



Penanganan Insiden Keamanan Informasi



**DIREKTORAT PENANGGULANGAN DAN PEMULIHAN PEMERINTAH
BADAN SIBER DAN SANDI NEGARA**

<https://www.bssn.go.id>

About Me,,



Nama : Nur Dwi Muryanto, S.ST



Jabatan :

Sandiman Pertama pada Direktorat Penanggulangan dan Pemulihan Pemerintah, Deputi III



Contacts :

Email : nur.dwi@bssn.go.id

Phone/WA : 0856 8252 818



outline

01

Pendahuluan

Landasan Hukum, Sistem Transaksi Elektronik,
Definisi Insiden

02

Siklus Penanganan Insiden Kaminfo

Alur Penanganan Insiden Kaminfo

03

Penanganan Insiden Kaminfo

Prosedur dan Langkah Penanganan Insiden Kaminfo

Pendahuluan



Landasan Hukum



INPRES

INPRES No.3 Th.2003 tentang Kebijakan dan Strategi Nasional Pengembangan eGov

Undang-Undang

UU No.11 Th.2008 tentang Informasi dan Transaksi Elektronik (UU ITE)

Undang-Undang

UU No.14 Th.2008 tentang Keterbukaan Informasi Publik (UU KIP)

PP

PP No. 82 Th. 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik

Penyelenggaraan Sistem Elektronik

Pasal 15 dan 16 UU ITE



Kewajiban Penyelenggara Sistem Elektronik

- 1) Keandalan
- 2) Keamanan
- 3) Tanggung jawab atas ketersediaan

dapat melindungi keotentikan,
integritas, kerahasiaan,
ketersediaan, dan
keteraksesan

tersedianya prosedur atau
petunjuk dalam
Penyelenggaraan
Sistem Elektronik yang
didokumentasikan

Sistem Elektronik Strategis



Sistem Elektronik yang dapat berdampak serius terhadap :

- Kepentingan umum;
- Pelayanan publik;
- Kelancaran penyelenggaraan negara; atau
- Pertahanan dan keamanan negara



(Penjelasan Peraturan Pemerintah No. 82 Tahun 2012 Pasal 11)

Insiden



- Insiden adalah:
Kejadian tak terduga yang menyebabkan gangguan operasi normal
- Insiden Keamanan
 - Suatu kejadian **pelanggaran** terhadap kebijakan keamanan (security policy)
 - Akses secara **tidak sah** terhadap sistem atau informasi
 - Suatu peristiwa yang **menghalangi / mengganggu** akses yang sah terhadap sistem atau informasi





Data insiden Id-SIRTI 2017 :

- Terdapat 205 Juta Serangan
- Domain go.id (pemerintah) paling banyak terkena serangan
- Sebanyak 15 ribu serangan mengarah pada website

NOTIFIER DOMAIN

 Special defacements only ☒ Fulltext/Wildcard ☒ Onhold (Unpublished) only ☒

 Date :

 Total notifications: **3,089** of which **3,089** single ip and **0** mass defacements

Legend:

H - Homepage defacement

M - Mass defacement (click to view all defacements of this IP)

R - Redefacement (click to view all defacements of this site)

L - IP address location

★ - Special defacement (special defacements are important websites)

We don't accept notifications through email, IP address notifications, notifications with fake and/or created subdomains by notifier or with wrong attack methods selected.

