
Sharing Knowledge
Penanganan Insiden (Incident Response)

OUTLINE

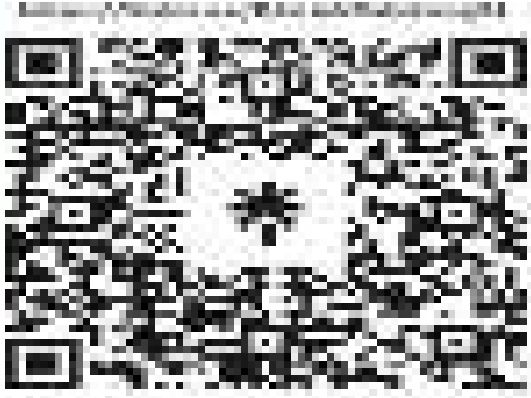
[illegible]

[illegible]

[illegible]

[illegible]

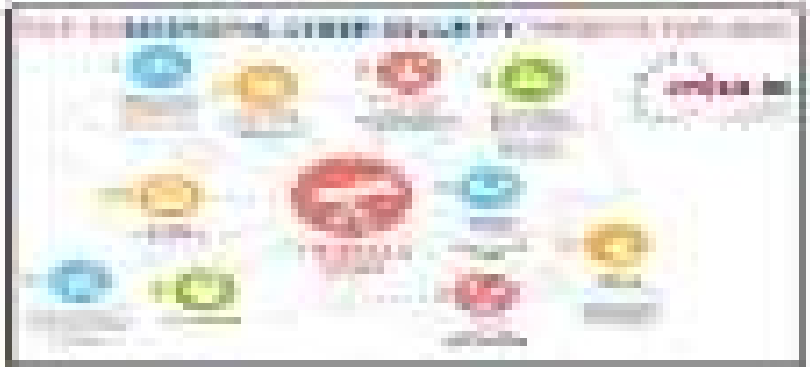
KELENGKAPAN MATERI DAN BAHAN



403,990,813

THREAT ACTOR

COMMON CYBER ATTACK



TARGET ORGANISASI

LATAR BELAKANG:
KEBANGKAN WEB DEFACE JUDI ONLINE PADA SITUSRAPA KEMENTERIAN


JUDI ONLINE

SERANGAN WEB DEFACEMENT

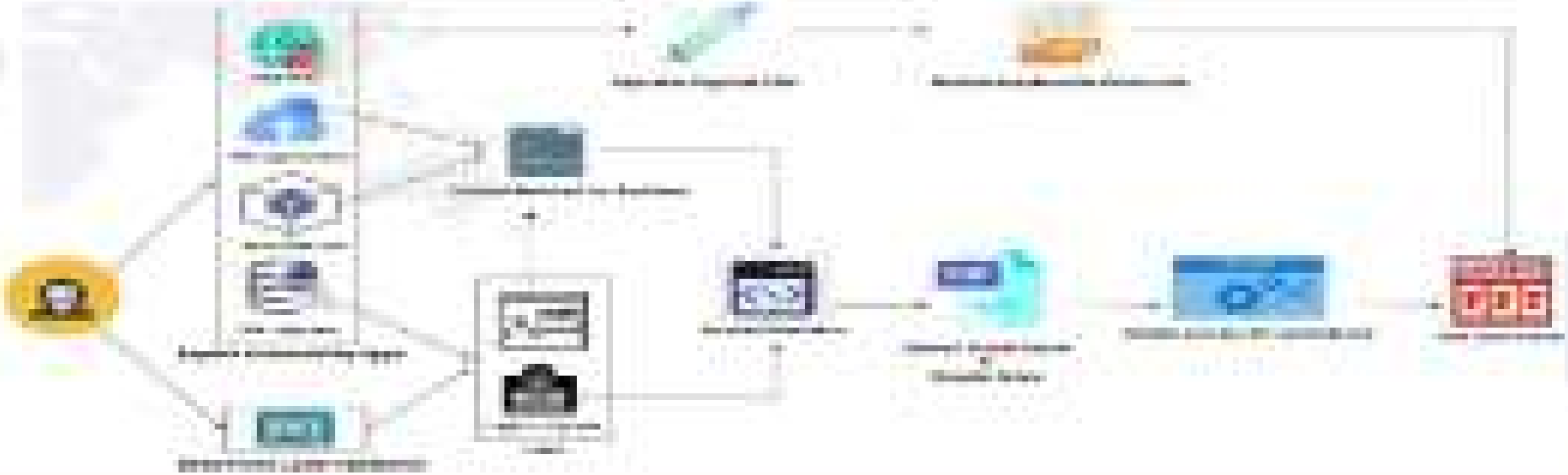
Web Defacement adalah serangan yang dilakukan untuk mengeksploitasi sistem melalui celah yang rentan dengan memanfaatkan kelemahan dari sistem sehingga *threat actor* (penyerang) dapat memasuki, memodifikasi, atau menghapus konten halaman web yang telah diakses.

Web defacement pada umumnya situs yang tidak aman atau tidak update, situs pemerintah atau komersial, situs yang sedang populer atau sensasional, situs yang memiliki kelemahan pada sistem operasi.

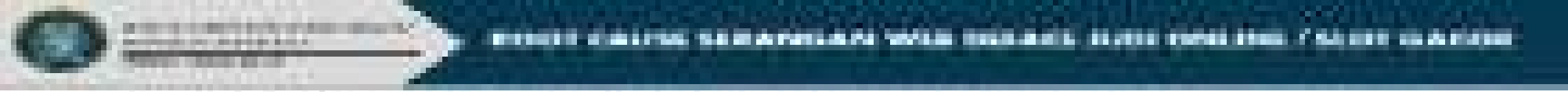
Web defacement pada situs akan berdampak pada penyampaian pesan yang tidak sesuai, kehilangan akses pengelolaan halaman web, dan kerusakan pada sistem yang terinfeksi, bahkan dapat berdampak pada kerugian finansial.

Web defacement dapat dilakukan dengan berbagai cara, seperti penyerang yang mengetahui cara kerja protokol, serta dapat menyalahgunakan kelemahan dari kelalaian pengguna (*human error*).

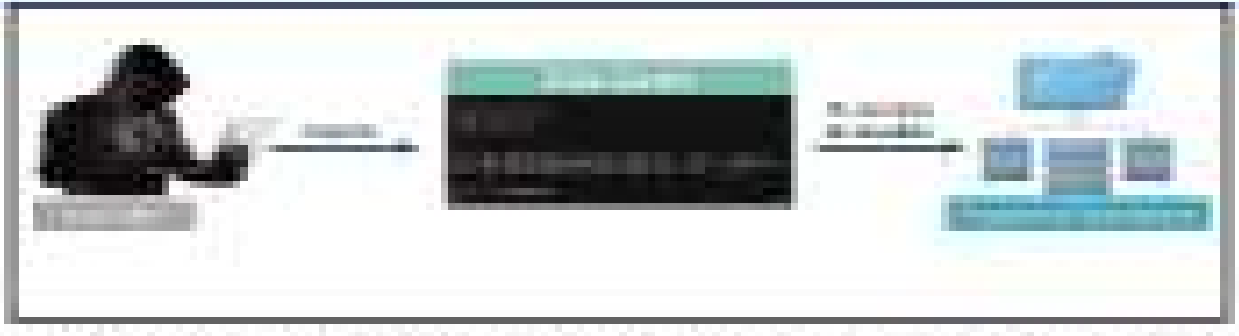
ALUR SERANGAN SERANGAN WEB DEFACE JUDI ONLINE / SLOT GACOR



ATTACK VECTOR SERANGAN WEB DEFACE JUDI ONLINE / SLOT GACOR



SQL INJECTION



SQL Injection adalah teknik serangan keamanan komputer dimana penyerang dapat menginjeksi kode berbahaya yang dirancang oleh aplikasi, dengan tujuan untuk mempengaruhi database. Serangan ini terjadi ketika aplikasi web tidak memvalidasi input pengguna secara memadai sebelum mengirimkannya ke server database.

