## Macam-Macam Serangan Pada Komputer & Sejarah Perkembangan Virus

## 

## Ridho Surya

## 1710031802135

## 6B

## Teknik Informatika

## STMIK Amik Riau

## Tahun 2021/2022

## 1.Intrusion

Pada penyerang jenis ini , seseorang penyerang akan bisa menggunakan system computer yang kita  miliki , sebagaian penyerang jenis ini menginginkan akses sebagaimana halnya pengguna yang mempunyai hak untuk mengakses system.

## 2.Intelligence

Intelligence merupakan proses pengumpulan segala infomasi yang berkaitan dengan sistem target. Banyak cara yang dapat ditempuh, antara lain melalui internet, email, buku atau jurnal, chat atau bahkan dari mantan karyawan/i yang pernah bekerja sebagai pengelola sistem. Cara lainnya adalah mengais sampah, makna sampah tersebut konotatif. Yang dimaksud data atau dokumen yang telah dihapus oleh admin. Kegiatan ini yang paling menguras waktu dari seluruh proses hacking. Kemungkinan gagal cukup besar.

## 3.Land Attack

Serangan Land Attack dalah serangan kepada sistem dengan menggunakan program yang bernama “land”. Apabila serangan diarahkan kepada sistem Windows, maka sistem yang tidak diproteksi akan menjadi hang (dan bisa keluar layar biru). Demikian pula apabila serangan diarahkan ke sistem UNIX versi lama, maka sistem akan hang. Jika serangan diarahkan ke sistem Windows NT, maka sistem akan sibuk dengan penggunaan CPU mencapai 100% untuk beberapa saat sehingga sistem terlihat seperti macet. Program land menyerang server yang dituju dengan mengirimkan packet palsu yang seolah-olah berasal dari server yang dituju.Dengan kata lain, source dan destination dari packet dibuat seakan-akan berasal dari server yang dituju. Akibatnya server yang diserang menjadi bingung.

## 4.Logic Bomb

Logic Bomb adalah Program yang dimasukan ke dalam sebuah computer yang bekerja guna memeriksa kumpulan kondisi di system , apabila kondisi – kondisi yang dimaksud ditemukan oleh program tersebut , maka program akan mengeksekusi perintah – perintah yang terdapat di dalamnya .

Logic bomb dapat dibuat untuk melakukan segala macam kerusakan pada sistem yang mereka jalankan, dan dapat mengandalkan satu atau lebih pemicu sebelum mereka berangkat. logic bomb berbasis waktu , juga disebut bom waktu , adalah bentuk umum, di mana tindakan yang dilakukan oleh kode hanya terjadi pada tanggal dan waktu tertentu.

**Berikut adalah beberapa pemicu umum untuk logic bomb:**

1. Ketika Perangkat [USB](https://www.teknoiot.com/usb-type-c-inilah-ulasan-lengkapnya/) dimasukkan atau dilepas.

2. File khusus dibuat, dibuka, diubah, atau dihapus.

3. Perintah tertentu dimasukkan ke dalam komputer.

## 5.Operation System Fingerprinting

Istilah ini mengacu kepada kegiatan menganalisis sistem operasi pada sistem yang akan diserang. Ada beberapa cara yang bisa dilakukan. CAra yang paling umum ialah melakukan telnet ke server. Jika server yang dituju mempunyai fasilitas telnet, biasanya ada banner yang menunjukkan sistem operasi yang dipakai.

Cara lain adalah menggunakan aplikasi netcat. Cara yang lebih canggih adalah dengan menggunakan menganalisis respon sistem terhadap request tertentu. Misalnya analisis nomor urut paket TCP/IP yang dikeluarkan oleh server dapat mempersempit jenis OS yang digunakan.

