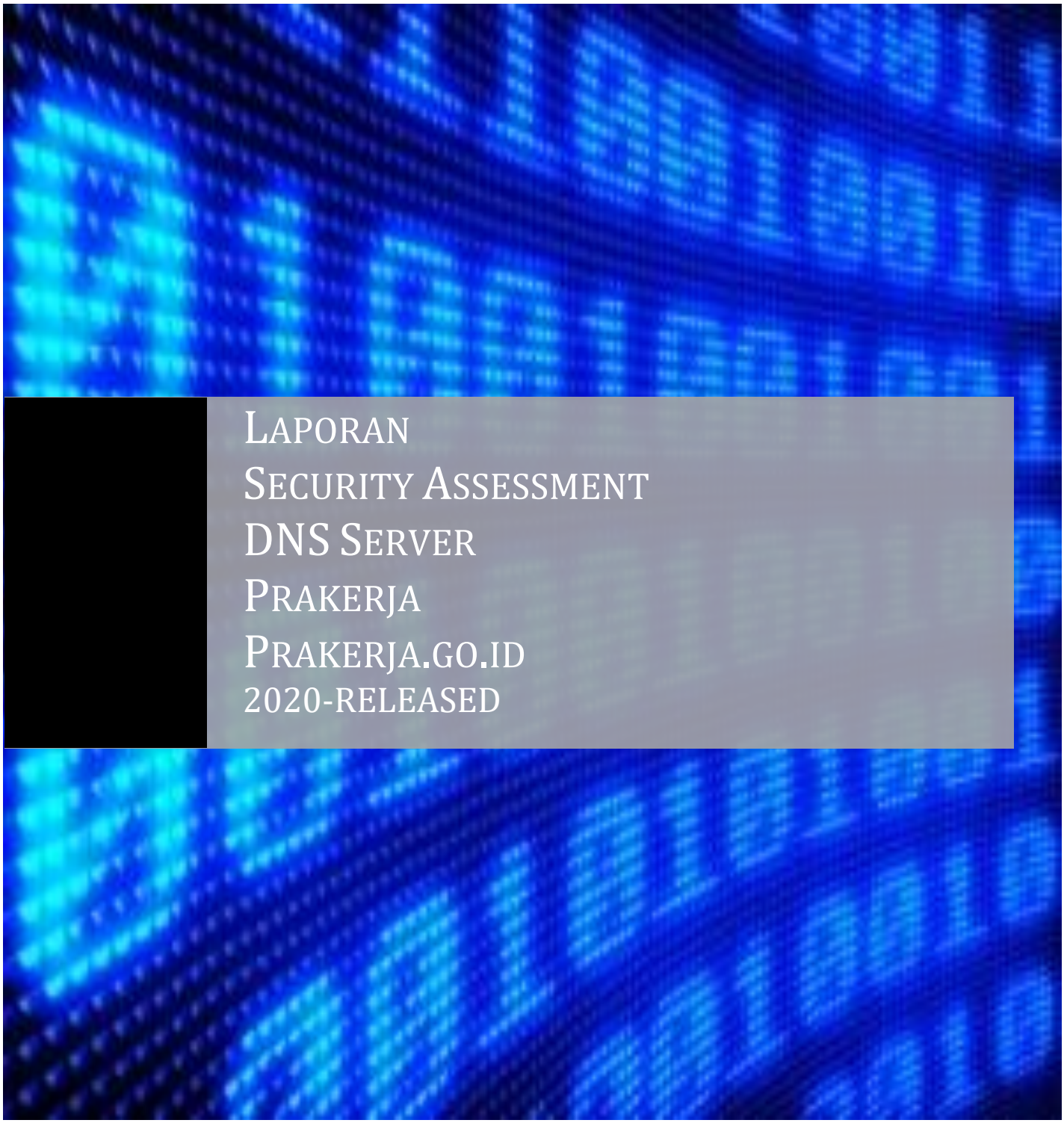


LAPORAN
SECURITY ASSESSMENT
DNS SERVER
PRAKERJA
PRAKERJA.GO.ID
2020-RELEASED

Oleh:

