LAPORAN PRAKTIKUM KEAMANAN SIBER TUGAS 10

KELAS PRAKTIKUM KEAMANAN SIBER C– TIK

KELOMPOK :

1. **ELSA ESTER LOKAS** **220211060213**
2. **GABRIELLA IGNATIA MANENGKEY** **220211060195**
3. **JUSTISYA INJILIA TUMBEL** **220211060229**

PROGRAM STUDI TEKNIK INFORMATIKA
JURUSAN ELEKTRO
FAKULTAS TEKNIK

UNIVERSITAS SAM RATULANGI

2025

Lab – Incident Handling

Objectives

Apply your knowledge of security incident handling procedures to formulate questions about given incident scenarios.

Background / Scenario

Computer security incident response has become a vital part of any organization. The process for handling a security incident can be complicated and involve many different groups. An organization must have standards for responding to incidents in the form of policies, procedures, and checklists. To properly respond to a security incident, the security analyst must be trained to understand what to do, and must also follow all of the guidelines outlined by the organization. There are many resources available to help organizations create and maintain a computer incident response handling policy, but the NIST Special Publication 800-61 is specifically called by the CCNA CyberOps SECOPS exam topics. This publication can be found here:

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Scenario 1: Worm and Distributed Denial of Service (DDoS) Agent Infestation

Study the following scenario and discuss and determine the incident response handling questions that should be asked at each stage of the incident response process. Consider the details of the organization and the CSIRC when formulating your questions.

This scenario is about a small, family-owned investment firm. The organization has only one location and less than 100 employees. On a Tuesday morning, a new worm is released; it spreads itself through removable media, and it can copy itself to open Windows shares. When the worm infects a host, it installs a DDoS agent. It was several hours after the worm started to spread before antivirus signatures became available. The organization had already incurred widespread infections.

The investment firm has hired a small team of security experts who often use the diamond model of security incident handling.

Preparation:

- **Apakah Perusahaan memiliki kebijakan keamanan siber yang sudah diperbarui?**
- **Apakah ada pelatihan keamanan reguler untuk semua karyawan, terutama mengenai ancaman melalui removable media?**
- **Apakah perangkat lunak antivirus dan anti-malware sudah diperbarui secara berkala?**
- **Apakah jaringan internal memiliki segmentasi untuk membatasi penyebaran worm?**
- **Apakah ada rencana respons insiden yang sudah diuji dan disosialisasikan kepada staf TI?**
- **Apakah ada kontrol terhadap penggunaan dan akses removable media?**

Detection and Analysis:

- **Kapan dan bagaimana infeksi pertama kali terdeteksi?**
- **Sistem atau perangkat apa saja yang menunjukkan gejala infeksi worm?**
- **Apakah ada pola lalu lintas jaringanyang tidak biasa (indikasi DDoS agent aktif)?**
- **Apakah ada log atau alert dari system IDS/IPS yang menunjukkan penyebaran worm?**
- **Apakah file yang mencurigakan berhasil dianalisis dan diverifikasi sebagai worm?**
- **Apakah ada indikasi bahwa data telah dikompomikan atau disalahgunakan oleh worm?**

- **Apakah worm ini telah mengubah konfigurasi system atau mematikan layanan penting?**

Containment, Eradication, and Recovery:

Penahanan :

- **Sistem mana saja yang perlu segera diputus dari jaringan untuk mencegah penyebaran worm lebih lanjut?**
- **Apakah ada prosedur isolasi system yang terdampak (misalnya, memutus koneksi internet atau LAN)?**
- **Apakah removable media yang digunakan telah dikarantina atau disita untuk analisis lebih lanjut?**
- **Apakah akses pengguna ke system dikurangi sementara selama proses mitigasi?**
- **Bagaimana cara membatasi komunikasi keluar dari DDoS agent yang sudah terinstal di host terinfeksi?**

Pembersihan :

- **Apakah semua file dan registry yang berkaitan dengan worm dan DDoS agent sudah dihapus?**
- **Apakah system antivirus/amtimalware telah diperbarui dan dijalankan secara menyuluruh di semua system?**
- **Apakah semua removable media yang digunakan telah dipindai dan dibersihkan?**
- **Apakah konfigurasi system dan keamanan jaringan telah dikembalikan ke kondisi aman?**

Pemulihan :

- **Kapan system yang terdampkan dapat dihubungkan Kembali ke jaringan denga naman?**
- **Apakah system telah diuji untuk memastikan tidak ada sis worm atau agen DDoS?**
- **Apakah data telah diverifikasi keutuhannya dan dikembalikan dari backup yang bersih jika diperlukan?**
- **Apakah layanan penting organisasi sudah Kembali normal?**

