MODUL PERKULIAHAN:
KEAMANAN SIBER

Penyusun 1	Penyusun 2	Penyusun 3
Denpasar, <*Arial, 9pt>	Denpasar, <*Arial, 9pt>	Denpasar,
(Nama Dosen dan gelar) <*Arial, 9pt>	(Nama Dosen dan gelar) <*Arial, 9pt>	Nama Dosen dan gelar) <*Arial, 9pt>

INFORMASI MATA KULIAH

Jumlah SKS	**4**
Jenis Matakuliah	Teori
Kegiatan Pembelajaran	Daring
Persyaratan Sarana Peserta/Spesifikasi/ Tools/Media ajar yang akan digunakan	

CAPAIAN DAN DESKRIPSI MK

Capaian Pembelajaran Mata Kuliah (CPMK)	Deskripsi Singkat MK
• CPMK-06-17: Mampu menjelaskan dan menguasai teknik pengamanan sistem dan jaringan komputer untuk mengidentifikasi dan mencegah serangan cyber dengan mengimplementasikan aspek-aspek keamanan informasi. • CPMK-07-4: Mampu menjelaskan dan menguasai konsep dasar teori jaringan mahasiswa mampu memahami konsep jaringan komputer, mengetahui perangkat-perangkat jaringan, protokol jaringan, OSI dan TCP/IP model, konsep IP Address dan kelas-kelas dalam IP Address, Routing dengan media virtual seperti menggunakan packet tracer, memahami jaringan nirkabel, mengetahui serangan dalam jaringan dan mengetahui firewall.	Keamanan siber adalah matakuliah yang mempelajari tentang konsep dan teknik untuk pengamanan aplikasi, sistem dan jaringan komputer serta data digital dari kejahatan cyber yang dapat menggangu proses bisnis dan mengakibatkan kerugian.

REFERENSI

Referensi
[1] Sadikin, R. (2012). Kriptografi Untuk Keamanan Jaringan dan Implementasinya dalam bahasa java. Yogyakarta: Andi [2] Weidman, G. (2014). Penetration Testing A Hands-On Introduction to Hacking. [3] Situmeang, M.S (2020). Cyber Law, Bandung: Cakra 2020

BAB 1 Pengantar Malware

A.1 Definisi Malware

Malware, atau *malicious software*, adalah perangkat lunak berbahaya yang dirancang untuk menyusup, merusak, atau mencuri data tanpa sepengetahuan atau izin pengguna. Malware bisa mengambil berbagai bentuk, termasuk virus, worm, trojan, ransomware, spyware, dan adware, masing-masing dengan cara kerjanya yang unik. Secara umum, tujuan malware meliputi:

1. **Kerusakan Sistem**
   Menghapus, mengubah, atau mengganggu kinerja perangkat.
2. **Pencurian Data**
   Mengambil informasi pribadi seperti kata sandi, data keuangan, atau informasi sensitif.
3. **Pengambilalihan Kontrol**
   Mengakses atau mengontrol perangkat pengguna untuk tujuan seperti spamming, mining cryptocurrency, atau menjalankan botnet.

Malware menyebar melalui berbagai metode, seperti lampiran email, unduhan dari situs berbahaya, aplikasi pihak ketiga, atau kerentanan dalam sistem operasi. Deteksi dan analisis malware adalah bagian penting dari keamanan siber untuk melindungi perangkat dan jaringan dari serangan lebih lanjut.

A.1.1 Jenis-Jenis Malware

- **Virus**
  Malware yang menempel pada file atau program, dan hanya aktif ketika file tersebut dijalankan. Virus bisa menyebar ke perangkat lain dan sering menyebabkan kerusakan atau penghapusan data.
- **Worm**
  Malware yang menyebar sendiri melalui jaringan tanpa memerlukan file host. Worm dapat memperbanyak dirinya dan mengonsumsi banyak sumber daya jaringan, menyebabkan perlambatan atau bahkan crash.
- **Trojan Horse (Trojan)**
  Malware yang menyamar sebagai perangkat lunak yang sah untuk mengelabui pengguna agar menginstalnya. Setelah diaktifkan, Trojan dapat mencuri data, menghapus file, atau membuka akses bagi malware lainnya.
- **Ransomware**
  Jenis malware yang mengenkripsi data korban dan meminta tebusan untuk memulihkan akses. Ransomware umumnya menyebar melalui lampiran email yang berbahaya atau unduhan dari situs tidak terpercaya.
- **Spyware**
  Malware yang memantau aktivitas pengguna tanpa izin untuk mengumpulkan informasi, seperti data login atau aktivitas peramban, yang kemudian dapat dikirim ke pihak ketiga.
- **Adware**
  Malware yang menampilkan iklan yang tidak diinginkan pada perangkat pengguna. Selain mengganggu, adware juga dapat mengarahkan pengguna ke situs web yang berbahaya.
- **Rootkit**

Jenis malware yang dirancang untuk menyembunyikan aktivitas berbahaya dari deteksi. Rootkit memungkinkan penyerang mendapatkan akses sistem tingkat tinggi (root) pada perangkat korban.

