Oleh:

Rizky Fauzi – Santri Pondok siber Bandung

Keterangan Dokumen

Title	*Security Assessment DNS Server*
Version	*2021-RELEASED*
Author	*Pondok Siber bandung*
Auditor	*Rizky Fauzi*
Reviewed By	*Aiman Alauddin*
Approved By	
Document Classification	***Confidential/Sangat Rahasia***

Catatan Revisi

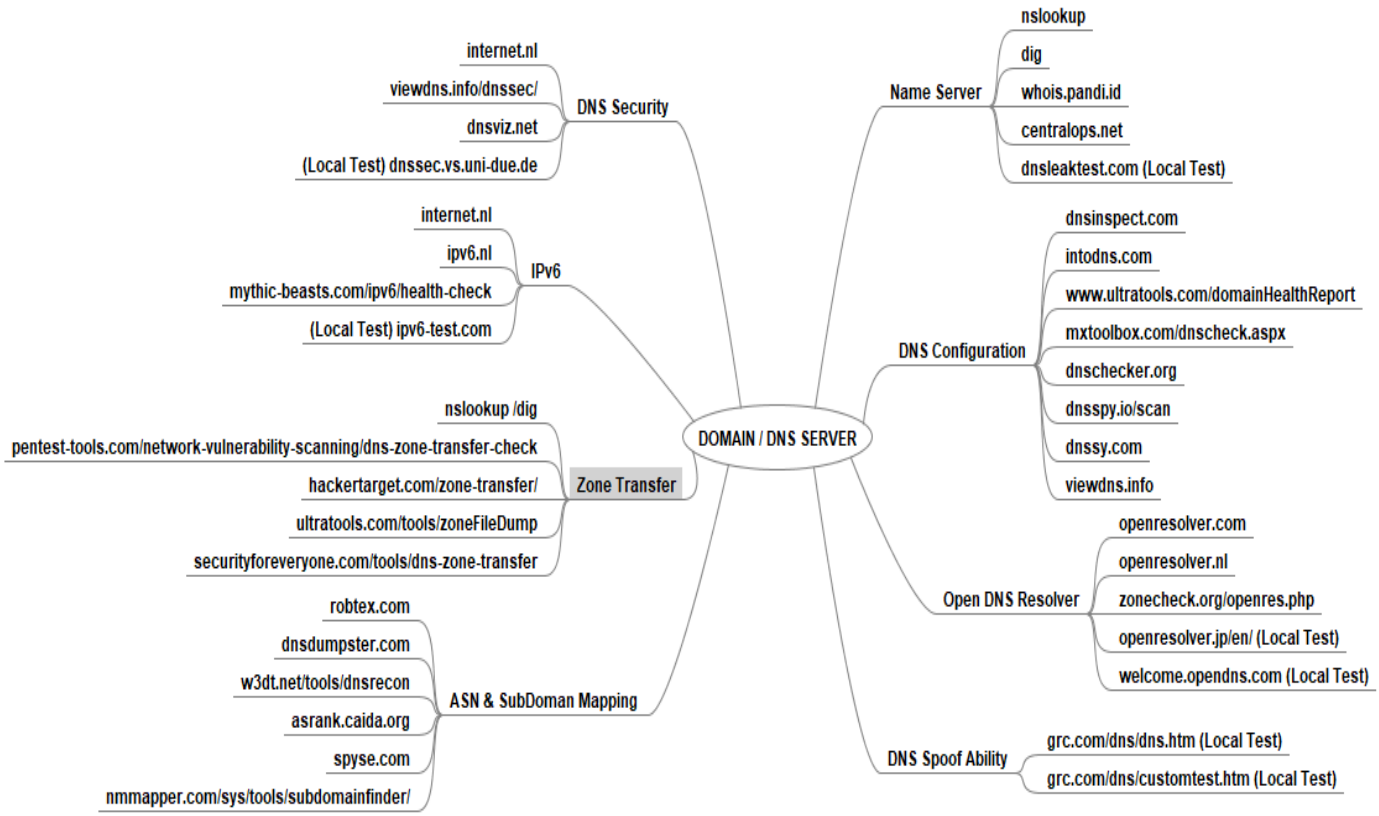
Version	***Date***	***Author***	***Description***

Daftar Isi

A. Executive Summary

Tim Indeks Pondok Siber telah melakukan Penilaian terhadap konfigurasi dasar DNS Server pada domain perpusnas.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	AS Number & Sub-Domain Mapping	✗
7	DNS Spoofability Test (Optional) – Tidak dilakukan pengujian	-

