



# PANDUAN PENANGANAN INSIDEN WEB DEFACEMENT



DINAS KOMUNIKASI, INFORMATIKA DAN STATISTIK PROVINSI BALI



[csirt.baliprov.go.id](http://csirt.baliprov.go.id)



[aduancsirt.baliprov.go.id](http://aduancsirt.baliprov.go.id)

  
 **Versi Dokumen**

No	Tanggal	Versi Dokumen	Oleh	Keterangan
1	Desember 2021	Versi 1.0	Diskominfo Prov. Bali	-

## Kata Pengantar

Puji syukur kehadiran Tuhan Yang Maha Esa, atas segala limpahan rahmat, nikmat serta karunia-Nya yang tak ternilai dan tak dapat dihitung sehingga kami dapat menyelesaikan penyusunan “Panduan Penanganan Insiden Web *Defacement*”. Panduan ini disusun dalam rangka memberikan acuan bagi pihak yang berkepentingan dalam pelaporan insiden siber. Panduan ini berisikan langkah-langkah yang harus diambil apabila terjadi serangan Web *Defacement*, yang dimulai dari tahap persiapan sampai dengan tahap pembuatan laporan dari penanganan serangan. Panduan ini tentu saja masih banyak kekurangan dan masih jauh dari kesempurnaan karena keterbatasan ilmu dan referensi kami. Untuk itu, kami selalu berusaha melakukan evaluasi dan perbaikan secara berkala agar bisa mencapai hasil yang lebih baik lagi.

Akhir kata, kami ucapkan terima kasih kepada segala pihak yang telah membantu dalam penyusunan panduan ini.

Bali, 2 Desember 2021



  
 **Daftar Isi**

<b>Daftar Isi .....</b>	<b>iv</b>
<b>Panduan Penanganan Insiden Web <i>Defacement</i>.....</b>	<b>1</b>
<b>1. TUJUAN.....</b>	<b>1</b>
<b>2. RUANG LINGKUP .....</b>	<b>1</b>
<b>3. PROSEDUR PENANGANAN WEB <i>DEFACEMENT</i>.....</b>	<b>2</b>
<b>3.1. Persiapan.....</b>	<b>3</b>
<b>3.2. Identifikasi dan Analisis .....</b>	<b>4</b>
<b>3.3. Mitigasi .....</b>	<b>4</b>
<b>3.4. Penghapusan Konten .....</b>	<b>5</b>
<b>3.5. Pemulihan.....</b>	<b>5</b>
<b>3.6. Tindak Lanjut .....</b>	<b>5</b>
<b>LAMPIRAN I – BAGAN PENANGANAN INSIDEN .....</b>	<b>7</b>
<b>A. TAHAP PERSIAPAN .....</b>	<b>7</b>
<b>B. TAHAP IDENTIFIKASI DAN ANALISIS.....</b>	<b>8</b>
<b>C. TAHAP MITIGASI .....</b>	<b>9</b>
<b>D. TAHAP PENGHAPUSAN KONTEN .....</b>	<b>9</b>
<b>E. TAHAP PEMULIHAN .....</b>	<b>10</b>
<b>F. TAHAP TINDAK LANJUT.....</b>	<b>10</b>



# Panduan Penanganan Insiden Web *Defacement*

## 1. TUJUAN

Penanganan yang terencana dan terorganisir sangatlah diperlukan dalam hal terjadinya insiden web *defacement*, supaya hal tersebut dapat dilakukan, maka diperlukan adanya suatu prosedur yang standar untuk melakukan penanganan terhadap insiden tersebut. Secara umum tujuan prosedur standar ini adalah untuk memberikan arahan secara *best practices* dalam penanganan insiden web *defacement*, sedangkan secara khusus adalah sebagai berikut :

