	100
Web	100

A

PARENT

NS Records at Parent Servers

We have successfully fetched domain's NS records from parent name server (*b.dns.id.*).
Domain NS records:

- `ns1.kominfo.go.id. TTL=3600 [180.250.112.15] [NO GLUE6]`
- `ns2.kominfo.go.id. TTL=3600 [202.89.117.3] [NO GLUE6]`

Name Servers Distributed on Multiple ASNs

OK. Name servers are dispersed on 2 different Autonomous Systems:

- **AS7713:**
  - *ns1.kominfo.go.id.*
- **AS45320:**
  - *ns2.kominfo.go.id.*

Name servers should be dispersed (topologically and geographically) across the Internet to avoid risk of single point of failure (RFC 2182).

B.3. DNS Security Test		
Tujuan : Untuk mengetahui apakah DNS Server yang digunakan sudah menerapkan DNS Security.		
Tools : https://internet.nl, http://dnsviz.net, https://dnssec-debugger.verisignlabs.com		
Hasil Penilaian dan Rekomendasi		
No	**Konfigurasi yang tidak bersesuaian**	**Hasil**
1	**DNSSEC signed**	✓
2	**DNSSEC validity**	✓
Rekomendasi :		
CVSS:3.0/		

Keterangan :

✓ : Konfigurasi sudah bersesuaian dengan best practice

✗ : Terdapat ketidaksesuaian konfigurasi

Proses Pengujian :

1. https://internet.nl/

DNSSEC existence

Verdict:
Your domain is DNSSEC signed.

Technical details:

Domain	Registrar
kominfo.go.id	None

Test explanation:
We check if your domain, more specifically its SOA record, is DNSSEC signed.

If a domain redirects to another domain via `CNAME`, then we also check if the CNAME domain is signed (which is conformant with the DNSSEC standard). If the CNAME domain is not signed, the result of this subtest will be negative.

Note: the validity of the signature is not part of this subtest, but part of the next subtest.

DNSSEC validity

Verdict:
Your domain is secure, because its DNSSEC signature is valid.

Technical details:

Domain	Status
kominfo.go.id	secure

Test explanation:
We check if your domain, more specifically its SOA record, is signed with a valid signature making it 'secure'.

If a domain redirects to another signed domain via `CNAME`, then we also check if the signature of the CNAME domain is valid (which is conformant with the DNSSEC standard). If the signature of the CNAME domain is not valid, the result of this subtest will be negative.

B.4. Ipv6 Test		
Tujuan : Untuk mengetahui apakah DNS Server yang digunakan pada domain kominfo.go.id sudah menerapkan Ipv6.		
Tools : https://internet.nl		
Hasil Penilaian dan Rekomendasi		
No	**Konfigurasi yang tidak bersesuaian**	**Hasil**
1	**IPv6 addresses for name servers**	✗
2	**IPv6 reachability of name servers**	✗
Rekomendasi : mengimplementasikan penggunaan IPv6 pada name server		
CVSS:3.0/		

Keterangan :

✓ : Konfigurasi sudah bersesuaian dengan best practice

✗ : Terdapat ketidaksesuaian konfigurasi

Proses Pengujian :

1. https://internet.nl/

Name servers

IPv6 addresses for name servers

Verdict:
None of the name servers of your domain has an IPv6 address.

Technical details:

Name server	IPv6 address	IPv4 address
ns2.kominfo.go.id.	None	202.89.117.3
ns1.kominfo.go.id.	None	180.250.112.15

Test explanation:
We check if your domain name has at least two name servers with an IPv6 address. This is consistent with the "Technical requirements for the registration and use of .nl domain names" d.d. 13 November 2017 by SIDN (.nl TLD registry) that require each .nl domain to have at least two name servers.

IPv6 reachability of name servers

Verdict:
This subtest did not run, because either a parent test that this subtest depends on gave a negative result, or not enough information was available to run this subtest.

Test explanation:
We check if all name servers, that have an AAAA record with IPv6 address, are reachable over IPv6.

