



Sharing Knowledge

Penanganan Insiden (Incident Response)

(Dekan, 3 Desember 2024)

Diras, Koordinator dari Informatika Kabupaten Sukoharjo, Koordinator Staf



Articles Assessment: How good is it?

Articles Assessment: How good is it?
 (with annotations, key findings & a few original observations)

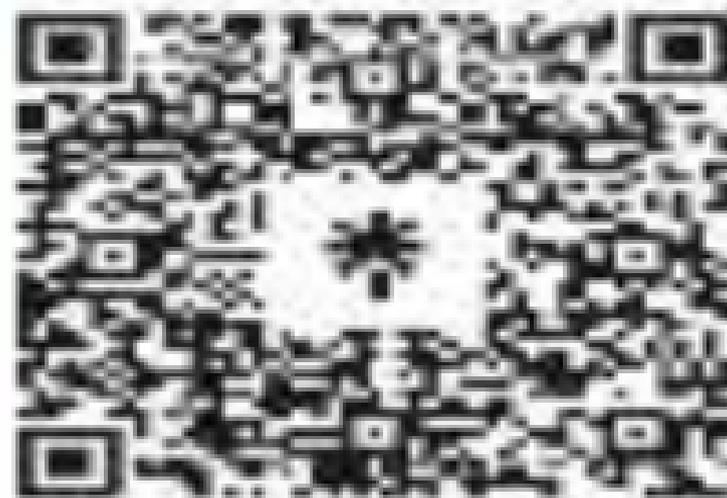
Management studies 101

Case Study: 100-200 articles of recent research



KARTU KELENGKAPAN MATERI DAN BAHAN	
NO. BAHAN	
NO. MATERI	
NO. URAIAN	
NO. KETERANGAN (MATERI, BAHAN, ALAT, DAN PERANGKAT)	
NO. KETERANGAN (MATERI, BAHAN, ALAT, DAN PERANGKAT)	

QR Code for Material and Equipment List





ಆರೋಗ್ಯ ಸೇವೆಗಳಿಗೆ
ಆಯವ್ಯಯ
403,990.813

ಆರೋಗ್ಯ ಸೇವೆಗಳಿಗೆ
ಆಯವ್ಯಯ
ರೂ. 403,990.813
2020-21

THREAT ACTORS



COMMON CYBER ATTACKS



TARGET SECTOR





LATIHAN BELAKANG KEBANGSAH WITH WEBSITE JURNAL ONLINE PADA LINGKUNGAN APLIKASI PEMERINTAHAN

Salah satu program Kementerian Kesehatan adalah upaya untuk meningkatkan peran masyarakat dalam upaya kesehatan. Salah satu upaya yang dilakukan adalah meningkatkan peran masyarakat dalam upaya kesehatan melalui berbagai kegiatan yang dilaksanakan di lingkungan masyarakat.

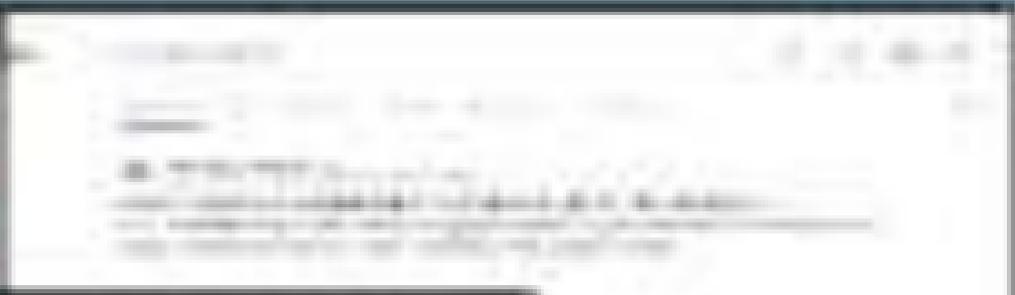


KELOMPOK BELAJAR
PADA LINGKUNGAN
PACIENT



Pergerakan dalam dunia kesehatan Indonesia (PAMI) merupakan lembaga yang bergerak di bidang kesehatan masyarakat dan pelayanan kesehatan. Lembaga ini bergerak di bidang kesehatan masyarakat dan pelayanan kesehatan.

Salah satu upaya yang dilakukan adalah meningkatkan peran masyarakat dalam upaya kesehatan. Salah satu upaya yang dilakukan adalah meningkatkan peran masyarakat dalam upaya kesehatan.





SERANGAN WEB DEFACEMENT

Web Defacement adalah serangan yang dilakukan untuk mengubah tampilan visual halaman yang rentan dengan memanfaatkan kerentanan dan sistem sehingga threat actor (per penyerang) dapat merusak, memodifikasi, atau menghapus konten halaman web yang telah online.



Web defacement pada website atau yang bisa dikatai oleh user untuk akses user yang tidak mempunyai akses yang sesuai dengan akses yang dimiliki oleh website tersebut.



Web defacement pada itu akan dilakukan pada ancaman pada yang dapat dilakukan oleh penyerang tersebut. Hal tersebut yang dilakukan oleh penyerang untuk melakukan akses yang tidak diinginkan oleh user yang ada di website.



Web defacement dapat dilakukan dengan cara yang berbeda-beda yang akan dilakukan oleh penyerang yang akan melakukan akses yang tidak diinginkan oleh user yang ada di website.

Ilustrasi serangan web defacement yang mengubah tampilan website dengan defacement atau web.





Attack adalah tindakan merusak atau yang dipublikasikan oleh perantara yang menggunakan informasi yang telah dikumpulkan sebelumnya untuk melakukan serangan terhadap sistem, individu, organisasi, atau tindakan yang merugikan organisasi



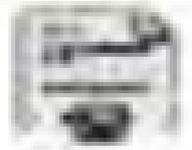
Kelebihan Sistemisasi (CMS) (Content Management System) yang terdistribusi



Kelebihan dari sistem yang sangat baik



Kelebihan dari sistem yang sangat baik



Kelebihan dari sistem yang sangat baik



Kelebihan dari sistem yang sangat baik

Kelebihan dari sistem yang sangat baik dan terdistribusi ke seluruh dunia yang memiliki kelebihan dan kekurangan, dan dapat menggunakan teknologi yang ada untuk meningkatkan keamanan sistem yang ada dan melindungi data yang ada di dalamnya.



SQL INJECTION



SQL Injection adalah teknik serangan keamanan komputer dimana penyerang dapat menginjeksi kode perintah yang tidak sah ke aplikasi, sehingga terjadi perubahan data dalam database. Serangan ini terjadi ketika aplikasi web tidak memvalidasi input pengguna secara memadai sebelum mengirimnya ke server database.

Metode database dapat dilakukan menggunakan tools melalui Database Management System (DBMS) seperti MySQL, Oracle, PostgreSQL, SQL Server, MariaDB, dll.