Tim Pondok Siber

Keterangan Dokumen

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

Catatan Revisi

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

Daftar Isi

A. *Executive Summary* 4

B. Proses Security Assessment DNS Server 6

B.1. Name Server 6

B.2. DNS Configuration 8

B.3. DNS Security 9

B.4. IPv6 10

B.5. Open DNS Resolver 11

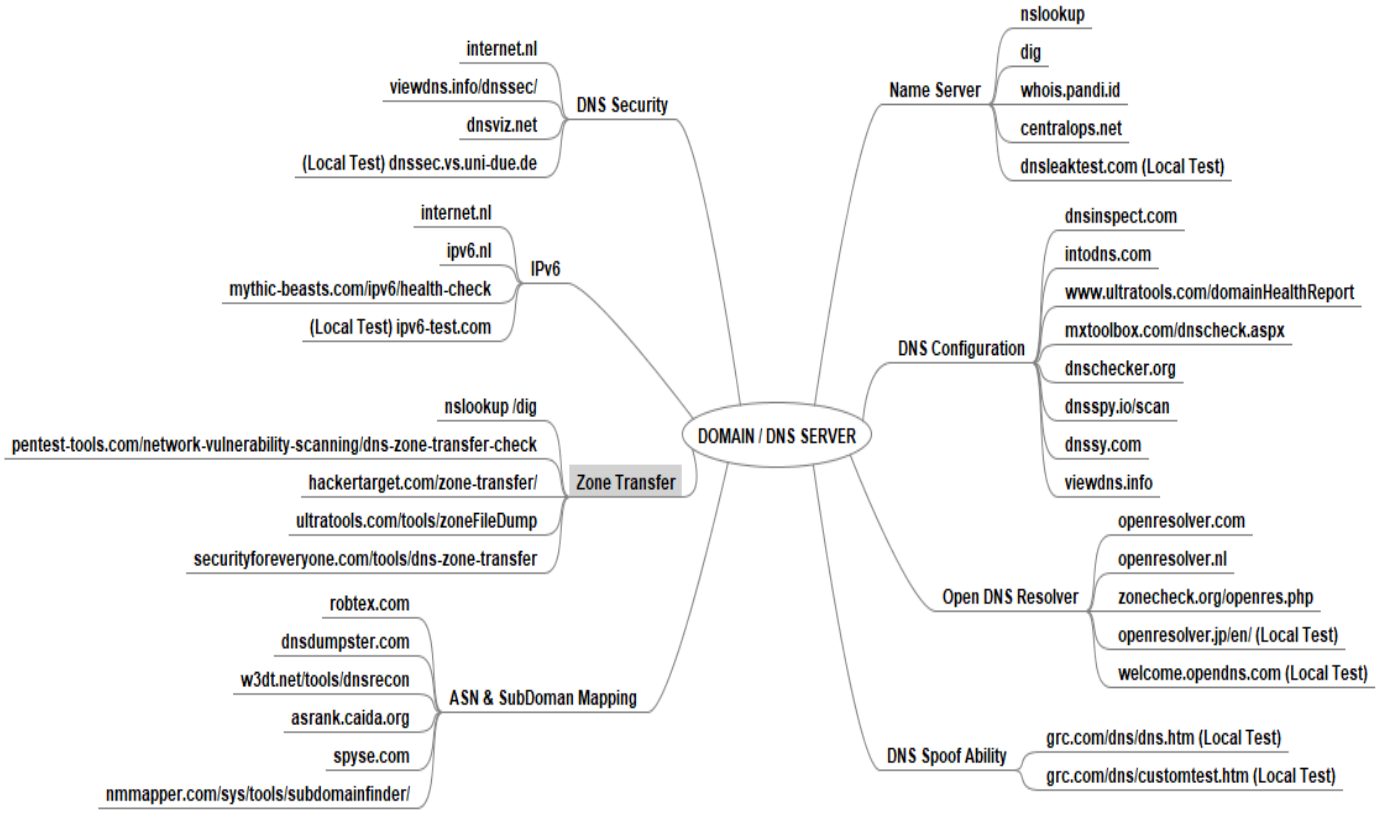
B.6. Zone Transfer 12

B.7. AS Number & Sub-Domain 13

A. Executive Summary

Tim Indeks Kerentanan Internet Domain Indonesia (KIDI) telah melakukan Penilaian terhadap konfigurasi dasar DNS Server pada domain prakerja.go.id sesuai dengan 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

Bandung, 25 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 prakerja.go.id , antara lain : • Tanggal dibuat, expire dan update domain terakhir, • Registrant Contact/Admin Contact/Technical Contact/Billing Contact, Registrar. • 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**
1	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 :

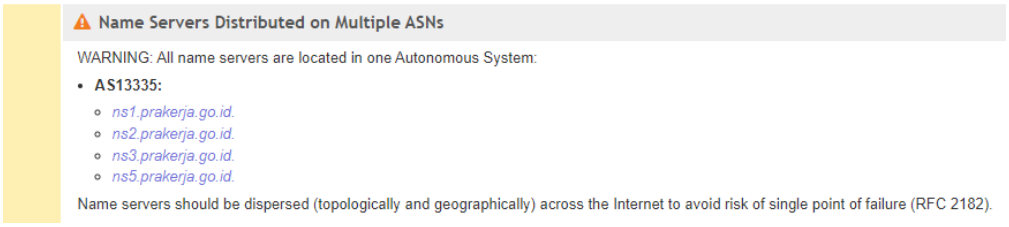
✓ : Konfigurasi sudah bersesuaian dengan best practice

✗ : Terdapat ketidaksesuaian konfigurasi

Proses Pengujian :

