DINAS PENGAMANAN DAN PERSANDIAN
SATUAN SIBER

STANDAR OPERASIONAL PROSEDUR
PENANGANAN INSIDEN *WEB DEFACEMENT*

TAHUN 2023

VERSI DOKUMEN

No	Tanggal	Versi Dokumen	Oleh	Keterangan
1.	November 2023	Versi 2.0	Satsiber Dispamsanau	

DAFTAR ISI

PROSEDUR PENANGANAN INSIDEN *WEB DEFACEMENT* DI LINGKUNGAN TNI AU

1. PENDAHULUAN

Deface website atau *web defacement* adalah serangan terhadap suatu *website* dengan memodifikasi tampilannya baik sebagian atau seluruhnya. Baik penggantian gambar *website*, munculnya iklan *pop-up* yang mengganggu, atau bahkan seluruh bagian dari halaman website. Ibaratnya, *defacement* sama seperti tindakan vandalisme digital. Serangan ini cukup "*obvious*", pasalnya pelaku biasanya akan meninggalkan jejak. Motivasinya bermacam-macam, bisa untuk propaganda, memberi peringatan, menunjukan celah keamanan, atau sekedar pamer *skill*.

Seringkali, pelaku tidak melakukan perusakan berbahaya. Tapi, pada beberapa kasus, pelaku bisa saja mengunggah *malware* atau menghapus file penting di *server*. Perubahan tak terduga pada file-file ini mengindikasikan keamanan *website* yang rentan akan kejahatan internet dan *website* tersebut memiliki celah atau cacat pada sistem keamanannya.

2. TUJUAN

Penanganan yang terencana dan terorganisir sangatlah diperlukan dalam hal terjadinya insiden *web defacement* di lingkungan TNI Angkatan Udara, supaya hal tersebut dapat dilakukan, maka diperlukan adanya suatu prosedur yang standar untuk melakukan penanganan terhadap insiden tersebut. Secara umum tujuan standar operasional prosedur (SOP) ini adalah untuk memberikan arahan secara *best practices* dalam penanganan insiden *web defacement* di lingkungan TNI AU, 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.

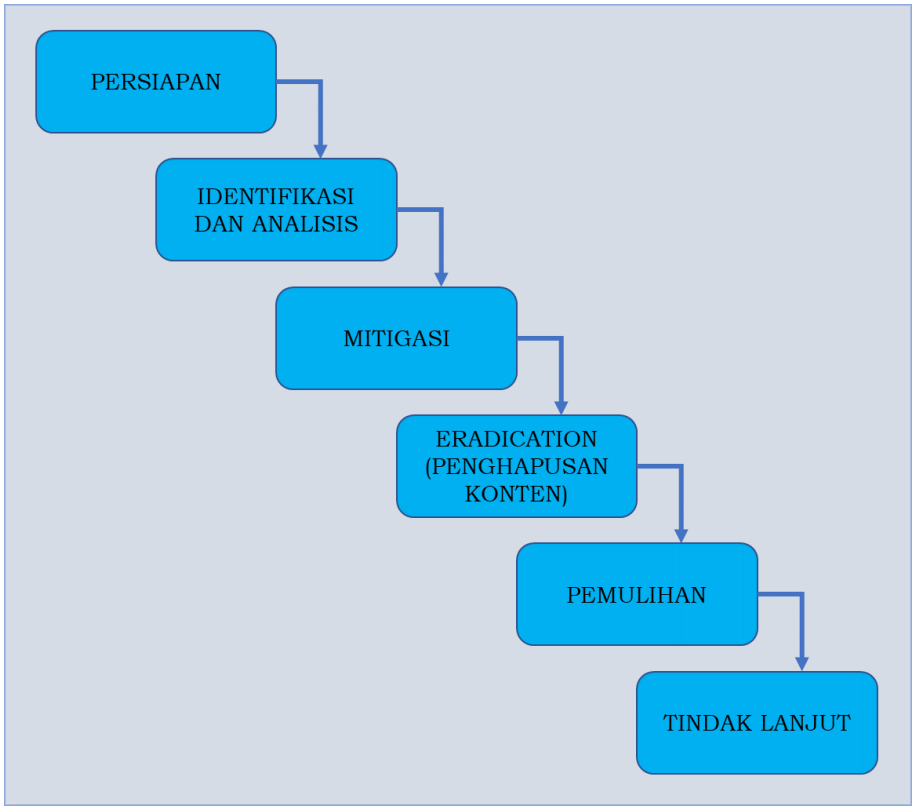
g. Mencegah adanya serangan lanjutan dan mencegah kerusakan agar tidak lebih meluas.