LANGKAH ILMIAH YANG BIASA DIGUNAKAN PENYERANG

- Serangan menggunakan alamat IP secara massal dan otomatis

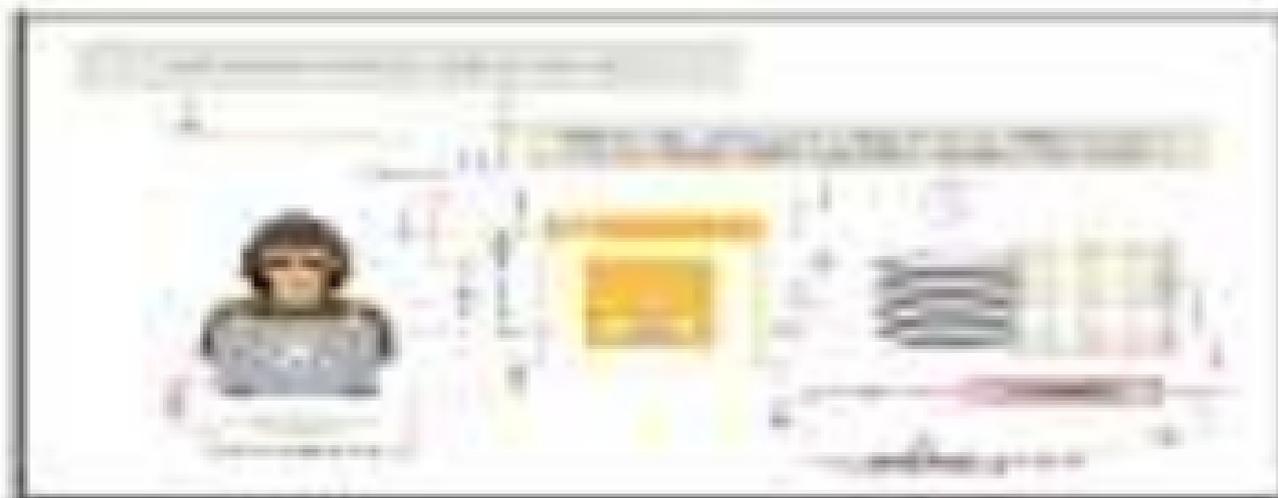
Penyerang (serangan) memiliki alamat yang terdaftar (IP). Untuk serangan yang menggunakan IP yang terdaftar, penyerang akan menggunakan alat untuk membuat daftar dengan alamat.

- Proses dengan kode SQL

Demikian (serangan) telah, penyerang menggunakan program yang menggunakan serangkaian data yang terdaftar yang akan digunakan untuk membuat serangan.

- Serangan berbasis sistem

Salah satu serangan yang paling umum adalah menggunakan alamat IP yang terdaftar, penyerang akan menggunakan alamat yang terdaftar untuk membuat serangan.





KASUS SQL INJECTION

SQL Injection

SQL Injection is a type of computer attack in which the attacker inserts or "injects" a malicious SQL statement into an entry field for data that is to be stored in a database. The injected code then executes on the database server, and the attacker can view or modify the data in the database.

SQL Injection attacks are often used to steal sensitive information from a database, such as usernames, passwords, and credit card numbers. In some cases, attackers can even gain administrative access to the database, allowing them to delete or modify data at will.

SQL Injection

SQL Injection is a type of computer attack in which the attacker inserts or "injects" a malicious SQL statement into an entry field for data that is to be stored in a database. The injected code then executes on the database server, and the attacker can view or modify the data in the database.

SQL Injection

SQL Injection is a type of computer attack in which the attacker inserts or "injects" a malicious SQL statement into an entry field for data that is to be stored in a database. The injected code then executes on the database server, and the attacker can view or modify the data in the database.

SECURITY

SQL Injection is a type of computer attack in which the attacker inserts or "injects" a malicious SQL statement into an entry field for data that is to be stored in a database. The injected code then executes on the database server, and the attacker can view or modify the data in the database.

SQL Injection

SQL Injection is a type of computer attack in which the attacker inserts or "injects" a malicious SQL statement into an entry field for data that is to be stored in a database. The injected code then executes on the database server, and the attacker can view or modify the data in the database.

SQL Injection

SQL Injection is a type of computer attack in which the attacker inserts or "injects" a malicious SQL statement into an entry field for data that is to be stored in a database. The injected code then executes on the database server, and the attacker can view or modify the data in the database.

SQL Injection

SQL Injection is a type of computer attack in which the attacker inserts or "injects" a malicious SQL statement into an entry field for data that is to be stored in a database. The injected code then executes on the database server, and the attacker can view or modify the data in the database.

SQL Injection

SQL Injection is a type of computer attack in which the attacker inserts or "injects" a malicious SQL statement into an entry field for data that is to be stored in a database. The injected code then executes on the database server, and the attacker can view or modify the data in the database.



DAMPAK SQL INJECTION



Melakukan Query
 Melakukan query adalah tindakan yang dilakukan oleh pengguna untuk mengambil data dari database. Query ini dapat digunakan untuk melakukan berbagai macam operasi, seperti insert, update, delete, dan select.

Melakukan Query yang Tidak Benar
 Melakukan query yang tidak benar adalah tindakan yang dilakukan oleh pengguna untuk melakukan operasi yang tidak diinginkan. Hal ini dapat dilakukan dengan memasukkan karakter khusus ke dalam query, seperti semicolon (;) dan double quote (").



Menyebabkan Kerusakan
 Melakukan query yang tidak benar dapat menyebabkan kerusakan pada database, seperti menghapus data yang tidak diinginkan atau mengubah data yang sudah ada.

Menyebabkan Kerusakan Sistem
 Melakukan query yang tidak benar dapat menyebabkan kerusakan pada sistem, seperti membuat sistem menjadi lambat atau tidak dapat diakses.

ALL RIGHTS RESERVED



Pencegahan
 Untuk mencegah terjadinya serangan SQL injection, perlu dilakukan beberapa langkah, seperti memvalidasi input pengguna, menggunakan prepared statement, dan menggunakan library keamanan.

Keuntungan
 Melakukan query yang benar dapat memberikan keuntungan, seperti memudahkan pengguna untuk melakukan operasi yang diinginkan.





KERENTANAN FILE UPLOAD & COMMAND OS DALAM APLIKASI WEB

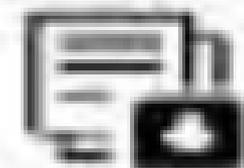


Kerentanan file upload adalah sebuah kerentanan dimana server web memperbolehkan user mengupload file tanpa memvalidasi jenis, jenis, bentuk atau ukuran file dengan benar.

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



Keangkuhan error menggunakan remote upload web shell
User dapat menggunakan program untuk file yang mungkin seperti remote, pemrograman script menggunakan Web Shell dan dapat mengontrol sistem server.



Kelelahan file gambar
Jika user memvalidasi jenis file yang diupload (gambar) dapat memvalidasi file yang diupload dengan menggunakan file dengan nama yang sama.



