# WEB DEFACEMENT : JUDI ONLINE

Dokumen tentang langkah - langkah penanggulangan insiden *web defacement* Judi Online dan Mitigasi

DIREKTORAT OPERASI KEAMANAN SIBER

**Incident Response Team**

# TABLE OF CONTENT

# PENDAHULUAN

Beberapa waktu ini banyak ditemukan insiden serangan siber yang terjadi di Indonesia. Salah satu insiden siber tersebut yaitu insiden Web Defacement yang terjadi pada situs Pemerintahan dan Pendidikan. Web defacement yang sangat marak belakangan ini tentang “Web Defacement Slot Gacor atau Judi Online” di mana penyerang melakukan perubahan tampilan pada situs dengan mengganti tampilan menjadi judi online.

Dokumen ini disusun atas maraknya insiden yang terjadi. Dokumen berisikan tentang bagaimana alur serangan web defacement terjadi dan bagaimana cara melakukan penanggulangan dan pemulihan atas insiden yang terjadi serta bagaimana cara mitigasi untuk meminimalisir kemungkinan terkena serangan Web Defacement pada sebuah situs website.

JAKARTA, JUNI 2023

Ditandatangani secara elektronik oleh:
**DIREKTUR OPERASI KEAMANAN SIBER**

**Andi Yusuf, M.T.**
Pembina Tk. I (IV/b)


# WEB DEFACEMENT

*Web defacement* merupakan suatu serangan pada *website* yang mengubah tampilan asli atau konten dari sebuah *website*. Pelaku serangan *web defacement* disebut sebagai ***defacer***. *Web defacement* seringkali dimanfaatkan untuk menguji kemampuan *defacer* dan sebagai tindakan vandalisme elektronik. *Web defacement* dapat juga dimanfaatkan untuk kepentingan agenda politik, karena dapat menurunkan reputasi atau kredibilitas dari pihak tertentu.

Serangan *web defacement* dapat dilakukan dengan memanfaatkan sebuah kelemahan dari sistem sehingga memungkinkan pelaku memiliki akses masuk hingga ke server dan memiliki kewenangan untuk mengganti atau menghapus konten suatu *website*. Terdapat berbagai metode untuk melakukan *web defacement*, cara yang sering dijumpai yaitu eksploitasi pada kerentanan *plugins framework* dan *SQL Injection* yang memungkinkan akses administratif.

*Web defacement* belakangan ini marak terjadi pada situs milik pemerintah dan pendidikan, terutama *web defacement* judi online. Insiden ini terdeteksi cukup masif hingga menyebabkan puluhan bahkan ratusan situs terdampak. Dampak nyata dari *web defacement* judi online yaitu situs menampilkan halaman judi online. Salah satu alasan hal tersebut banyak menyasar situs milik pemerintah dan pendidikan diindikasikan sebagai cara untuk menghindari situs di-*block* oleh pihak berwenang.

## DAMPAK

### Reputasi

Tampilan halaman judi online yang tidak pantas atau ilegal pada situs pemerintah akan menciptakan kesan negatif terhadap integritas.

### Kepercayaan

Masyarakat akan meragukan keamanan dan keandalan situs pemerintah, serta kemampuan pemerintah dalam melindungi data sensitif dan informasi publik.