Time	Notifier	H	M	R	L	★ Domain	OS	View
2018/10/03	Hidden Ghost Team				R	★ gaw.kototabang.bmkg.go.id/hgt.htm	Linux	mirror
2018/10/03	Hidden Ghost Team				R	★ egov.bmkg.go.id/hgt.htm	Linux	mirror
2018/10/03	Hidden Ghost Team				R	★ geopal.sulteng.bmkg.go.id/hg...	Linux	mirror
2018/10/03	alexa anderson					★ eulp.malangkab.go.id/pelaporan...	Linux	mirror
2018/10/03	EX12T CYBER TEAM					★ sim-smep.malangkab.go.id/index...	Linux	mirror
2018/10/02	Noniod7				R	★ www.kab-kupang.go.id/dprd/	Linux	mirror
2018/09/30	./MrTahuSumedang					★ nakertrans.banyuwangikab.go.id...	Linux	mirror
2018/09/29	TEH Squad Cyber	H				★ www.dispora.murarakab.go.id	Linux	mirror
2018/09/29	TEH Squad Cyber	H				★ www.dpp.murarakab.go.id	Linux	mirror
2018/09/29	TEH Squad Cyber	H				★ www.dlhp.murarakab.go.id	Linux	mirror
2018/09/29	p0r7s				R	★ pa-masamba.go.id/arsipurat/Ha...	Linux	mirror
2018/09/29	p0r7s				R	★ www.pa-sungguminasa.go.id/arsl...	Linux	mirror
2018/09/29	213_90N6				H	★ dppka.tapselkab.go.id	Win 2012	mirror
2018/09/27	4nzel4					★ skum.pn-parigi.go.id/index.php...	Linux	mirror
2018/09/27	KID2ZON3					★ dinppkp.purworejokab.go.id/sad...	Linux	mirror
2018/09/26	W3LL SQUAD					★ agenda.dumakota.go.id/index.htm	Linux	mirror
2018/09/25	xC4pric0m					★ genom.litbang.pertanian.go.id/...	Linux	mirror
2018/09/25	Prz					★ simperindag.mojokertokab.go.id	Linux	mirror
2018/09/25	EX12T CYBER TEAM	H				★ www.sikon.tubankab.go.id/matam...	Linux	mirror
2018/09/25	RxR					★ kp.id.kepriprov.go.id/24.php	Linux	mirror
2018/09/22	k4L0ng666				R	★ pt-pontianak.go.id/mcc.html	Linux	mirror
2018/09/22	Xaveroz_Tersakiti					★ dinasperdagangan.pareparekota...	Linux	mirror
2018/09/22	Ästra					★ pindah-luarkota.pekalangankota...	OpenBSD	mirror
2018/09/22	ghost7				R	★ dinkes.mojokertokota.go.id/ind...	Linux	mirror
2018/09/21	LCR999X				R	★ klatenkab.go.id/hacked/	Linux	mirror

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30

DISCLAIMER: all the information contained in Zone-H's cybercrime archive were either collected online from public sources or directly notified anonymously to us. Zone-H is neither responsible for the reported computer crimes nor it is directly or indirectly involved with them. You might find some offensive contents in the mirrored defacements. Zone-H didn't produce them so we cannot be responsible for such contents. [Read more](#)

Insiden Web Defacement

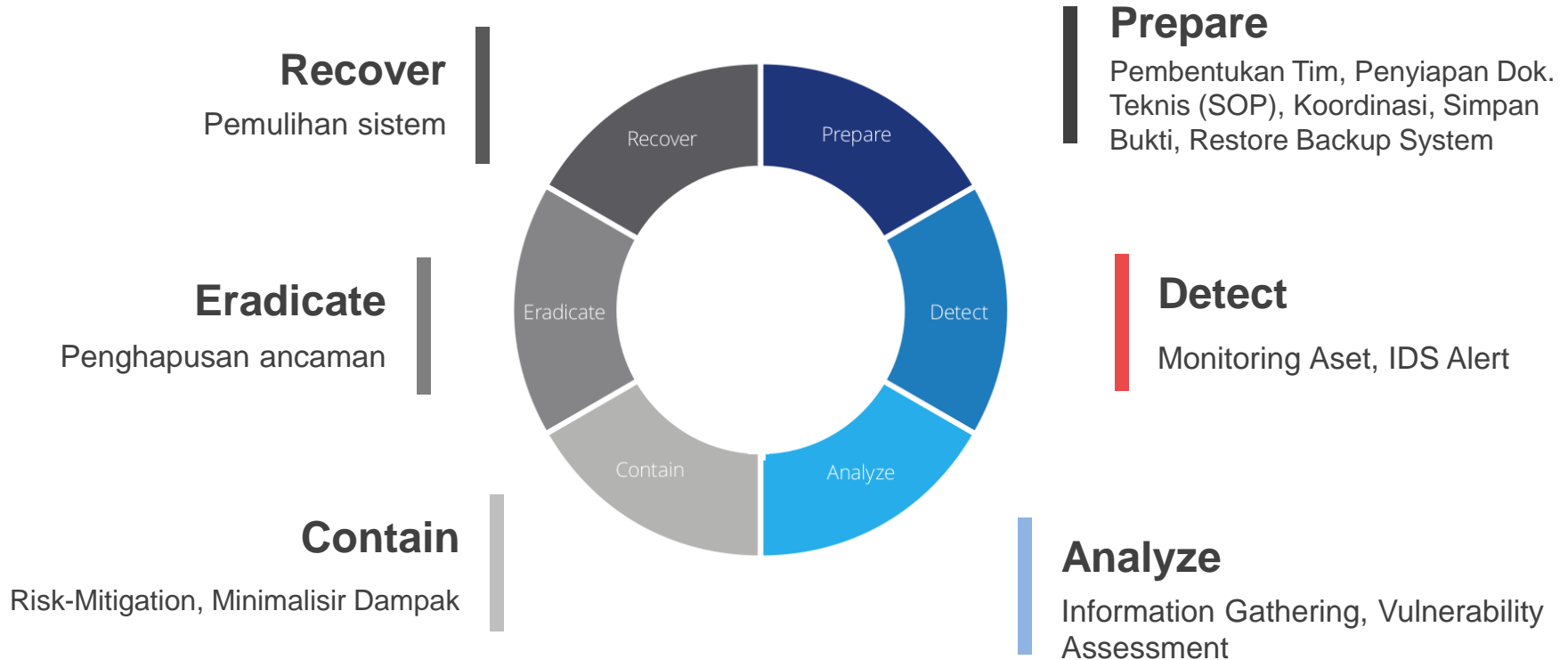
- Deface :
 - mengganti file
 - menyisipkan file
 - lubang keamanan
- Penggunaan free CMS dan open source tanpa adanya modification.
- default konfigurasi = celah keamanan
- Tidak updatenya source atau tidak menggunakan versi terakhir dari CMS.