Beberapa database populer seperti Relational Database Management System (RDBMS) seperti MySQL, Oracle, PostgreSQL, SQL Server, MariaDB, dll.

LANGKAH UMUM YANG BIASA DIGUNAKAN PENYERANG

- **Menebak menggunakan celah keamanan database**

Penyerang mencoba memodifikasi atau parameter URL pada aplikasi web yang rentan untuk mendapatkan akses tidak sah, memodifikasi data, atau melakukan aksi lainnya dengan benar.

- **Mencoba eksploitasi kode SQL**

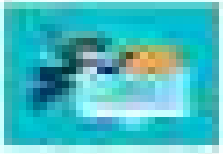
Eksploitasi menggunakan celah, penyerang memodifikasi pernyataan kode SQL menggunakan cara tertentu untuk mendapatkan akses yang memungkinkan mereka untuk melihat informasi yang sensitif dari server database.

- **Melakukan langkah-langkah lainnya**

Jika serangan menemukan penyerang, akan memungkinkan mereka untuk melihat, memodifikasi atau menghapus data yang tersedia untuk aplikasi web yang rentan yang bisa berupa informasi pribadi.


KASUS SQL INJECTION

DAMPAK SQL INJECTION

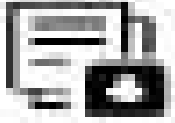


KERENTANAN *FILE UPLOAD & COMMAND OS* DALAM APLIKASI WEB

Kerentanan File upload adalah sebuah kerentanan dimana server web memperbolehkan user mengunggah file target memvalidasinya secara proper, kondisi akan ukuran file dengan benar.

Berikut adalah beberapa dampak utama dari kerentanan file upload dalam konteks keamanan web :

Mengunggah dll/ server menggunakan reliabilitas upload web shell
Aplikasi gagal memvalidasi properti mis: ekstensi file yang mengizinkan penggunaan nomor, pengguna yang dapat mengunggah Web Shell dan dapat mengontrol server.



Menimpa file penting
Web juga gagal memvalidasi nama file yang diunggah, pengguna dapat menimpa file penting dengan mengunggah file dengan nama yang sama.

Jumlah aktivitas (bisa)
Aplikasi gagal memvalidasi ukuran file yang mengizinkan sehingga nomor, pengguna dapat mengisi ruang disk yang tersedia yang berpotensi menyebabkan kegagalan layanan (denial of service).

PENANGANAN INSIDEN SIBER

PROSEDUR PENANGANAN INSIDEN SIBER

A. FASE *PREPARATION*

Fase ini meliputi kegiatan-kegiatan untuk mempersiapkan segala sesuatu dalam menghadapi sesuatu kemungkinan yang

- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]

Kab. Tabalong telah membentuk TTIS / CSIRT pada bulan November 2024

Note:
Setiap langkah penanganan insiden siber yang telah dilakukan dilaporkan kepada TobalongKab-CSIRT

B. FASE *DETECTION*

Pada DetectDex, mahasiswa diajarkan untuk mengenali tanda-tanda serangan siber yang mungkin terjadi pada sistem mereka. Mereka belajar bagaimana cara memantau aktivitas jaringan, mengidentifikasi perilaku yang mencurigakan, dan mengenali tanda-tanda serangan siber yang sedang berlangsung.

- Aktivitas tidak biasa pada jaringan, seperti lonjakan lalu lintas yang tidak wajar atau upaya akses yang mencurigakan.
- Perubahan pada sistem, seperti file yang hilang atau rusak, atau perubahan pada konfigurasi sistem yang tidak diizinkan.
- Pemberitahuan dari sistem keamanan, seperti alarm atau notifikasi yang menunjukkan adanya ancaman.
- Laporan dari pengguna lain yang mungkin telah mengalami serangan siber.

C. FASE *ANALYSIS*

Fase Analisis yaitu melakukan investigasi mendalam terhadap masalah atau kesempatan yang teridentifikasi. Tujuannya adalah untuk memahami akar penyebab, dampak, dan peluang yang tersembunyi.

- Melakukan analisis konsumsi digital untuk mengevaluasi pola waktu yang dihabiskan oleh pengguna di platform seperti media sosial, game online, dan e-commerce.
- Menggunakan metode survei, wawancara, dan observasi untuk memahami motivasi, kebiasaan, dan preferensi pengguna dalam berinteraksi dengan teknologi.
- Menganalisis data untuk mengidentifikasi tren, pola perilaku, dan segmentasi pengguna berdasarkan usia, lokasi, dan jenis aktivitas digital.
- Mengevaluasi dampak konsumsi digital terhadap produktivitas, kesehatan, dan interaksi sosial pengguna.

DETEKSI DAN ANALISIS

Dalam pelaksanaan deteksi dan analisis ini tanggap insiden siber dapat memicu pada pemblokiran telepon berikut dengan berbagai contoh sebelumnya tools yang dapat digunakan

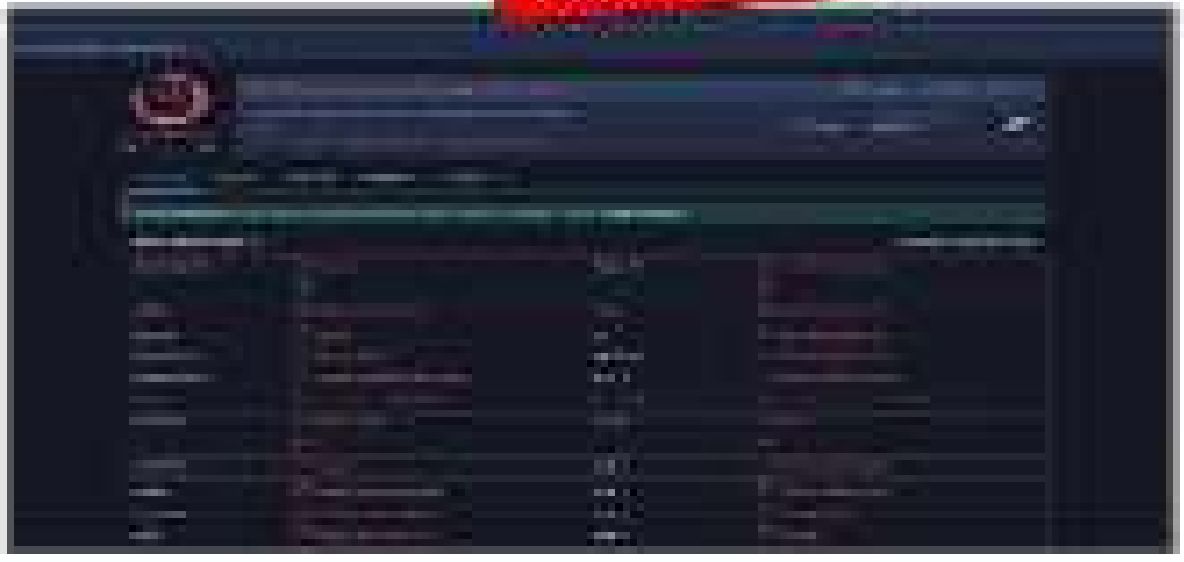
CONTOH DETEKSI DAN ANALISIS

Untuk mendeteksi **email phishing** yang merupakan salah satu **ancaman** dan penyebaran **malware** dapat dilakukan dengan melihat *header email* atau *view source original email*

