INDONESE FRAMEWORK REBORN

Cyber Jawara Workshop 2021

Aiman Alauddin Fadhlullah A.F

17/07/2023

Whoami

Aiman Alauddin F Al-Fatih

Pendidikan:

S1 Sistem Informasi STMIK AMIK Bandung

D2 I'dad Lughawi LIPIA Jakarta

TOT Pemantapan nilai-nilai kebangsaan LEMHANNAS RI 2022 angkatan III

Sertifikasi:

C|EH MASTER

C|EH

C|EH Practical

ICSI CNSS

CEI

Pentest+

CySA+

Pengalaman Bekerja:

- Konsultan Pentest Swasta
- Pondok Pesantren Siber Bandung
- Badan Siber dan Sandi Negara
- Id-SIRTII/CC

Pengalaman Mengajar/Mentoring:

- Kopassus
- Kemenkumham RI
- DiskominfoTIK DKI
- Cyber Defence Kemhan RI
- Kemenkeu RI
- Owasp Jakarta Chapter
- KAIROS South Korea
- Cyber Defence TNI-AU
- Telkom Prima Cipta Certifia
- EC-COUNCIL C|EH
- JICA - Universitas Indonesia CSIRT Course
- PT.Xirka Darma Persada
- Pusdiklat BSSN

Mengapa Menggunakan INDONESE FRAMEWORK ?