**Ada beberapa tools yang dapat digunakan untuk mendeteksi OS, yaitu**

1. nmap
2. queso

## 6.Smurf Attack

Smurf Attack ialah serangan yang dilakukan dengan mengubah alamat IP dari datangnya request atau (IP Spoofing). Penggunaan IP Spoofing jenis ini memungkinkan respon dari ping tadi yang dialamatkan ke komputer yang alamatnya dipalsukan. Akibatnya, komputer akan dibanjiri paket data. Hal tersebut akan mengakibatkan pemborosan bandwith jaringan. Komputer bisa juga menjadi hang karena terus dibanjiri dengan paket data.

Untuk menjaga agar jaringan tidak menjadi perantara bagi serangan ini, broadcast adressing harus dimatikan di router, kecuali jika sangat dibutuhkan untuk keperluan multicast. Alternatif lain engan memfilter permohonan ICMP echo pada firewall. Ada baiknya juga kita memiliki upstream firewall yang diset untuk memfilter ICMP echo atau membatasi traffic echo agar presentasinya lebih kecil dibandingkan traffic jaringan seluruhnya.

## 7.Scanning

Scanning merupakan kegiatan para ha\*ker atau cra\*ker untuk mengidentifikasi sistem yang menjadi target serangan dan juga mencari celah keamanan yang akan digunakan untuk menembus suatu sistem. Kegiatan scanning dari sisi jaringan sangat berisik dan juga mudah dikenali, kecuali apabila menggunkan stealth scanning. Scanning tool yang paling terkenal ialah nmap. Selain itu ada juga SuperScan dan UltraScan yang banyak dipakai pada sistem Windows.

Untuk pencengahan, program scanner pada umumnya menggunakan paket SYN dan ACK untuk mendeteksi celah keamanan pada suatu sistem. Juga dengan memasang firewall, seperti zone alarm.

## 8.Back door

Backdoor adalah perangkat lunak yang digunakan untuk mengakses sistem, aplikasi, atau jaringan tanpa harus menangani proses autentikasi. Backdoor dapat membantu user yang membuat backdoor (peretas) dapat masuk ke dalam sistem tanpa harus melewati proses autentifikasi. Backdoor juga dapat diartikan sebagai mekanisme yang digunakan untuk mengakses sistem atau jaringan.

Awalnya backdoor dibuat para programmer untuk mendapatkan akses khusus untuk masuk ke dalam program yang mereka kembangkan. Apalagi saat terjadi masalah pada program mereka, seperti crash maupun masalah yang diakibatkan oleh bug. Pada saat terjadi masalah itu, backdoor menjadi salah satu solusi yang berhasil dibuat.

Namun, sejalan dengan perkembangan teknologi informasi, backdoor yang sebelumnya menjadi solusi, saat ini menjadi salah satu celah yang digunakan mengambil akses sistem secara paksa. Backdoor disisipkan ke dalam kode sistem maupun sebuah program secara diam-diam sehingga pengguna tidak mengetahui ada backdoor pada sistemnya. Akibatnya, pembuat backdoor tadi dapat masuk dan mendapatkan akses ke dalam sistem pengguna bahkan dapat mengakses keseluruhan sistem.

# MENGENAL VIRUS KOMPUTER, SEJARAH, JENIS, SERTA PENANGGULANGANNYA

Virus Komputer merupakan suatu program atau aplikasi yang dapat memperbanyak, dan menyebar dengan sendirinya, dan menyebabkan efek negatif pada komputer yang terjangkit. Biasanya virus masuk kedalam komputer dengan cara menyisipkan dirinya dalam suatu file ataupun program. Efek yang ditimbulkan virus komputer pun beragam, mulai dari hilangnya file dari komputer, timbul error yang tidak biasa (misalnya freeze), program tidak dapat digunakan, hingga file yang dicuri. Virus juga dapat memungkinkan untuk merusak hardware pada komputer. Komputer yang terjangkit banyak virus biasanya sudah tidak bisa di bersihkan dengan antivirus lagi, dan salah satu caranya adalah membersihkan / format harddisk dalam komputer.