CONTOH DETEKSI DAN ANALISIS

CONTOH DETEKSI DAN ANALISIS

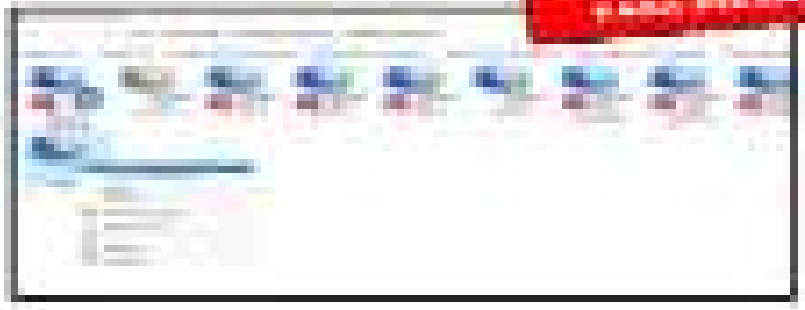
VIRUSTOTAL.COM

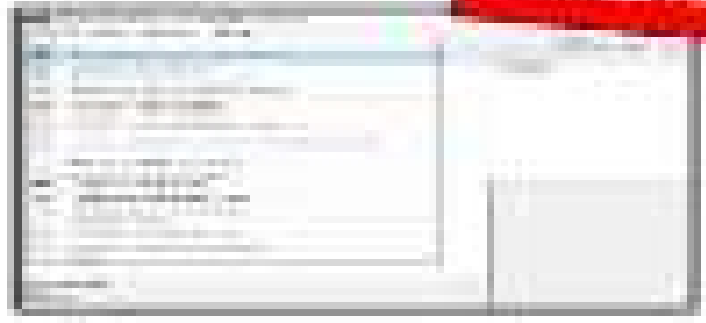


Virustotal adalah layanan open source yang memungkinkan pengguna untuk melakukan **deteksi dan analisis** dengan mengunggah file atau memasukkan URL untuk dipindai oleh berbagai mesin pemindai antivirus dan alat malware terkemuka

CONTOH DETEKSI DAN ANALISIS

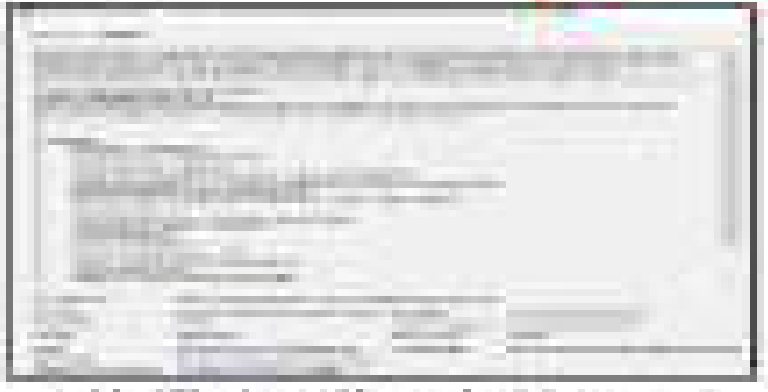
CONTOH DETEKSI DAN ANALISIS

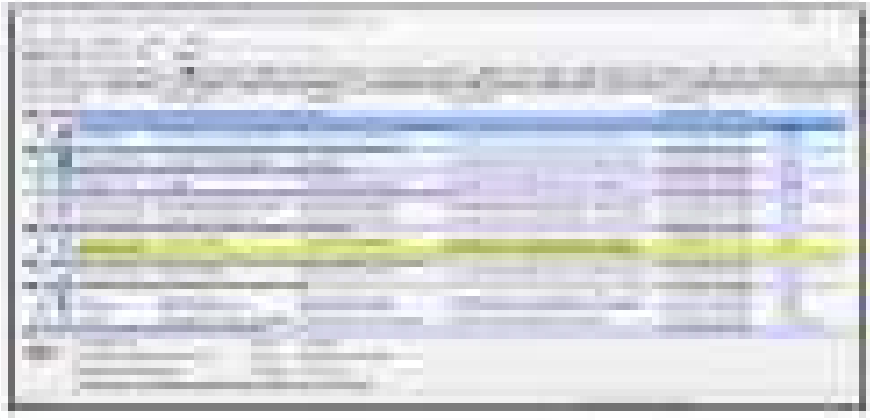




CONTOH DETEKSI DAN ANALISIS

CONTOH DETEKSI DAN ANALISIS





D. FASE *CONTAINTMENT*

Fase Containment (pengendalian) merupakan tindakan-tindakan untuk mencegah pengembangan insiden lebih lanjut. Tujuannya adalah untuk mengendalikan, membatasi, dan mencegah kerusakan lebih lanjut.

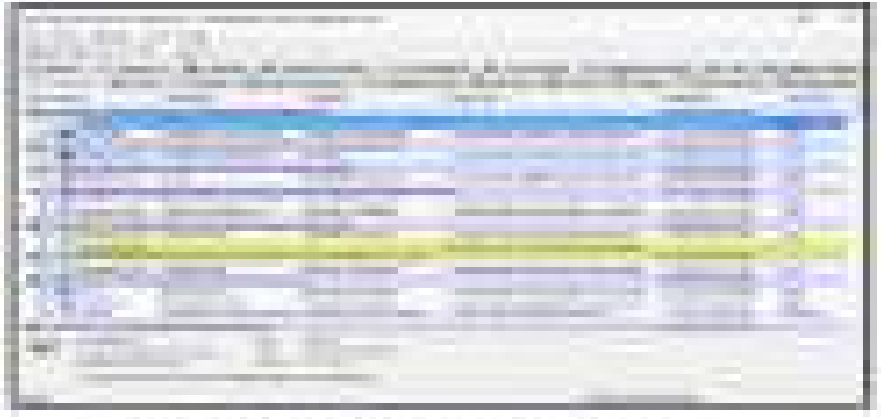
- Hal ini termasuk tidak hanya mengisolasi perangkat yang terinfeksi dari jaringan yang lebih luas, tetapi juga mengambil tindakan tambahan untuk mencegah penyebaran lebih lanjut dan memastikan bahwa ancaman tersebut tidak menyebar.
- Jika penyerang memanfaatkan proses atau layanan tertentu untuk melakukan serangan, tim kemungkinan akan menghentikan proses tersebut untuk mengisolasi penyimpangan dan mencegah serangan.
- Jika ditemukan bukti bahwa penyerang telah mengeksploitasi kerentanan, tim kemungkinan akan menambal atau memperbaiki kerentanan tersebut untuk mencegah penyalahgunaan lebih lanjut oleh penyerang.
- Memutuskan atau membatasi koneksi ke atau dari sistem atau perangkat yang terpengaruh untuk mencegah komunikasi dengan infrastruktur penyerang atau untuk mencegah malware menyebar ke sistem yang berdekatan.