Keterangan :

✓ : Konfigurasi sudah bersesuaian dengan best practice

✗ : Terdapat ketidaksesuaian konfigurasi

Cianjur, 31 Desember 2021

Rizky Fauzi
Santri pondok siber Bandung

B. Proses Audit Domain dan DNS Server

B.1. Name Server		
Tujuan : Untuk mengetahui informasi umum tentang Name Server pada domain perpusnas.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**
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***

```
perpusnas.go.id     IN    NS    bima.pnri.go.id                    86400s  (1.00:00:00)
perpusnas.go.id     IN    NS    ns2.perpusnas.go.id                86400s  (1.00:00:00)
```

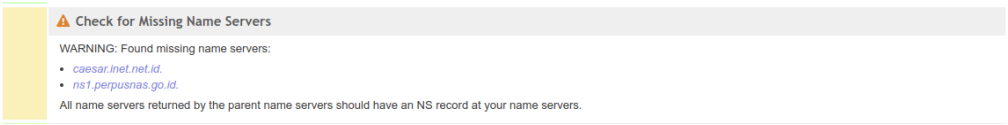
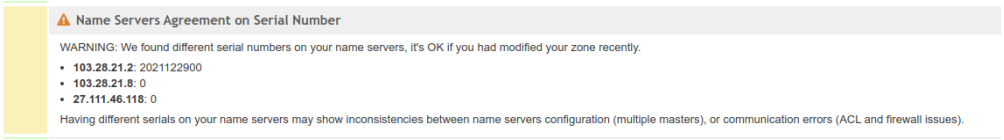
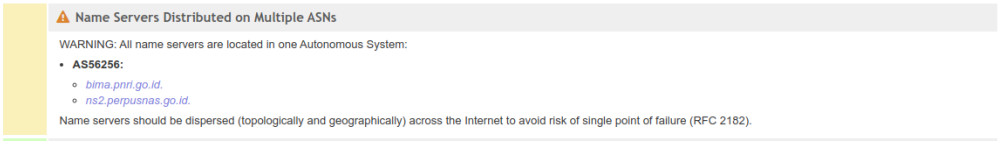
B.2. DNS Configuration

Tujuan :

Untuk mengetahui dan menilai sejauh mana penerapan konfigurasi DNS Server dan implementasinya pada domain perpusnas.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 : 	✗
2	Temuan 2 : 	✗
3	Temuan 3 : 	✗

