MAKALAH

CYBER CRIME DAN CYBER LAW

Disusun oleh :

MUHAMMAD ASFAR DANI

22650168

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS DAYANU IKHSANUDDIN

PASARWAJO

2024

A. Hacking

Hacking adalah aktivitas menyusup atau mengambil alih sistem komputer untuk tujuan seperti mencuri data atau merusak sistem. Contohnya adalah peretasan Equifax tahun 2017 yang mengekspos data 147 juta orang.

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.

B. Phishing

Phishing adalah penipuan untuk mencuri informasi sensitif dengan menyamar sebagai pihak terpercaya, seperti melalui email palsu. Contohnya adalah kasus phishing Twitter 2020 yang melibatkan akun terkenal.

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.

C. Malware

Malware adalah perangkat lunak berbahaya seperti virus atau trojan yang dirancang untuk merusak atau mencuri data. Serangan WannaCry 2017 adalah salah satu contoh yang melumpuhkan banyak sistem di dunia.

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.

D. Ransomware

Ransomware mengunci atau mengenkripsi data dan meminta tebusan untuk membukanya kembali. Contoh serangan adalah insiden Colonial Pipeline 2021 yang mengganggu distribusi bahan bakar di AS.

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.