E. FASE *ERADICATION*

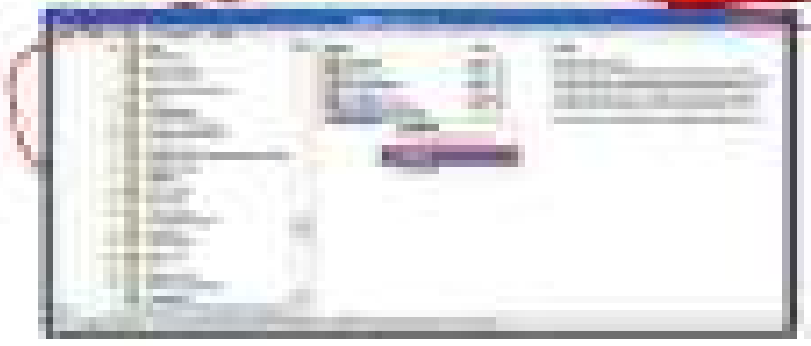
Fase Eradication adalah fase untuk menghilangkan akar masalah dan memastikan ancaman tidak akan muncul kembali. Tujuannya adalah untuk memastikan bahwa ancaman yang ditemukan telah dihilangkan dan tidak ada lagi jejak atau sisa yang dapat membahayakan sistem atau jaringan.

- Tim harus memastikan bahwa semua komponen yang terkena dampak telah dihapus dan dikembalikan ke kondisi semula.
- Setelah menghapus malware, langkah selanjutnya adalah memperbaiki untuk kerentanan tersebut.
- Tim harus memperbaiki konfigurasi sistem untuk menghindari konfigurasi yang mungkin telah diubah oleh penyerang.
- Semua kredensial yang terkompromi, seperti password, harus diganti dengan yang baru dan lebih kuat.
- Tim harus memastikan bahwa semua patch dan pembaruan keamanan telah diterapkan pada sistem yang terkena dampak.
- Langkah-langkah tambahan mungkin perlu diambil untuk memastikan bahwa ancaman tidak akan kembali, seperti meningkatkan pemantauan atau menerapkan kontrol keamanan baru.

CONTOH FASE *ERADICATION*



CONTOH FASE *ERADICATION*



- [illegible]
- [illegible]
- [illegible]
- [illegible]

F. FASE *RECOVERY*

Fase Recovery (pemulihan) adalah tindakan untuk memulihkan layanan dan data yang terganggu atau dihentikan dari sistem atau perangkat yang terinfeksi serangan siber agar dapat kembali beroperasi normal dan aman setelah mengalami serangan tersebut.

- Mengembalikan data dan konfigurasi sistem dari backup yang telah disiapkan sebelum terjadinya serangan
- Memulihkan atau menghidupkan kembali sistem, aplikasi, dan layanan yang terdampak agar dapat digunakan secara normal
- Menggantikan semua kredensial atau password yang terpengaruh oleh serangan dengan yang baru dan lebih aman
- Memperkuat sistem, baik melalui penambahan keamanan atau menghilangkan celah yang digunakan oleh penyerang
- Memberitahukan kepada pelanggan, mitra bisnis, atau pihak terkait tentang insiden tersebut, serta langkah-langkah yang diambil untuk memulihkan layanan dan melindungi data mereka

F. FASE *POST-INCIDENT* - *LESSON LEARNED*

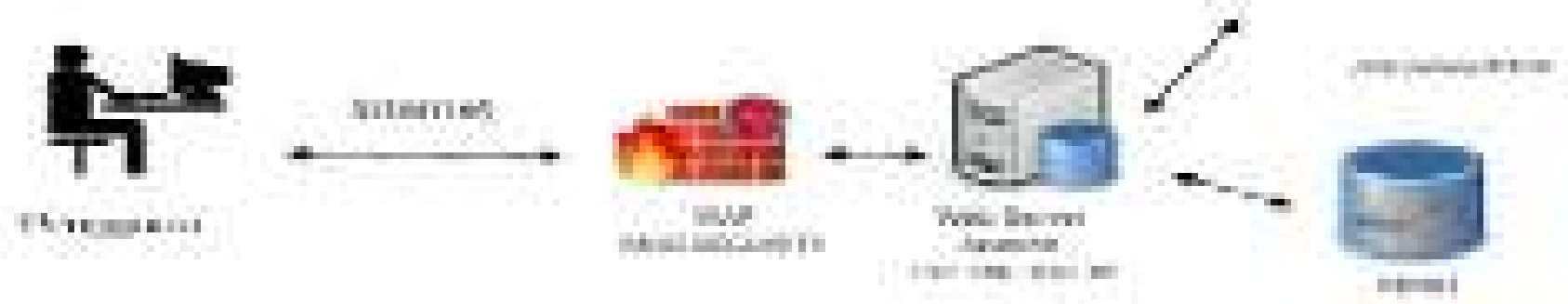
[illegible]

LAB SIMULATION

CASE SCENARIO:

- [illegible]
- [illegible]
- [illegible]

Perlapan Arsitektur Web



Persiapan Software

1. [illegible]

2. [illegible]

3. [illegible]

4. [illegible]

5. [illegible]

6. [illegible]

HAK AKSES SISTEM TERDAMPAK

Akses SSH Server Port 2222 (username : password)

[redacted]

Akses Halaman Website Administrator [redacted]

[redacted]

Akses Database Website (Mysql)

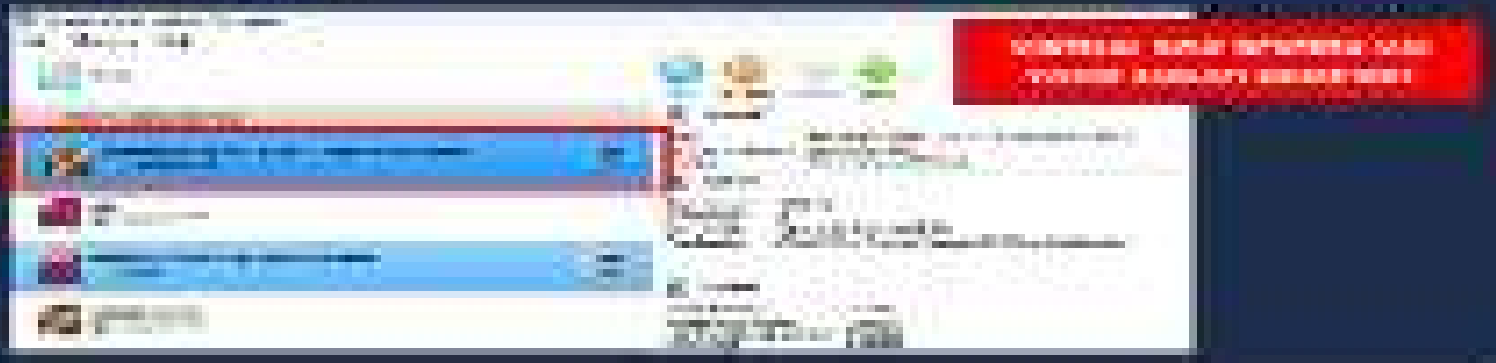
[redacted]

Alamat Folder / Home Directory Website Target

[redacted]