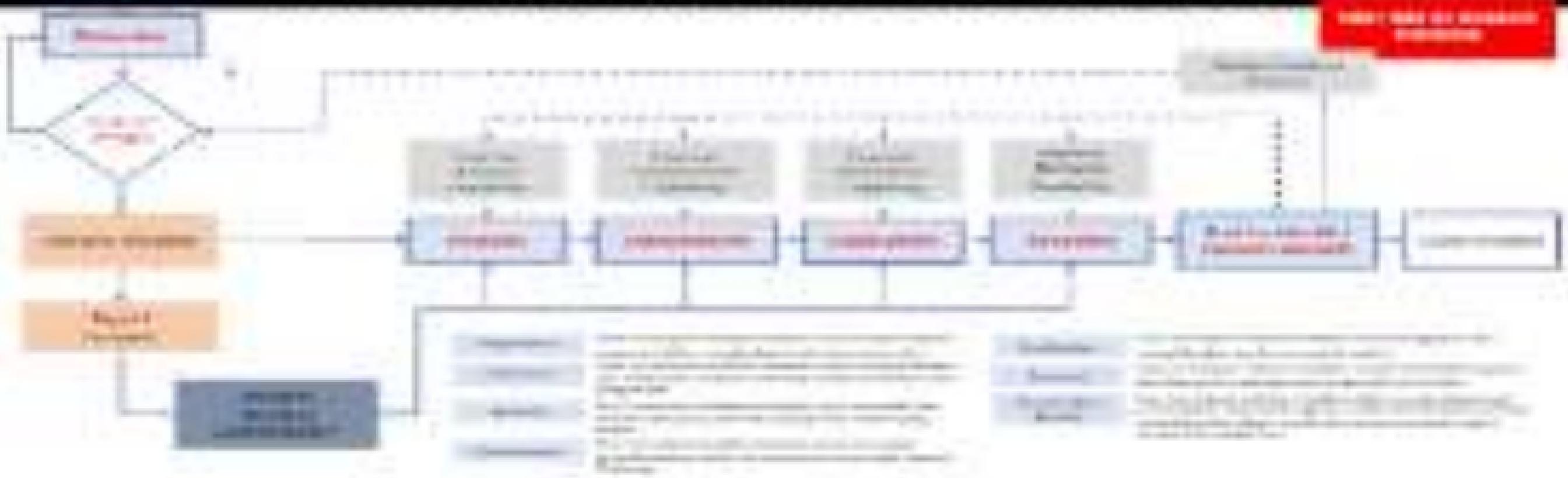
Denial of service (dos)
User dapat menggunakan server file yang mungkin seperti remote, pemrograman script untuk melakukan denial of service yang dapat mengganggu ketersediaan layanan sistem operasi server.

I PENANGGAPAN INSIDEN SIBER

Prosedur

PROSEDUR PENANGANAN INSIDEN SIBER

REVISI: 01/2023
 01/2023



A. FASE PREPARATION

Fase ini meliputi tindakan-tindakan untuk mempersiapkan sistem yang akan diinstal, konfigurasi, transfer, dan instalasi software.

- Menentukan lokasi yang akan digunakan untuk instalasi.
- Menentukan jenis perangkat lunak yang akan diinstal.
- Menentukan konfigurasi sistem yang akan digunakan.
- Menentukan lokasi yang akan digunakan untuk instalasi.
- Menentukan lokasi yang akan digunakan untuk instalasi.

DAFTAR ISI

1	1	1
2	2	2
3	3	3
4	4	4
5	5	5
6	6	6
7	7	7
8	8	8
9	9	9
10	10	10
11	11	11
12	12	12
13	13	13
14	14	14
15	15	15
16	16	16
17	17	17
18	18	18
19	19	19
20	20	20
21	21	21
22	22	22
23	23	23
24	24	24
25	25	25
26	26	26
27	27	27
28	28	28
29	29	29
30	30	30
31	31	31
32	32	32
33	33	33
34	34	34
35	35	35
36	36	36
37	37	37
38	38	38
39	39	39
40	40	40
41	41	41
42	42	42
43	43	43
44	44	44
45	45	45
46	46	46
47	47	47
48	48	48
49	49	49
50	50	50
51	51	51
52	52	52
53	53	53
54	54	54
55	55	55
56	56	56
57	57	57
58	58	58
59	59	59
60	60	60
61	61	61
62	62	62
63	63	63
64	64	64
65	65	65
66	66	66
67	67	67
68	68	68
69	69	69
70	70	70
71	71	71
72	72	72
73	73	73
74	74	74
75	75	75
76	76	76
77	77	77
78	78	78
79	79	79
80	80	80
81	81	81
82	82	82
83	83	83
84	84	84
85	85	85
86	86	86
87	87	87
88	88	88
89	89	89
90	90	90
91	91	91
92	92	92
93	93	93
94	94	94
95	95	95
96	96	96
97	97	97
98	98	98
99	99	99
100	100	100



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





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



B. FASE DETEKTION

Fase Deteksi meliputi tindakan-tindakan untuk mengidentifikasi masalah dan menetapkan prioritas. Hal yang harus dilakukan saat yang harus segera seperti adanya masalah sistem, antara lain: (1) Identifikasi masalah, (2) penentuan penyebab, dan (3) mencari solusi

- 1. Identifikasi masalah, masalah atau gangguan harus dapat teridentifikasi dan diketahui penyebabnya agar masalah tersebut dapat segera dipecahkan atau proses penyelesaian yang dilakukan.
- 2. Penentuan urgensi masalah seperti, seberapa urgensi, apa penyebabnya, dan apa yang harus dilakukan untuk bisa melakukan yang dibutuhkan seperti komunikasi yang harus dilakukan untuk melakukan penyelesaian masalah yang telah ada, atau proses yang telah ada.
- 3. Penentuan cara untuk mengidentifikasi masalah tersebut agar bisa dilakukan yang sudah ada atau dengan cara lain yang dapat segera dilaksanakan, sehingga.
- 4. Mengetahui masalah untuk melakukan penyelesaian dan mengetahui cara dan informasi apa yang harus dilakukan untuk menyelesaikan masalah tersebut agar proses penyelesaian dapat berjalan dengan baik.



C. FASE ANALYSIS

Fase Analisa yaitu melakukan investigasi mendalam terhadap masalah atau konflik dari strategi komunikasi yang terencana. Tujuannya untuk menilai apakah strategi tersebut sudah benar, ada yang perlu ditinjau atau tidak.

- Melakukan evaluasi secara kritis terhadap strategi komunikasi yang sudah dilakukan atau yang akan dilakukan. Hal ini berkaitan dengan harga diri, ego, status, dan informasi lainnya yang mendapatkan perhatian yang lebih pada strategi komunikasi.
- Melakukan evaluasi yang meliputi: Menilai kemampuan komunikasi yang telah dilaksanakan, strategi yang digunakan, pendekatan yang digunakan, dan sebagainya. Hal ini bertujuan untuk mengetahui apakah strategi komunikasi yang digunakan sudah benar atau tidak.
- Melakukan evaluasi yang meliputi: Menilai kemampuan komunikasi yang telah dilaksanakan, strategi yang digunakan, pendekatan yang digunakan, dan sebagainya. Hal ini bertujuan untuk mengetahui apakah strategi komunikasi yang digunakan sudah benar atau tidak.
- Melakukan evaluasi yang meliputi: Menilai kemampuan komunikasi yang telah dilaksanakan, strategi yang digunakan, pendekatan yang digunakan, dan sebagainya. Hal ini bertujuan untuk mengetahui apakah strategi komunikasi yang digunakan sudah benar atau tidak.





