NAMA **: FIKA ARIANTI**

NIM **: 22650185**

TUGAS MATA KULIAH **: CYBERCRIME & CYBERLAW**

1. HACKING

Kata “hacking” seringkali diidentikkan dengan aktivitas ilegal dan merusak, namun sebenarnya hacking memiliki istilah yang jauh lebih luas dan juga memiliki konsep yang lebih mendalam. Hacking atau peretasan adalah aktivitas percobaan mengeksploitasi kelemahan dalam suatu sistem atau jaringan komputer untuk mendapatkan akses tanpa izin, seringkali tujuannya adalah mengubah atau mencuri *resource* yang seharusnya tidak dapat diakses. Aktivitas ini biasanya dilakukan oleh penjahat siber yang dikenal sebagai hacker.

JENIS - JENIS :

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

CONTOH KASUS :

- Peretasan Situs BPJS Kesehatan : Pada Mei 2021, situs BPJS Kesehatan diretas oleh hacker yang mengakibatkan kebocoran data 279 juta penduduk di Indonesia yang dijual di Raid Forums dengan seharga 0,15 bitcoin (Rp84,4 juta).

2. PHISING

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

JENIS – JENIS :

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

CONTOH KASUS :

- Kasus phishing Twitter (2020): Beberapa akun Twitter terkenal diretas, termasuk Elon Musk dan Joe Biden, untuk menjalankan skema penipuan Bitcoin.

3. MALWARE

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

JENIS – JENIS :

1. Virus: Menyebar dengan menginfeksi file lain dan menyebar di komputer atau jaringan.
2. Worm: Menyebar sendiri tanpa bantuan, biasanya melalui jaringan.
3. Trojan Horse: Tampak seperti perangkat lunak yang sah tapi sebenarnya berbahaya.
4. Spyware: Memata-matai aktivitas pengguna dan mencuri informasi pribadi.
5. Adware: Menampilkan iklan tanpa izin pengguna.

CONTOH KASUS :

- Malware WannaCry (2017): Menyebar secara global dan memengaruhi rumah sakit, bisnis, dan pemerintah, mengunci data pengguna hingga membayar tebusan.

4. 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 :

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

CONTOH KASUS :

- Serangan ransomware Colonial Pipeline (2021): Menyebabkan kekacauan dalam pasokan bahan bakar di AS setelah jaringan perusahaan minyak ini terkena serangan ransomware oleh grup DarkSide.