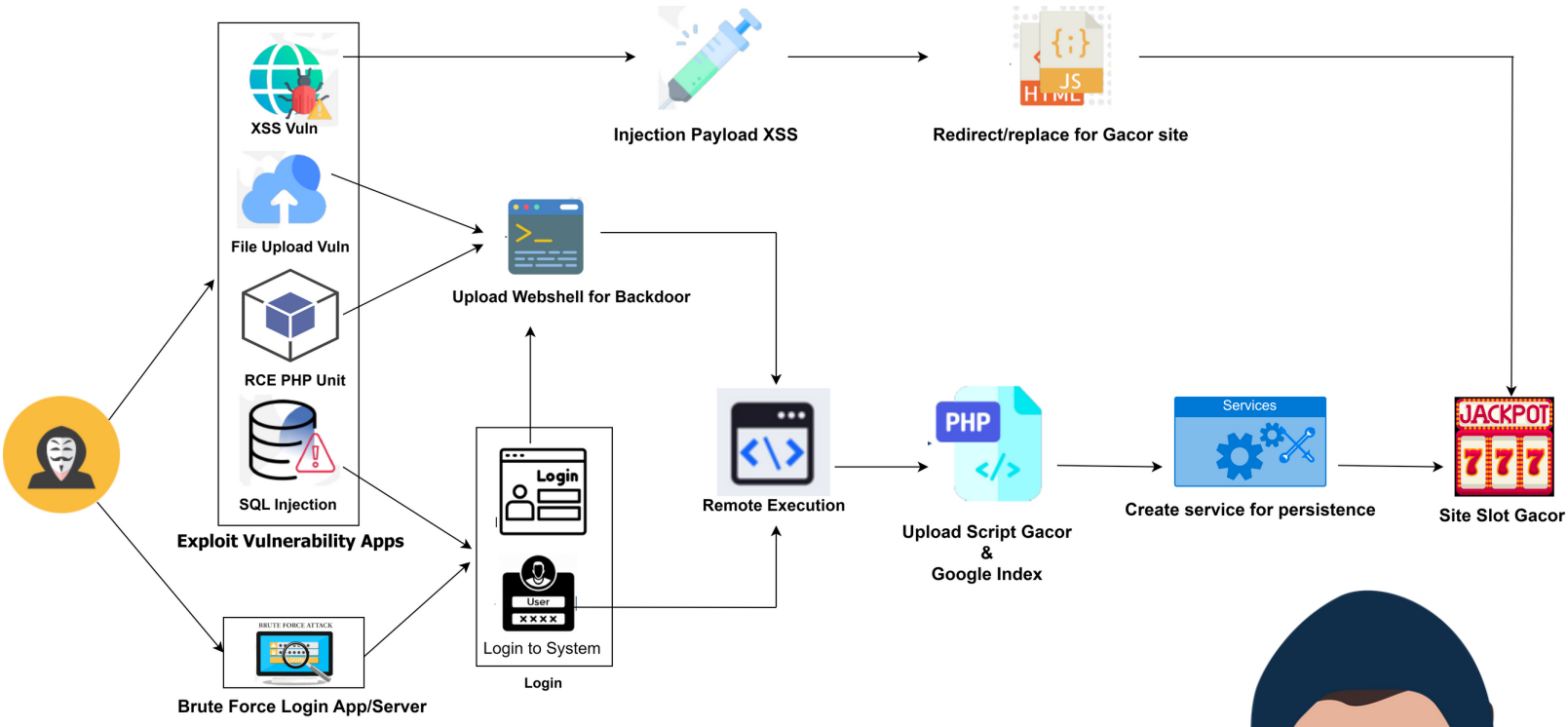
### Availability

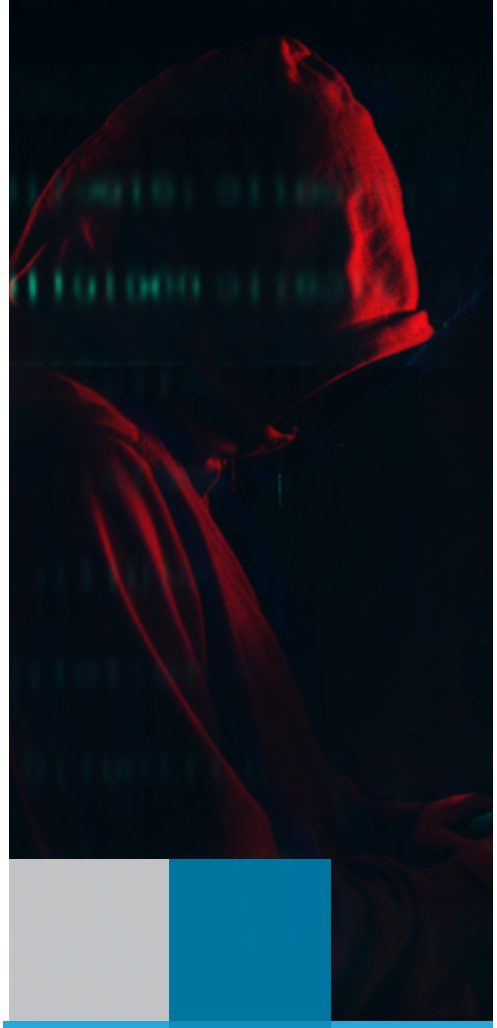
*Defacement* dapat menyebabkan gangguan pada layanan yang disediakan oleh situs pemerintah serta dapat menyebabkan ketidaknyamanan dan ketidakpuasan masyarakat terhadap pemerintah.

# ALUR SERANGAN

Alur serangan merupakan suatu metode atau jalan yang digunakan oleh penyerang untuk melancarkan serangan.

Alur serangan menggambarkan cara penyerang memanfaatkan kelemahan atau celah dalam sistem untuk memperoleh akses tidak sah terhadap sistem



WEB DEFACEMENT : ATTACK VECTOR

# A INITIAL ACCESS

*Initial access* melibatkan upaya dalam memanfaatkan kerentanan dan kesalahan pada konfigurasi untuk dapat masuk kedalam sistem. *Web defacement* judi online diidentifikasi memanfaatkan *Exploit Vulnerability Apps* dan *Brute Force Attack* untuk masuk ke dalam sistem.

- **Exploit Vulnerability Apps**

Penyerang melakukan percobaan eksploitasi kerentanan pada *software* dan teknologi sistem yang digunakan. Kerentanan dapat berupa *bug* atau *security misconfiguration.* Berikut beberapa *initial access* yang dimanfaatkan penyerang dalam *defacement* judi online.

### a. XSS Vulnerability

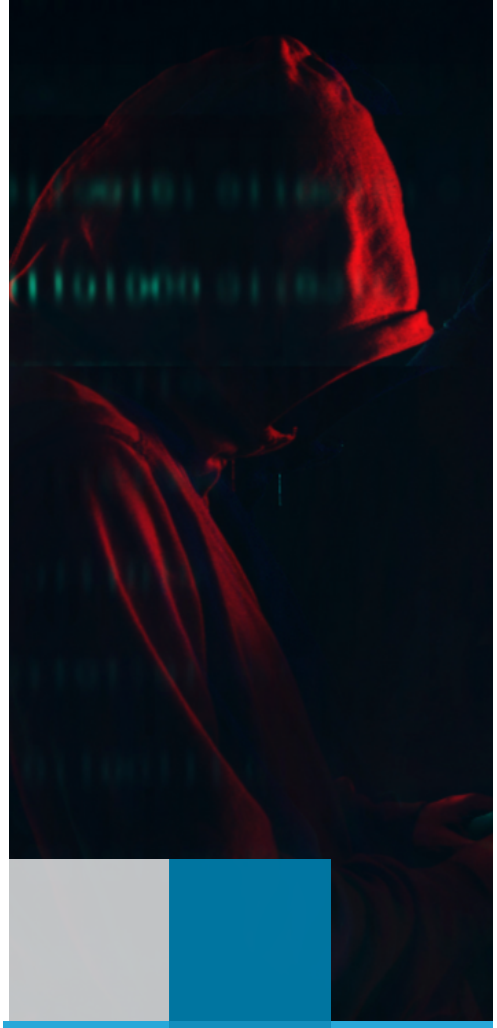
Penyerang memanfaatkan kerentanan XSS (*Cross Site Scripting)* untuk melakukan *injection payload XSS* dengan tujuan untuk menyisipkan *script* judi online sehingga *script* akan tertanam pada salah satu halaman *legitimate* yang secara otomatis ketika diakses akan tereksekusi dan menampilkan halaman judi online.

### b. File Upload Vulnerability

Penyerang memanfaatkan kerentanan *file upload* yang tidak menerapkan filtering dan sanitasi dengan baik sehingga penyerang dapat melakukan *upload webshell* atau *backdoor*.