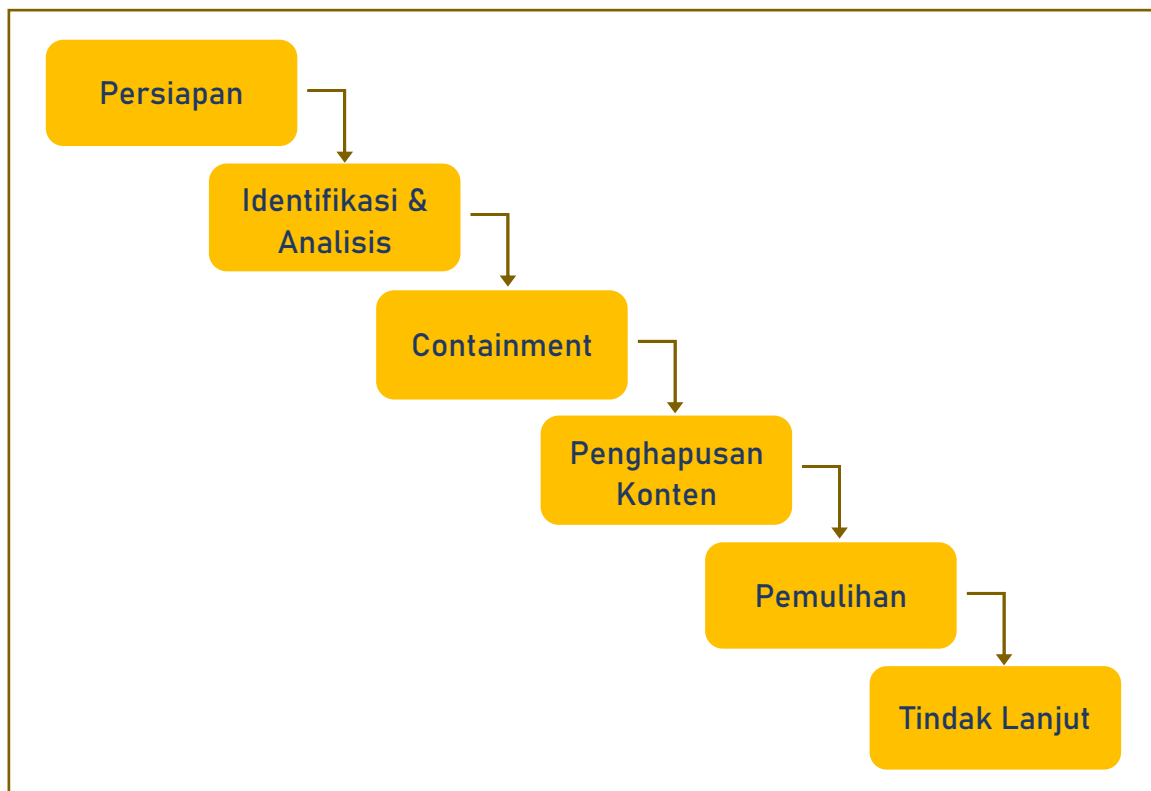
- a. Memastikan adanya sumber daya yang memadai untuk menangani insiden yang terjadi
- b. Menjamin pihak-pihak yang bertanggung jawab dalam penanganan insiden bekerja sesuai dengan tugas dan kewajiban masing-masing
- c. Menjamin aktivitas dari penanganan insiden dapat terkoordinasi dengan baik
- d. Melakukan pengumpulan informasi yang akurat
- e. *Sharing* pengetahuan dan pengalaman di antara anggota tim penanganan insiden
- f. Meminimalisir dampak dari insiden yang terjadi.
- g. Mencegah adanya serangan lanjutan dan mencegah kerusakan agar tidak lebih meluas

## 2. RUANG LINGKUP

Prosedur standar penanganan insiden ini berisi langkah-langkah yang harus diambil apabila terjadi insiden web *defacement*, yang dimulai dari tahap persiapan sampai dengan tahap pembuatan laporan dari penanganan insiden. Web *defacement* dapat terjadi pada semua halaman web, baik milik sektor pemerintah, infrastruktur informasi kritikal nasional dan ekonomi digital. Prosedur standar penanganan insiden ini dapat dijadikan acuan bagi semua individu atau tim yang bertindak sebagai penanggung jawab/administrator dari suatu web server.