Siklus Penanganan Insiden



Incident Handling

Life Cycle of Incident Handling



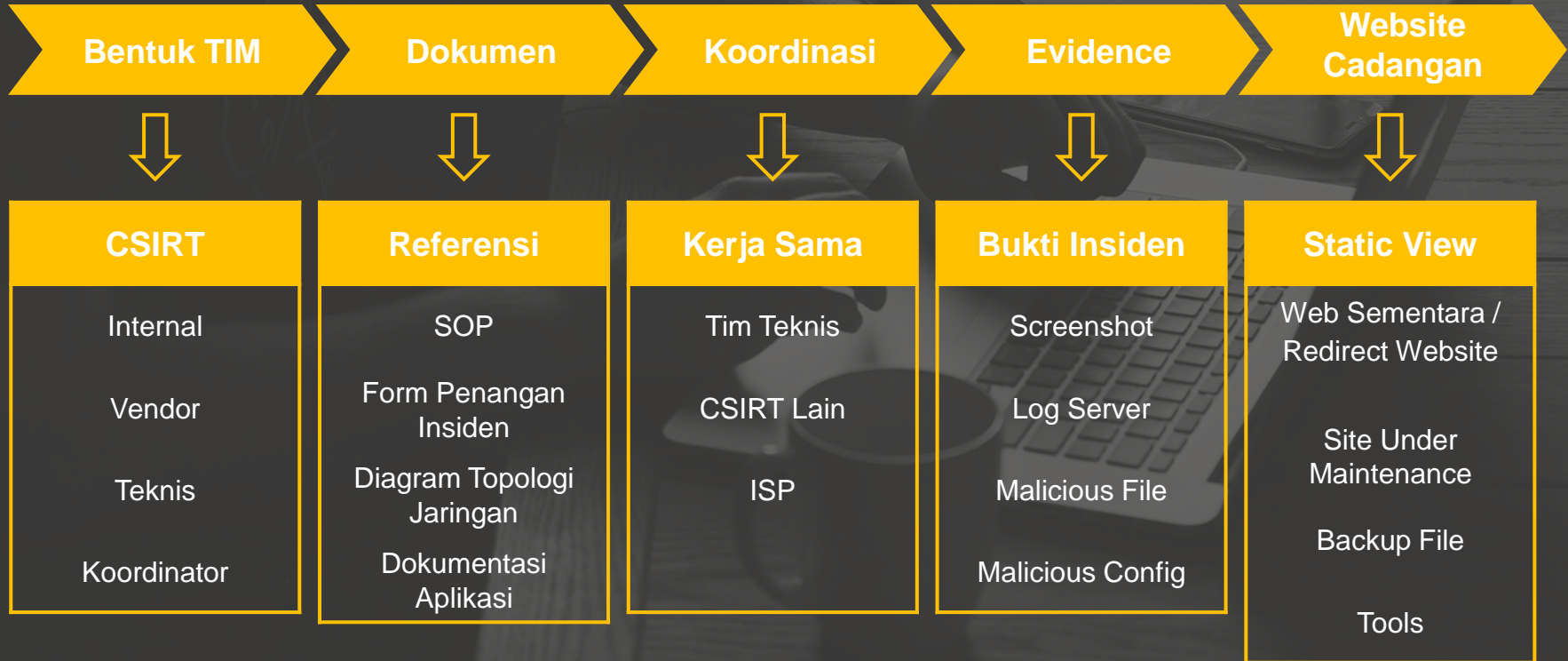
Incident Response



Tahapan Penanganan Insiden




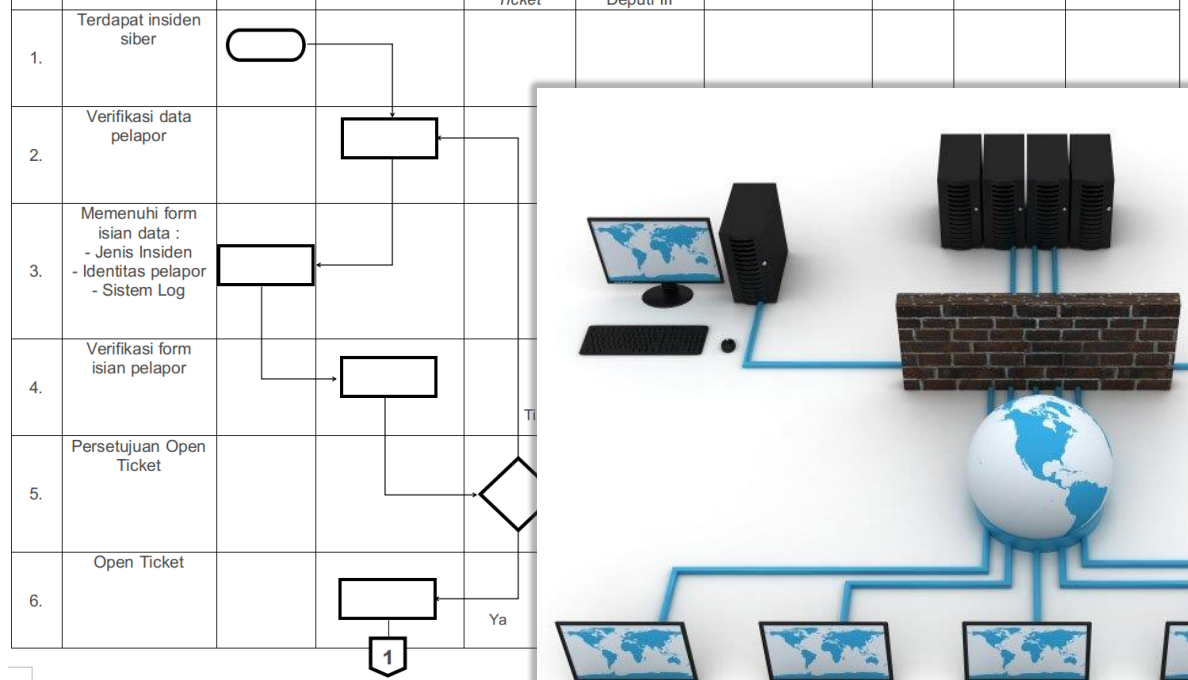
Tahap Persiapan



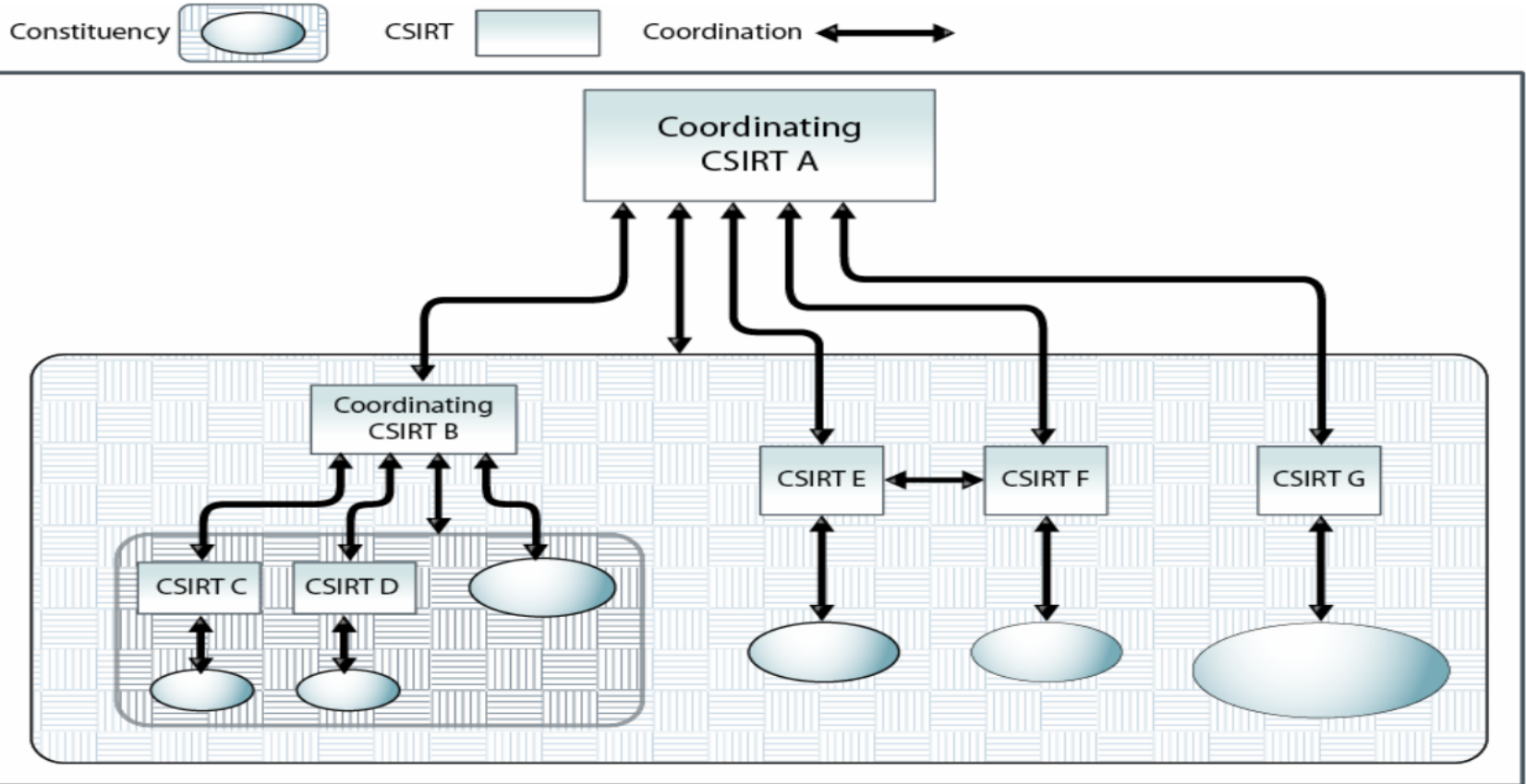
- CSIRT dianggap sebagai tim atau entitas dalam suatu lembaga yang menyediakan layanan dan dukungan kepada organisasi untuk mencegah, mengelola dan menanggapi insiden keamanan informasi.
- Tim-tim ini biasanya terdiri dari para spesialis yang bertindak sesuai dengan prosedur dan kebijakan untuk merespon dengan cepat dan efektif terhadap insiden keamanan dan untuk mengurangi risiko serangan cyber.



No.	Aktivitas	Pelaksana	Mutu Baku			Keterangan