Post-Incident Activity:

- **Apa saka Pelajaran yang bisa diambil dari insiden ini?**
- **Apakah dokumentasi insiden sudah disusun dengan lengkap untuk keperluarn audit atau evaluasi?**
- **Apakah kebijakan keaman perlu diperbaui berdasarkan hasil evaluasi insiden?**
- **Apakah karyawan dan tim TI perlu pelatihan tambahan untuk mencegah kejadian serupa?**
- **Apakah ada indicator kompromi yang bisa dibagikan ke komunitas keamanan (seperti CSIRC)?**

Scenario 2: Unauthorized Access to Payroll Records

Study the following scenario. Discuss and determine the incident response handling questions that should be asked at each stage of the incident response process. Consider the details of the organization and the CSIRC when formulating your questions.

This scenario is about a mid-sized hospital with multiple satellite offices and medical services. The organization has dozens of locations employing more than 5000 employees. Because of the size of the

organization, they have adopted a CSIRC model with distributed incident response teams. They also have a coordinating team that watches over the CSIRTs and helps them to communicate with each other.

On a Wednesday evening, the organization's physical security team receives a call from a payroll administrator who saw an unknown person leave her office, run down the hallway, and exit the building. The administrator had left her workstation unlocked and unattended for only a few minutes. The payroll program is still logged in and on the main menu, as it was when she left it, but the administrator notices that the mouse appears to have been moved. The incident response team has been asked to acquire evidence related to the incident and to determine what actions were performed.

The security teams practice the kill chain model and they understand how to use the VERIS database. For an extra layer of protection, they have partially outsourced staffing to an MSSP for 24/7 monitoring.

Preparation:

- **Apakah organisasi memiliki kebijakan keamanan siber yang diperbarui secara berkala?**
- **Apakah antivirus dan system deteksi intrusi (IDS) telah terpasang dan dikonfigurasi dengan benar?**
- **Apakah ada prosedur respons insiden yang terdokumentasi dengan baik?**
- **Apakah personel keamanan staf TI sudah mendapatkan pelatihan dalam mengahadapi worm dan infeksi DDoS?**
- **Apakah organisasi memiliki backup data yang aman dan diuji secara rutin?**
- **Apakah removable media dibatasi penggunannya atau sudah dilindungi dengan control keamanan?**

Detection and Analysis:

- **Bagaimana worm pertama kali terdeteksi? Melalui IDS, log, atau laporan pengguna?**
- **Apakah terdapat pola penyebaran tertentu dari worm melalui log jaringan atau aktivitas file sharing?**
- **Apakah worm meninggalkan signature tertentu yang bisa diidentifikasi oleh antivirus?**
- **Apakah log system menunjukkan waktu infeksi dan host mana saja yang terdampak?**
- **Apakah file yang tidak dikenal atau proses mencurigakan ditemukan di system korban?**
- **Apakah komunikasi outbound menunjukkan aktivitas mencurigakan yang terkait denganDDoS agent?**

Containment, Eradication, and Recovery:

Pengendalian :

- **Sistem mana yang harus segera diputus dari jaringan untuk menghentikan penyebaran worm?**
- **Apakah removable media harus diblokir sementara untuk semua pengguna?**
- **Apakah firewall perlu diperketat untuk memblokir traffic keluar masuk yang mencurigakan?**

Pembersihan :

- **Alat atau software apa yang digunakan untuk mebersihkan worm dari system?**
- **Apakah semua perangkat lunak antivirus telah diperbarui dengan signature terbaru?**
- **Apakah ada skrip otomatis yang bisa digunakan untuk memeriksa dan menghapus DDoS agent dari host?**

Pemulihan :

- **Apakah system sudah bisa dikembalikan dari backup yang aman?**

- **Bagaimana memverifikasi bahwa worm dan DDoS agent sudah benar-benar hilang dari jaringan?**
- **Apakah semua system yang terdampak sudah diperkuat (patched, updated) sebelum dihubungkan Kembali ke jaringan?**

Post-Incident Activity:

- **Apa Pelajaran yang bisa diambil dari insiden ini?**
- **Apakah perlu diperbarui kebijakan penggunaan removable media dan file sharing internal?**
- **Apakah organisasi perlu melakukan pelatihan ulang atau drill untuk staf TI dan pengguna biasa?**
- **Apakah perlu dibuat prosedur monitoring lanjuran untuk mencegah infeksi ulang?**
- **Apakah laporan lengkap insiden sudah disusun dan dikirim ke manajemen untuk evaluasi?**