A. FASE *PREPARATION*

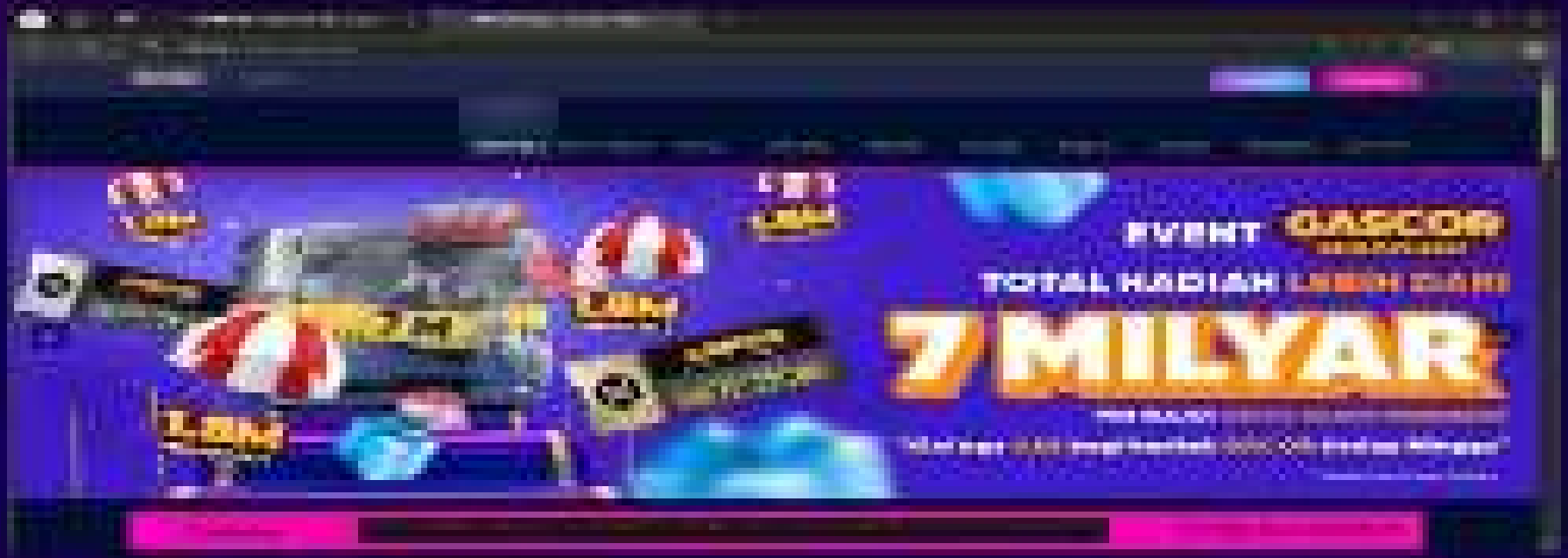
- [redacted]
- [redacted]
- [redacted]



B. DETECTION AND TRIAGE

B.a Triase Insiden

- Tapi di mainput tindakan-tindakan untuk mengidentifikasi dan melakukan verifikasi [illegible]
- B.b Triage Berdasarkan laporan notifikasi yang diterima oleh CoVI-CERT, maka [illegible] triage insiden ini akan memprioritaskan laporan yang [illegible] dengan cara memverifikasi folder yang berisi template web yang ter deface pada server
- Question !
  - Apa [illegible] yang dilakukan ?

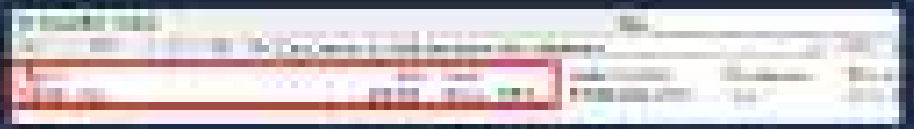

EVENT
TOTAL HADIAH
7 MILYAR

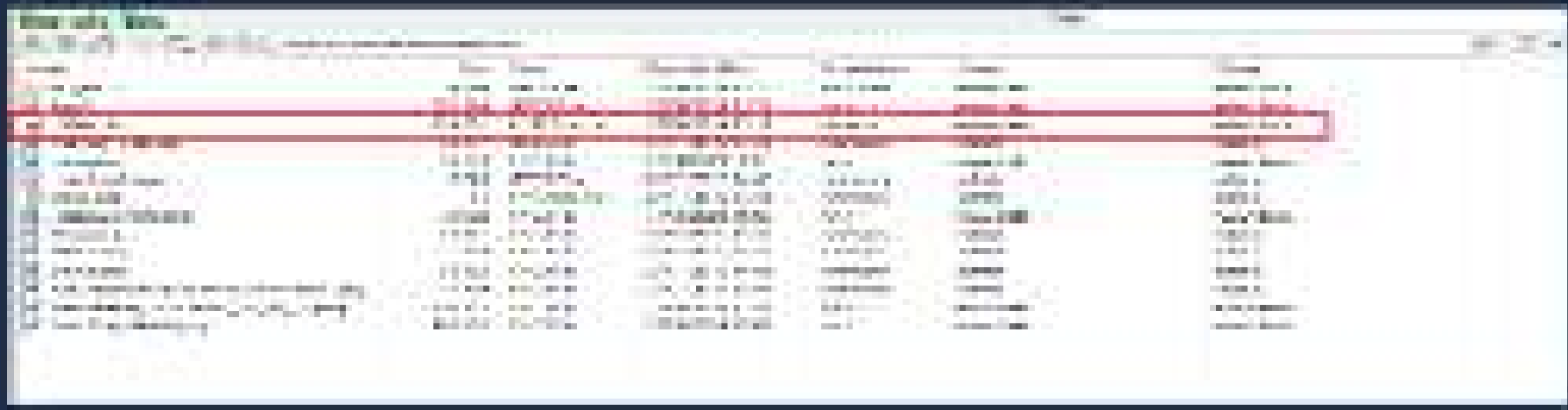
B.1 Deteksi Folder dan Halaman Mencurigakan Lainnya

- Untuk mendeteksi keberadaan Folder dan Halaman Lainnya yang dibuat oleh Attacker. Berikut adalah folder dan file yang biasanya dibuat oleh attacker

Questions 2:

- Apa nama path dan nama file shell pada nomor yang ditandai oleh Attacker
- Apa nama file Web Shell / Malware yang diletakkan oleh Attacker





C. ANALISIS

Fase ini meliputi tindakan-tindakan untuk mengelah dan menentukan jenis, skala dan dampak dari insiden yang terjadi. Fase ini diawali dengan melakukan akuisisi terhadap barang bukti digital.