		Pengolah Data Kelembagaan	Kelengkapan	Waktu	Output	
1	Terjadi Insiden Web Defacement					
2	Persiapan Penanganan Insiden Web Defacement :		- Surat Tugas	60 menit	Dokumen	



Pola Koordinasi CSIRT



Point of Contacts

SURAT PERNYATAAN KESEDIAAN MENJADI *POINT OF CONTACT*

Saya yang bertanda tangan di bawah ini :

Nama : _____
Jabatan : _____
Alamat Email : _____
Nomor Telp/HP : _____
Nama Instansi : _____

Bahwa dalam rangka penanganan insiden siber dengan ini menyatakan bahwa saya :

1. bersedia berperan sebagai *Point Of Contact* (POC) yaitu pihak yang menjadi kontak apabila terjadi insiden siber pada instansi saya,
2. akan berkoordinasi aktif dengan CSIRT terkait (BSSN) ketika terjadi insiden siber pada instansi saya.

Jakarta, Agustus 2018



Home News Events Archive Archive 🌟 Onhold Notify Stats Register Login 🔴

Mirror saved on: 2018-09-22 01:40:46

Notified by: ghost7

Domain: http://dinkes.mojokertokota.go.id/index.php/post_berita/lists

Web server: Unknown

System: Linux

THIS MIRROR IS ONHOLD AND HAS NOT BEEN VERIFIED YET. FAKE DEFAACEMENTS WILL BE

This is a CACHE (mirror) page of the site when it was saved by our robot on 2018-09-22 01:40:46

IP address: 104.18.40.168 🇺🇸

[Notifier stats](#)



Home News Events Archive Archive 🌟 Onhold Notify Stats Register Login 🔴

Mirror saved on: 2018-09-26 06:02:37

Notified by: W3LL SQUAD

System: Linux

THIS MIRROR IS ONHOLD AND HAS NOT BEEN VERIFIED YET. FAKE DEFAACEMENTS WILL BE DELETED WHEN REVIEWED BY OUR STAFF.