### 3. PROSEDUR PENANGANAN WEB *DEFACEMENT*

Terdapat 2 (dua) cara bagi institusi/perorangan untuk meletakkan suatu halaman web, yaitu meletakkan pada *server* yang dikelola sendiri atau meletakkan halaman webnya pada web *hosting*. Bagi yang meletakkan halaman webnya pada web *hosting*, maka apabila terjadi web *deface* harus melakukan koordinasi dengan pihak web *hosting*. Koordinasi ini ditujukan untuk memudahkan penanganan dari web yang telah ter-*deface*. Setiap pengelola web *hosting* seharusnya memiliki prosedur untuk menangani insiden web *defacement*. Secara umum tahap-tahap dalam menangani suatu insiden dapat digambarkan sebagai berikut :



Gambar 1. Tahap Penanganan Insiden

Berdasarkan gambaran tahap-tahap penanganan suatu insiden, dapat dibuat suatu prosedur standar untuk melakukan tindakan apabila terjadi suatu insiden. Prosedur standar penanganan insiden web *deface* dapat diuraikan sebagai berikut :

### 3.1. Persiapan

Dalam melakukan penanganan insiden, perlu dilakukannya tahapan persiapan yang bertujuan untuk mempersiapkan segala sesuatu yang dibutuhkan pada saat penanganan insiden web *defacement*. Adapun prosedur sebagai berikut :

- a. Pembentukan tim penanganan insiden perlu dilakukan baik berasal dari institusi yang mengalami insiden (internal) atau juga bisa berasal dari luar institusi (eksternal) jika memang sangat diperlukan;
- b. Menyiapkan dokumen yang dibutuhkan dalam proses penanganan insiden. Dokumen ini antara lain adalah :
  - *Standar Operation Procedure*;
  - *Form-form* yang akan digunakan : *form* penanganan insiden, *form chain of custody*;
  - Gambaran diagram terbaru yang menggambarkan hubungan antar komponen-komponen aplikasi yang membangun *website* (*web server*, aplikasi web, para *user*, diagram *network*);
  - Dokumentasi dari sistem operasi, aplikasi, protokol dan anti virus yang terdapat pada *web server*.
- c. Lakukan koordinasi insiden dengan tim yang dapat menangani secara teknis, koordinasi dengan tim CSIRT ataupun *Point of Contact* untuk mendapatkan informasi tambahan dalam penanganan insiden;
- d. Menyimpan bukti insiden antara lain *screenshot* insiden web *defacement*, *log server* ataupun *log* perangkat pendukung *server*. Jika menemukan file yang mencurigakan dapat dilakukan pendokumentasian file tersebut. Untuk kegiatan forensik, dapat juga dilakukan proses *imaging* baik seluruh *storage server* ataupun memori (RAM) yang digunakan;
- e. Menentukan tempat (ruangan) untuk menangani insiden baik kegiatan rapat tim maupun kegiatan analisis insiden;
- f. Menyiapkan *tool* dan media yang dibutuhkan untuk menangani insiden. *Tools* yang dapat disiapkan antara lain *Scanning Tools*, *Forensic Tools*, dan *Monitoring Tools*. Media dapat berupa *storage external*.

## 3.2. Identifikasi dan Analisis

Pada tahap ini dilakukan proses identifikasi untuk memastikan bahwa insiden yang telah terjadi dapat diketahui sumber serangannya. Selain itu juga untuk mengumpulkan informasi yang cukup tentang insiden tersebut sehingga tim dapat memprioritaskan langkah selanjutnya dalam menangani insiden.

Dalam proses identifikasi, prosedur yang dilakukan adalah sebagai berikut :

- a. Memeriksa *file-file* yang bersifat statis, apakah terjadi perubahan dan kapan perubahan itu terjadi. Memeriksa semua *link* yang ada pada halaman web (*src, meta, css, script*);
- b. Memeriksa semua *log file*. *File log* yang dapat diperiksa antara lain *Error Log, Access Log, Database Log, Auth Log, Install Log, Event Log, Firewall Log, IDS/IPS Log, Switch/Router Log*;
- c. Memeriksa folder pada *website* yang bersifat publik (akses *write*, biasanya untuk menyimpan *file upload*) untuk indikasi *file backdoor, malware, trojan*, atau *malicious file* lainnya;
- d. Memeriksa kembali kode *sql* yang digunakan pada web aplikasi, apakah terdapat *bug* pada *code* tersebut. Memeriksa pada implementasi fitur *Login/Logout*, Koneksi *Database*, dan Menampilkan Isi *Database*;
- e. Memeriksa *version* setiap aplikasi/*library* yang digunakan. Periksa versi *web server*, versi aplikasi dan versi *database*;
- f. Memeriksa setiap koneksi yang terhubung ke *server* tersebut;
- g. Memeriksa layanan/*service* yang sedang berjalan. Periksa semua *port* yang terbuka, periksa *cronjob* (*service* otomatis harian), periksa *last login* untuk *user*, periksa *history*;
- h. Dalam melakukan tahapan ini, *tools* yang dapat digunakan antara lain: *NMap, Nikto, Accunetic, Nessus*.