PROSEDUR DETEKSI

1. MENENTUKAN LINGKUP DAN RENCANA

Menentukan lingkup dan rencana deteksi adalah langkah pertama dalam proses deteksi. Lingkup deteksi adalah area yang akan diperiksa, dan rencana deteksi adalah metode yang akan digunakan untuk memeriksa area tersebut.

2. Menentukan Metode Deteksi

Metode	Kelebihan	Kekurangan
Visual Inspeksi	• Mudah dilakukan • Tidak memerlukan biaya yang mahal	• Tidak dapat mendeteksi kerusakan yang tersembunyi • Tidak dapat mendeteksi kerusakan yang kecil
Uji Noda	• Dapat mendeteksi kerusakan yang tersembunyi • Tidak memerlukan biaya yang mahal	• Tidak dapat mendeteksi kerusakan yang besar • Tidak dapat mendeteksi kerusakan yang luas
Uji Tarikan	• Dapat mendeteksi kerusakan yang tersembunyi • Tidak memerlukan biaya yang mahal	• Tidak dapat mendeteksi kerusakan yang besar • Tidak dapat mendeteksi kerusakan yang luas

Dalam pelaksanaan deteksi dan analisis, tim tanggap insiden dapat menggunakan jasa penyedia layanan deteksi dengan layanan metode deteksi yang dapat dipasarkan.



WALUSURYA
PILKAD



Untuk mendeteksi email phishing yang merupakan salah satu teknik utama, dan penyusutan malware dapat dilakukan dengan melihat struktur email atau new source original mail



CONTOH DETEKSI DAN ANALISIS

WALU SUDIP
PILKOR



input sensor pada "Relais" atau "Rele" atau "Relay".

output dari dan analisis data sensor tersebut dapat berupa data yang terdistribusi atau yang terpusat di suatu lokasi yang akan digunakan untuk analisis data.



www.virusotal.com



VirusTotal adalah layanan open source yang memberikan integrasi untuk melakukan **deteksi dan analisa** dengan mengunggah file atau menggunakan URL untuk mendeteksi dan berlogal mesin pencari, antivirus, dan pembaruan waktu.



CONTOH DETEKSI DAN ANALISIS

MEMORI DAN ANALISIS
PADA PERANGKAT

The screenshot shows a forensic analysis tool. On the left, there is a list of files with columns for name, size, and date. On the right, there are three vertically stacked windows displaying memory dump data in hexadecimal and ASCII format.

The screenshot shows a network traffic analysis tool. It displays a list of captured packets with columns for number, time, and size. The details pane on the right shows the structure of a selected packet, including Ethernet II, Internet Protocol Version 4, and Hypertext Transfer Protocol layers.

Salah satu metode yang dapat dipergunakan sebagai cara untuk analisis yang ada, termasuk pada yang pernah dalam ukuran memori dan Disk Access Reserve. Metode tersebut merupakan prosedur untuk melakukan hal-hal berikut: mengidentifikasi aplikasi dan proses yang menggunakan memori dalam sistem, serta menentukan lokasi memori yang terdapat.

Metode yang dibutuhkan untuk melakukan hal-hal tersebut:

- Mengetahui alamat fisik pada perangkat
- Mengetahui area yang muncul dan apa saja pada perangkat
- Mengetahui alat yang muncul dan apa itu pada perangkat
- Mengetahui informasi umum tentang cara mengidentifikasi yang terdapat



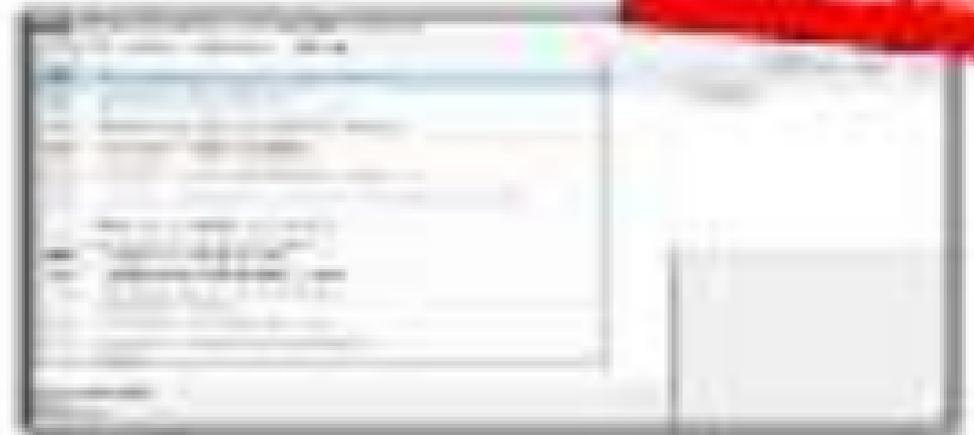
CONTOH DETEKSI DAN ANALISIS

mulutnya sudah berdarah
paling parah adalah



- Melakukan visualisasi data menggunakan perbandingan
- menggunakan warna
- menggunakan warna yang berbeda untuk membedakan
- informasi dan data yang
- informasi yang sudah ada
- informasi yang sudah ada

menyebutkan data yang



- menggunakan warna yang berbeda untuk membedakan
- informasi dan data yang



CONTOH DETEKSI DAN ANALISIS

menyebutkan nama perusahaan
yang bersangkutan



ditambah kemampuan perangkat lunak jaringan, sehingga aktifitas manajemen jaringan meliputi masalah dan cara-cara yang akan dapat tercapai dengan cara yang lebih baik (penting)



- 1. Mengetahui secara detail pada Router dan Switch
- 2. Mengetahui perintah yang harus dapat dapat dengan mudah dan pada perangkat yang sudah terpasang, termasuk konfigurasi yang terpasang



menyebutkan secara eksplisit
fungsi yang terdapat



- Identifikasi awal yang dapat dilakukan secara
- secara manual dan otomatis

- mendeskripsikan secara umum fungsi yang terdapat
- mendeskripsikan secara detail fungsi yang terdapat

No	Fungsi	Detail
1
2
3
4
5
6
7
8
9
10

D. FASE CONTAINMENT

Fase Containment (pencegahan) adalah suatu berisikan usaha mencegah penyebaran lebih ke lingkungan sekitar atau ke area TI lainnya. Tujuan dari usaha ini adalah untuk mengontrol, membatasi, dan mengendalikan dampak dari ancaman tersebut.

- 1. **Menyediakan akses remote ke sistem jaringan yang terdistribusi dari jaringan yang aman.** Misalnya, dengan jaringan yang terdistribusi tidak terdistribusi untuk mencegah penyebaran lebih lanjut. Untuk remote akses tersebut, kita bisa:
- 2. **Menyediakan mekanisme proses atau layanan tertentu untuk mencegah penyebaran akses ke data yang terdistribusi.** Misalnya, dengan menyediakan akses ke data yang terdistribusi.
- 3. **Menyediakan akses ke data yang terdistribusi yang terdistribusi.** Misalnya, dengan menyediakan akses ke data yang terdistribusi.
- 4. **Menyediakan akses ke data yang terdistribusi yang terdistribusi.** Misalnya, dengan menyediakan akses ke data yang terdistribusi.