3. RUANG LINGKUP

SOP penanganan insiden ini berisi langkah-langkah yang harus diambil apabila terjadi insiden *web defacement* di lingkungan TNI AU, yang dimulai dari tahap persiapan sampai dengan tahap pembuatan laporan dari penanganan insiden. *Web defacement* dapat terjadi pada semua halaman *web* jajaran TNI AU, infrastruktur informasi vital TNI AU dan *web* informasi digital lainnya. SOP penanganan insiden ini dapat dijadikan acuan bagi semua individu atau tim yang bertindak sebagai penanggung jawab/administrator dari suatu *web server*.

4. PROSEDUR PENANGANAN *WEB DEFACEMENT*

Terdapat 2 (dua) cara bagi satker/perorangan untuk meletakan suatu halaman *web*, yaitu meletakan pada *server* yang dikelola secara terpusat di Pusat Data *Server* TNI AU, dikelola sendiri atau meletakan halaman *web*nya pada *web hosting*. Bagi yang meletakkan halaman *web*nya pada Pustas TNI AU, maka apabila terjadi *web deface* harus melakukan koordinasi dengan staf Pustas TNI AU. Sedangkan bagi yang meletakkan halaman *web*nya 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* memiliki prosedur untuk menangani insiden *web defacement*. Proses penanganan insiden *web defacement* dapat dilaksanakan dalam kurun waktu hingga 14 hari kerja. 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 defacement* dapat diuraikan sebagai berikut:

4.1. **Persiapan**

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

1) *Standar Operation Procedure* (SOP).

2) *Form-form* yang akan digunakan: *form* penanganan insiden, *form chain of custody*.

3) Gambaran diagram terbaru yang menggambarkan hubungan antar komponen-komponen aplikasi yang membangun *website* (*web server*, aplikasi *web*, para *user*, diagram *network*).

4) 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 penanangan 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*.

4.2. **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*.

4.3. **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.

4.4. *Eradication* (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*.

4.5. Pemulihan

Pada tahapan ini bertujuan untuh 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 webserver* dengan *file database* pada partisi yang digunakan.

4.6. **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 aplilkasi 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 membatu proses *incident handling*.

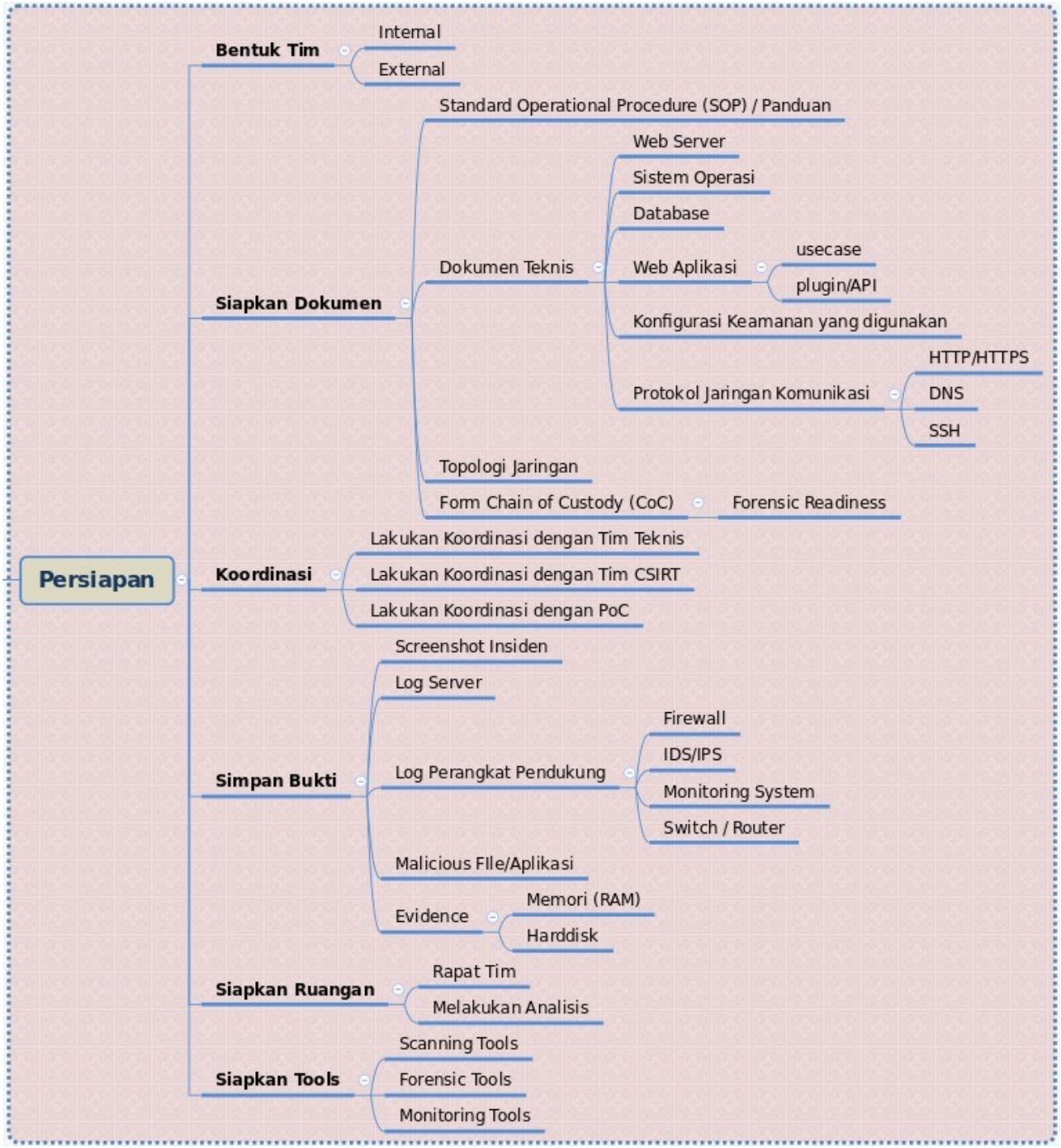
e. Menuliskan bukti-bukti yang ditemukan, hal ini terkait dengan proses hukum kedepannya.