## 3.3. Mitigasi

Untuk mengurangi dampak peningkatan resiko (mitigasi) perlu dilakukan hal-hal sebagai berikut :

- a. Perlu dilakukan pembangunan *website* sementara agar publikasi informasi pada *website* tetap berjalan. Atau dapat juga dilakukan pembangunan *site under maintenance*;
- b. Lakukan *backup* sistem, untuk keperluan forensik ataupun untuk mengumpulkan bukti-bukti insiden;



- c. Pembatasan akses terhadap sumber serangan yang ditemukan antara lain sumber IP, sumber *port*, serta akun user yang digunakan oleh penyerang.

### 3.4. Penghapusan Konten

Setelah ditemukan aplikasi ataupun *file* yang bersifat *malicious*, maka tahap selanjutnya adalah melakukan penghapusan konten tersebut. Adapun tahapannya adalah sebagai berikut :

- a. Lakukan hapus *file malicious*, antara lain : *file defacement*, *file backdoor*, *file rootkit* ataupun *file malware*;
- b. Lakukan *uninstall* aplikasi yang ditemukan sebagai aplikasi *malicious*.


### 3.5. Pemulihan

Pada tahapan ini bertujuan untuk memulihkan kembali halaman web kepada keadaan semula. Prosedur yang dapat dilakukan adalah sebagai berikut:

- a. Mengaktifkan (*me-restore*) *file-file* yang telah di-*backup*. *File* dapat berupa *file* pada *web server*, *file database*. Dan gunakan aplikasi *checksum* sebagai *data integrity checker* pada *file backup* tersebut;
- b. Lakukan *update/upgrade/patch* semua aplikasi yang digunakan pada *web server*. Jika menggunakan CMS, *update* versi web aplikasi, *plugins*, *themes* yang digunakan. Jika menggunakan API dapat melakukan *update library* yang digunakan. Selain itu perlu dilakukan *update rules* pada konfigurasi keamanan yang digunakan;
- c. Lakukan *automatic updates* pada setiap aplikasi yang digunakan;
- d. Lakukan pembaruan seluruh akun yang digunakan baik pada sistem operasi, web aplikasi;
- e. Lakukan *hardening server* ataupun aplikasi yang digunakan seperti memasang *Web Application Firewall (WAF)*, memasang aplikasi anti-*defacement (DotDefender, Nagios, Webguard)*;
- f. Pisahkan antara *file web server* dengan *file database* pada partisi yang digunakan.