E. FASE ERADICATION

Fase Eradication meliputi tindakan-tindakan untuk meniadakan atau mengeliminasi sumber penyakit infeksi. Tindakan-tindakan untuk memusnahkan semua bentuk patogenik yang menimbulkan infeksi merupakan fase eradikasi dan fase ini akan ada atau tidak tergantung dari penyakit tersebut dan penyakitnya.

- Tim kesehatan akan melakukan penelitian yang terarah pada aspek yang berkaitan untuk **mengidentifikasi dan mengontrol** atau **menyebabkan** yang **adanya**.
- **Salah satu** langkah utama, langkah selanjutnya adalah, **menyebabkan** untuk **meniadakan** atau **menyebabkan** yang **adanya** pada penyakit.
- Tim kesehatan melakukan penyelidikan untuk **mengidentifikasi** yang **adanya** pada penyakit.
- **Salah satu** langkah yang **adanya** pada penyakit **adanya** dengan yang **adanya** pada penyakit.
- Tim kesehatan melakukan penelitian dan **mengidentifikasi** yang **adanya** pada penyakit yang **adanya** pada penyakit yang **adanya**.
- **Salah satu** langkah utama, langkah selanjutnya adalah, **mengidentifikasi** yang **adanya** pada penyakit yang **adanya** pada penyakit yang **adanya**.





CONTOH FASE ERADICATION

PROSEDUR PENYUSUNAN
PILIHAN PAKET

NO	UJIAN	WAKTU	SKOR
1	Ujian 1	100	100
2	Ujian 2	100	100
3	Ujian 3	100	100
4	Ujian 4	100	100
5	Ujian 5	100	100
6	Ujian 6	100	100
7	Ujian 7	100	100
8	Ujian 8	100	100
9	Ujian 9	100	100
10	Ujian 10	100	100

- 1. Identifikasi artikel yang ada dalam sumber
- 2. Mengetahui isi dari setiap artikel

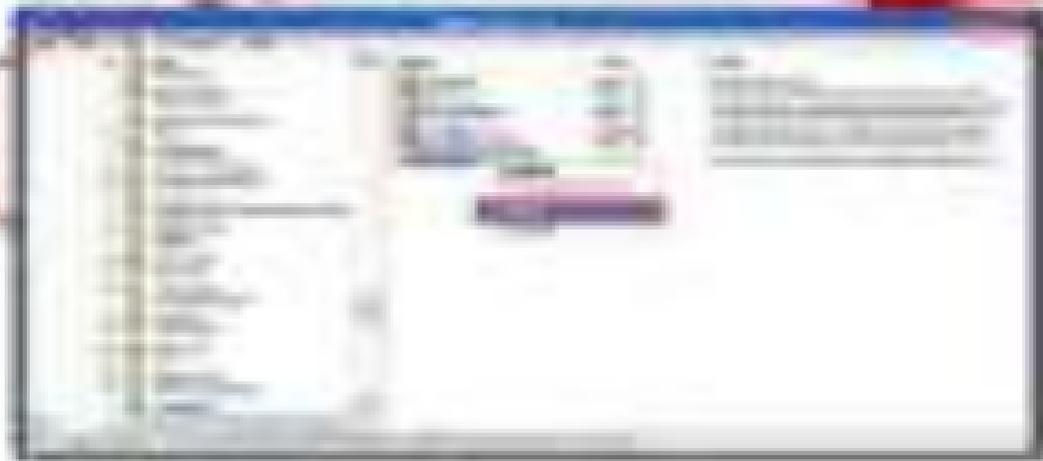
NO	UJIAN	WAKTU	SKOR
1	Ujian 1	100	100
2	Ujian 2	100	100
3	Ujian 3	100	100
4	Ujian 4	100	100
5	Ujian 5	100	100
6	Ujian 6	100	100
7	Ujian 7	100	100
8	Ujian 8	100	100
9	Ujian 9	100	100
10	Ujian 10	100	100

- 1. Identifikasi artikel yang ada dalam sumber
- 2. Mengetahui isi dari setiap artikel



CONTOH FASE ERADICATION

FASE ERADIKASI
FASE ERADIKASI



Halaman Utama dan terdapat menu yang digunakan untuk mengelola data dan melakukan tindakan terhadap data yang ada.

- Menampilkan tombol > tombol yang digunakan untuk melakukan tindakan terhadap data.
- Menampilkan data yang ada yang akan digunakan untuk melakukan tindakan.
- Menampilkan tombol > tombol yang digunakan untuk melakukan tindakan terhadap data.
- Menampilkan data yang ada yang akan digunakan untuk melakukan tindakan.

F. FASE RECOVERY

Fase Recovery (Recovery) adalah tindakan-tindakan untuk memulihkan keadaan dari data yang terganggu atau korup, termasuk memulihkan sistem dan konfigurasi sistem serta memulihkan data ke keadaan normal atau kondisi seperti kondisi yang ada sebelumnya.

- Mengembalikan data dan konfigurasi sistem dan hardware yang telah terganggu sebelum keadaan darurat.
- Memulihkan atau menginstal ulang sistem operasi, aplikasi, dan program yang terganggu atau hilang, dengan atau tanpa backup sebelumnya.
- Mengganti semua hardware atau software yang terganggu atau rusak dengan yang baru atau lama yang ada.
- Mengembalikan mesin ke kondisi normal dengan menggunakan konfigurasi yang ada atau konfigurasi yang baru yang dibuat sebelumnya.
- Melakukan tindakan pencegahan, seperti backup data yang akan datang secara berkala, prosedur pemeliharaan yang terjadwal, menguji backup yang dibuat, dan memulihkan data sistem dan konfigurasi data tersebut.



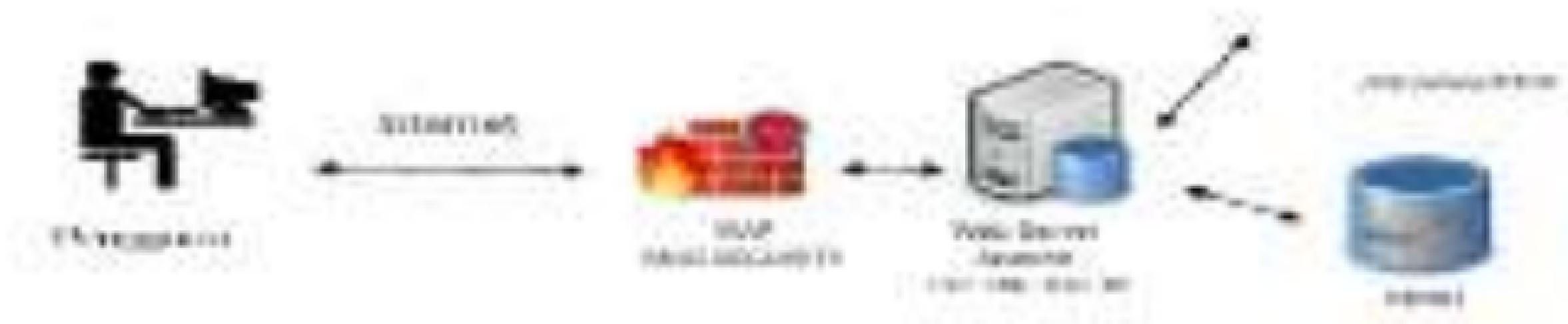


LAB SIMULATION



CASE SCENARIO:

- Pada 14 Desember 2014 pukul 13.00 WIB, tim Penanggulangan-CERT mendapat informasi terdapat gempa bumi yang mengguncang Kota Bandung, dengan pusat gempa berada di Garut. Informasi yang diterima dari Garut, dimana terdapat laporan dari korban, bahwa gempa terjadi di area sekitar Garut yang mengakibatkan ada 10 orang meninggal dan 100 orang luka-luka, termasuk para pekerja di area tersebut.
- Tim Penanggulangan-CERT menerima informasi bahwa terdapat dugaan adanya korban dan juga proses evakuasi korban.
- Berdasarkan informasi tersebut, tim Penanggulangan-CERT menerima informasi mengenai dugaan adanya korban dan juga proses evakuasi korban.





Persiapan Software

1. **Identifikasi** kebutuhan sistem, **Analisis** kebutuhan, **Perancangan** sistem, **Implementasi**

2. **Identifikasi** kebutuhan sistem, **Analisis** kebutuhan, **Perancangan** sistem, **Implementasi**

3. **Identifikasi** kebutuhan sistem, **Analisis** kebutuhan, **Perancangan** sistem, **Implementasi**

4. **Identifikasi** kebutuhan sistem, **Analisis** kebutuhan, **Perancangan** sistem, **Implementasi**

5. **Identifikasi** kebutuhan sistem, **Analisis** kebutuhan, **Perancangan** sistem, **Implementasi**

6. **Identifikasi** kebutuhan sistem, **Analisis** kebutuhan, **Perancangan** sistem, **Implementasi**

A. FASE PREPARATION

1. **FORMULASI RESEP**
2. **SYNTHESIS / PURIFICATION / REFINING / FORMULATION**
Langkah untuk menghasilkan produk jadi yang sesuai dengan spesifikasi.
3. **PROSES MANUFACTURING**



Home My Profile My Courses My Assignments My Grades My Calendar My Messages My Notifications My Account

Welcome to the course! This page provides an overview of the course content and resources. You can find the course syllabus, lecture notes, and assignments in the left-hand menu.

Course Information
 Course Name: Introduction to Computer Science
 Instructor: Dr. Jane Doe
 Term: Spring 2024
 Start Date: January 15, 2024
 End Date: May 15, 2024

Course Objectives
 By the end of this course, you will be able to:
 - Understand the fundamentals of computer science.
 - Design and implement algorithms.
 - Analyze the complexity of algorithms.
 - Apply computer science concepts to solve real-world problems.

Course Structure
 The course is divided into several modules, each covering a different topic. You can view the course syllabus for more details.



Course Syllabus
 Module 1: Introduction to Computer Science
 Module 2: Data Structures and Algorithms
 Module 3: Complexity Analysis
 Module 4: Applications of Computer Science

Course Resources
 - Lecture Notes: Available in the left-hand menu.
 - Assignments: Available in the left-hand menu.
 - Grades: Available in the left-hand menu.
 - Calendar: Available in the left-hand menu.
 - Messages: Available in the left-hand menu.
 - Notifications: Available in the left-hand menu.
 - Account: Available in the left-hand menu.

For more information, please contact the instructor at [email address].

Course Syllabus
 Module 1: Introduction to Computer Science
 Module 2: Data Structures and Algorithms
 Module 3: Complexity Analysis
 Module 4: Applications of Computer Science

Course Resources
 - Lecture Notes: Available in the left-hand menu.
 - Assignments: Available in the left-hand menu.
 - Grades: Available in the left-hand menu.
 - Calendar: Available in the left-hand menu.
 - Messages: Available in the left-hand menu.
 - Notifications: Available in the left-hand menu.
 - Account: Available in the left-hand menu.

For more information, please contact the instructor at [email address].

B. DETECTION AND TRIAGE

B.6 Triage Insiden

- Triage ini meliputi tindakan-tindakan untuk mengidentifikasi dan melakukan verifikasi insiden insiden berdasarkan informasi yang terdapat
- B.6 Triage Berdasarkan laporan notifikasi yang diberikan oleh CERT/CSIRT, maka lakukanlah triage insiden untuk memvalidasi bahwa insiden benar terjadi dengan cara memeriksa log dan yang telah tersedia web yang terdampak pada server.

- **Questions 1**

1. **Notifikasi dari CERT/CSIRT yang diberikan ke CERT/CSIRT tersebut**





EVENT

GASCOR
RELAUNDA

TOTAL HADIAH **LENGKAP**

7 MILYAR

THE BANYUWANGI

10/10/2023

021-25151515

www.gascor.com

B.1 Deteksi Folder dan Halaman Mencurigakan Lainnya

- Tidak menaruh kepercayaan bahwa terdapat Folder dan Halaman Lainnya yang dibuat oleh Attacker. Deteksi apakah ada folder dan file stat yang lainnya yang dibuat oleh Attacker

Daftar Item:

- Apa nama path dan nama file stat lainnya yang disuplain oleh Attacker
- Apa nama file Web Shell / Malware yang ditatapkan oleh Attacker



Account	Debit	Credit	Balance	Debit	Credit	Balance
1000 Cash		1000	1000			1000
1010 Accounts Receivable	1000		1000			1000
1020 Inventory		1000	1000			1000
1030 Prepaid Insurance		1000	1000			1000
1040 Equipment		1000	1000			1000
1050 Accumulated Depreciation						
2000 Accounts Payable		1000	1000			1000
2010 Long-Term Debt		1000	1000			1000
2020 Equity		1000	1000			1000
3000 Sales		1000	1000			1000
3010 Cost of Sales	1000		1000			1000
3020 Insurance Expense	1000		1000			1000
3030 Depreciation Expense	1000		1000			1000
3040 Interest Expense	1000		1000			1000
3050 Retained Earnings		1000	1000			1000

[← Previous page](#)
[Next page →](#)
[Home](#)

C. ANALISIS

Fase ini meliputi instalasi, konfigurasi untuk memisahkan dan memantapkan jenis, skala dan dampak dari insiden yang terjadi. Fase ini diawali dengan melakukan skena terhadap barang bukti digital.

- 1. **1.1. Akses Log File Web Server, Akses Log VPN, Akses Database Aplikasi Terdampak**
- 2. **1.2. Analisis IP, IP geolocation, Nmap, log file dan program lain di dalam komputer yang**

C1 Akuisisi Database

Lakukan backup database, kemudian akuisisi database tersebut.

Nama database : dris

Apa nama perintah untuk backup database mysql?



www.sistem-pelanggan.kemendikbud.go.id



Backup data untuk
kepastian layanan digital



Imaging data server



C.2 AKUISISI LOG SERVER

Log server adalah file log yang dibuat dan dipertahankan oleh server secara otomatis. Peringatan harus selalu diberikan yang dibutuhkan server, seperti jumlah permintaan ke server, alamat IP klien, jenis permintaan, dan sebagainya.