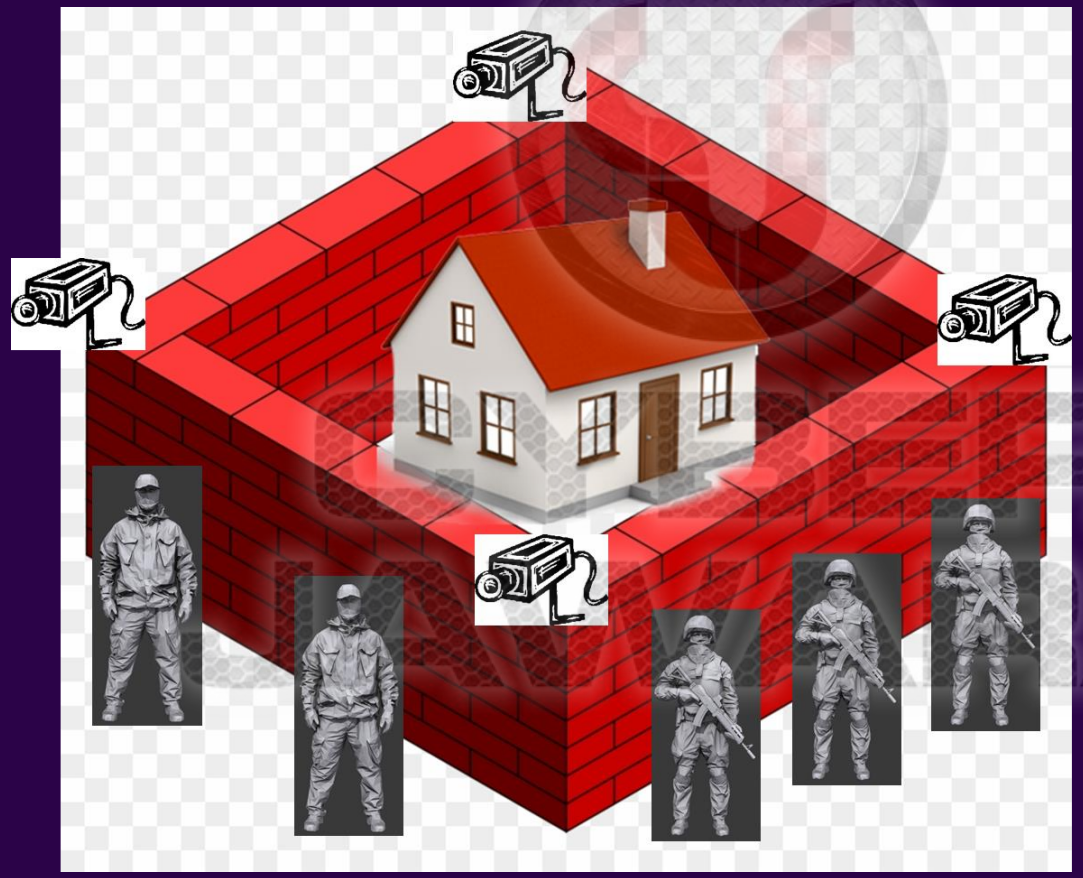
INDONESE FRAMEWORK

- Framework penilaian postur keamanan/security assessment
- Tidak memerlukan izin kepada pemilik asset aplikasi berbasis internet
- Mempermudah Penilaian postur keamanan dengan struktur yang disediakan suatu framework
- Teknis penilaian menggunakan metode dan tools yang biasa digunakan juga oleh Hacker
- Instruksi yang mendetail dan mudah digunakan
- Framework ini menyediakan cara termudah dalam teknis penilaian
  - Tidak perlu instalasi tools hacking
  - Hampir sama sekali tidak berinteraksi langsung dengan target penilaian
- Maintained by community (terbuka untuk berbagai masukan)

INternet DOmain & NEtwork Security

- Dirancang tahun 2014
- Creator Iwan Sumantri (eks Wakil Ketua Id-SIRTII bid Riset)
- Maintainer Komunitas IT Security
  - NCSD
  - Pondok Siber Bandung
- 4 versi perubahan sampai dengan 2023
  - Indeks KDI, Indeks KIDI, 2020 Released dan Reborn 2023

Gambaran bagaimana INDONESE bekerja



Acuan penilaian INDONESE dalam aktivitas Security Assessment

1. Checklist INDONESE FRAMEWORK
2. IETF
   a) IETF RFC 1035 (https://www.ietf.org/rfc/rfc1035.txt)
   b) IETF RFC 2821 (https://tools.ietf.org/html/rfc2821)
   c) IETF RFC 2616

Hasil pengerjaan INDONESE dalam aktivitas Security Assessment

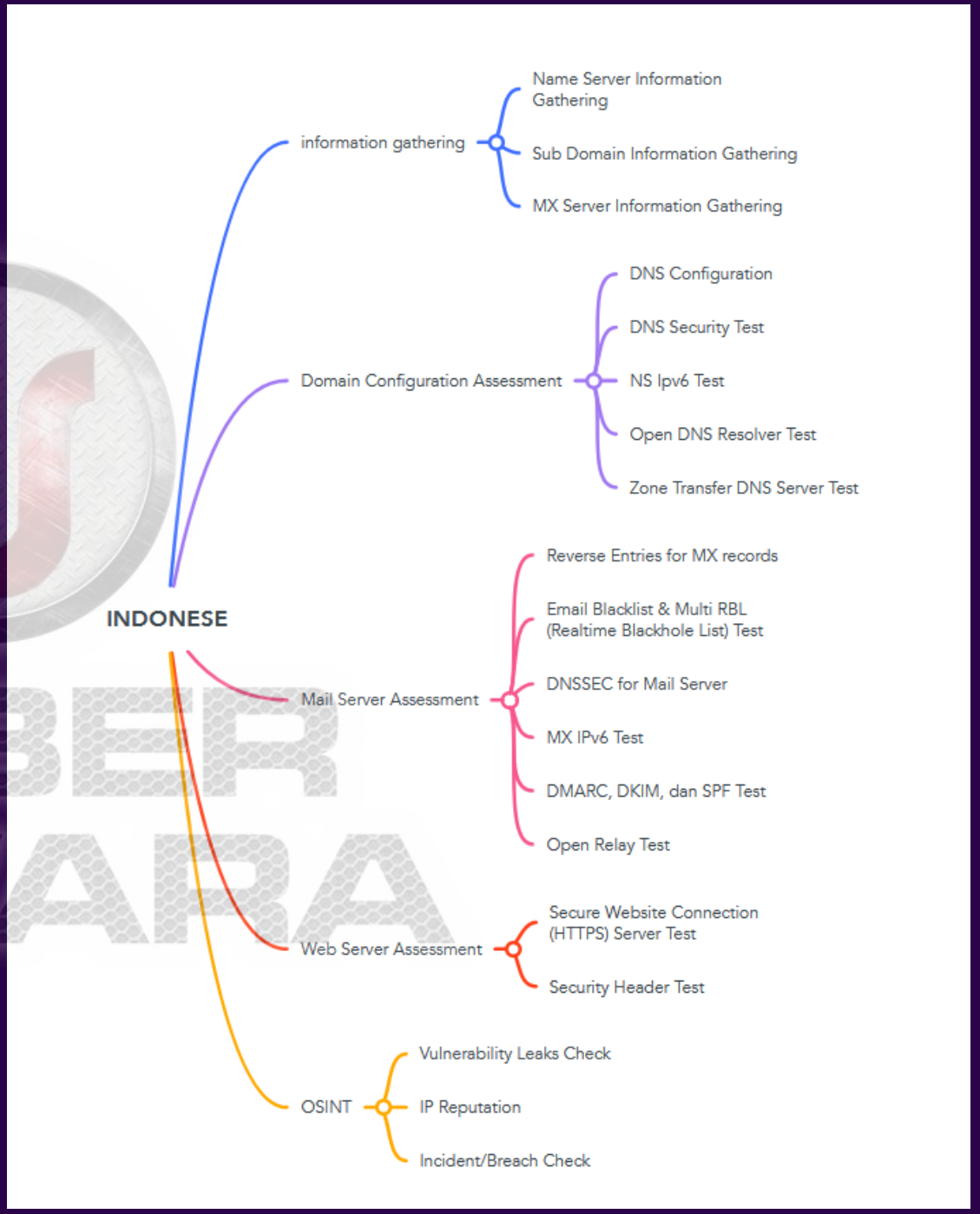
- INDEKS KDI KEMENTERIAN REPUBLIK INDONESIA TAHUN 2015
- INDEKS KDI KEMENTERIAN REPUBLIK INDONESIA TAHUN 2016
- INDEKS KIDI KEMENTERIAN REPUBLIK INDONESIA TAHUN 2017
- PRE-ASSESSMENT UNTUK KEGIATAN PENETRATION TESTING BEBERAPA KEMENTERIAN, LEMBAGA TINGGI NEGARA, PROVINSI DAN BANK KONVENSIONAL.
- APTIKOM FEST PROVINSI RIAU
- APTIKOM FEST PROVINSI JAWA BARAT
- APTIKOM FEST PROVINSI KALIMANTAN TENGAH

