# MODUL 6

# ANCAMAN PERANGKAT LUNAK BERBAHAYA

## 6.1 Tujuan Praktikum

1. Mengetahui dan memahami pengertian dari perangkat lunak berbahaya.
2. Mengetahui dan memahami macam-macam perangkat lunak berbahaya.
3. Mengetahui dan memahami Teknik pembuatan perangkat lunak berbahaya.
4. Mengetahui dan memahami solusi dari ancaman perangkat lunak berbahaya.

## 6.2 Alat dan Bahan

1. Laptop
2. Mouse
3. VirtualBox
4. OS Windows XP

## 6.3 Dasar Teori

### 6.3.1 Pengertian Perangkat Lunak Berbahaya

Perangkat lunak berbahaya (*malicious software* atau *malware*) adalah jenis perangkat lunak yang dirancang untuk melakukan tindakan merusak, merugikan, atau tidak sah pada sistem komputer, perangkat mobile, atau jaringan komputer. Perangkat lunak berbahaya merupakan ancaman serius dalam dunia digital dan dapat menyebabkan kerugian finansial, hilangnya data berharga, dan masalah privasi. *Malware* dapat masuk pada sistem komputer dengan melalui jaringan internet. Umumnya, perangkat lunak ini disisipkan pada unduhan pada situs web illegal, iklan, *Email Phising*, dan lain-lain. *Malware* tidak diciptakan oleh sembarang orang. Prangkat lunak ini diciptakan oleh para *hacker* yang memiliki pemahaman tinggi akan perangkat lunak dengan tujuan tertentu.

### 6.3.2 Karakteristik Umum dari Perangkat Lunak Berbahaya

1. Merusak atau merugikan

   *Malware* seringkali dirancang untuk merusak atau merugikan sitem atau data pengguna. Ini bisa termasuk menghapus, mengubah, atau

mengenkripsi file, mengganggu kinerja sistem, atau bahkan menghancurkan sistem operasi.

2. Pencurian Informasi

   Beberapa jenis *malware*, seperti *spyware* atau *keyloggers*, digunakan untuk mencuri informasi rahasia seperti kata sandi, nomor kartu kredit, atau data pribadi lainnya.

3. Pengendalian Jarak Jauh

   *Malware* dapat memberikan penyerang akses jarak jauh ke komputer atau perangkat yang terinfeksi. Ini memungkinkan penyerang untuk mengendalikan perangkat dan menggunakannya untuk tujuan jahat.

4. Penyebaran dan Infeksi

   Beberapa jenis *malware*, seperti *virus* atau *worm*, dapat menyebar dari satu sistem ke sistem lainnya melalui jaringan atau perangkat penyimpanan. Mereka dapat menginfeksi banyak komputer dalam waktu singkat.

5. Ekstorsi (*Ransomware*)

   *Ransomeware* adalah jenis *malware* yang meng-enskripsi data pengguna dan kemudia meminta pembayaran tebusan (*ransom*) agar data di-dekripsi. Jika tebusan tidak dibayar, data tersebut dapat hilang selamanya.

6. Penyusupan dan Penyamaran

   Beberapa *malware* mencoba untuk menyusup ke dalam sistem tanpa diketahui dan menyamar sebagai perangkat lunak yang sah atau tidak berbahaya agar tidak terdeteksi.

7. Penyebaran Lewat *Phising*

   *Malware* juga seringkali tersebar melalui pesan *phising* yang menipu pengguna agar mengundug atau menjalankan perangkat lunak berbahaya tersebut.

8. Eksploitasi Kerentanan

   *Malware* dapat memanfaatkan kerentanan keamanan dalam sistem atau perangkat untuk melakukan serangan. Ini adalah alasan mengapa selalu penting untuk memperbarui perangkat lunak dan sistem Anda.

### 6.3.3 Macam-Macam Perangkat Lunak Berbahaya

1. *Malware (Malicious Software)*

   *Malware (Malicious Software)* merupakan software yang dibuat oleh seseorang dengan tujuan untuk merugikan seorang pengguna. Dampak dari adanya *malware* disebuah perangkat memungkinkan *malware* tersebut untuk melakukan pencurian informasi dan menghabiskan sumber daya pada perangkat tersebut.

2. *Virus*

   *Virus* merupakan sebuah *software* yang dapat melakukan penggandaan dan menyebarkan dirinya kedalam sebuah program, dokumen dan lain-lain. Dampak dari virus yaitu merusak data pada dokumen, mengganggu, dan juga terdapat virus yang hanya berdiam diri tanpa melakukan aktifitas yang merugikan dan tidak melakukan apa-apa.

3. *Trojan*

   *Trojan* merupakan jenis *malware* yang sering digunakan pada sebuah perangkat lunak. Hal tersebut bertujuan untuk pencuria dan peretasan untuk mendapat akses ke perangkat tersebut. Dampak dari trojan memungkinkan perangkat seorang dapat diambil oleh seorang *hacker.*

4. *Spyware*

   *Spyware* merupakan jenis *malware* yang ter-*install* pada sebuah perangkat tanpa diketahui oleh pengguna. Dampak dari *spyware* adalah mencuri informasi sensitive dari pengguna perangkat dengan merode mengintai.