- **Backdoor**
  Malware yang menciptakan pintu belakang pada perangkat, memungkinkan penyerang untuk mengakses perangkat korban secara diam-diam dan melakukan serangan lebih lanjut.
- **Keylogger**
  Malware yang merekam setiap ketikan pada perangkat korban. Keylogger sering digunakan untuk mencuri data login, informasi keuangan, dan informasi pribadi lainnya.
- **Botnet**
  Sekumpulan perangkat yang terinfeksi malware, yang dikendalikan oleh penyerang untuk melakukan tindakan tertentu, seperti serangan *Distributed Denial of Service (DDoS)* atau mengirimkan spam dalam skala besar.

A.1.2 Cara Penyebaran Malware

Malware dapat menyebar melalui berbagai metode yang sering kali memanfaatkan kerentanan sistem atau kelalaian pengguna. Berikut adalah beberapa cara umum penyebaran malware:

1. **Lampiran dan Tautan Email**
   Salah satu cara paling umum adalah melalui lampiran atau tautan dalam email yang tampak sah. Pengguna yang membuka lampiran atau mengklik tautan tersebut bisa tanpa sadar mengunduh dan menginstal malware.
2. **Download dari Situs Tidak Terpercaya**
   Pengguna dapat mengunduh malware yang disamarkan sebagai perangkat lunak sah dari situs yang tidak terpercaya atau tidak aman. File unduhan dari situs-situs ini sering kali mengandung malware.

3. **Iklan Berbahaya (Malvertising)**
   Iklan berbahaya di situs web dapat mengarahkan pengguna ke situs yang mengunduh malware ke perangkat mereka tanpa sepengetahuan pengguna. Ini juga dikenal sebagai *drive-by download*.
4. **Perangkat Lunak Bajakan atau Aplikasi Pihak Ketiga**
   Banyak malware disisipkan dalam perangkat lunak bajakan atau aplikasi yang diunduh dari sumber pihak ketiga yang tidak terpercaya. Saat pengguna menginstal perangkat lunak ini, malware ikut terinstal.
5. **Exploit Kits dan Kerentanan Perangkat Lunak**
   Malware dapat menyebar melalui exploit kits yang memanfaatkan kerentanan keamanan dalam sistem operasi atau aplikasi. Begitu perangkat rentan diakses, malware diinstal tanpa interaksi pengguna.
6. **Penggunaan Perangkat Keras yang Terinfeksi**
   Perangkat keras seperti USB flash drive, hard disk eksternal, atau perangkat lainnya yang telah terinfeksi malware dapat menyebarkan infeksi ketika dicolokkan ke perangkat yang aman.

7. **Aplikasi Mobile yang Berbahaya**

Di perangkat seluler, malware dapat menyebar melalui aplikasi yang diunduh dari sumber tidak terpercaya atau toko aplikasi yang tidak resmi. Aplikasi ini dapat mengakses data pribadi atau bahkan menyebarkan malware lebih lanjut.

8. **Media Sosial dan Pesan Instant**
   Tautan atau file yang dibagikan melalui media sosial dan pesan instan sering kali digunakan untuk menyebarkan malware. Pengguna yang mengklik tautan atau membuka file ini bisa saja terinfeksi tanpa sadar.
9. **Jaringan Public (Public Wi-Fi)**
   Penggunaan jaringan Wi-Fi publik yang tidak aman juga dapat menjadi sarana penyebaran malware, di mana peretas bisa menginjeksikan malware ke perangkat yang terhubung ke jaringan tersebut.
10. **Script macro**
    Beberapa malware disebarkan melalui dokumen yang berisi skrip atau makro berbahaya. Dokumen seperti ini dapat muncul dalam format Word atau Excel dan sering kali diunduh melalui email atau situs web tidak terpercaya.