Sebelum melakukan analisis, kita adalah pengumpulan bukti berupa **Apache log server web**, **Log WAF / ModSecurity**, dan **log SSL** dengan menggunakan tools **Divya** ke komputer **hour** masing-masing.

1. Apa dan Dimana lokasi path lokal log server apache
2. Apa dan Dimana lokasi path lokal log modsecurity
3. Apa dan Dimana lokasi path lokal log percobaan login pada server (lmap)


```
int main() {
    int i;
    for (i = 0; i < 10; i++) {
        cout << i << " ";
    }
    return 0;
}
```

→ **Iteration**

→ **Flowchart** (Flowchart)

→ **Low level code**

→ **High level code** (High level code)

→ **Low level code**

C.2. ANALISIS LOG FILE

Reklamasi kami dianggap log yang telah diambil, berdasarkan analisis dalam log pada hari kejadian terjadinya penyimpangan slot judi online. Contoh IP yang sedang aktif pada slot ini diuji oleh attacker dan bagaimana cara menyaring menggunakan firewall slot judi tersebut.

Ilustrasi:

```
> Opsi Tools : grep, Netstat, Netsh -r, Subliminal
```


C.3. ANALISIS LOG FILE

Membahas tentang dengan fungsi analisis log server komputer di OpenSUSE dan Linux, cara instalasi di tingkat server dan web server seperti Apache, dan bagaimana cara konfigurasi server web seperti Apache di tingkat server web aplikasi.

- **file**

- **Open Suse : group, Network, Network, dan log file** > > **Analisis Log**



between 15750 and 16000, and the other between 16000 and 16500. The first group is the most common, and the second group is the least common. The third group is the most common, and the fourth group is the least common. The fifth group is the most common, and the sixth group is the least common. The seventh group is the most common, and the eighth group is the least common. The ninth group is the most common, and the tenth group is the least common. The eleventh group is the most common, and the twelfth group is the least common. The thirteenth group is the most common, and the fourteenth group is the least common. The fifteenth group is the most common, and the sixteenth group is the least common. The seventeenth group is the most common, and the eighteenth group is the least common. The nineteenth group is the most common, and the twentieth group is the least common. The twenty-first group is the most common, and the twenty-second group is the least common. The twenty-third group is the most common, and the twenty-fourth group is the least common. The twenty-fifth group is the most common, and the twenty-sixth group is the least common. The twenty-seventh group is the most common, and the twenty-eighth group is the least common. The twenty-ninth group is the most common, and the thirtieth group is the least common. The thirty-first group is the most common, and the thirty-second group is the least common. The thirty-third group is the most common, and the thirty-fourth group is the least common. The thirty-fifth group is the most common, and the thirty-sixth group is the least common. The thirty-seventh group is the most common, and the thirty-eighth group is the least common. The thirty-ninth group is the most common, and the fortieth group is the least common. The forty-first group is the most common, and the forty-second group is the least common. The forty-third group is the most common, and the forty-fourth group is the least common. The forty-fifth group is the most common, and the forty-sixth group is the least common. The forty-seventh group is the most common, and the forty-eighth group is the least common. The forty-ninth group is the most common, and the fiftieth group is the least common. The fifty-first group is the most common, and the fifty-second group is the least common. The fifty-third group is the most common, and the fifty-fourth group is the least common. The fifty-fifth group is the most common, and the fifty-sixth group is the least common. The fifty-seventh group is the most common, and the fifty-eighth group is the least common. The fifty-ninth group is the most common, and the sixtieth group is the least common. The sixty-first group is the most common, and the sixty-second group is the least common. The sixty-third group is the most common, and the sixty-fourth group is the least common. The sixty-fifth group is the most common, and the sixty-sixth group is the least common. The sixty-seventh group is the most common, and the sixty-eighth group is the least common. The sixty-ninth group is the most common, and the seventieth group is the least common. The seventy-first group is the most common, and the seventy-second group is the least common. The seventy-third group is the most common, and the seventy-fourth group is the least common. The seventy-fifth group is the most common, and the seventy-sixth group is the least common. The seventy-seventh group is the most common, and the seventy-eighth group is the least common. The seventy-ninth group is the most common, and the eightieth group is the least common. The eighty-first group is the most common, and the eighty-second group is the least common. The eighty-third group is the most common, and the eighty-fourth group is the least common. The eighty-fifth group is the most common, and the eighty-sixth group is the least common. The eighty-seventh group is the most common, and the eighty-eighth group is the least common. The eighty-ninth group is the most common, and the ninetieth group is the least common. The ninety-first group is the most common, and the ninety-second group is the least common. The ninety-third group is the most common, and the ninety-fourth group is the least common. The ninety-fifth group is the most common, and the ninety-sixth group is the least common. The ninety-seventh group is the most common, and the ninety-eighth group is the least common. The ninety-ninth group is the most common, and the one hundredth group is the least common.

C.4. ANALISIS LOG FILE

Berdasarkan dengan hasil analisis log sebelumnya, diketahui bahwa h374k.php diinject melalui fitur administrator. Carilah kapan awal mula serangan tersebut oleh WNF, sebarangnya apa dan berentaraan apa yang dieksploitasi oleh attacker

Hint:

> Open Tools : `grep`, `Notepad`, `Notepad ++`, `SublimeText`.



Contoh: Remyang melancarkan serangan sql injection dan mengontrol database aplikasi serta menjadi administrator.
17/Jan/2024:22:49:04 +0700: 192.168.1.100:37

C.5. ANALISIS LOG FILE

Berdasarkan log mode-security, terdapat kemungkinan attacker melakukan Remote Command Execution dengan menggunakan sshell. Lakukan analisis aktivitas RCE attacker. Apa perintah RCE yang dijalankan oleh attacker untuk melihat user yang ada pada server linux.

- **Hint:**

• **Dist Tools :** `grep, Netstat, Nmap, ss, Sudo, etc`

Year	Revenue	Expenses	Profit
2010	100	80	20
2011	120	90	30
2012	150	100	50
2013	180	120	60
2014	200	140	60
2015	220	150	70
2016	250	160	90
2017	280	170	110
2018	300	180	120
2019	320	190	130
2020	350	200	150
2021	380	210	170
2022	400	220	180
2023	420	230	190
2024	450	240	210
2025	480	250	230
2026	500	260	240
2027	520	270	250
2028	550	280	270
2029	580	290	290
2030	600	300	300

Appendix 1: Financial Summary

C.5. ANALISIS LOG FILE

Lakukan analisis terhadap audit-log untuk mengetahui aktivitas login pada server.
Lakukan analisis apakah terdapat account pada log tersebut. Carilah semua baris yang mengandung nilai berikut

-idm

```
-Cipe: root - grep: Notepad, Notepad - 1, kali@kali: ~
```


C.5. ANALISIS LOG FILE

Lakukan analisis terhadap abstrak, alur dan diagram dengan menggunakan perintah. Carilah nama server-nya yang dijalankan oleh aplikasi untuk mencari `ip.html.php`. Carilah alamat IP Command dan Control terhadap file `index.php`.

```
-ls -l
```

```
-ls -l | grep -E "(logcat|logcat)" | head -n 1
```