- C.1. Akuisisi Log File Web Server: Akuisisi Log Web Akuisisi Database Aplikasi Terdampak :
- C.2. Analisis IP Penyerang: Apakah terjadi serangan dari alamat IP penyerang :

C1 Akusisi Database

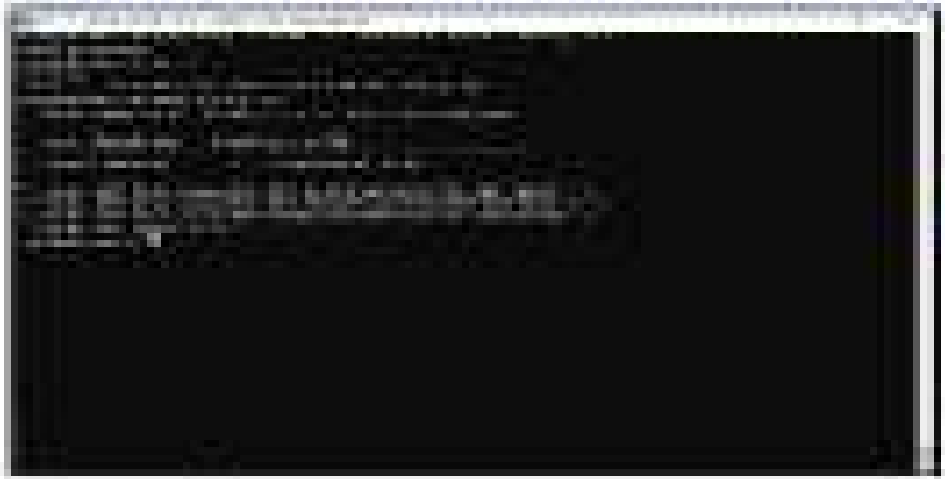
Lakukan backup database, kemudian akuisisi database tersebut...
Nama database : drill

Apa nama perintah untuk backup database mysql

```
mysqldump -u [user] -p [database_name] > backup.sql
```

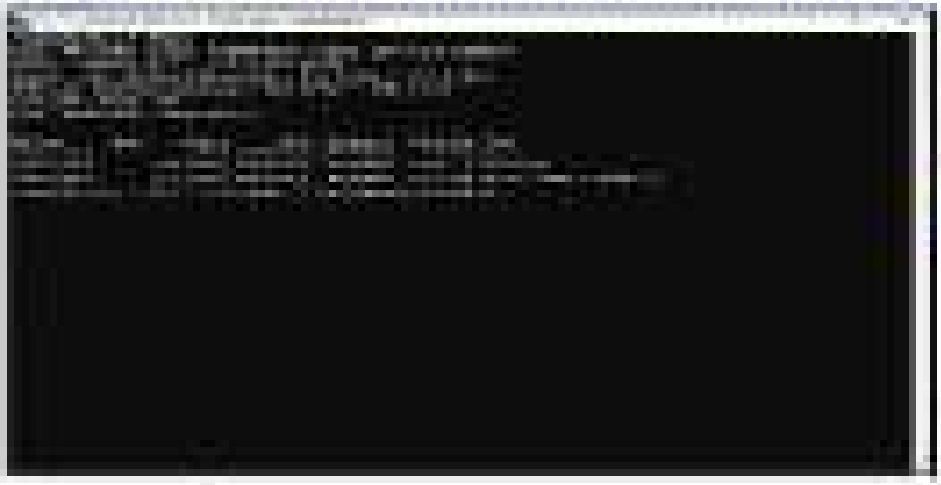
Backup data untuk
kapan kamu membutuhkannya

Backup database



Command

Imagine data server

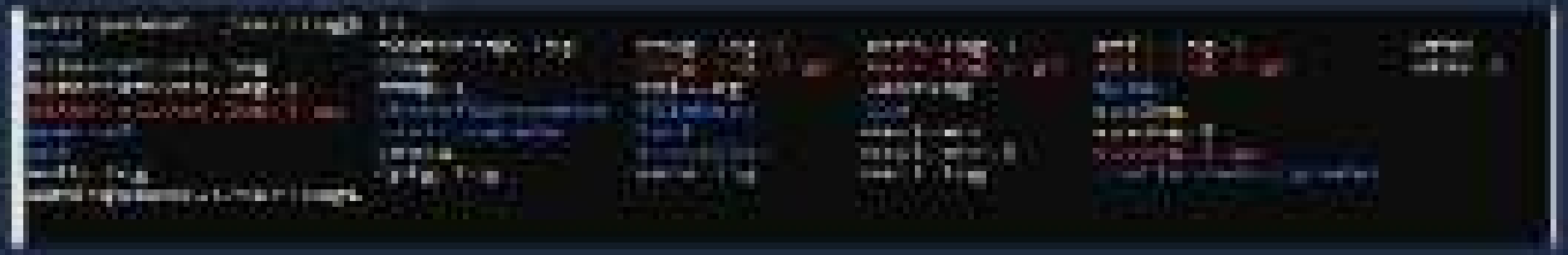


C.2 AKUISISI LOG SERVER

Log server adalah file log yang dibuat oleh atau digeneware oleh server secara otomatis. Peningkatan berisi aktifitas aktivitas yang dilakukan server, seperti jumlah permintaan halaman, alamat IP klien, jenis permintaan, dan sebagainya.

Sebelum melakukan analisis, lakukanlah pengumpulan bukti berupa **akses log server web , Log WAF / Modsecurity, dan Log SSH** dengan menggunakan tools Dirubo ke komputer lokal masing-masing.

1. Apa dan Dimana lokasi path lokasi log server apache
2. Apa dan Dimana lokasi path lokasi log modsecurity
3. Apa dan Dimana lokasi path lokasi log percobaan login pada server linux



Jawaban : /var/log/auth.log -> Log 3531

C.2. ANALISIS LOG FILE

Berdasarkan dengan log yang telah diambil, kemudian analisis adanya log pada hari kejadian terjadinya penyisipan slot judi online. Carilah IP Penyerang serta kapan slot.html diinject oleh attacker dan bagaimana cara penyerang menyisipkan halaman slot judi tersebut.

Hint:

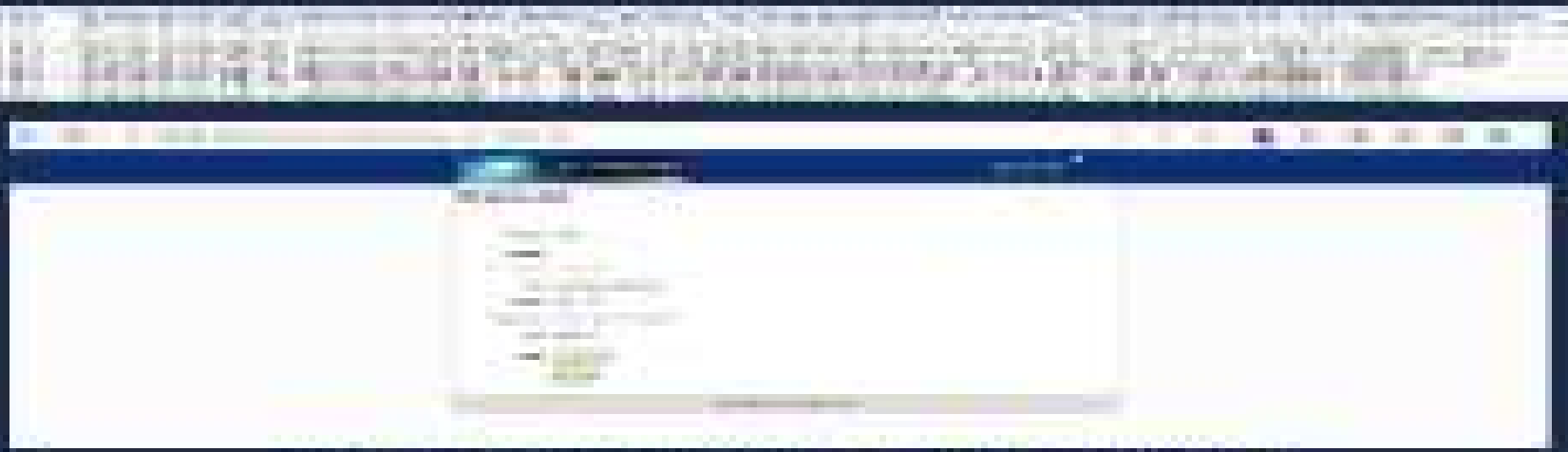
> Opsi tools : grep, Notepad, Notepad ++, Solusi lain ter