f. Memberikan analisa dan penjelasan apa yang harus dilakukan sehingga insiden serupa tidak terulang kembali.

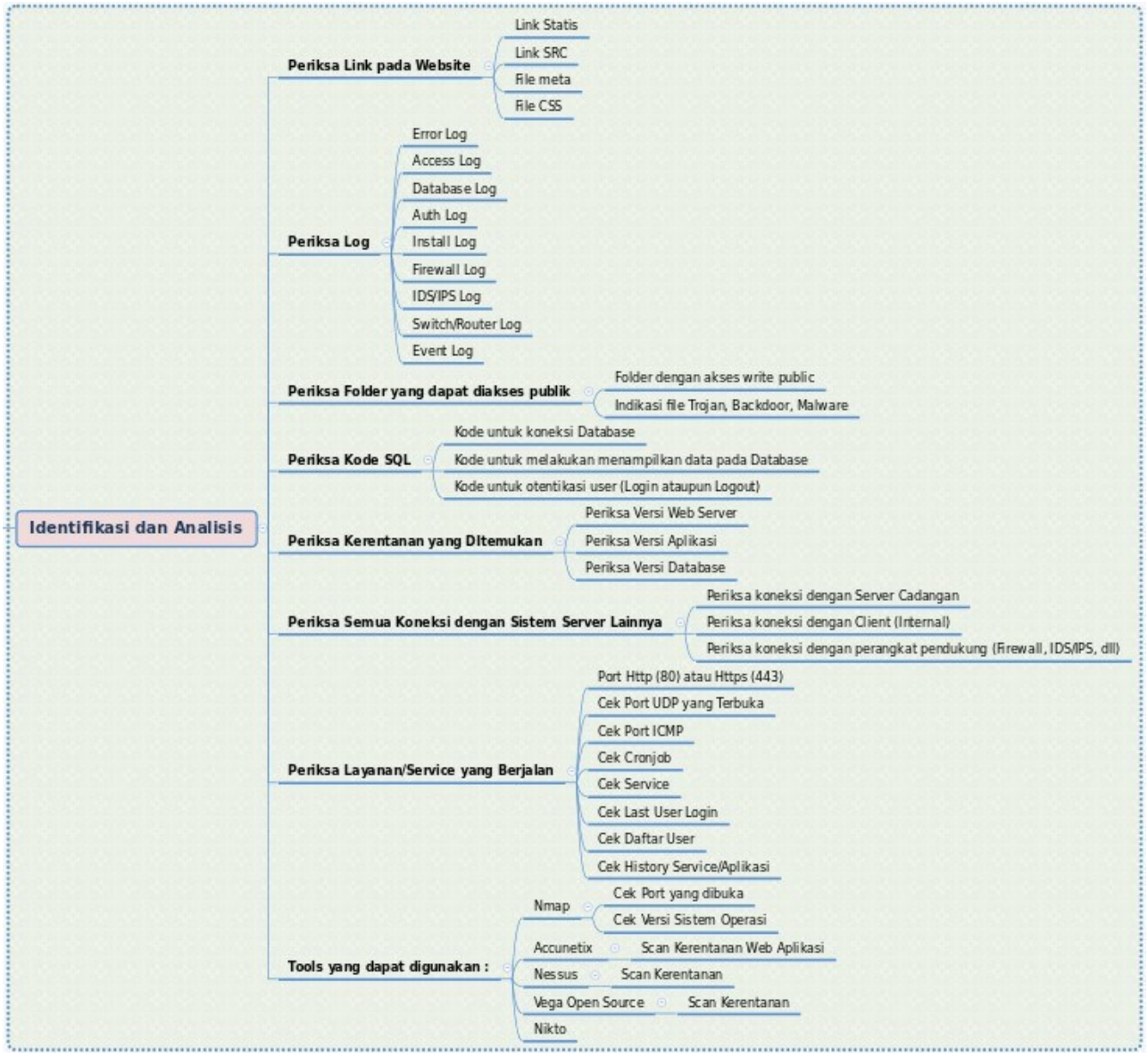
g. Membuat evaluasi dan rekomendasi.