### c. PHP Unit Vulnerability

Penyerang sering memanfaatkan kerentanan PHP Unit yang dapat berdampak pada *remote code execution*. Penyerang akan melakukan instalasi *backdoor* atau *webshell*.



WEB
DEFACEMENT

### d. SQL Injection

Kerentanan *SQL Injection* juga menjadi salah satu *attack vector* yang sering dimanfaatkan penyerang dalam melakukan *defacement* judi online. Kredensial hasil *SQL Injection* dapat digunakan untuk *login* aplikasi bahkan ke sistem.

- **Brute Forece Login**

Penyerang sering kali melakukan *brute force attack* pada aplikasi dan juga pada layanan *remote access* yang diaktifkan (SSH). Dalam beberapa kasus diketahui bahwa *brute force* terjadi karena penggunaan *password* yang tidak kuat sehingga dapat dengan mudah dilakukan *brute force attack*. Contoh penggunaan *password* yang dijumpai berhasil dilakukan *brute force* antara lain **12345**, **password, admin** dan lainnya.

# B Execution

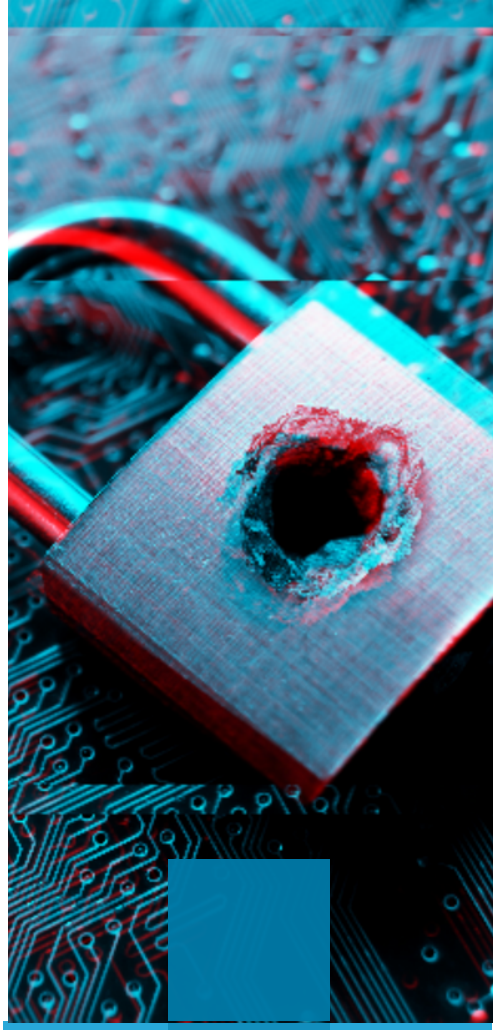
Penyerang akan melakukan aktivitas pada server untuk dapat melakukan penyisipan *script* judi online, beberapa aktivitas yang dilakukan antara lain:

- ***Remote Execution***

Penyerang memanfaatkan backdoor yang telah tertanam pada server untuk melakukan remote code execution seperti melakukan pembuatan akun, serta membuat file-file deface. Beberapa webshell atau backdoor yang sering ditemukan pada defacement judi online yaitu Lzt.zip.gz.txt.php, Mad.php (https://github.com/MadExploits/Gecko), dan alfa.php (https://github.com/backdoorhub/shell-backdoor-list/blob/master/shell/php/alfa.php)

- ***Upload script Judi Online dan Google Index***

Penyerang akan melakukan modifikasi pada file .htaccess untuk mengizinkan beberapa file webshell untuk dapat diekseskusi pada folder yang telah ditentukan. Kemudian penyerang akan membuat folder Slot-Gacor yang berisi file index.php dan Google Indexing dengan tujuan supaya akan tampil paling atas pada mesin pencarian Google.



# C Persistence

Penyerang melakukan mekanisme *persistence* untuk memastikan akses mereka terhadap server korban tetap tersedia. Berikut beberapa mekanisme *persistence* yang terjadi pada *defacement* judi online

- **Penyisipan Backdoor/Webshell**

Penyisipan dan *upload backdoor* atau *webshell* sering ditemukan pada insiden *defacement*. Penyerang memanfaatkan *webshell* sebagai pintu untuk masuk ke server. Beberapa *webshell* yang sering ditemukan antara lain **Lzt.zip.gz.txt.php**, **Mad.php, b374k.php,** dan **alfa.php.**

