**Assignment**

**Individual**

**KDS – Name SME**

**Session 10**

**To** **be Submitted Week 11**

**Tugas Personal ke-3**

1. Jelaskan kegunaan intrusion detection system. Selain untuk network, sebutkan juga kegunaan teknik intrusion detection system untuk hal yang lainnya dan jelaskan bagaimana cara kerjanya.

**Answer:**

**Kegunaan Intrusion Detection System (IDS)** untuk mendeteksi aktivitas yang mencurigakan pada sebuah sistem atau jaringan dan memberikan sebuah peringatan terhadap sistem atau administrator jaringan dan melakukan analisis dan mencari bukti dari percobaan penyusupan.

**Kegunaan IDS untuk hal lainnya** yaitu mendokumentasikan ancaman yang ada pada organisasi sehingga membantu dalam mengidentifikasi langkah-langkah keamanan yang tepat untuk mendidik manajemen tentang ancaman yang dihadapi organisasi.

**Cara Kerja Pertama IDS** akan melibatkan pencocokan lalu listas jaringan dengan basis data yang berisi cara-cara serangan dan penyusupan yang sering dilakukan penyerang sehingga membutuhkan pembaruan terhadap basis data signature IDS yang bersangkutan, **yang disebut sebagai Signature-based IDS**.

**Cara Kerja Kedua IDS** dengan mendeteksi adanya anomaly, **yang disebut sebagai Anomaly-based IDS** melibatkan pola lalu lintas yang mungkin sebuah serangan dapat dilakukan oleh penyerang menggunakan teknik statistik untuk membandingkan lalu lintas yang sedang dianalisis dengan lalu lintas normal yang biasa terjadi.

**Cara Kerja Ketiga** dengan memantau berkas-berkas sistem operasi dengan cara melihat apakah ada percobaan untuk mengubah berkas sistem operasi seperti berkas log.

**REFERENCES :**

Whitman, M.E., Mattoro, H.J. (2013). Principles of Incident Response and Disaster Recovery.

1. Jelaskan apa isi dari dokumen incident response plan dan bagaimana cara menulis dokumen incident response plan ini.

**Answer:**

**Isi Dokumen Incident Response Plan (IRP)** adalah kemungkinan penyusupan yang terjadi baik di dalam maupun di luar sistem organisasi, dan kemungkinan kerusakan luas pada data, sistem, dan jaringan sehingga dapar mengambil tindakan tepat waktu.

**Cara Menulis Dokumen IRP:**

1. **Preparation**

* Selama tahap preparation, dokumentasikan, uraikan, dan jelaskan peran dan tanggung jawab tim di perusahaan, termasuk menetapkan kebijakan keamanan dasar sebagai panduan dasar di perusahaan.

1. **Identification**

* Mengidentifikasi jika sistem telah disusupi dan lakukan analisa seperti siapa yang menemukan pertama kali ada penyusupan serta dokumentasi semua hal tersebut.

1. **Containment**

* Mempertimbangkan apa yang dapat dilakukan untuk mengatasi dampak penyusupan seperti “Bagaimana strategi jangka panjang untuk menghadapi dampak serangan tersebut?”.

1. **Eradication**

* Melakukan patching vulnerabilities di dalam sistem, menghapus malicious software, update versi software yang sudah lama, dan lain sebagainya dan pastikan bahwa ini dilakukan tanpa kehilangan data berharga dalam prosesnya.

1. **Recovery**

* Membuat sistem kembali online setelah serangan atau insiden dengan menguji, memantau, dan memverifikasi sistem yang terpengaruh.

1. **Lessons Learned**

* Mendiskusikan jika sesuatu dapat dilakukan secara berbeda dan belajar dari serangan itu untuk memastikan bahwa itu tidak terjadi lagi dan jika itu terjadi, situasinya akan ditangani dengan lebih baik.

**REFERENCES :**

Whitman, M.E., Mattoro, H.J. (2013). Principles of Incident Response and Disaster Recovery.

1. Di kelas dijelaskan mengenai RTO (Recovery Time Objective) dan RPO (Recovery Point Objective), apa kegunaan dari dua parameter ini.

**Answer:**

**Recovery Time Objective (RTO)** adalah periode waktu yang dibutuhkan untuk memulihkan aplikasi, fungsi, dan sistem organisasi setelah terjadi insiden atau singkatnya downtime maksimum yang diizinkan.

**Recovery Point Objective (RPO)** adalah menunjukkan jumlah dan seberapa sering data yang dipulihkan setelah insiden atau singkatnya jumlah dan frekuensi Data Loss maksimum yang diizinkan.

**REFERENCES :**

Whitman, M.E., Mattoro, H.J. (2013). Principles of Incident Response and Disaster Recovery.

1. Peralatan hardware dan software apa saja yang selalu perlu dibawa oleh seseorang yang ditugaskan untuk menangani incident?

**Answer:**

• POC (Point of Contact) List

• Incident Response Systems

• Information Gathering Systems

• Mail / Web /dB Servers

• Monitoring system

• Remote Access

• Printer & FAX

• Shredder

• Whiteboard & Projector

• Notebook Computers

• Security Policy

• Security Plan

• Incident Response Policy

• Incident Response Plan

**REFERENCES :**

Whitman, M.E., Mattoro, H.J. (2013). Principles of Incident Response and Disaster Recovery.

1. Setelah menangani masalah atau incident yang terjadi, apa langkah selanjutnya yang harus dilakukan, terangkan dengan detail.

**Answer:**

1. **Identification from Past Incident**

🡪 Mengidentifikasi jika sistem telah disusupi dan lakukan analisa seperti siapa yang menemukan pertama kali ada penyusupan serta dokumentasi semua hal tersebut.

1. **Containment from Past Incident**

🡪 Mempertimbangkan apa yang dapat dilakukan untuk mengatasi dampak penyusupan seperti “Bagaimana strategi jangka panjang untuk menghadapi dampak serangan tersebut?”.

1. **Eradication from Past Incident**

🡪 Melakukan patching vulnerabilities di dalam sistem, menghapus malicious software, update versi software yang sudah lama, dan lain sebagainya dan pastikan bahwa ini dilakukan tanpa kehilangan data berharga dalam prosesnya.

1. **Recovery Plan from Past Incident Occured**

🡪 Membuat sistem kembali online setelah serangan atau insiden dengan menguji, memantau, dan memverifikasi sistem yang terpengaruh.

1. **Lessons Learned from Past Incident**

* Mendiskusikan jika sesuatu dapat dilakukan secara berbeda dan belajar dari serangan itu untuk memastikan bahwa itu tidak terjadi lagi dan jika itu terjadi, situasinya akan ditangani dengan lebih baik.

**REFERENCES :**

Whitman, M.E., Mattoro, H.J. (2013). Principles of Incident Response and Disaster Recovery.