Sejarah Virus

* **1981**, Virus ‘in the wild’ pertama ditemukan. Virus yang bernama Elk Cloner ini menyebar melalui floppy disk pada komputer Apple II .
* **1983**, Fred Cohen dalam paper -nya yang berjudul ‘Computer Viruses – Theory and Experiments ’ memberikan definisi pertama mengenai virus komputer dan memaparkan eksperimen yang telah dilakukannya untuk membuktikan konsep dari sebuah virus komputer. Bersama dengan Len Adelman, ia menciptakan sebuah contoh virus pada komputer VAX 11/750 dengan sistem operasi Unix .
* **1986,** Sepasang kakak adik dari Pakistan, Basit dan Amjad, menciptakan sebuah boot sector virus pertama yang diberi nama Brain. Brain sering kali disebut sebagai virus komputer pertama di dunia . PC-based Trojan pertama diciptakan dalam bentuk program shareware yang diberi nama PC-Write . Dalam beberapa laporan disebutkan bahwa file virus pertama, Virdem , juga ditemukan pada tahun yang sama. Virdem diciptakan oleh Ralf Burger.
* **1987**, Virus-virus file infector seperti Leigh mulai bermunculan, kebanyakan menyerang file COM seperti COMMAND.COM . Pada tahun yang sama muncul virus penyerang file-file EXE pertama, Suriv 01 dan 02 serta Jerusalem . Mainframe IBM mengalami serangan worm IBM Christmas Worm dengan kecepatan replikasi setengah juta kopi per jam.
* **1987**, Virus-virus file infector seperti Leigh mulai bermunculan, kebanyakan menyerang file COM seperti COMMAND.COM . Pada tahun yang sama muncul virus penyerang file-file EXE pertama, Suriv 01 dan 02 serta Jerusalem . Mainframe IBM mengalami serangan worm IBM Christmas Worm dengan kecepatan replikasi setengah juta kopi per jam.
* **1988**, Virus pertama yang menyerang komputer Macintosh , MacMag dan Scores , muncul. Pada tahun yang sama didirikan CERT (Computer Emergency Response Team) oleh DARPA dengan tujuan awalnya untuk mengatasi serangan Morris Worm yang diciptakan oleh Robert Morris.
* **1989**, AIDS Trojan muncul sebagai trojan yang menggunakan samaran sebagai AIDS information program . Ketika dijalankan trojan ini akan mengenkripsi hard drive dan meminta pembayaran untuk kunci dekripsinya.
* **1990**, Virus Exchange Factory (VX) BBS yang merupakan forum diskusi online para pencipta virus didirikan di Bulgaria. Mark Ludwig menulis buku “The Little Black Book of Computer Viruses” yang berisi cara-cara untuk menciptakan berbagai jenis virus komputer.
* **1991**, Virus polymorphic pertama, Tequila , muncul di Swiss. Virus ini dapat mengubah dirinya untuk menghindari deteksi. Kehadiran virus Michaelangelo yang menjadi ancaman bagi seluruh dunia, namun demikian kerusakan yang ditimbulkan pada akhirnya tidak terlalu hebat. Kemuculan beberapa tool yang dapat digunakan untuk menciptakan virus seperti Dark Avenger Mutation Engine (DAME) yang dapat mengubah virus apa pun menjadi virus polymorphic , dan Virus Creation Lab (VCL) yang merupakan kit pertama yang dapat digunakan untuk menciptakan virus.
* **1995**, Para hacker dengan nama ‘Internet Liberation Front’ melakukan banyak serangan pada hari Thanksgiving . Beberapa badan yang menjadi korban serangan ini adalah Griffith Air Force Base, Korean Atomic Research Institute, NASA, GE, IBM, dll. Virus macro pertama yang menyerang aplikasi Microsoft Word, Concept , dikembangkan.
* **1996**, Kemunculan virus Boza yang didesain khusus untuk menyerang file-file Windows 95, virus Laroux yang merupakan virus penyerang Microsoft Excel pertama, virus Staog yang merupakan virus Linux pertama.
* **1998**, Kemunculan virus Java pertama, Strange Brew . Back Orifice merupakan trojan pertama yang dapat digunakan sebagai tool untuk mengambil alih kendali komputer remote melalui Internet. Pada tahun ini, virus-virus macro lainnya bermunculan.
* **1999**, Kemunculan virus Melissa yang merupakan kombinasi antara virus macro yang menyerang aplikasi Microsoft Word dan worm yang menggunakan address book pada aplikasi Microsoft Outlook dan Oulook Express untuk mengirimkan dirinya sendiri melalui email.