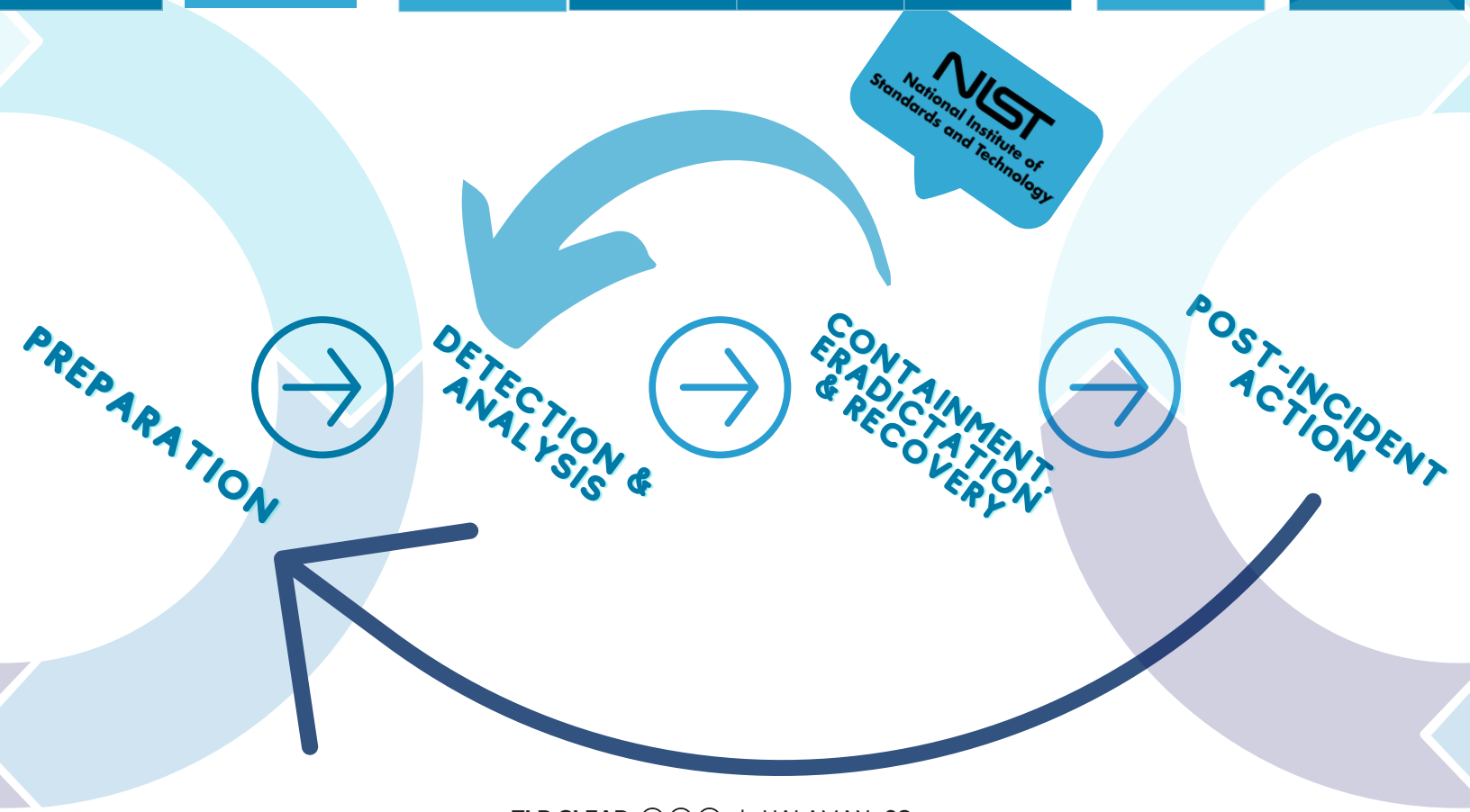
- **Pembuatan Process dan Service**

Beberapa kasus dijumpai bahwa penyerang juga melakukan *persistence* dengan membuat *process* dan *service* yang secara terus-menenus berjalan untuk memastikan bahwa tampilan judi online tidak dapat dihapus. Ketika folder Slot-Gacor dihapus, secara otomatis *services* dan *process* akan melakukan generate folder dan isinya kembali. *Services* yang ditemukan pada insiden defacement judi online antara lain **jj.service, ii.srevice,** dan **cahce-l.service.**

Bruce Schneier

If someone steals your password, you can change it. But if someone steals your thumbprint, you can't get a new thumb.

# PENANGANAN INSIDEN : WEB DEFACEMENT






Sumber: Computer Security Incident Handling Guide NIST 800-52

# A Preparation

Tahap ini adalah tahap dimana kebijakan, prosedur, teknologi, dan sumber daya manusia harus disiapkan secara matang. Dalam suatu organisasi/institusi, kemampuan melakukan respon yang cepat terhadap suatu insiden merupakan suatu keharusan. Persiapan digunakan untuk mempersiapkan segala sesuatu untuk melakukan penanganan insiden. Beberapa hal yang perlu dipersiapkan dalam tahap preparation antara lain:

- **Pembentukan Tim Tanggap Insiden Siber**

Pembentukan tim tanggap insiden siber dapat membantu memfokuskan langkah penanganan insiden yang akan dilakukan, sehingga proses penanganan insiden dapat dilakukan dengan cepat dan tepat.

- **Penyiapan Dokumen Legal**

Dalam melakukan penanganan insiden tentu akan melibatkan dokumen-dokumen terkait dengan sistem baik berupa spesifikasi sistem. Beberapa dokumen yang perlu disiapkan antara lain:

1. Dokumen topologi jaringan
2. Dokumen kebijakan atau prosedur penggunaan sistem
3. Dokumen informasi aset aset
4. Dokumen *Chain of Custody* (CoC)
5. Dokumen *Business Continue Plan* (BCP), jika terjadi gangguan pada proses bisnis
6. Dokumen *Incident Response Plan* (IRP).

- **Melakukan Koordinasi Dengan Pihak - Pihak Terkait**

Koordinasi menjadi hal yang penting dalam melakukan penanganan insiden. Dengan telah terbentuknya Tim Tanggap Insiden Siber atau CSIRT maka dapat melakukan koordinasi dengan CSIRT Sektoral serta CSIRT Organisasi lainnya sehingga dapat dilakukan sharing informasi dalam mempercepat proses penanganan insiden. Koordinasi dapat dilakukan dengan antara lain:

1. CSIRT Sektoral
2. CSIRT Organisasi
3. Aparat Penegak Hukum
4. Nat-CSIRT (BSSN)

## • Menyiapkan Jump Kit Penanganan Insiden

**Jump Kit** merupakan peralatan atau *tools* yang digunakan untuk melakukan penanganan insiden, dalam hal ini insiden *web defacement* judi online. Berikut merupakan beberapa *tools* yang dapat digunakan untuk proses penananganan dan analisis insiden *web defacemen* judi online.

| Evidence Collection | Computer Forensics | IoC Scanner |
|---|---|---|
| dd | FTK Imager | ThorLite |
| FTK imager | Autopsy | Yara Rules |
| KAPE | Volatility | Redline |

## • Melakukan Identifikasi Aset Terdampak

Ketika telah terjadi insiden, maka perlu dengan segera dilakukan proses identifikasi aset terdampak. Identifikasi aset terdampak bertujuan untuk melakukan isolasi dan mengganti sistem atau layanan terdampak menggunakan sistem *backup*.