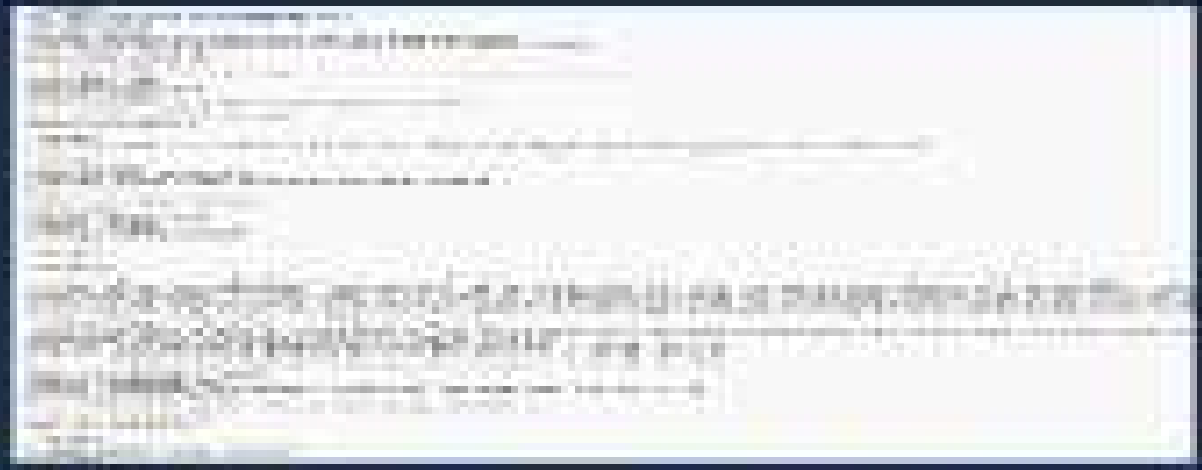
C.3. ANALISIS LOG FILE

Berikut merupakan dengan hasil analisis log serangan dibersihkan tadinya sebelumnya dilanjutkan melakukan web shell b374k.php. Contoh bagian dari beberapa serangan dilanjutkan pada upload

- filter:

- Cara kerja : grep -v filename filename > filename



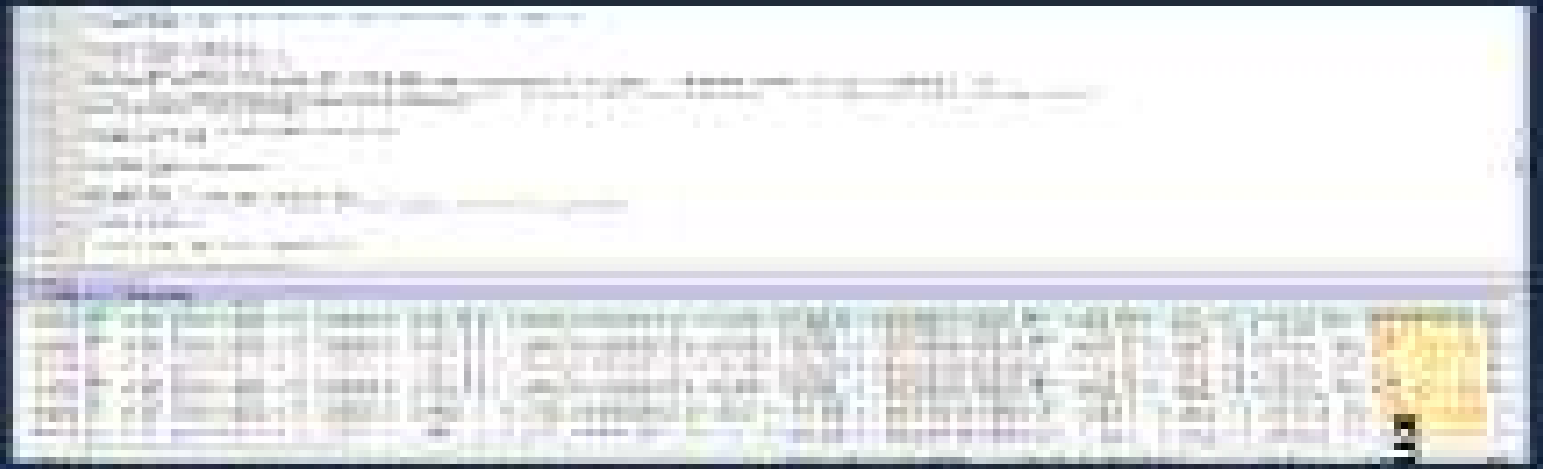


C.4. ANALISIS LOG FILE

Berdasarkan dengan hasil analisis log sebelumnya diketahui bahwa b374k.php diunggah dimana melalui fitur administrator. Carilah kapan awal mula serangan terdeteksi oleh WAF, serangannya apa dan berentarian apa yang dieksploitasi oleh attacker

Hint:

> Opsi Tools : grep, Notepad, Notepad ++, SublimText



Jawaban : Penyerang melancarkan serangan sql injection dan memperoleh database aplikasi serta kredensial administrator.
17/Jun/2021 22:59:01 | 0700 | 192.168.100.37

C.5. ANALISIS LOG FILE

Berdasarkan log modsecurity, terdapat kemungkinan attacker melakukan Remote Command Execution dengan memanfaatkan webshell. Lakukan analisis aktivitas RCE attacker. Apa perintah RCE yang dijalankan oleh attacker untuk melihat user yang ada pada server linux

- Hint:

- Dasar Teori : grep, Notepad, Notepad ++, SublimText

C.5. ANALISIS LOG FILE

Lakukan analisa terhadap authlog untuk mengecek aktivitas login pada server.
Lakukan analisa apakah terdapat percobaan pada log tersebut. Berilah screen screenshot yang dilakukan oleh attacker

...filter:

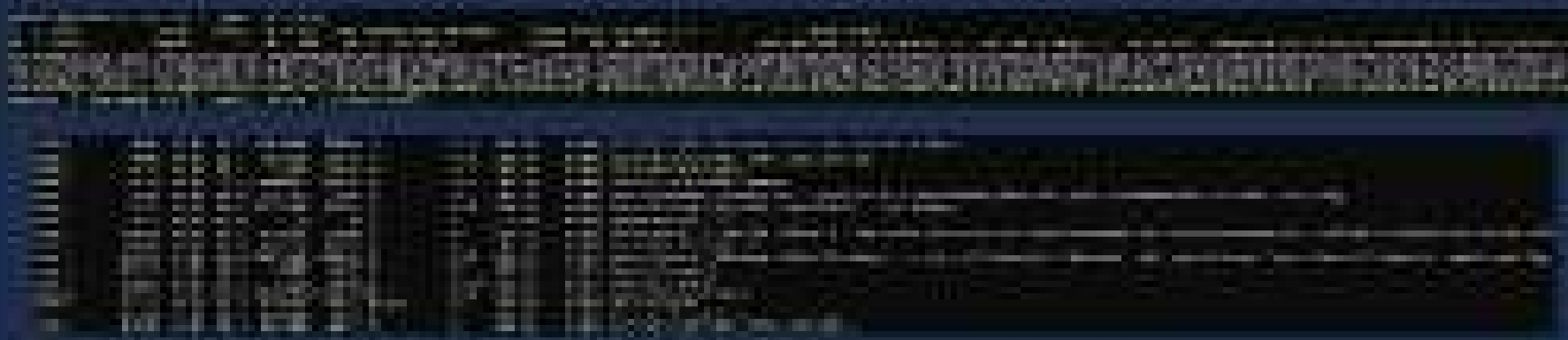
```
~ Cara: Search : grep, Nyalapasti, Nyalapasti -i -r, Isolation level
```