Output INDONESE
dalam aktivitas Security Assessment

- Information Gathering
  - Nameserver
  - IP Publik
  - Infrastruktur IT (Logical)
  - Keberadaan Aset Sistem Informasi berbasis web
- Assessment
  - Best practises
- OSINT
  - IP Reputation
  - Breach/Incident history
  - Vulnerability
  - Backdoor aktif.

Teknik : Recon & Enumeration

Cakupan INDONESE dalam aktivitas Security Assessment



Checklist INDONESE

Hasil Penilaian		
No	**Teknis/Metode Penilaian**	**Hasil**
Domain Configuration Assessment		
1	B.1. DNS Configuration	
2	B.2. DNS Security Test	
3	B.3. NS Ipv6 Test	
4	B.4. Open DNS Resolver Test	
5	B.5. Zone Transfer DNS Server Test	
Mail Server Assessment		
6	C.1. Reverse Entries for MX records	
7	C.2. Email Blacklist & Multi RBL (Realtime Blackhole List) Test	
8	C.3. DNSSEC for Mail Server	

13	D.2. Security Header Test	
OSINT		
14	Vulnerability Leaks Check	
15	IP Reputation	
16	Incident/Breach Check	

Keterangan :

✔ : Tidak terdapat temuan sesuai kriteria INDONESE

✘ : Terdapat temuan sesuai kriteria INDONESE

INFORMATION GATHERING

INFORMATION GATHERING

- A.1. Name Server Information Gathering
- A.2. Sub Domain Information Gathering
- A.3. MX Server Information Gathering

CYBER JAWARA

Name Server Information Gathering

A.1. Name Server Information Gathering	
Tujuan : Untuk mengetahui informasi umum tentang Name Server pada domain <DOMAIN INSTITUSI>, yang didapatkan dari informasi WHOIS dan Record DNS	
Tools Utama:	https://centralops.net/co/DomainDossier.aspx
Tools Alternatif:	-
Tools membutuhkan Akun	**TIDAK**
Referensi	-

Name Server Information Gathering

Address lookup

canonical name	**kemendagri.go.id.**
aliases	
addresses	**103.152.88.232** **103.245.225.232**

```
Name Server: ns1.kemendagri.go.id
Name Server: ns2.kemendagri.go.id
DNSSEC: Unsigned
```

Network Whois record

Queried **whois.apnic.net** with "**103.152.88.232**"...

```
% Information related to '103.152.88.0 - 103.152.88.255'
```