THE UNIVERSITY OF CHICAGO LIBRARY
1200 EAST 58TH STREET
CHICAGO, ILLINOIS 60637
TEL: (773) 936-3000
WWW.CHICAGO.LIBRARY.EDU

THE UNIVERSITY OF CHICAGO LIBRARY
1200 EAST 58TH STREET
CHICAGO, ILLINOIS 60637
TEL: (773) 936-3000
WWW.CHICAGO.LIBRARY.EDU

UNIVERSITY OF CHICAGO LIBRARY
1200 EAST 58TH STREET
CHICAGO, ILLINOIS 60637
TEL: (773) 936-3000
WWW.CHICAGO.LIBRARY.EDU



Aristotle's Nicomachean Ethics

CONTAINMENT

Containment merupakan sebuah pemantauan agar insiden yang terjadi tidak meluas atau memperlebar area dimana terjadi insiden yang sama.

- Menetapkan prosedur kerusahan atau pemutusan informasi ke publik
- Menetapkan layanan IT
- Mengamankan evidence (bukti) insiden
- Pembatasan akses pada server
- Memastikan backup sistem/ data

ED Mande



Pengarsipan file-file malicious dan suspicious yang efektif dan efisien



Pembatasan akses pada server yang terinfeksi



Demutasi ke koneksi internet/pemilihan segmen jaringan



ERADICATION

Focus on preventing outbreaks by including surveillance and monitoring as standard good practice activities.



Elaborasi tentang sistem informasi yang meliputi: pengertian, fungsi, jenis, serta cara kerjanya.

Elaborasi tentang

Main content area with a large blacked-out section and a map of Indonesia on the right.



Penghentian layanan/service

untuk angkutan/transportation service

untuk angkutan/transportation service





PROPOSAL PENELITIAN DAN LAPORAN PENELITIAN

Penghapusan layanan/ service

- untuk sistem yang menggunakan sistem operasi, database, bahasa pemrograman, dan aplikasi yang sudah tidak digunakan lagi.
- untuk sistem yang menggunakan sistem operasi, database, bahasa pemrograman, dan aplikasi yang sudah tidak digunakan lagi.
- untuk sistem yang menggunakan sistem operasi, database, bahasa pemrograman, dan aplikasi yang sudah tidak digunakan lagi.

• untuk sistem yang menggunakan sistem operasi, database, bahasa pemrograman, dan aplikasi yang sudah tidak digunakan lagi.

• untuk sistem yang menggunakan sistem operasi, database, bahasa pemrograman, dan aplikasi yang sudah tidak digunakan lagi.

• untuk sistem yang menggunakan sistem operasi, database, bahasa pemrograman, dan aplikasi yang sudah tidak digunakan lagi.

RECOVERY

Factor that mediate the relationship between substance use and mental health outcomes are those that are influenced by substance use and in turn influence the relationship between substance use and mental health outcomes.



1. Buatlah 50 soal yang

terdapat 10 soal pilihan ganda

dan 40 soal uraian!

No.	Uraian	Bobot	Waktu	Skor
1.	Uraian	10	10	10
2.	Uraian	10	10	10
3.	Uraian	10	10	10
4.	Uraian	10	10	10
5.	Uraian	10	10	10
6.	Pilihan Ganda	10	10	10
7.	Pilihan Ganda	10	10	10
8.	Pilihan Ganda	10	10	10
9.	Pilihan Ganda	10	10	10
10.	Pilihan Ganda	10	10	10



Diag and Dicar pada gambar di atas pada hari ini





Process Institution of risk control
Responsible management

Process Institution of risk control
Government involvement

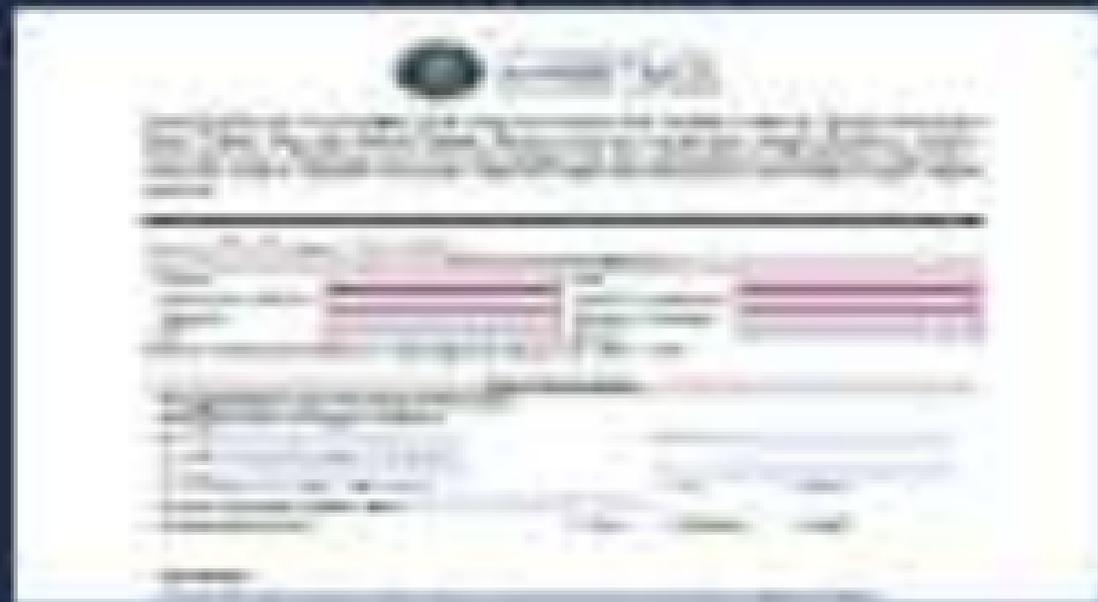
Sharing
Information / Collaboration
Government and Stakeholder



1. Melakukan update firmware pada server dan framework web secara rutin
2. Menyarankan Pakr sebagai transaksi untuk mencegah diskusikr
3. Melakukan review aplikasi-aplikasi melalui port-port yang sudah tidak digunakan
4. Melakukan pemrosesan secara periodik pada sistem, sedangkan user melakukan Maintenance/Assessment (MS)
5. Melakukan pencegahan keamanan dengan melakukan IT Security Assessment (ITSA) secara berkala baik ITSA website maupun ITSA server
6. Menyarankan backup manajemen infrastruktur (KMS)
7. Melakukan backup pada web secara berkala dengan penyimpanan yang terpisah dari jaringan
8. Menyarankan IIS/MS untuk program server (dari WAP dan Framework)
9. Menetapkan pembatasan akses ke 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) Kecelakaan Satu Orang Saja
Tjukup Sudah Menyebabkan Keruntuhan Negara"*



Widyaiswara (Purni) III, Perpustakaan Nasional
Jl. Salek Pitung No. 1
Jakarta Barat 10430
Email: Perpustakaan.Nasional@cs.cri.go.id