CYBER SECURITY EXERCISE

Kota Madiun, 24 - 25 Oktober 2022

CYBER SECURITY EXERCISE (PERSIAPAN)

Teknis Pelaksanaan :

- Peserta akan dibagi menjadi beberapa kelompok dengan anggota terdiri dari 3 atau 4 orang
- Peserta akan berperan sebagai tim MadiunKota_CSIRT dan membantu Instansi ABC dalam penanganan kebocoran data tersebut
- Koordinasi dan komunikasi menggunakan email
- Peserta bisa melakukan download materi persiapan pada:

  https://s.id/CyberExercise

```
****** Selamat Datang pada Aplikasi SIMPEG Online ********
ilakan Akses via Web Browser pada laman http://127.0.0.1
untu login: ^[
```

SIMPEG ONLINE

Sistem Informasi Manajemen Kepegawaian

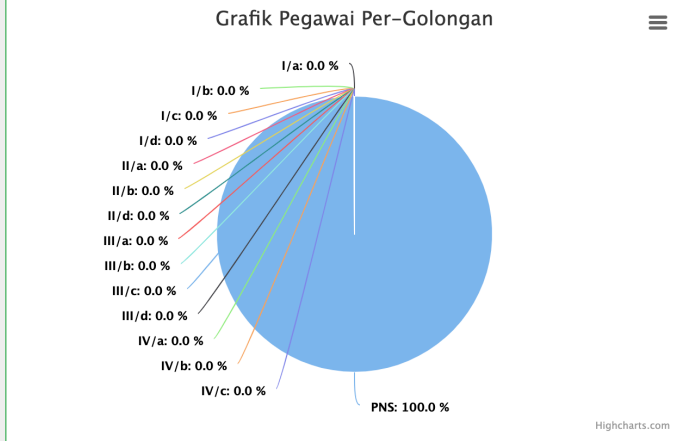
Alamat : Bintaro, Jakarta Selatan
Telepon : 0217805814
Email : 0217805813

Sistem Informasi Kepegawaian (SIMPEG)

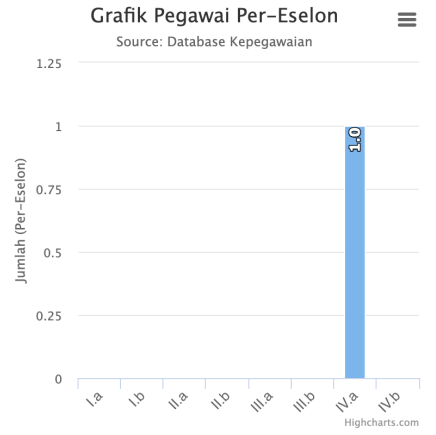
Login

Jumlah Pegawai : 19 Orang

Golongan



Eselon



Selamat Beristirahat
&
Terima Kasih

https://s.id/CyberExercise

- Taufiq : 085655444214
- Raden : 082131888810

CYBER SECURITY EXERCISE

Skenario:

Instansi ABC di Kota Madiun terindikasi mengalami kebocoran data.
Terindikasi beberapa informasi pada database dan ditemukan tersebar diperjual belikan
pada situs jual beli online.

Tim MadiunKota_CSIRT sebagai tim respon insiden siber diminta untuk membantu melakukan investigasi menyeluruh pada aset instansi tersebut dan mendapatkan bukti-bukti serangan dan insiden kebocoran data.

Teknis Pelaksanaan :

- Peserta akan dibagi menjadi beberapa kelompok dengan anggota terdiri dari 3 atau 4 orang
- Peserta akan berperan sebagai tim MadiunKota_CSIRT dan membantu Instansi ABC dalam penanganan kebocoran data tersebut
- Koordinasi dan komunikasi menggunakan email

CYBER SECURITY EXERCISE

Dimohon untuk masing-masing tim menunjuk:

1. **Ketua Tim**
2. **Narahubung**
3. **Investigator**

Mengirimkan email ke:

Investigasi@madiunkota.go.id

Selamat Mengerjakan

&

Terima Kasih

Selamat pagi Tim CSIRT,

Terima kasih sebelumnya karena telah memberikan informasi kepada kami terkait adanya insiden keamanan siber yang terjadi pada salah satu Aset kami.

Berdasarkan hasil analisa awal kami, ditemukan beberapa informasi pada database yang telah tersebar dan diperjualbelikan pada sebuah situs jual-beli secara online dan itu kami konfirmasikan bahwa informasi tersebut berasal dari aset kami. Namun kami kesulitan dalam melakukan investigasi secara menyeluruh pada aset yang diindikasikan telah disusupi.

Dapatkah anda membantu kami, dalam hal melakukan investigasi secara menyeluruh pada aset kami untuk mendapatkan bukti-bukti serangan dan insiden kebocoran data pada aset kami?
NB : Untuk sistem yang terkena insiden, sudah kami lakukan Backup dalam bentuk OVA (Virtualisasi).

Username : "simpeg"
password : "simpeg1234!"

Terima kasih..
Penanggungjawab Keamanan IT
Instansi ABC

Case 0

Selamat siang Tim CSIRT,

Dengan asumsi bahwa sistem telah disusupi, lakukan analisa mendalam untuk menemukan bukti insiden dengan menggunakan sistem backup dari instansi ABC (OVA File).
a. Temukan alamat direktori (directory path) program atau aplikasi yang mencurigakan yang ada pada sistem tersebut?
b. Tuliskan bukti insiden berupa nama program atau aplikasi, kapan terakhir program atau aplikasi dilakukan modifikasi serta pemilik program atau aplikasi tersebut?
c. Sebagai pencatatan signature program atau aplikasi yang mencurigakan, lampirkan nilai diggest masing-masing program atau aplikasi tersebut?