Sub Domain Information Gathering

Hostname	IP Address	Type	Reverse DNS
kemendagri.go.id	103.245.225.232	A	
layananonline.dukcapil.kemendagri.go.id	103.77.185.10	A	
mail.bangda.kemendagri.go.id	103.116.173.134	A	mail.bangda.kemendagri.go.id
seruyankab.sipd.kemendagri.go.id	103.245.225.58	A	
keuda.kemendagri.go.id	103.245.225.36	A	
padangpariamankab.sipd.kemendagri.go.id	103.245.225.58	A	
waykanankab.sipd.kemendagri.go.id	103.245.225.58	A	
gisa.dukcapil.kemendagri.go.id	134.209.110.80	A	
malakakab.sipd.kemendagri.go.id	103.245.225.58	A	
sangihekab.sipd.kemendagri.go.id	103.245.225.58	A	
sampangkab.sipd.kemendagri.go.id	103.245.225.58	A	
dukcapil.kemendagri.go.id	118.97.79.23	A	
dashboardsvc.ekososbud.kemendagri.go.id	103.8.238.192	A	files.smartcity.layanan.go.id
api-auth.siormas.kemendagri.go.id	103.8.238.192	A	files.smartcity.layanan.go.id
simonev-rb.kemendagri.go.id	103.245.225.127	A	
usersvc.ekososbud.kemendagri.go.id	103.8.238.192	A	files.smartcity.layanan.go.id

MX Server Information Gathering

mx:kemendagri.go.id Find Problems Solve Email Delivery Problems mx

Pref	Hostname	IP Address	TTL		
10	antispam.kemendagri.go.id	103.245.225.108 IDNIC-DEPDAGRI-AS-ID (AS131765)	15 min	Blacklist Check	SMTP Test
20	mx2.kemendagri.go.id	103.152.88.108 IDNIC-DEPDAGRI-AS-ID (AS131765)	15 min	Blacklist Check	SMTP Test

	Test	Result
✓	DMARC Record Published	DMARC Record found
✓	DMARC Policy Not Enabled	DMARC Quarantine/Reject policy enabled
✓	DNS Record Published	DNS Record found

Domain Configuration Assessment

DNS Configuration

Report for kemendagri.go.id

Input domain name ... Run Report »

Report created on: Mon, 17 Jul 2023 19:42:32 GMT

Share this report: | permalink

Parent	100
NS	91
SOA	100
MX	95
Mail	60
Web	100

B

PARENT

NS Records at Parent Servers

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

- `ns1.kemendagri.go.id.` TTL=3600 [103.245.225.100] [NO GLUE6]
- `ns2.kemendagri.go.id.` TTL=3600 [103.245.225.101] [NO GLUE6]

Missing Glue

OK. Parent name servers are offering glue for domain's name servers. We received name servers list and it's IP addresses from parent name server (*e.dns.id.*).

Name Servers Have A Records

OK. Found A records for all name servers.

- *ns1.kemendagri.go.id.* → 103.245.225.100
- *ns2.kemendagri.go.id.* → 103.245.225.101

Name Servers Distributed on Multiple Networks

WARNING: All name servers are located in one C class network:

- **103.245.225.0/24:**
  - *ns1.kemendagri.go.id.*
  - *ns2.kemendagri.go.id.*

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

Name Servers Distributed on Multiple ASNs

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

- **AS131765:**
  - *ns1.kemendagri.go.id.*
  - *ns2.kemendagri.go.id.*

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

Name Servers Versions

WARNING: Name servers software versions are exposed:

- **103.245.225.100**: *"PowerDNS Authoritative Server 4.2.1"*
- **103.245.225.101**: *"Mau tau aje"*

Exposing name server's versions may be risky, when a new vulnerability is found your name servers may be automatically exploited by *script kiddies* until you patch the system. Learn how to hide version.

DNS Security Test

Signed domain name (DNSSEC)

Too bad! Your domain is *not* signed with a valid signature (DNSSEC). Therefore visitors with enabled domain signature validation, are *not* protected against manipulated translation from your domain into rogue internet addresses. You should ask your name server operator (often your registrar and/or hosting provider) to enable DNSSEC.

Show details

DNSSEC existence

Verdict:
Your domain is insecure, because it is *not* DNSSEC signed.

Technical details:

Domain	Registrar
kemendagri.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.

NS Ipv6 Test

Name servers of domain

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.kemendagri.go.id.	None	103.245.225.101
ns1.kemendagri.go.id.	None	103.245.225.100

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.