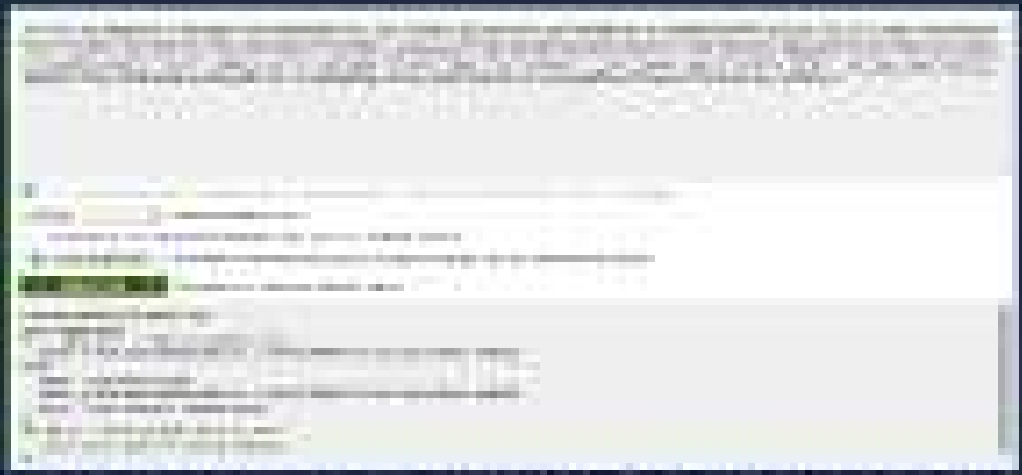
C.5. ANALISIS LOG FILE

Lakukan analisis terhadap aktivitas akunbaru dengan kembali masuk admin. Cocokkan nama variabel berbahaya yang dijalankan oleh attacker untuk memodifikasi galeri.php. Cantumkan Alamat IP Command and Control terhadap file Gallery.php

- Hint:

- Opsi: basis : grep, Notepad, Notepad ++, Isolation tool



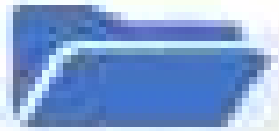


Javadoc : cnrt.uselrical. Inac.0159.65.1 25.2/7/gacor.html

CONTAINMENT

Containment merupakan aktivitas pencegahan agar insiden yang terjadi tidak meluas atau menyebabkan efek lainnya terjadi insiden yang sama.

- Memberitahukan pemakai komputer dan pemberitahuan informasi lainnya
- Ketersediaan layanan IT
- Mengamankan evidence (bukti) insiden
- Pembatasan akses pada server
- Melakukan backup sistem/aplikasi



Pengunjian file-file malicious dan suspicious yang ditemukan

Pembatasan akses pada server terdampak

Analyze the memory broker

Pembuktian akan pada
proses persidangan

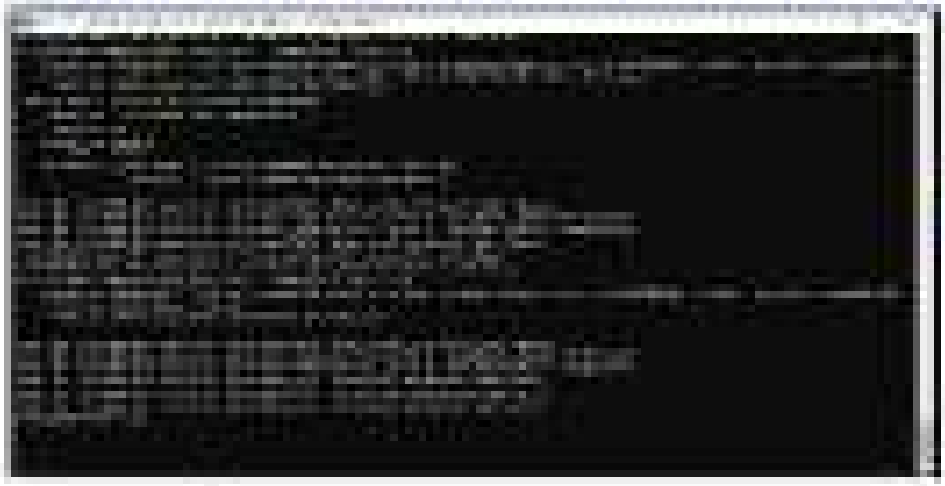
Bukti yang sah untuk
kepentingan forensik digital

Setting firewall pada linux

Command

```
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
```

Demonstrasi konsep interrupt/permisahan segmen jaringan



ERADICATION

Fase ini meliputi tindakan-tindakan untuk menghapus atau menghilangkan [illegible]

Penghentian program/proses malicious dan suspicious

Penghapusan file malicious dan suspicious

Pada tahap ini kamu akan melakukan evaluasi terhadap hasil yang telah kamu kerjakan.

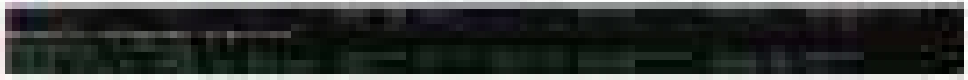
Ringkas pekerjaan.

Pengertian layanan/service

Penghapusan layanan/service

Pada tahap ini kamu akan menghapus file malicious yang telah kamu temukan.

Terkait filezilla.exe malicious.



RECOVERY

Fase ini mencakup [illegible] untuk [illegible] yang [illegible] telah [illegible] sehingga [illegible] dapat [illegible] seperti [illegible].

Pembuatan dokumen laporan penanganan

Pembuatan dokumen lessons learned

Sharing informasi/pengalaman penanganan insiden

1. Melakukan update/upgrade pada server dan framework web secara rutin
2. Menerapkan [illegible]
3. Melakukan review aplikasi-aplikasi maupun port yang sudah tidak digunakan
4. Melakukan pemantauan secara proaktif pada sistem sehingga bisa melakukan [illegible]
5. Melakukan pengecekan kerentanan dengan melakukan IT Security Assessment (ITSA) secara berkala. Saat ITSA website maupun ITSA server
6. Menerapkan [illegible]
7. Melakukan backup pada web secara berkala dengan penyimpanan yang terpisah dari lokasi
8. Menerapkan [illegible]
9. Menerapkan pembatasan pada file yang dapat diunggah ke server melalui website untuk menghindari adanya file berbahaya yang diunggah oleh user

PENYUSUNAN LAPORAN

Lakukan penyusunan laporan penanganan insiden berdasarkan bukti dan hasil analisis yang telah dilakukan.


"Ingatlah! Kesilafan Satu Orang Sahaja
Tjukup Sudah Menjerbakan Keruntuhan Negara"