This is a CACHE (mirror) page of the site when it was saved by our robot on 2018-09-26 06:02:37

Domain: <http://agenda.dumaikota.go.id/index.htm>

Web server: Apache

IP address: 203.153.21.6 🇮🇩

[Notifier stats](#)

Hacked By Nurmala

Now you see me, I am back
This was not a joke or dream, This is fucking reality
Have you checked emails from me?
it's funny where when someone wants to help you, you blame him

[Greetz]

4D#R4BBT | DeXONE | Z0y0n3-cr1ptzGangz | Sh1nta17 | 64V | L0ltz | D0p4rs | F4LK4 | LCR25!

Copyright 2018 | W3LL SQUAD OFFICIAL



Home News Events Archive Archive 🌟 Onhold Notify Stats Register Login Disclaimer Contact

Attribution-NonCommercial-NoDerivs 3.0 Unported License

dinkes.mojokertokota.go.id
22 September 2018

Google Advanced Search





[Semua](#) [Berita](#) [Maps](#) [Gambar](#) [Video](#) [Lainnya](#) [Setelan](#) [Alat](#)

[Negara mana saja ▼](#) [Setahun terakhir ▼](#) [Urut relevansi ▼](#) [Semua hasil ▼](#) [Hapus](#)

Kiat: Telusuri hasil dalam bahasa **Indonesia** saja. Anda dapat menentukan bahasa penelusuran di [Preferensi](#)

[kpaigoid hacked Notified by Dijehaji - Zone-H.org](#)
www.zone-h.org/mirror/id/31228074 ▼ [Terjemahkan halaman ini](#)
31 Mei 2018 - Mirror saved on: 2018-05-31 08:03:13. Notified by: Dijehaji; Domain: <http://kpai.go.id/readme.htm>; IP address: 180.250.62.75 Indonesia. System: Linux; Web ...

[wwwpajakgoid hacked Notified by Anonymous Arabe - Zone-H.org](#)
www.zone-h.org/mirror/id/31256242 ▼ [Terjemahkan halaman ini](#)
10 Jun 2018 - Mirror saved on: 2018-06-10 12:26:14. Notified by: Anonymous Arabe; Domain: <http://www.pajak.go.id>; IP address: 103.28.106.67 Indonesia. System: F5 Big-IP ...

[wwwpancasilagoid hacked Notified by J\(\)H - Zone-H.org](#)
www.zone-h.org/mirror/id/31569858
14 Agt 2018 - Mirror saved on: 2018-08-14 12:18:17. Notified by: J()H; Domain: <https://www.pancasila.go.id/owned.htm>; IP address: 103.8.238.30 Indonesia. System: Linux ...

[gpansorsurabayaorid hacked Notified by nikotravolta - Zone-H.org](#)
www.zone-h.org/mirror/id/31785304 - [Terjemahkan halaman ini](#)
10 jam yang lalu - Mirror saved on: 2018-10-23 02:37:21. Notified by: nikotravolta; Domain: <https://>

site:zone-h.org *.id

Simpan Log

Log Server/Aplikasi/Security Device

Analisis Log

Log merupakan sebuah dokumentasi dari seluruh kegiatan yang dilakukan oleh Server, Aplikasi ataupun Perangkat keamanan yang digunakan dalam sebuah sistem