Terima kasih..
Penanggungjawab Keamanan IT
Instansi ABC

Case 1

Selamat siang Tim CSIRT,
Lakukan identifikasi dan analisa pada Direktori Utama Website yaitu pada "/var/www/html" serta pada public directory pada "/var/www/html/asset" untuk mengetahui adanya Malicious File atau tidaknya.

Beberapa sintaks yang dapat dilakukan :
1. Sintaks untuk list directory : ls -alrt
2. Sintaks untuk cetak signature MD5 : md5sum <nama_file_yg_suspicious>

Terima kasih..
Penanggungjawab Keamanan IT
Instansi ABC

Hint 1

Selamat siang Tim CSIRT,

Dengan mengacu pada bukti insiden yang ditemukan, lanjutkan investigasi untuk menemukan identitas penyerang. Lakukan hal sebagai berikut :

a. Lakukan log analisis pada log website (access.log) dan menemukan identitas penyerang (alamat IP) yang berhasil masuk ke dalam sistem?

b. Serangan apa saja yang dilakukan oleh penyerang tersebut?

Terima kasih..

Penanggungjawab Keamanan IT

Instansi ABC

Case 2

Selamat siang Tim CSIRT,

Lakukan download access.log aplikasi tersebut apabila diperlukan.
Untuk dapat melakukan analisa log, gunakan aplikasi editor (notepad++) atau httplogviewer.
Lakukan analisa dengan melakukan filter nama backdoor/malicious file/alamat IP

Atau menggunakan Command Line Interface (CLI) dengan sintaks :
sudo cat /var/log/apache2/access.log | awk '{print $1}' | sort -n | uniq -c | sort -nr | head -20
sudo cat /var/log/apache2/access.log | grep <nama_file_malicious> | awk '{print $1}' | sort -n | uniq -c | sort -nr | head -20
sudo cat /var/log/apache2/access.log | grep <alamat_IP_penyerang>

Terima kasih..
Penanggungjawab Keamanan IT
Instansi ABC

Hint 2

Selamat siang Tim CSIRT,

Sebagai informasi, sistem yang digunakan oleh Instansi ABC membuka layanan File Transfer Protocol sebagai media pertukaran File secara internal.
Hal ini menjadi analisa lanjutan untuk menelusuri pada aplikasi tersebut.
a. Lakukan analisa mendalam pada log aplikasi pertukaran file tersebut?
b. Apakah terdapat bukti insiden, temukan dan buktikan kapan pertama kali serangan yang berhasil masuk?
c. Apakah terdapat kerawanan pada aplikasi tersebut?? (jika ada, sebutkan jenis CVE nya)

Terima kasih..
Penanggungjawab Keamanan IT
Instansi ABC

Case 3

Selamat siang Tim CSIRT,
Untuk dapat melakukan analisa log, gunakan aplikasi editor (notepad++) atau httplogviewer. Lakukan download trace.log aplikasi tersebut.
Lakukan analisa dengan melakukan filter nama backdoor/malicious file

Atau menggunakan Command Line Interface (CLI) dengan sintaks :
sudo cat /var/log/proftpd/trace.log | grep <nama_bckdoor_file>

Terima kasih..
Penanggungjawab Keamanan IT
Instansi ABC

Hint 3

Selamat siang Tim CSIRT,

Dengan memantau System Authentication Logs, temukan hal-hal sebagai berikut :

a. File apa dan dimana proses dilakukan eskalasi user oleh penyerang?
b. Apakah ditemukan aktivitas penambahan user, jika ditemukan :
    - Nama user tersebut?
    - Aktivitas apa saja yang dilakukan oleh user tersebut?

Terima kasih..
Penanggungjawab Keamanan IT
Instansi ABC

Case 4

Selamat siang Tim CSIRT,

Untuk dapat melakukan analisa log, gunakan aplikasi editor (notepad++) atau httplogviewer. Lakukan download auth.log aplikasi tersebut.
Lakukan analisa dengan melakukan filter waktu kejadian

Atau menggunakan Command Line Interface (CLI) dengan sintaks :
sudo cat /var/log/auth.log | grep –a “waktu_kejadian_insiden”
sudo cat /var/log/auth.log | grep –a “Jun 10”

Terima kasih..
Penanggungjawab Keamanan IT
Instansi ABC

Hint 4

Selamat siang Tim CSIRT,

Dengan berdasarkan analisa sebelumnya, kerentanan apakah yang dimanfaatkan oleh penyerang untuk melakukan eskalasi?

Terima kasih..
Penanggungjawab Keamanan IT
Instansi ABC

Case 5

Selamat siang Tim CSIRT,

Kami mendapatkan informasi bahwa Sistem Operasi yang digunakan telah lama tidak dilakukan update dan upgrade.

Lakukan pemeriksaan sistem operasi tersebut.

Sintaks yang dapat dilakukan :
lsb_release -a
uname -a

Terima kasih..
Penanggungjawab Keamanan IT
Instansi ABC

Hint 5

Selamat siang Tim CSIRT,

Setelah dilakukan analisa environment yang terkena insiden tersebut, mohon kiranya dapat dilakukan pembuatan Laporan Penanganan Insiden dengan mencantumkan rekomendasi apa saja yang perlu dilakukan guna penanganan insiden ini.

NB. Kirimkan Laporan Penanganan Insiden Kebocoran Data

Terima kasih atas kerjasamanya..

Terima kasih..
Penanggungjawab Keamanan IT
Instansi ABC

Case 6