'IPv4-mapped IPv6 addresses' (RFC 4291, beginning with ::ffff:) will fail in this test, as they do *not* provide IPv6 connectivity.

Open DNS Resolver Test

Recursive resolver is not detected on 103.152.88.232

IP address 103.152.88.232 is **not vulnerable** to DNS Amplification attacks.

Recursive resolver is not detected on 103.245.225.232

IP address 103.245.225.232 is **not vulnerable** to DNS Amplification attacks.

Zone Transfer DNS Server Test

```
; <<>> DiG 9.10.3-P4-Debian <<>> axfr @ns2.kemendagri.go.id kemendagri.go.id
; (1 server found)
;; global options: +cmd
kemendagri.go.id.       86400   IN      SOA     ns1.kemendagri.go.id. hostmaster.kemendagri.go.id. 2023071403 28800 7200 604800 86400
kemendagri.go.id.       86400   IN      RRSIG   NSEC 13 3 86400 20230727000000 20230706000000 18066 kemendagri.go.id.
UXURQB/IpR5WBurW4HdpN3C9gMmY2Qo+7mYWYHOZSHg+bGf8pAar666A X6eHhkSAiyjK+Ue2erQmKuX7jxr/xw==
kemendagri.go.id.       86400   IN      NSEC    _7fe111a2d0bba9d707439266b2bf7dcf.kemendagri.go.id. A NS SOA MX TXT RRSIG NSEC DNSKEY
kemendagri.go.id.       900     IN      RRSIG   TXT 13 3 900 20230727000000 20230706000000 18066 kemendagri.go.id.
Wf8lsa9QjlC0erlLPaUNGKyHfptbUyd/iwV5lohOv7VH42Wjgi1A5njp en8JkZqqznVMfOgT9qKQyPPWjbbG8g==
kemendagri.go.id.       900     IN      TXT     " KEMENTERIAN DALAM NEGERI"
kemendagri.go.id.       900     IN      TXT     "ZOOM_verify_BkHn1rPagVaXUNJAkNKgTc"
kemendagri.go.id.       900     IN      TXT     "bsaupWkVT6pULVYD+OOK06c/ZWDk/7OlNCr0yrxG+b8="
kemendagri.go.id.       900     IN      TXT     "google-site-verification=YuBlkMLvusaVKXWdanXrL-givjy1eaQ3gukSUhHaeJU"
kemendagri.go.id.       900     IN      TXT     "v=spf1 a:antispam.kemendagri.go.id a:mx2.kemendagri.go.id ip4:103.245.225.109 ip4:103.245.225.108
ip4:103.152.88.108 ~all"
kemendagri.go.id.       900     IN      RRSIG   MX 13 3 900 20230727000000 20230706000000 18066 kemendagri.go.id.
SkcUlZaAg2eDC3PfMTNN5FLPoxrtaX4TdMC+B+YF5T1gYgBRH0oR8tzc NMZmNa4pj47s50RXq0OtTbtHiKFcLw==
kemendagri.go.id.       900     IN      MX      10 antispam.kemendagri.go.id.
kemendagri.go.id.       900     IN      MX      20 mx2.kemendagri.go.id.
kemendagri.go.id.       3600    IN      RRSIG   NS 13 3 3600 20230727000000 20230706000000 18066 kemendagri.go.id.
Q+ylK7SvCBZjZFkb7coW7ITZkLELnTqXlZ2pyfEafHrOr5ZSDmM2lu73 6Z6DKjL+bV7nmEbc/SoTsqxkwevKBw==
kemendagri.go.id.       3600    IN      NS      ns1.kemendagri.go.id.
kemendagri.go.id.       3600    IN      NS      ns2.kemendagri.go.id.
kemendagri.go.id.       900     IN      RRSIG   A 13 3 900 20230727000000 20230706000000 18066 kemendagri.go.id.
2NCtyuf/PjDAd+dlQvGD0Hu+M2Lk2w0A7bEkU9PAgY5FSlQsu8tIRRFd ll4pSc9yoZhiZCGmyGC1m+JXjdSPnw==
kemendagri.go.id.       900     IN      A       103.152.88.232
kemendagri.go.id.       900     IN      A       103.245.225.232
```

TERIMA KASIH

Aiman Alauddin

087772662245

Ibnu_masud93@hotmail.com

https://www.linkedin.com/in/aiman93

IG : ibnumasudmanman