WEB DEFACEMENT

# B Detection & Analysis

## MERUPAKAN

tahap yang dilakukan secara berulang dengan tujuan untuk dapat mendeteksi adanya *malicious file, backdoor,* atau *webshell* pada sistem dan melakukan analisis untuk menemukan *root cause* insiden yang terjadi. Langkah-langkah yang dapat dilakukan dalam melakukan penanganan insiden *web defacement* judi online antara lain:

- **Melakukan akuisisi & pengumpulan barang bukti digital**

**Setelah dilakukan identifikasi aset dan dilakukan isolasi, maka selanjutnya dilakukan pengumpulan barang bukti digital untuk proses analisis. Pengumpulan barang bukti digital dapat dilakukan secara *full acquisition* atau dengan pengumpulan artefak-artefak.**

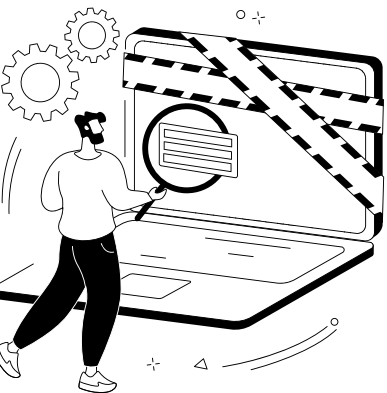
1. Pengambilan artefak pada Windows dapat menggunakan tools KAPE GUI.
2. Pengambilan artefak pada Linux dapat dilakukan pada Log akses (/var/log/), bash history (/root dan /home)
3. *Full Acquisition* pada Windows dapat menggunakan tools FTK Imager.
4. *Full Acquisition* pada Linux dapat menggunakan tools dd dengan perintah:

```
dd if=/dev/sdb of=USB_image.dd bs=4k
conv=noerror,sync status=progress
```

## • Melakukan Scanning Pada Server Terdampak

*Scanning* dapat dilakukan secara langsung pada server terdampak atau pada file hasil akuisisi (full akuisisi/image). *Scanning* dapat dilakukan dengan menggunakan *tools opensource,* seperti **Thor Lite Scanner** yang dapat digunakan untuk mendeteksi kemungkinan *malicious file/backdoor/webshell* (**https://www.nextron-systems.com/thor-lite/**). Setelah dilakukan *scanning* maka dapat dilakukan validasi hasil *scanning* untuk menghindari *false positif*. Berikut merupakan perintah untuk melakukan *scanning* spesifik folder menggunakan Thor Lite Scanner

**sudo ThorLinux -a Filescan --intense --norescontrol --cross-platform --alldrives -p [path]**


## • MELAKUKAN PENGECEKAN KONEKSI COMMAND AND CENTER (CnC)

*Command and Center (CnC)* merupakan infrastruktur yang digunakan oleh penyerang untuk melakukan kontrol terhadap server yang telah terinfeksi. Untuk melakukan pengecekan terhadap kemungkinan CnC maka dapat dilakukan pengecekan port-port terbuka yang memiliki keterangan LISTENING dan ESTABLISHED. Pengecekan port *suspicious* dapat dilakukan dengan cara dibawah dan selanjutnya dilakukan validasi terhadap beberapa port yang diindikasikan sebagai *suspicious*.

- ***Pada Linux***

*sudo netstat -tulpn*

```
reed@ubuntu:~$ netstat -tulpn
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 10.0.3.1:53             0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:11211         0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:5432          0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      -
```

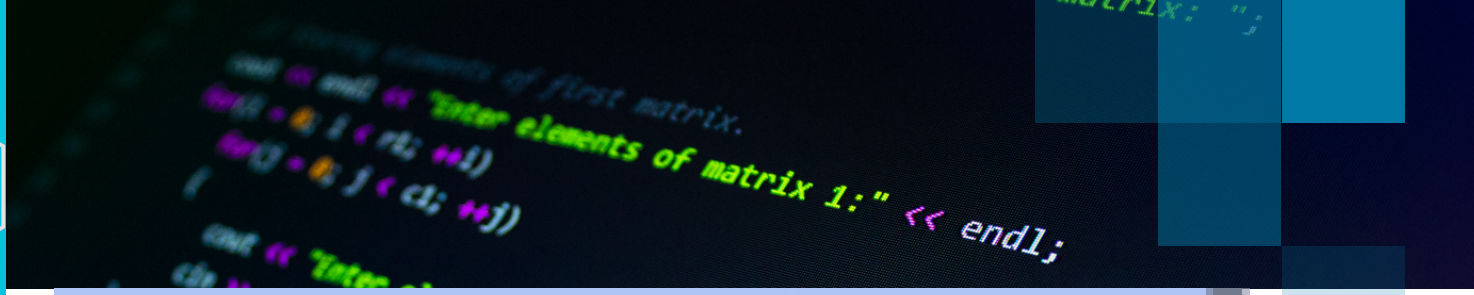
- ***Pada Windows***

*netstat -ano*

```
C:\Windows\System32>netstat -ano

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       1912
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:902            0.0.0.0:0              LISTENING       13504
  TCP    0.0.0.0:912            0.0.0.0:0              LISTENING       13504
  TCP    0.0.0.0:1042           0.0.0.0:0              LISTENING       31380
  TCP    0.0.0.0:1043           0.0.0.0:0              LISTENING       31380
  TCP    0.0.0.0:1947           0.0.0.0:0              LISTENING       4648
  TCP    0.0.0.0:2968           0.0.0.0:0              LISTENING       3740
  TCP    0.0.0.0:3655           0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING       15448
  TCP    0.0.0.0:5357           0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:7070           0.0.0.0:0              LISTENING       6852
  TCP    0.0.0.0:9012           0.0.0.0:0              LISTENING       4112
  TCP    0.0.0.0:9013           0.0.0.0:0              LISTENING       4112
```




## • Melakukan Pengecekan Mekanisme Presistent

Mekanisme persistent yang digunakan oleh penyerang *web defacement* judi online salah satunya yaitu membuat **Slot-Gacor** tidak dapat dihapus, sehingga ketika folder Slot-Gacor dihapus secara otomatis akan muncul kembali. Untuk melakukan pengecekan mekanisme persistent tersebut dapat menggunakan *tools* **auditd** pada Linux. Auditd merupakan layanan pada Linux yang berfungsi untuk melakukan pencatatan seluruh aktivitas pada Linux, sehingga ketika terdapat *process* dan *service* yang berjalan secara terus-menerus, auditd akan mencatatnya. Berikut merupakan cara melakukan pengecekan mekanisme persistent:

