**NAMA : TIARA**

**NIM : 2265016**

1. **Hacking**

Hacking adalah proses untuk mengakses sistem komputer atau jaringan tanpa izin, yang sering dilakukan dengan tujuan merusak, mencuri data, atau mendapatkan keuntungan tertentu. Hacker dapat memiliki berbagai motif, termasuk untuk kejahatan atau untuk tujuan yang lebih positif seperti penelitian keamanan (white hat).

## Jenis – jenis Hacking:

* White Hat Hacking (Ethical Hacking): Hacker yang bekerja untuk membantu organisasi dengan menemukan dan memperbaiki kerentanannya. Mereka sering dipekerjakan oleh perusahaan untuk melakukan pengujian penetrasi atau audit keamanan.
* Black Hat Hacking: Hacker yang melakukan serangan dengan niat jahat, seperti mencuri data, merusak sistem, atau mendapatkan akses tanpa izin untuk keuntungan pribadi.
* Gray Hat Hacking: Hacker yang beroperasi di antara white hat dan black hat. Mereka mungkin mengeksploitasi kerentanannya tanpa izin, tetapi tidak memiliki niat jahat. Meskipun begitu, tindakan mereka tetap ilegal.

## Contoh Kasus Hacking:

* Kasus Sony Pictures (2014): Sebuah kelompok hacker yang dikenal sebagai 'Guardians of Peace' berhasil membobol sistem Sony Pictures dan mencuri sejumlah besar data perusahaan, termasuk email pribadi karyawan dan film yang belum dirilis. Serangan ini diperkirakan dilakukan oleh aktor negara yang terkait dengan Korea Utara sebagai balasan terhadap film 'The Interview'.

1. **Phishing**

Phishing adalah teknik penipuan di mana penyerang menyamar sebagai entitas terpercaya (seperti bank, layanan online, atau organisasi terkenal) untuk mendapatkan informasi sensitif seperti password, data pribadi, atau informasi kartu kredit dari korban.

## Jenis – jenis Phishing:

* Email Phishing: Penyerang mengirimkan email palsu yang terlihat seolah-olah berasal dari sumber yang tepercaya, meminta korban untuk mengklik link atau melampirkan file berbahaya.
* Spear Phishing: Phishing yang lebih terarah, di mana penyerang menargetkan individu atau organisasi tertentu dengan informasi yang dipersonalisasi untuk membuat serangan terlihat lebih sah.
* Whaling: Bentuk phishing yang menargetkan eksekutif atau orang penting dalam organisasi dengan pesan yang lebih bernuansa dan meyakinkan.

## Contoh Kasus Phishing:

* Kasus Phishing PayPal (2019): Penyerang mengirim email yang menyamar sebagai pemberitahuan dari PayPal, mengklaim bahwa akun korban dibatasi dan meminta mereka untuk mengklik tautan untuk 'memverifikasi' informasi akun mereka. Email tersebut mengarahkan korban ke situs web palsu yang meminta informasi login, yang kemudian digunakan untuk mencuri dana dari akun korban.

1. **Malware**

Malware (malicious software) adalah perangkat lunak yang dirancang untuk merusak, mengakses, atau mengendalikan sistem komputer tanpa izin. Malware dapat menyebabkan kerusakan besar pada perangkat atau mencuri informasi pribadi.

## Jenis – jenis Malware:

* Virus: Program berbahaya yang menyebar dan menginfeksi file atau program lain, biasanya menyebabkan kerusakan pada file atau sistem.
* Worm: Malware yang dapat menyalin dirinya sendiri ke komputer lain melalui jaringan tanpa interaksi manusia.
* Trojan Horse: Malware yang menyamar sebagai perangkat lunak yang sah atau bermanfaat, tetapi menyembunyikan fungsi berbahaya di dalamnya
* Spyware: Malware yang dirancang untuk memantau aktivitas pengguna dan mengumpulkan informasi pribadi tanpa izin.
* Adware: Program yang menyebabkan iklan tidak diinginkan muncul di komputer pengguna.

## Contoh Kasus Malware:

* Kasus Stuxnet (2010): Malware yang sangat canggih ini ditemukan menyerang fasilitas nuklir Iran. Stuxnet didesain untuk merusak mesin – mesin industri dengan merusak pengaturan kontrol sistem yang digunakan untuk operasi sentrifugal. Serangan ini diperkirakan adalah hasil dari upaya negara tertentu yang ingin merusak program nuklir Iran.

1. **Ransomware**

Ransomware adalah jenis malware yang mengenkripsi data di komputer atau jaringan dan meminta pembayaran tebusan (ransom) untuk mengembalikan akses ke data tersebut.

## Jenis – jenis Ransomware:

* Encrypting Ransomware: Jenis ransomware yang mengenkripsi file atau seluruh sistem pengguna, membuat data tidak dapat diakses tanpa kunci enkripsi yang hanya diberikan setelah pembayaran dilakukan.
* Locker Ransomware: Ransomware yang mengunci sistem komputer korban, mencegah akses ke desktop atau perangkat, dan hanya membuka akses setelah pembayaran tebusan dilakukan.
* Scareware: Malware yang memberikan peringatan palsu tentang masalah atau ancaman pada perangkat, yang kemudian meminta korban untuk membayar untuk perbaikan atau untuk menghindari konsekuensi lebih lanjut.

## Contoh Kasus Ransomware:

* Kasus WannaCry (2017): Serangan ransomware ini menginfeksi lebih dari 200.000 komputer di 150 negara, terutama di rumah sakit, perusahaan, dan infrastruktur pemerintah. WannaCry mengenkripsi file di komputer yang terinfeksi dan menuntut pembayaran tebusan dalam Bitcoin untuk mendekripsi data tersebut. Banyak organisasi terpaksa menghentikan operasi mereka karena serangan ini.
* Kasus NotPetya (2017): Sebuah ransomware yang menargetkan komputer di Ukraina, tetapi kemudian menyebar ke seluruh dunia. Meskipun menyerupai serangan ransomware, tujuan utama NotPetya adalah merusak dan menghancurkan data, bukan mendapatkan pembayaran. Serangan ini berdampak besar pada perusahaan multinasional dan infrastruktur penting.