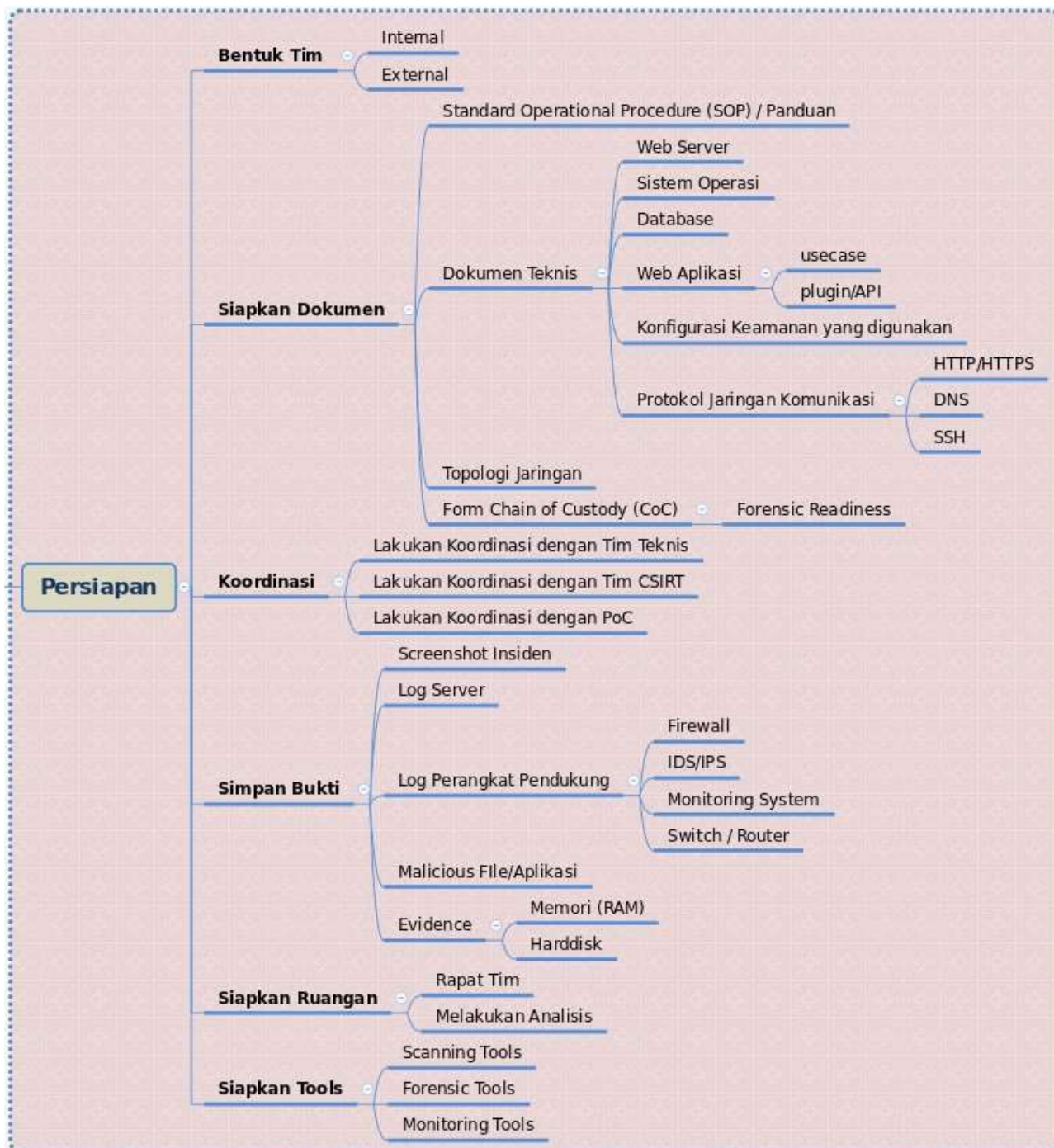
### 3.6. Tindak Lanjut

Sebagai tindak lanjut penanganan insiden, perlu dilakukan hal-hal sebagai berikut :