- **Pada Linux**

- **Melakukan auditd**

```
sudo apt install auditd
sudo nano /etc/audit/rules.d/10-procmon.rules
```

tambahkan *rules* berikut:

```
-a exit,always -F arch=b64 -S execve -k procmon
-a exit,always -F arch=b32 -S execve -k procmon
```

```
sudo service auditd restart
```

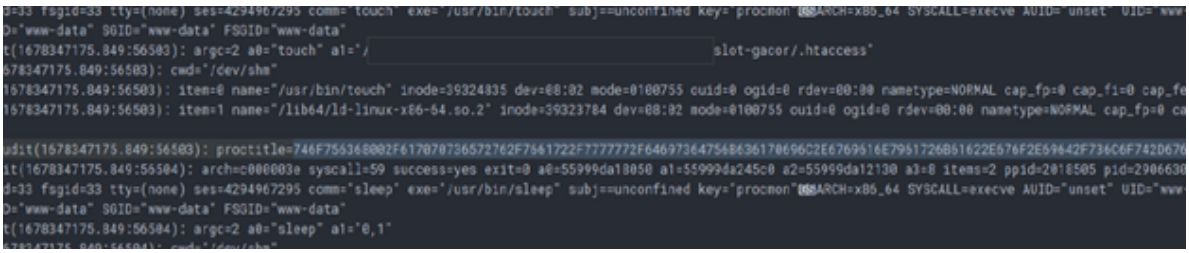
Selanjutnya dilakukan pemantauan pada file audit.log yang terdapat pada folder /var/log/audit/

Untuk menampilkan isi file audit.log dapat menggunakan perintah

```
sudo tail -f /var/log/audit/audit.log
```

atau

```
sudo cat /var/log/audit/audit.log
```




- **Menggunakan list services**

Untuk mengecek *services* yang berjalan dapat juga dilakukan dengan menggunakan perintah

```
sudo systemctl list-units -type service | grep running
```

untuk mengetahui detail *services* yang berjalan dapat menggunakan perintah

```
sudo service name_service status
```

Beberapa nama *services* yang ditemukan pada kasus *defacement* judi online antara lain **cache-l.service**, **ii-service,** dan **jj-service** dengan keterangan *services* "Jendral Maya Still Alive".

- **Menggunakan list process**

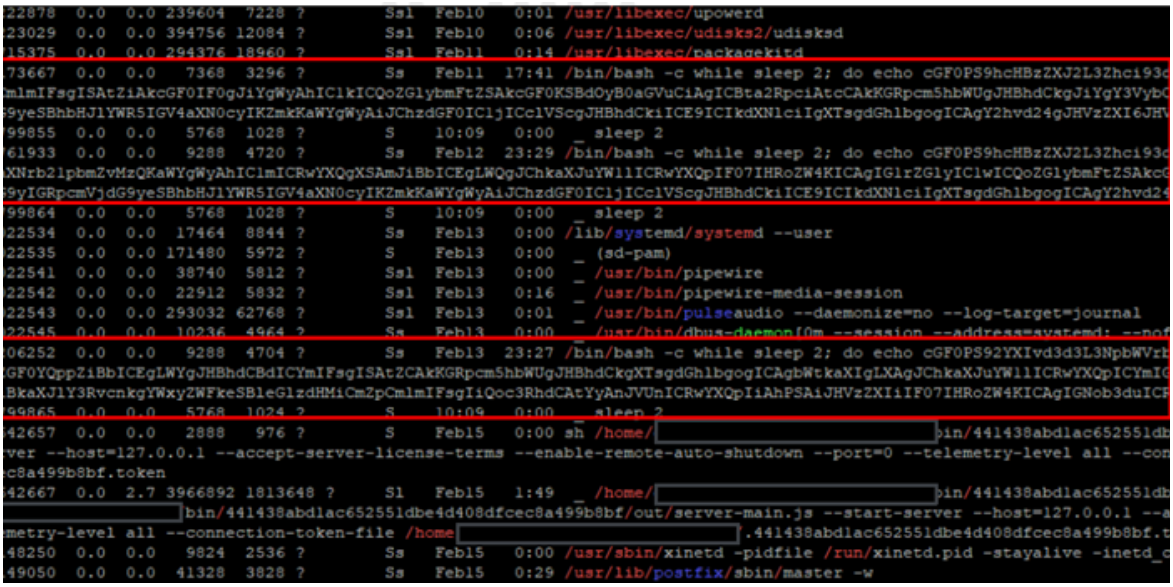
Perintah yang dapat digunakan untuk mengetahui proses yang berjalan adalah sebagai berikut:

```
sudo ps aux
```

atau

```
sudo ps aux | www-data
```

Beberapa kasus *defacement* judi online menggunakan mekanisme persistent dengan menjalankan proses dengan *bash script* yang terencode **base64.**




- **Pada Windows**

Untuk melakukan pengecekan *suspicious services* pada Windows dapat menggunakan GUI yaitu dengan mengetikan **Windows + R** lalu ketik **services.msc**. selanjutnya dapat dilakukan pengecekan daftar *services* yang berjalan apakah terdapat *services* mencurigakan.

