NAMA: WA ODE BALQIS SELVIA

NIM : 22650170

CYBER CRIME & CYBER LAW

A. Hacking

Hacking adalah tindakan tidak sah untuk menyusup atau mengambil alih sistem atau jaringan komputer untuk tujuan tertentu, seperti pencurian data, kerusakan sistem, atau keuntungan finansial.

Jenis-jenis:

- **White Hat Hacking**: Hacker "baik" yang bekerja untuk mengamankan sistem, sering disebut sebagai "ethical hacking."
- **Black Hat Hacking**: Hacker "jahat" yang bertujuan untuk merusak, mencuri data, atau memperoleh keuntungan.
- **Grey Hat Hacking**: Hacker yang kadang-kadang melanggar hukum, tapi tidak dengan maksud jahat, seperti mengekspos kelemahan keamanan sistem.

Contoh Kasus:

- Peretasan Sony Pictures (2014): Kelompok peretas bernama *Guardians of Peace* membobol sistem Sony Pictures, mencuri data karyawan, email internal, dan bahkan film yang belum dirilis. Mereka merilis data tersebut ke publik, yang menyebabkan kerugian besar bagi perusahaan..

B. Phishing

Phishing adalah upaya penipuan untuk mencuri informasi sensitif, seperti username, password, dan informasi kartu kredit, dengan cara menyamar sebagai entitas terpercaya.

Jenis-jenis:

- **Email Phishing**: Mengirim email yang tampak resmi untuk mencuri data.
- **Spear Phishing**: Target lebih spesifik dan menyesuaikan pesan untuk individu atau perusahaan tertentu.
- **Whaling**: Mengincar target berprofil tinggi, seperti CEO atau direktur perusahaan.
- **Pharming**: Menyalahgunakan URL untuk mengarahkan pengguna ke situs palsu.

Contoh Kasus:

- Kasus Penipuan dengan Email Palsu dari "Amazon": Korban menerima email palsu yang mengklaim ada masalah dengan pesanan mereka. Email ini mengarahkan mereka ke situs palsu yang menyerupai halaman login Amazon, di mana informasi login mereka dicuri

C. Malware

Malware (malicious software) adalah perangkat lunak berbahaya yang dirancang untuk merusak atau mendapatkan akses ke sistem komputer.

Jenis-jenis:

- **Virus**: Menyebar dengan menginfeksi file lain dan menyebar di komputer atau jaringan.
- **Worm**: Menyebar sendiri tanpa bantuan, biasanya melalui jaringan.

- **Trojan Horse**: Tampak seperti perangkat lunak yang sah tapi sebenarnya berbahaya.
- **Spyware**: Memata-matai aktivitas pengguna dan mencuri informasi pribadi.
- **Adware**: Menampilkan iklan tanpa izin pengguna.

Contoh Kasus:

- Serangan Malware Flashback pada Mac (2012): Malware Flashback menginfeksi lebih dari 600.000 perangkat Mac melalui kerentanan Java. Malware ini mencuri informasi pribadi pengguna dan memperlambat sistem.

D. **Ransomware**

Ransomware adalah jenis malware yang mengenkripsi data atau mengunci perangkat dan meminta uang tebusan agar korban dapat mengakses kembali data atau perangkat mereka.

Jenis-jenis:

- **Crypto Ransomware**: Mengenkripsi file dan meminta uang tebusan.
- **Locker Ransomware**: Mengunci akses ke perangkat, tapi tidak mengenkripsi file.
- **Scareware**: Mengancam pengguna untuk membayar tebusan dengan memunculkan peringatan palsu.

Contoh Kasus:

- Serangan Ransomware Maersk (2017): Perusahaan logistik raksasa, Maersk, menjadi korban ransomware *NotPetya*. Seluruh sistem mereka terganggu, menyebabkan kerugian operasional hingga $300 juta. Mereka harus membangun kembali seluruh infrastruktur IT mereka.