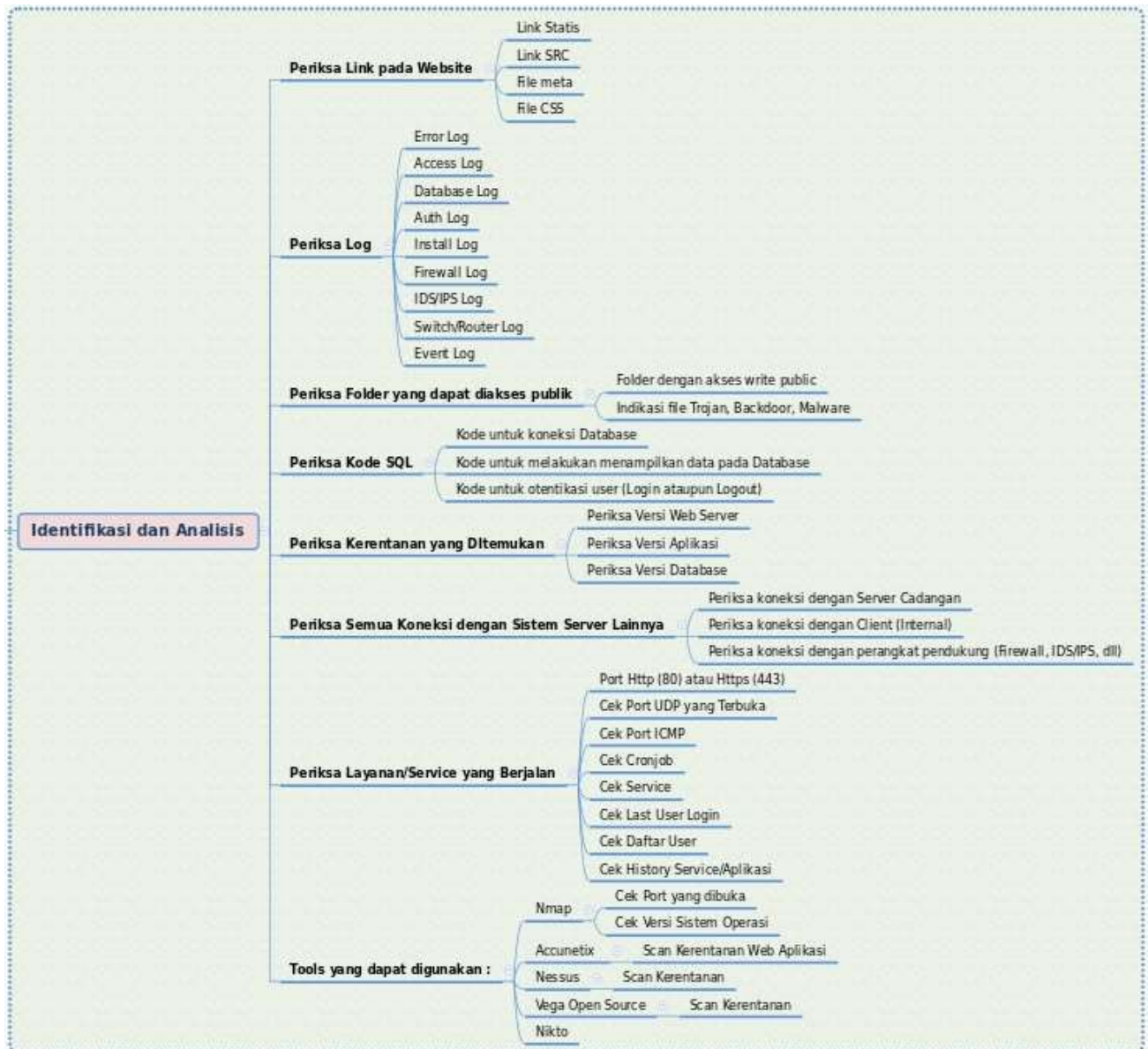
- 
- a. Lakukan uji keamanan web *server* dan aplikasi;
  - b. Memetakan kerentanan yang ditemukan, baik rentan terhadap serangan *SQL Injection*, *XSS*, *Misconfiguration*, atau sudah *deprecated*/usangnya versi aplikasi yang digunakan;
  - c. Membuat semua dokumentasi dan laporan terkait kegiatan dan waktu yang dibutuhkan pada proses *incident handling* yang telah dilakukan;
  - d. Menuliskan *tools* apa saja yang digunakan dalam membantu proses *incident handling*;
  - e. Menuliskan bukti-bukti yang ditemukan, hal ini terkait dengan proses hukum kedepannya;
  - f. Memberikan analisa dan penjelasan apa yang harus dilakukan sehingga insiden serupa tidak terulang kembali;
  - g. Membuat evaluasi dan rekomendasi.