5. *Worm*

   *Worm* merupakan sejenis virus yang dapat mereplikasi dirinya sendiri dan membagikan dirinya dengan media jaringan. Dampak dari *worm* adalah dapat digunakan untuk mencuri informasi sensitive, meng-*install backdoor,* dan masih banyak lagi Tindakan perusakan lainnya.

### 6.3.4 Dampak Serangan Perangkat Lunak Berbahaya

Masuknya *malware* pada komputer merupakan sebuah ancaman besar. Melalui berbagai cara dan serta jenisnya yang beragam, *malware* mampu menimbulkan masalah pada perangkat. Beriku merupakan dampak dari serangan *malware* pada perangkat:

1. Memperlambat Sistem Komputer

   Apabila *malware* berhasil masuk pada sistem perangkat, kinerja perangkat akan melambat. Dibutuhkan waktu lama untuk menyala serta dalam penggunaannya pun seluruh sistem menjadi sulit merespon. Hal ini tentu saja membuat pengguna kesulitan untuk menjalankan aktivitas pada komputer.

2. Kerusakan Data dan Dokumen

   Akibat lain dari adanya virus yang menyebar pada perangkat ialah kerusakan pada data serta dokumen. Pada beberapa kasus, kerusakan membuat isi dokumen menjadi berantakan. Namun, *malware* juga dapat menyebabkan sebuah dokumen tidak dapat dibuka.

3. Kendala Pada Aplikasi di Dalamnya

   *Malware* yang masuk pada sistem komputer seringkali memengaruhi beberapa aplikasi di dalamnya. Aplikasi dalam komputer menjadi sulit untuk dibuka, performa lambat, dan bahkan tidak dapat dibuka dama sekali. Bahkan, *malware* dapat menghapus aplikasi di komputer.

4. Sistem Tidak Dapat Dibuka

   Dampak serius yang harus diperhatikan yaitu hilangnya akses pada komputer. Perangkat dapat dihidupkan, tetapi tidak dapat digunakan dan dijalankan. Ini merupakan salah saru bentuk serangan *ransomware*.

5. Perubahan Data Menjadi Virus

   *Malware* dapat mengubah sebuah data menjadi virus. Hal ini merupakan salah satu cara penyebaran virus pada perangkat. Tidak hanya pada satu data, apabila virus dibiarkan maka akan menyerang seluruh data pada komputer.

### 6.3.5 Solusi Agar Terhindari Ancaman Perangkat Lunak Berbahaya

Untuk terhindar dari perangkat lunak berbahaya (*malware*) dan menjaga keamanan perangkat, berikut adalah beberapa solusi yang dapat diterapkan:

1. Perangkat Lunak Keamanan

   Pasang perangkat lunak keamanan yang andal dan *up-to-date* pada perangkat, seperti *antivirus, antispyware,* dan *firewall*. Pastikan perangkat lunak ini selalu diperbaharui agar dapat mendeteksi dan mengatasi ancaman terbaru.

2. Pembaruan rutin

   Selalu perbarui sistem operasi, perangkat lunak, dan aplikasi Anda ke versi yang paling baru. Pembaruan seringkali memperbaiki kerentanan keamanan yang dapat dieksploitasi oleh *malware*.

3. Unduh dari sumber resmi

   Hindari mengunduh perangkat lunak dari sumber yang tidak resmi atau tidak terpercaya. Gunakan toko aplikasi resmi seperti Google Play atau Apple App Store untuk perangkat *mobile* dan situs web resmi untuk perangkat desktop.

4. Jangan klik pada tautan atau lampiran yang mencurigakan

   Jangan meng-klik tautan atau membuka lampiran dalam email, pesan teks, atau pesan media sosial yang mencurigakan atau berasal dari sumber yang tidak dikenal. Ini dapat menghindari serangan *phising* dan pengiriman *malware* melalui email.

5. Bijak dalam ber-internet

   Jangan mengunjungi situs web yang mencurigakan atau tidak aman. Hindari mengunduh materi illegal atau berbahaya, seperti konten bajakan atau *crack*.

6. Gunakan kata sandi kuat

   Gunakan kata sandi yang kuat untuk akun *online* Anda, dan jangan gunakan kata sandi yang sama untuk banyak situs web atau layanan.

Pertimbangkan menggunakan manajer kata sandi untuk mengelola kata sandi Anda.

7. Jangan aktifkan makro otomatis

   Jika Anda menggunakan program seperti Microsoft Office, jangan aktifkan makro otomatis dalam dokumen yang Anda unduh dari internet. *Malware* sering menggunakan makro untuk mengeksekusi skrip berbahaya.

8. Edukasi diri

   Tingkatkan kesadaran diri Anda tentang ancaman yang ada dan tanda-tanda serangan *malware.* Pelajari cara mengidentifikasi email *phising* atau situs web palsu.

9. Backup data secara rutin

   Buat salinan cadangan data penting Anda secara teratur. Ini dapat membantu Anda memulihkan data jika Anda menjadi korban serangan *ransomware* atau kehilangan data karena *malware* lainnya.

10. Monitoring aktivitas sistem

    Selalu perhatikan aktivitas dan kinerja sistem Anda. Jika Anda melihat tanda-tanda yang mencurigakan, seperti penggunaan CPU yang tinggi atau aktivitas jaringan yang tidak biasa, segera selidiki masalah tersebut.