A.1.3 Dampak Malware

1. **Kerugian Finansial**
   Malware seperti ransomware mengenkripsi data penting dan meminta tebusan dari korban. Selain itu, malware juga bisa mencuri informasi keuangan seperti kartu kredit dan data perbankan yang kemudian digunakan untuk penipuan atau transaksi ilegal.
2. **Kehilangan Data**
   Malware yang merusak atau menghapus data penting dapat menyebabkan kehilangan informasi pribadi atau bisnis yang bernilai tinggi. Hal ini dapat berdampak pada produktivitas dan keberlangsungan operasional suatu organisasi.
3. **Kebocoran Data Pribadi dan Privasi**
   Malware seperti spyware dan keylogger bisa mencuri informasi sensitif seperti kredensial login, data pribadi, dan aktivitas peramban. Data ini kemudian bisa dijual di pasar gelap atau digunakan untuk serangan lebih lanjut.
4. **Pengambilalihan dan Kontrol Jarak Jauh**
   Malware seperti backdoor dan rootkit memungkinkan penyerang untuk mengambil alih sistem korban secara jarak jauh. Ini dapat menyebabkan kontrol penuh atas perangkat, memungkinkan serangan lebih lanjut, termasuk penambahan perangkat ke botnet.

BAB 2 Teknik Analisis Malware

A.2 Analisis Statik (Static Analysis)

Analisis statik melibatkan pemeriksaan malware tanpa mengeksekusinya. Teknik ini mencakup dekompilasi, analisis file, dan string dalam file.

A. Analisis File dan Metadata

1. **File Command**
   Perintah ini menampilkan informasi dasar tentang jenis file yang digunakan. Berguna untuk mengetahui apakah file adalah executable atau jenis lainnya. Contoh : `file nama_file_malware`
2. **ExifTool**
   Untuk menampilkan metadata dan informasi lainnya yang mungkin terkandung dalam file.
   Contoh : `exiftool nama_file_malware`

B. Analisis String

Strings: Menampilkan string ASCII atau Unicode yang ada dalam file. Hal ini dapat membantu menemukan petunjuk seperti URL, alamat IP, atau pesan tersembunyi. Contoh : `strings nama_file_malware`

C. Disassembly

Objdump: Menyediakan disassembly dari file biner, memudahkan analisis kode assembly dalam file malware. Contoh : `objdump -d nama_file_malware`

Ghidra atau **Radare2**: Alat disassembler yang lebih mendalam. Kali Linux biasanya tidak menyertakan Ghidra secara bawaan, tetapi Radare2 sudah ada dan sangat berguna untuk analisis lebih lanjut. Contoh: `radare2 -A nama_file_malware`

B. Analisis Dinamis (Dynamic Analysis)

Analisis dinamis melibatkan eksekusi malware di lingkungan terkontrol untuk memantau perilakunya. Karena risiko tinggi, pastikan untuk menggunakan sandbox atau mesin virtual.

1. Sandboxing dengan Cuckoo

Cuckoo Sandbox: Kali Linux mendukung integrasi dengan Cuckoo untuk analisis dinamis. Setelah instalasi dan konfigurasi, Anda dapat menjalankan file dalam sandbox dan memonitor aktivitas malware seperti perubahan file, registri, dan lalu lintas jaringan.

2. Pemantauan Proses dan Sistem

Sysdig: Digunakan untuk memonitor aktivitas sistem selama eksekusi malware. Sysdig dapat merekam semua kejadian dalam sistem, seperti penggunaan file, jaringan, dan proses.

Contoh : `Sysdig`

Strace: Untuk memonitor sistem call yang dilakukan oleh program. Strace memungkinkan melihat bagaimana malware berinteraksi dengan sistem operasi.

Contoh : `strace -o output.txt ./nama_file_malware`

C. Analisis Jaringan

Wireshark: Alat penganalisa jaringan untuk menangkap dan menganalisis lalu lintas jaringan. Ini berguna untuk mengidentifikasi komunikasi jaringan yang dilakukan oleh malware.

Wireshark

Tcpdump: Alternatif ringan untuk Wireshark untuk menganalisis jaringan.

Contoh : `tcpdump -i eth0 -w capture.pcap`

D. Reverse Engineering

Reverse engineering adalah teknik lanjutan untuk menganalisis kode biner malware agar dapat memahami fungsionalitas yang lebih dalam.

Radare2

Radare2 adalah alat reverse engineering open-source yang kuat yang memungkinkan disassembly, debugging, dan modifikasi biner.

Contoh: `radare2 -A nama_file_malware`

Beberapa fitur Radare2:

pd: Perintah untuk mendisassembly beberapa instruksi.

V: Mode visual untuk melihat kode dengan lebih jelas.

afl: Menampilkan daftar fungsi yang ditemukan dalam biner.

b. Ghidra

Ghidra: Ghidra adalah alat reverse engineering yang dikeluarkan oleh NSA. Alat ini tidak termasuk dalam Kali Linux secara default, tetapi dapat diunduh dan diinstal. Ghidra memiliki GUI dan banyak fitur yang membantu dalam proses dekompilasi.

Latihan :

Studi Kasus Analisis Malware Sederhana

Lakukan analisis statik dan dinamis untuk sebuah file malware dengan menggunakanTools-tools dalam Kali Linux seperti strings, Wireshark, Procmon, dan Ghidra.