Untuk melakukan pengecekan *process*, pada Windows dapat menggunakan tools *command-line* **tasklist.** Ketikkan tasklist pada command-line sehingga akan muncul daftar *process* yang berjalan.

```
C:\Windows\System32>tasklist

Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0          8 K
System                           4 Services                   0     11.248 K
Secure System                  140 Services                   0     74.672 K
Registry                       192 Services                   0     55.084 K
smss.exe                       868 Services                   0      1.100 K
csrss.exe                     1412 Services                   0      6.524 K
wininit.exe                   1544 Services                   0      6.292 K
services.exe                  1616 Services                   0     13.616 K
LsaIso.exe                    1624 Services                   0      3.612 K
lsass.exe                     1652 Services                   0     31.652 K
svchost.exe                   1772 Services                   0     41.660 K
fontdrvhost.exe               1800 Services                   0      3.092 K
```

## • Melakukan Pencarian Malicious File atau Suspicious File

Selain menggunakan metode *scanning* Thor Lite Scanner, untuk menemukan *malicious file* atau *suspicious file* dapat dilakukan dengan menggunakan pencarian melalui *command-line*. Untuk melakukan pencarian diperlukan *keyword* seperti "**Slot-Gacor**", "**shell.php**", dan lainnya.

```
sudo apt install locate && update
sudo locate slot- atau sudo locate gacor
sudo locate nama_shell.php
```

atau menggunakan *command find*

```
sudo find / -type f -executable -printf "%T+ %p\n" 2>/dev/null | grep -Ev "000| /site-packages|/python|/node_modules|\.sample|gems" | sort -r | head -n 100
```

## • Melakukan analisis pada barang bukti digital yang telah dikumpulkan

- **Pada Linux**

  Analisis barang bukti dapat dilakukan pada log akses dan log system (**auth, wtmp, btmp, auditd**). Seluruh log tersebut tersimpan pada folder **/var/log/**. Log akses terdapat pada **/var/log/apache2 atau /var/log/httpd**

- **Pada Windows**

  Log akses server Windows secara default terdapat pada folder *engine website***.** Pada web server XAMPP terdapat pada folder **xampp/apache/logs**. Selain melakukan analisis pada log akses, terdapat **windows event log** yang terdapat pada folder

  **C:\Windows\System32\winevt\logs** atau **C:\Windows\System32\config.**

  Untuk melakukan analisis secara otomatis pada Windows Event Log dapat menggunakan *tools* **Hayabusa** yang dapat diunduh pada laman https://github.com/Yamato-Security/hayabusa. Hayabusa akan melakukan *scanning* Windows Event Log berdasarkan Sigma *rules*.

# C CONTAINMENT, ERADICATION & RECOVERY

- ***Melakukan pengarsipan dan penghapusan file malicious dan suspicious yang ditemukan***

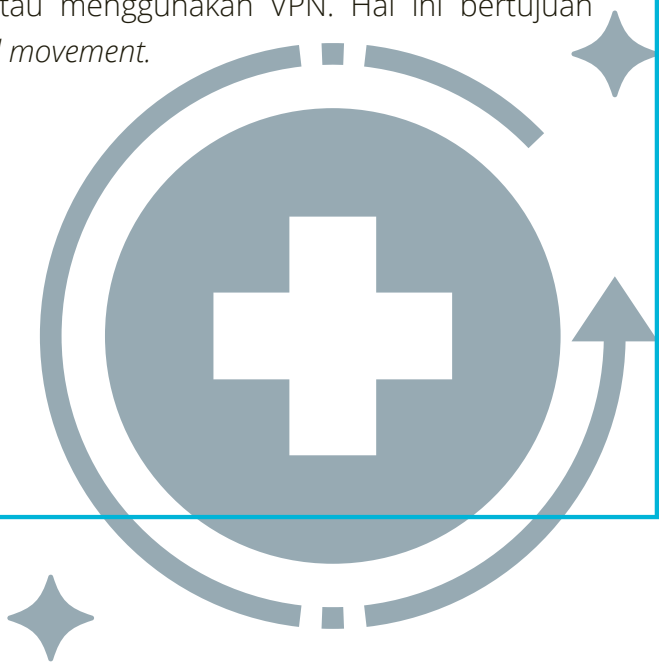
Pengarsipan *file malicious* dan *suspicious* termasuk *script* judi online sebelum dilakukan penghapusan bertujuan untuk analisis lebih lanjut dan dapat memanfaatkan file-file tersebut untuk membuat *rules* deteksi untuk perangkat keamanan. Setelah file-file tersebut diarsipkan, selanjutnya dapat dilakukan pembersihan atau penghapusan

- ***Melakukan modifikasi file .htaccess***

Penyerang melakukan modifikasi file **.htaccess** untuk mengizinkan *malicious file* dengan ekstensi tertentu dapat dieksekusi. Oleh karena itu perlu dilakukan modifikasi kembali pada file .htaccess.

- **Melakukan Pembatasan Akses pada Server Terdampak**

Pembatasan akses pada server terdampak dilakukan dengan cara melakukan *blocking* alamat IP yang terindikasi melakukan aktivitas *malicious*. Selain itu juga dapat dilakukan penutupan port untuk *remote access,* sehingga akses ke server hanya dapat dilakukan secara local atau menggunakan VPN. Hal ini bertujuan untuk menghindari kemungkinan *lateral movement.*



- **Melakukan Kill Process dan Service Malicious atau Suspicious**

Pada beberapa kasus *defacement* judi online diketahui bahwa terdapat *process* dan *services* yang berjalan secara terus-menerus sebagai mekanisme persistent. Oleh karena itu perlu dilakukan pengarsipan file *process* dan *services* tersebut untuk analisis lebih lanjut dan selanjutnya dilakukan penghentian atau *kill proccess*.



- ## Sistem Operasi Linux

### Kill Process

```
sudo kill -9 PID_process
```

### Kill & delete Service

```
sudo service name_service stop
sudo service name_service disable
sudo rm /etc/system/system/name_service.service
```

### Penghapusan file dan folder malicious/suspicious

```
sudo rm -r folder_slot
sudo rm name_shell.php
```

- ## Sistem Operasi Windows

### Kill Process

```
taskkill /PID pid_process /F
```

### Kill dan delete service

```
sc query state-all | find "name_service"
sc stop name_service
sc delete name_service
```

### Pengapusan file dan folder malicious/suspicious

Penghapusan pada Windows dapat dilakukan dengan menggunakan shift+delete

## • MELAKUKAN HARDENING SISTEM DAN SERVER

Sebelum dilakukan proses pemulihan, pastikan seluruh *malicious file* dan *suspicious* telah dilakukan pengarsipan dan penghapusan. Langkah selanjutnya yang dapat dilakukan yaitu:

### Hardening

Melakukan **audit user** pada server dan melakukan penghapusan user yang diindikasi bukan *user legitimate.*

Melakukan penggantian seluruh kredensial baik aplikasi maupun server. **Penggantian *password*** direkomendasikan mengikuti kaidah penggunaan *password* yang kuat.