BAGAN PENANGANAN INSIDEN

A. TAHAP PERSIAPAN

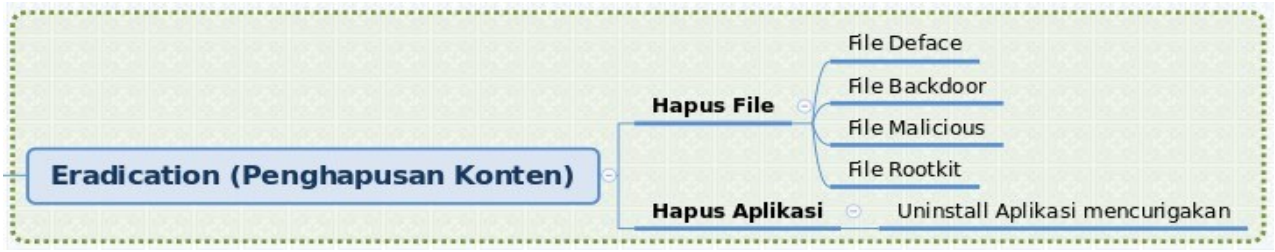


B. **TAHAP IDENTIFIKASI DAN ANALISIS**

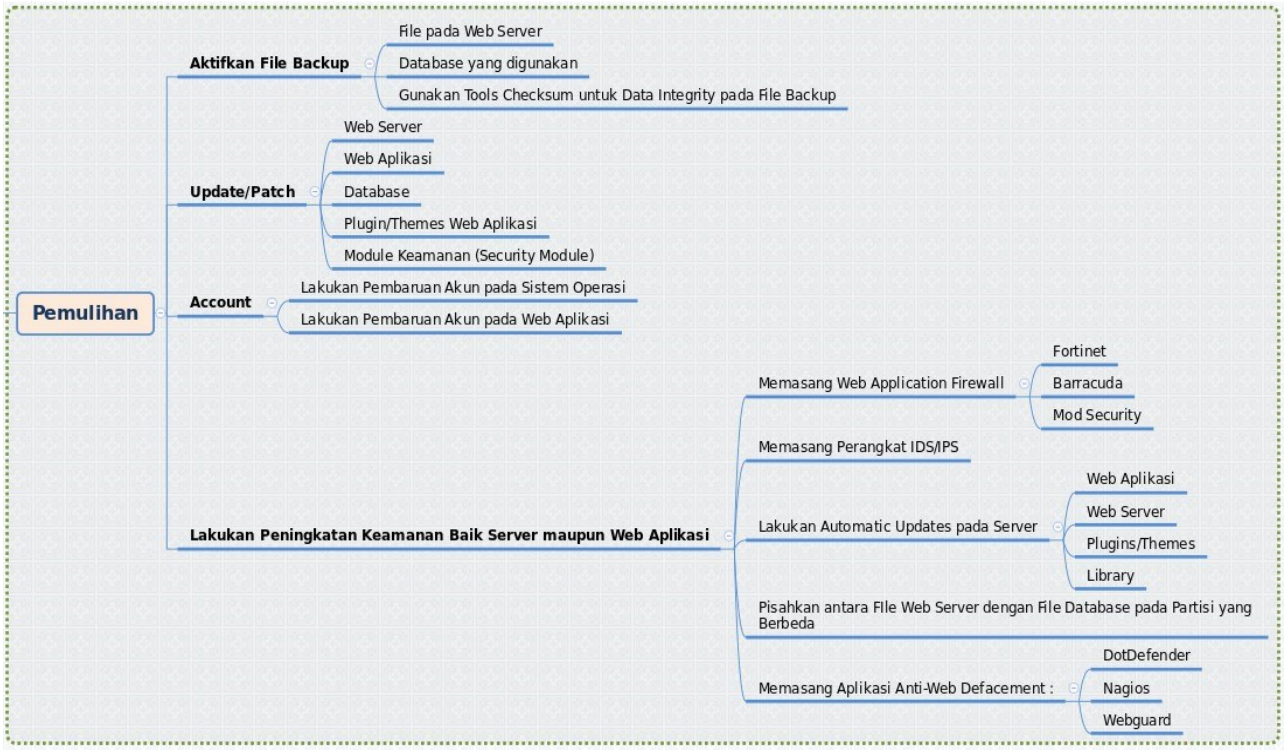


C. **TAHAP MITIGASI**

