Nama : Muhammad Zulfikran
NIM : 22650174

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 situs BPJS Kesehatan**
  Pada Mei 2021, situs BPJS Kesehatan diretas dan menyebabkan kebocoran data 279 juta penduduk Indonesia. Data tersebut dijual di Raid Forums dengan harga 0,15 bitcoin atau sekitar Rp84,4 juta.

- **Pembobolan internet banking BCA**
  Pada tahun 2001, internet banking BCA dibobol oleh Steven Haryanto, seorang mantan mahasiswa ITB Bandung dan karyawan media online.

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 phising pada nasabah bank di Indonesia pada Mei 2021. Pelaku menelepon dan menyamar sebagai karyawan bank, kemudian mengirimkan pesan berisi tautan dengan dalih pembaruan biaya. Korban mengeklik tautan tersebut dan menjawab pertanyaan tentang data sensitif akun m-banking.
- Kasus phising pada penyedia layanan kesehatan AS Elara Caring pada tahun 2020. Penyerang memperoleh akses ke akun email karyawan dan mengkompromikan informasi pribadi lebih dari 100.000 pasien lanjut usia.

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:

- **Microsoft Exchange Server**
  Pada awal 2021, Microsoft mendeteksi serangan pada Microsoft Exchange Server yang dilakukan oleh kelompok Hafnium. Serangan ini berhasil mengakses akun email dan memasang malware untuk mendapatkan akses jangka panjang.

- **News Malware**
  Peretas dapat menyisipkan malware ke dalam berita populer untuk mencuri data pengguna.

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:

1. **REvil atau Sodinokibi (2019-2021)**

- REvil adalah ransomware yang dioperasikan oleh kelompok kejahatan siber REvil, yang menyerang berbagai perusahaan besar dan menuntut tebusan besar. Pada tahun 2021, serangan REvil menargetkan Kaseya, sebuah perusahaan perangkat lunak manajemen TI.
- Dengan menggunakan kelemahan di perangkat lunak Kaseya, ransomware ini berhasil menyebar ke ratusan perusahaan klien Kaseya di seluruh dunia. Serangan ini menyebabkan gangguan besar dan menuntut tebusan hingga 70 juta dolar dalam bentuk Bitcoin.

2. **Conti (2020-2022)**

- Ransomware Conti menyerang berbagai organisasi besar, terutama di sektor layanan kesehatan dan layanan publik. Conti terkenal karena kecepatannya dalam mengenkripsi data di jaringan yang terinfeksi.
- Pada 2022, kebocoran internal dari kelompok Conti menunjukkan bahwa kelompok tersebut memiliki struktur organisasi yang mirip dengan perusahaan, dengan pembagian tugas yang jelas antara pengembang, perekrut, dan manajemen.