Exploit

Teknik hacking yang dilakukan



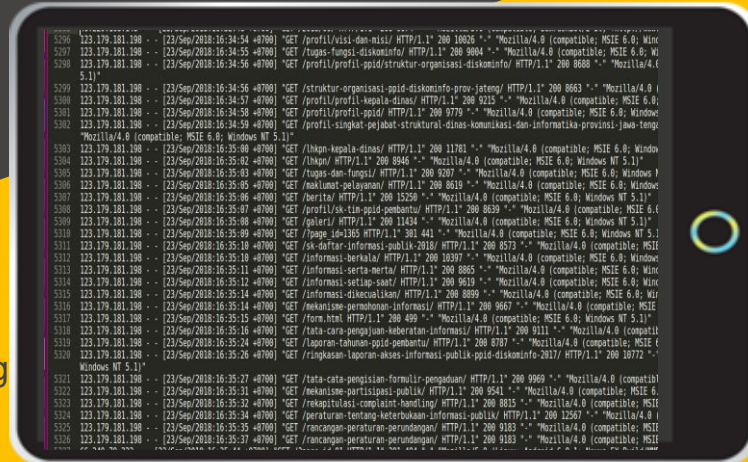
Malicious

Dapat mengetahui layanan/file malicious yang diupload ke server



Sumber Serangan

Alamat IP Penyerang terdokumentasi secara otomatis oleh sistem Log



Website Cadangan

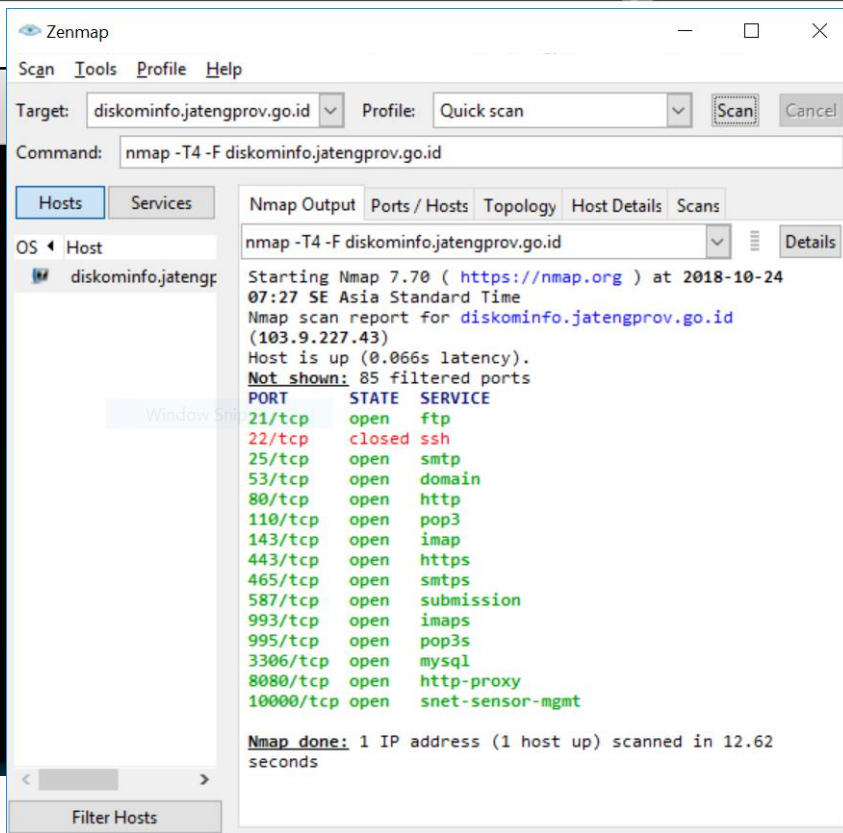
Under Maintenance

Maaf, atas ketidaknyamanan anda.
Saat ini portal anda sedang tidak aktif (ditutup), untuk proses
upgrade ke versi terbaru.

TOOLS NMAP



```
root@VVDKALI: ~  
File Edit View Search Terminal Help  
root@VVDKALI:~# nmap diskominfo.jatengprov.go.id  
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-23 20:12 WIB  
Nmap scan report for diskominfo.jatengprov.go.id (103.9.227.43)  
Host is up (0.039s latency).  
Not shown: 984 filtered ports  
PORT      STATE SERVICE  
20/tcp    closed ftp-data  
21/tcp    open  ftp  
22/tcp    closed ssh  
53/tcp    open  domain  
80/tcp    open  http  
110/tcp   open  pop3  
143/tcp   open  imap  
443/tcp   open  https  
465/tcp   open  smtps  
587/tcp   open  submission  
993/tcp   open  imaps  
995/tcp   open  pop3s  
2020/tcp  open  xinupageserver  
3306/tcp  open  mysql  
8080/tcp  open  http-proxy  
10000/tcp open  snet-sensor-mgmt  
  
Nmap done: 1 IP address (1 host up) scanned in 69.21 seconds  
root@VVDKALI:~#
```



IDENTIFIKASI & ANALISIS



TUJUAN :



Pahami sifat dan ruang lingkup kejadian



Pengumpulan Informasi

Prioritas penanganan insiden, biasanya diikuti dengan penaanan sistem



Adakah data rahasia?

IDENTIFIKASI & ANALISIS



HAL-HAL YANG DILAKUKAN :



KONFIRMASI

- Periksa halaman web yang telah diubah
- Gunakan tools security checks (Zone-h)



DETEKSI SUMBER SERANGAN

- Periksa perubahan pada file statis, kapan berubah?
- Periksa semua link web
- Periksa semua log
 - Access log apache server (usr/local/apache/logs/access.log)
 - Error log apache server (usr/local/apache/logs/error.log)
- Adakah malicious file?