B.5. Open DNS Resolver Test		
Tujuan : Untuk mengetahui apakah DNS Server yang digunakan pada domain kominfo.go.id memiliki konfigurasi “Open DNS” Referensi : https://www.us-cert.gov/ncas/alerts/TA13-088A		
Tools : http://openresolver.com/		
Hasil Penilaian dan Rekomendasi		
No	**Name Server Open DNS**	**Hasil**
1	180.250.112.15	✓
2	202.89.117.3	✓
Rekomendasi :		
CVSS:3.0/		

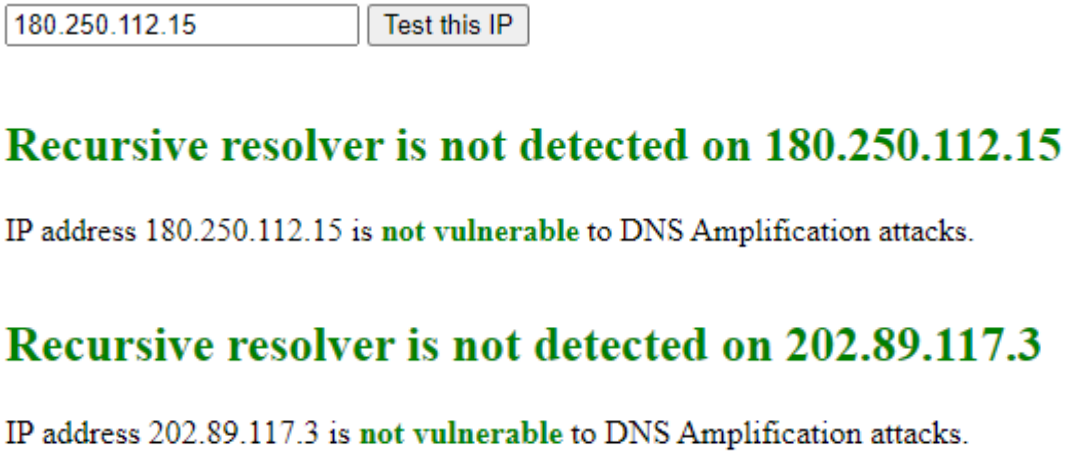
Keterangan :

✓ : Konfigurasi sudah bersesuaian dengan best practice

✗ : Terdapat ketidaksesuaian konfigurasi

Proses Pengujian :

1. http://openresolver.com/



B.6. Zone Transfer DNS Server (Domain Enumeration) Test

Tujuan :

Untuk mengetahui apakah zone transfer atau zone data atau zone file pada Authoritative DNS Server domain kominfo.go.id dapat ditampilkan.

Referensi :

https://en.wikipedia.org/wiki/DNS_zone_transfer

http://www.exploit-db.com/download_pdf/13687/

Tools : nslookup, dig, https://hackertarget.com/zone-transfer/

Hasil Penilaian dan Rekomendasi

No	Name Server yang rentan	Hasil
1.	180.250.112.15	✓
2.	202.89.117.3	✓

Rekomendasi :

CVSS:3.0/

Keterangan :

✓ : Konfigurasi sudah bersesuaian dengan best practice

✗ : Terdapat ketidaksesuaian konfigurasi

Proses Pengujian :

1. https://hackertarget.com/zone-transfer/

Online Test of a **zone transfer** that will attempt to get all DNS records for a target domain. The zone transfer will be tested against all name servers (NS) for a domain.

kominfo.go.id

```
; <<>> DiG 9.10.3-P4-Debian <<>> axfr @ns1.kominfo.go.id kominfo.go.id
; (1 server found)
;; global options: +cmd
; Transfer failed.


; <<>> DiG 9.10.3-P4-Debian <<>> axfr @ns2.kominfo.go.id kominfo.go.id
; (1 server found)
;; global options: +cmd
; Transfer failed.
```

B.7. AS Number & Sub-Domain Mapping		
Tujuan : Untuk mengetahui informasi AS Number dan penggunaan Backup Network pada domain.		
Tools : robtex.com, dnsdumpster.com,		
Hasil Penilaian dan Rekomendasi		
No	**Kondisi eksisting DNS dan Infrastruktur**	**Hasil**
1	Terdapat 2 atau lebih ASN dan Name Server berada pada subnet (ASNs) yang berbeda.	✔
	Temuan 1 :	
	Rekomendasi :	
2	Terdapat informasi host atau sub-domain dengan IP Private	✘
	Temuan 1 :	
	Rekomendasi :	
CVSS:3.0/