Menerapkan keamanan pada *remote access.* Penerapan keamanan pada *remote access* dapat dilakukan dengan menerapkan **VPN** atau ***whitelist* dan *blacklist IP*** yang diizinkan untuk akses ke server secara *remote*. Selain itu juga dapat dilakukan **kustomisasi port SSH** dari *default* port 22 menjadi port lain. Cara lain yang dapat diterapkan yaitu menerapkan ***port knocking*** dan menerapkan ***SSH Public Key Authentication.***

Melakukan **pembaruan *software,*** *plugins, theme* untuk mengurangi *attack vector*.

## • MELAKUKAN PEMULIHAN ATAU RECOVERY

**Setelah beberapa tahap hardening telah dilakukan, maka selanjutnya proses pemulihan atau recovery dapat dilakukan. Setalah proses pemulihan berhasil hendaknya sistem selalu dilakukan maintenance secara berkala dan pemantauan secara proaktif untuk mendeteksi dan menghindari kejadian serupa terjadi Kembali.**

# MITIGASI

# WEB DEFACEMENT

# MITIGASI

BERIKUT ADALAH LANGKAH-LANGKAH MITIGASI YANG DAPAT ANDA AMBIL SEBAGAI PENANGANAN PERTAMA SITUS WEB DARI SERANGAN WEB DEFACEMENT

1. AKTIFKAN LANDING PAGE PADA HALAMAN YANG TERKENA DEFACEMENT
2. LAKUKAN ANALISIS DAN SCANNING MALWARE SERTA VULNERABILITY
3. LAKUKAN PENGHAPUSAN MALWARE, PATCHING, PENGGANTIAN PASSWORD
4. LAKUKAN RECOVERY WEBSITE DAN NOTIFIKASI KEPADA SELURUH USER UNTUK MENINGKATKAN KEAMANAN
5. MENGHAPUS INDEXING GOOGLE MENGGUNAKAN GOOGLE SEARCH CONSOLE

# REKOMENDASI

## WEB DEFACEMENT

# REKOMENDASI

**Hal yang dapat dilakukan pemilik sistem sebagai upaya penguatan dan pencegahan terhadap serangan *Web Defacement* sesuai Panduan Keamanan Sistem Informasi (ISO/IEC 27002:2013) yaitu sebagai berikut :**

**A** ***Pembaruan Sistem***

- Rujukan: ISO/IEC 27002:2013, kontrol A.12.6.1 - Manajemen pembaruan sistem
- Pastikan sistem operasi, server web, basis data, dan perangkat lunak lainnya diperbarui secara teratur dengan memasang pembaruan keamanan terbaru. Hal ini akan mengurangi risiko eksploitasi kerentanan yang diketahui oleh penyerang.

**B** ***Pengaturan Keamanan***

- Rujukan: ISO/IEC 27002:2013, kontrol A.13.2.1 - Kebijakan keamanan sistem
- Terapkan kebijakan keamanan yang memadai untuk server *web* dan sistem terkait. Konfigurasikan server *web* dengan pengaturan keamanan yang sesuai, termasuk pengecualian file yang tidak perlu dan mematikan fitur yang tidak diperlukan.

**C** ***Kontrol Akses***

- Rujukan: ISO/IEC 27002:2013, kontrol A.9.1.2 - Manajemen hak akses pengguna
- Terapkan manajemen hak akses pengguna yang ketat. Berikan izin akses yang sesuai kepada pengguna berdasarkan prinsip kebutuhan paling sedikit (*principle of least privilege*).

**D** ***Pemantauan Keamanan***

- Rujukan: ISO/IEC 27002:2013, kontrol A.12.4.1 - Pemantauan penggunaan sistem
- Gunakan alat pemantauan keamanan untuk mengawasi aktivitas situs *web*. Tinjau log dan deteksi aktivitas yang mencurigakan, seperti upaya *login* yang tidak sah atau perubahan file yang tidak diinginkan.

# REKOMENDASI

## E Perlindungan *Password:*

- Rujukan: ISO/IEC 27002:2013, kontrol A.9.2.1 - Penggunaan *password* yang aman
- Terapkan kebijakan penggunaan *password* yang kuat. Pastikan pengguna menggunakan *password* yang kompleks, dan tetapkan kebijakan penggantian *password* secara berkala.

## F Backup Rutin

- Rujukan: ISO/IEC 27002:2013, kontrol A.12.3.1 - Manajemen *backup*
- Lakukan *backup* rutin dari situs *web* dan *database*. Simpan salinan cadangan di lokasi yang aman dan pastikan proses pemulihan (*restore*) berfungsi dengan baik jika diperlukan.

## G Pelatihan Keamanan

- Rujukan: ISO/IEC 27002:2013, kontrol A.10.1.1 - Kesadaran, pendidikan, dan pelatihan keamanan
- Lakukan pelatihan keamanan bagi pengguna dan administrator situs *web*. Tingkatkan kesadaran mereka tentang praktik keamanan, seperti menghindari mengklik tautan yang mencurigakan atau memperbarui perangkat lunak yang penting.

## H Audit Keamanan

- Rujukan: ISO/IEC 27002:2013, kontrol A.12.6.2 - Manajemen kerentanan teknis
- Lakukan audit keamanan secara teratur untuk mengidentifikasi kerentanan dan celah keamanan pada situs *web*. Tinjau dan perbaiki temuan secara teratur untuk meningkatkan keamanan.

**BADAN SIBER DAN SANDI NEGARA**


Badan Siber dan Sandi Negara
Jl. Harsono R. M. No. 70,
Ragunan, Jakarta 12550

Whatsapp
+62 811-1065-2018

Telegram
t.me/Id_SIRTII

Email
bantuan70@bssn.go.id