Containment



TUJUAN :



Tidak terjadi kerusakan lebih dalam pada web server



Melindungi server-server lain yang terhubung

Prosedur Containment



- Back up data (forensik dan pengumpulan bukti)
- Identifikasi semua service dan koneksi
- Identifikasi cara penyerang masuk system pertama kali
- Periksa kode-kode berbahaya dalam system (trojan, backdoor)
- Inventarisir kerentanan
 - Kode sql
 - Komponen yang memiliki akses write
 - Respon web saat url salah

Penghapusan Konten (Eradication)



TUJUAN :



Menghilangkan komponen yang mengganggu sistem



Mengurangi vector serangan

- Patch kerentanan
- Penerapan standar prosedur yang lebih kuat
- Penyesuaian pengaturan firewall
- dll



Prosedur **Eradication**



- Hapus malicious content (termasuk konten deface)
- Hapus aplikasi mencurigakan
 - Jalankan service yang diperlukan saja
- Patching keamanan aplikasi web
- Periksa dan hapus backdoor
- Lakukan vulnerability assessment



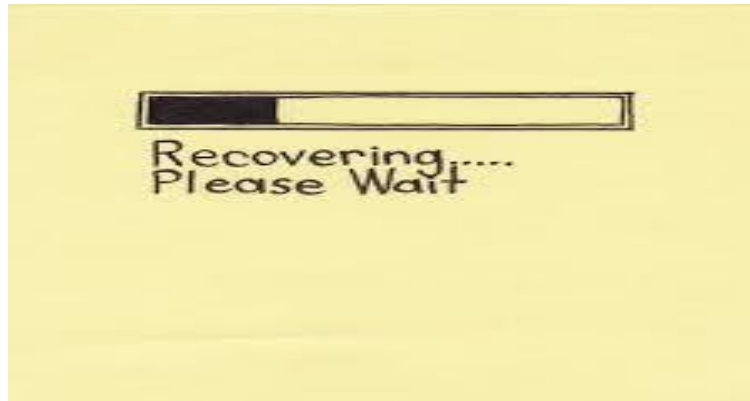
Pemulihan (Recovery)



TUJUAN :



Mengembalikan ke keadaan semula



Tindak Lanjut (Follow Up)



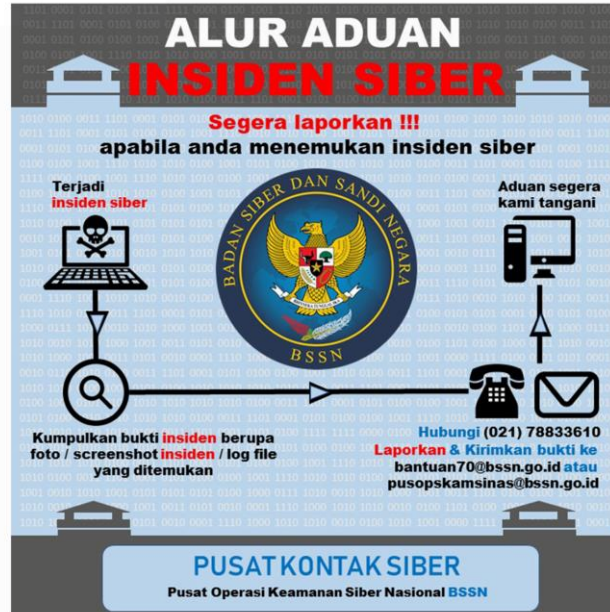
TUJUAN :

- *Lesson learned*
- Laporan akhir
- Bukti Arsip dan Dokumentasi
- Menutup proses penanganan insiden





ALUR ADUAN
INSIDEN SIBER



Prosedur Pengaduan Insiden Keamanan Siber



BADAN SIBER DAN
SANDI NEGARA

Serangan pada Aplikasi berbasis web



Top 10 kategori serangan pada aplikasi berbasis web:

1. SQL Injection	6. Sensitive Data Exposure
2. Broken Authentication & Session Management	7. Missing function Level Access
3. XSS	8. Cross Site Request Forgery
4. Insecure Direct Object reference	9. Using Component with Know Vurnerabilities
5. Security Misconfiguration	10. Unvalidated redirect & Forward

(sumber: OWASP top ten)

A close-up, shallow depth-of-field photograph of a person's hands typing on a laptop keyboard. The person has light-colored skin and is wearing a white long-sleeved shirt. Their fingernails are painted a dark red color. The background is a soft, out-of-focus white surface. Overlaid on the image is a large, semi-transparent white circle. Inside this circle, the words "THANK YOU" are written in a playful, blocky font using colorful wooden blocks. The word "THANK" is on the top row, and "YOU" is on the bottom row. To the right of the circle, there are three red circles of varying sizes, with the largest one being the most prominent.

THANK
YOU