CVSS:3.0/

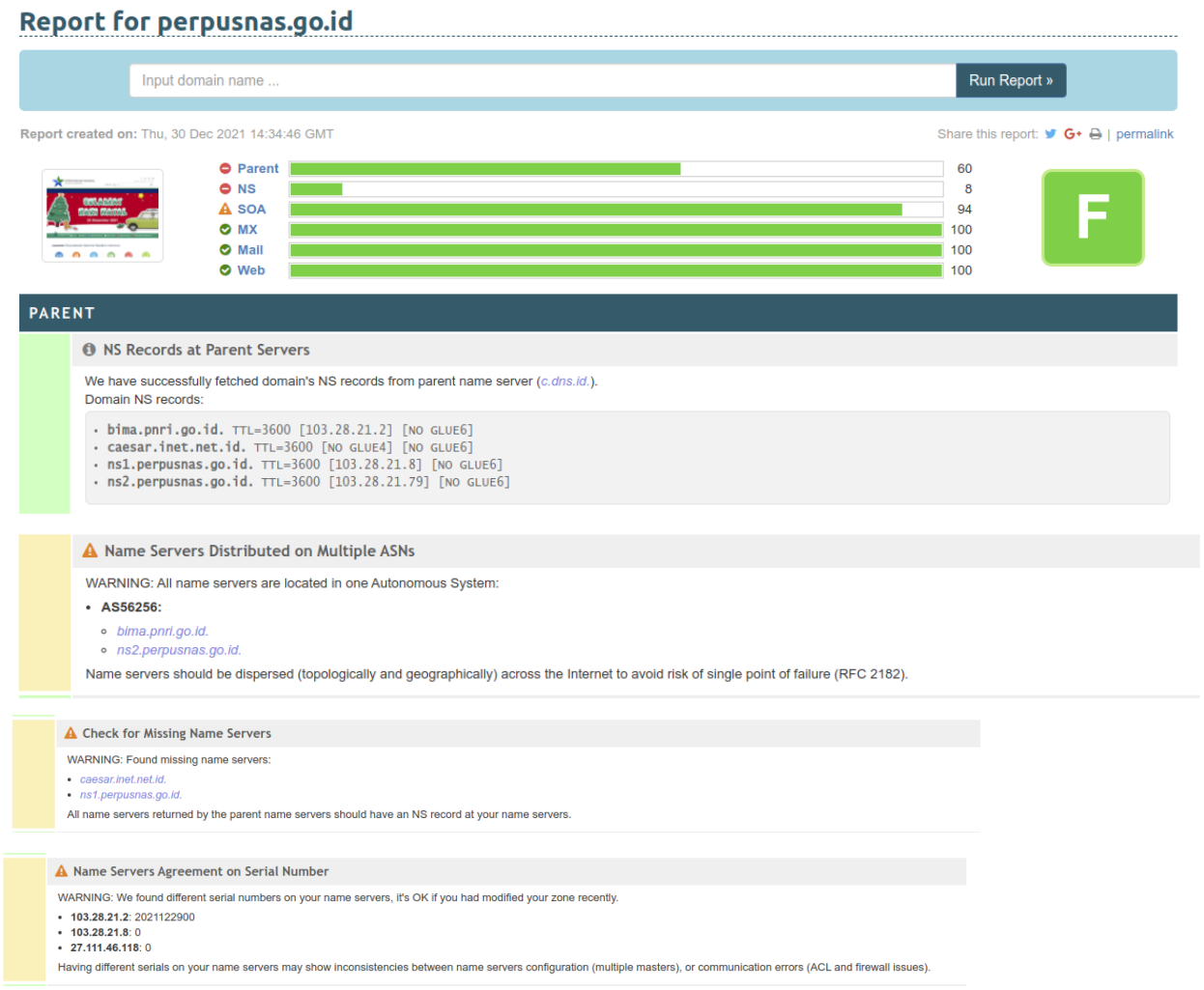
Keterangan :

: Konfigurasi sudah bersesuaian dengan best practice

: Terdapat ketidaksesuaian konfigurasi

Proses Pengujian :

1. http://dnsinspect.com



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 insecure, because it is *not* DNSSEC signed.

Technical details:

Domain	Registrar
www.perpusnas.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
www.perpusnas.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 perpusnas.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
bima.pnri.go.id.	None	103.28.21.2
ns2.perpusnas.go.id.	None	103.28.21.8

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.

Web server

IPv6 addresses for web server

Verdict:
None of your web servers has an IPv6 address.

Technical details:

Web server	IPv6 address	IPv4 address
www.perpusnas.go.id	None	103.28.21.59

Test explanation:
We check if there is at least one AAAA record with IPv6 address for your web server.

B.5. Open DNS Resolver Test		
Tujuan : Untuk mengetahui apakah DNS Server yang digunakan pada domain perpusnas.go.id memiliki konfigurasi “Open DNS” Referensi : • https://www.us-cert.gov/ncas/alerts/TA13-088A • CVE-2010-0382		
Tools : http://openresolver.com/		
Hasil Penilaian dan Rekomendasi		
No	**Name Server Open DNS**	**Hasil**
1	103.28.21.2	✓
2	103.28.21.8	✓
Rekomendasi :		
CVSS:3.0/		

Keterangan :

✓ : Konfigurasi sudah bersesuaian dengan best practice

✗ : Terdapat ketidaksesuaian konfigurasi

Proses Pengujian :

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

Or, use a form:

103.28.21.2 Test this IP

Recursive resolver is not detected on 103.28.21.2

IP address 103.28.21.2 is **not vulnerable** to DNS Amplification attacks.

Or, use a form:

103.28.21.8 Test this IP

Recursive resolver is not detected on 103.28.21.8

IP address 103.28.21.8 is **not vulnerable** to DNS Amplification attacks.

B.6. AS Number & Sub-Domain Mapping		
Tujuan : Untuk mengetahui informasi AS Number dan penggunaan Backup Network pada domain. Referensi: • RFC 2182		
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:

- **AS38764:**
  - *ns1.polri.go.id.*
  - *ns2.polri.go.id.*
  - *ns5.polri.go.id.*
  - *ns7.polri.go.id.*
  - *ns8.polri.go.id.*

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