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

prakerja.go.id	IN	NS	ns2.prakerja.go.id	86400s (1.00:00:00)
prakerja.go.id	IN	NS	ns3.prakerja.go.id	86400s (1.00:00:00)
prakerja.go.id	IN	NS	ns5.prakerja.go.id	86400s (1.00:00:00)
prakerja.go.id	IN	NS	ns1.prakerja.go.id	86400s (1.00:00:00)
213.58.22.104.in-addr.arpa	IN	HINFO	CPU: RFC8482 OS:	3789s (01:03:09)
22.104.in-addr.arpa	IN	NS	cruz.ns.cloudflare.com	25773s (07:09:33)
22.104.in-addr.arpa	IN	NS	kevin.ns.cloudflare.com	25773s (07:09:33)
5.d.a.3.6.1.8.6.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.0.7.4.6.0.6.2.ip6.arpa	IN	HINFO	CPU: RFC8482 OS:	3789s (01:03:09)
0.0.7.4.6.0.6.2.ip6.arpa	IN	NS	micah.ns.cloudflare.com	5337s (01:28:57)
0.0.7.4.6.0.6.2.ip6.arpa	IN	NS	leah.ns.cloudflare.com	5337s (01:28:57)

B.2. DNS Configuration		
Tujuan : Untuk mengetahui dan menilai sejauh mana penerapan konfigurasi DNS Server dan implementasinya pada domain prakerja.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	Temuan 1 :  	✗
	Rekomendasi : 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**

PARENT

NS Records at Parent Servers

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

- `ethan.ns.cloudflare.com. TTL=3600 [NO GLUE4] [NO GLUE6]`
- `meg.ns.cloudflare.com. TTL=3600 [NO GLUE4] [NO GLUE6]`

Name Servers Distributed on Multiple ASNs

WARNING: All name servers are located in one Autonomous System:

- **AS13335:**
  - *ns1.prakerja.go.id.*
  - *ns2.prakerja.go.id.*
  - *ns3.prakerja.go.id.*
  - *ns5.prakerja.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 : Domain tidak aman, karena karna harus ada tanda tangan DNSSEC.		
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 insecure, because it is *not* DNSSEC signed.

Technical details:

Domain	Registrar
prakerja.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:
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.

Technical details:

Domain	Status
prakerja.go.id	insecure

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 prakerja.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 : -		
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:
Two or more name servers of your domain have an IPv6 address.

Technical details:

Name server	IPv6 address	IPv4 address
ns1.prakerja.go.id.	2400:cb00:2049:1::a29f:8d2	162.159.8.210
ns2.prakerja.go.id.	2400:cb00:2049:1::a29f:99d	162.159.9.157
ns3.prakerja.go.id.	2400:cb00:2049:1::a29f:af9	162.159.10.249
ns5.prakerja.go.id.	2400:cb00:2049:1::a29f:bbb	162.159.11.187

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:
All name servers that have an IPv6 address are reachable over IPv6.

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 prakerja.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	162.159.8.210	✗
2	162.159.9.157	✗
3	162.159.10.249	✗
4	162.159.11.187	✗
Rekomendasi :		
CVSS:3.0/		

Keterangan :

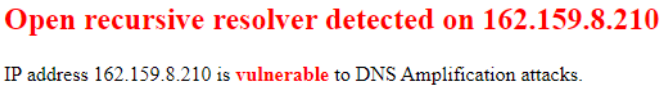
✓ : Konfigurasi sudah bersesuaian dengan best practice

✗ : Terdapat ketidaksesuaian konfigurasi

Proses Pengujian :

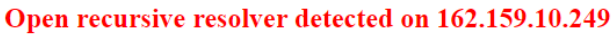
1. **http://openresolver.com/**

proses pengujian :

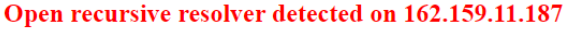


IP address 162.159.8.210 is **vulnerable** to DNS Amplification attacks.

IP address 162.159.9.157 is **vulnerable** to DNS Amplification attacks.



IP address 162.159.10.249 is **vulnerable** to DNS Amplification attacks.



IP address 162.159.11.187 is **vulnerable** to DNS Amplification attacks.

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 prakerja.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.	162.159.8.210	✗
2.	162.159.9.157	✗
3	162.159.10.249	✗
4	162.159.11.187	✗
Rekomendasi :		
CVSS:3.0/		

Keterangan :

✓ : Konfigurasi sudah bersesuaian dengan best practice

✗ : Terdapat ketidaksesuaian konfigurasi

Proses Pengujian :

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

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 : mengalokasikan lebih dari satu ASN (Referensi: RFC 2182)	
2	Terdapat informasi host atau sub-domain dengan IP Private	✗
	Temuan 1 :	
	Rekomendasi :	
CVSS:3.0/		

Keterangan :

✓ : Konfigurasi sudah bersesuaian dengan best practice

✗ : Terdapat ketidaksesuaian konfigurasi

⚠ Name Servers Distributed on Multiple ASNs

WARNING: All name servers are located in one Autonomous System:

- **AS13335:**
  - *ns1.prakerja.go.id.*
  - *ns2.prakerja.go.id.*
  - *ns3.prakerja.go.id.*
  - *ns5.prakerja.go.id.*

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