- **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:

- Penetration Testing pada Sistem Keamanan Bank, Seorang white hat hacker bekerja sebagai konsultan keamanan untuk bank besar. Mereka diberi izin untuk mencoba mengeksploitasi kelemahan dalam sistem keamanan bank tersebut, dengan tujuan menemukan dan mengatasi potensi celah sebelum dimanfaatkan oleh pihak yang berniat jahat.

C. 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:

Serangan Phishing Terhadap CEO (2016)

- Serangan Phishing Terhadap CEO (2016) Dalam salah satu kasus spear phishing terkenal, penyerang berhasil menipu CEO sebuah perusahaan besar dengan mengirim email yang tampaknya berasal dari seorang eksekutif senior di perusahaan itu. Email tersebut meminta pengalihan dana besar untuk transaksi bisnis yang mendesak. Karena email terlihat sah, CEO tersebut akhirnya mengirimkan sejumlah uang besar ke rekening penjahat.

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:

- **Adware "Gator" (1999)** Gator, juga dikenal sebagai Claria, adalah adware yang menyisipkan iklan pop-up pada komputer pengguna dan mengumpulkan data perilaku pengguna untuk menampilkan iklan yang lebih ditargetkan. Meskipun program ini awalnya ditawarkan sebagai aplikasi gratis, ia membawa risiko besar bagi privasi pengguna karena mengumpulkan data pribadi dan perilaku browsing tanpa izin yang jelas.

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:

Penetration Testing pada Sistem Keamanan Bank

- Penetration Testing pada Sistem Keamanan Bank, Seorang white hat hacker bekerja sebagai konsultan keamanan untuk bank besar. Mereka

diberi izin untuk mencoba mengeksploitasi kelemahan dalam sistem keamanan bank tersebut, dengan tujuan menemukan dan mengatasi potensi celah sebelum dimanfaatkan oleh pihak yang berniat jahat.