# LAMPIRAN I – BAGAN PENANGANAN INSIDEN

## A. TAHAP PERSIAPAN



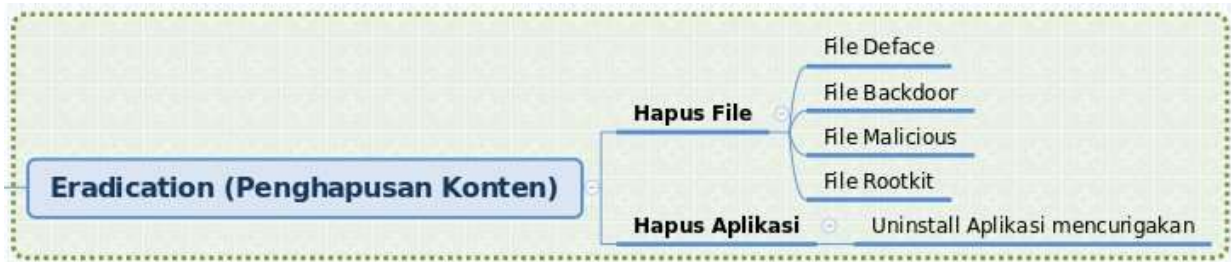
## B. TAHAP IDENTIFIKASI DAN ANALISIS



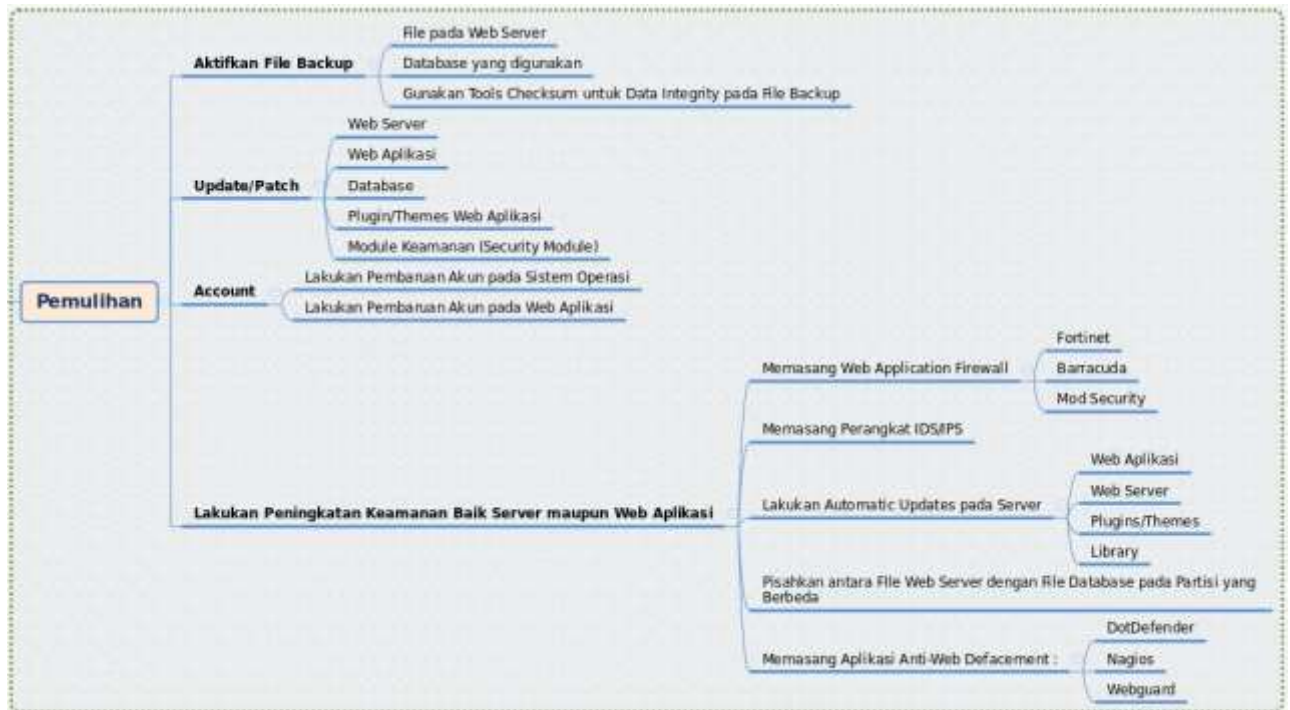
### C. TAHAP MITIGASI



### D. TAHAP PENGHAPUSAN KONTEN



## E. TAHAP PEMULIHAN



## F. TAHAP TINDAK LANJUT