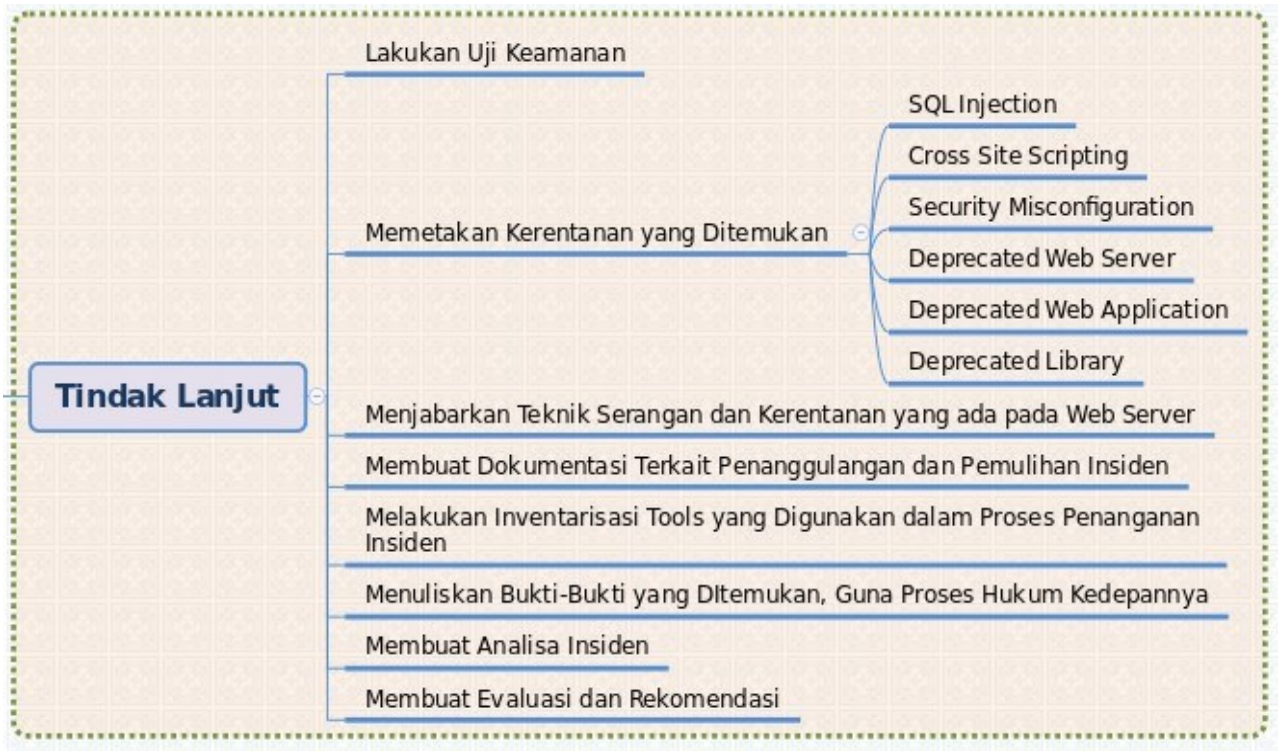
D. **TAHAP PENGHAPUSAN KONTEN**



E. **TAHAP PEMULIHAN**



F. **TAHAP TINDAK LANJUT**



Jakarta, November 2023

Kepala Satsiber,

Tri Priyo Widodo
Kolonel Sus NRP 525026