Virus Corner merupakan virus pertama menyerang file-file aplikasi MS Project . Virus Tristate merupakan virus macro yang bersifat multi-program menyerang aplikasi Microsoft Word , Excel , dan PowerPoint. Bubbleboy merupakan worm pertama yang dapat aktif hanya dengan membuka email melalui aplikasi Microsoft Outlook tanpa memerlukan attachment .

* **2000**, Serangan Distributed Denial of Service (DDoS) pertama membuat kerusakan pada situs-situs besar seperti Yahoo!, Amazon.com, dan lain-lain. Love Letter merupakan worm dengan kecepatan menyebar tertinggi pada saat itu yang menyebabkan kerusakan pada banyak sistem email di seluruh dunia. Liberty Crack yang merupakan worm pertama untuk peralatan PDA.
* **2001**, Gnuman (Mandragore) merupakan worm pertama yang menyerang jaringan komunikasi peer to peer . Worm ini menyamarkan diri dalam bentuk file MP3 yang dapat di download . Kemunculan virus yang didesain untuk menyerang baik sistem operasi Windows maupun Linux , seperti Winux atau Lindose. Virus LogoLogic-A menyebar melalui aplikasi MIRC dan e-mail.
* **2002**, Virus LFM-926 merupakan virus pertama yang menyerang file-file aplikasi Shockwave Flash. Donut merupakan worm pertama yang menyerang .NET services . SQLSpider merupakan worm yang menyerang aplikasi yang menggunakan teknologi Microsoft SQL Server.
* 2003, Merupakan tahun kejayaan worm. Worm dengan nama Slammer tercipta dan berhasil menginfeksi tidak kurang dari 75.000 komputer di seluruh dunia dalam waktu 10 menit setelah tercipta. Worm ini memiliki kecepatan reproduksi dan penyebaran tercepat yaitu 8.5 detik/worm. Pada tahun ini pula worm Sobig lahir dan merupakan worm yang mampu melakukan aktifitas spam besar-besaran, setiap e-mail yang dikirimkan akan memiliki nama pengirim <!– var prefix = ‘ma’ + ‘il’ + ‘to’; var path = ‘hr’ + ‘ef’ + ‘=’; var addy15158 = ‘big’ + ‘@’; addy15158 = addy15158 + ‘boss’ + ‘.’ + ‘com’; document.write( ” ); document.write( addy15158 ); document.write( ” ); //–>\n [big@boss.com](mailto:big@boss.com) <!– document.write( ‘‘ ); //–> Email telah dilindungi dari Spam Bots, Anda harus mengaktifkan Java untuk dapat melihatnya <!– document.write( ” ); //–> , worm yang memiliki pangkat MM (Mass mailer) ini telah mengakibatkan kerugian ekonomi sebesar US $ 29.7 Miliar. Belum lagi selesai terror worm Sobig, muncul lagi worm Blaster yang menyerang servis RPC (Remote Procedure Call) pada sistem operasi Windows, worm yang pernah membuat pihak Microsoft kalang kabut ini memiliki kecepatan penyebaran 4000 infeksi/jam.
* 2004, Worm dengan nama MyDoom merajai pervirusan dunia dengan tingkat infeksi yang tinggi dan menguasai 30% bandwidth yang digunakan internauts (pengguna internet) di seluruh dunia. Worm yang menyandang rating high risk dari beberapa vendor antivirus ini memiliki daya hancur yang lebih hebat dari worm Sobig dan Welchia, selain itu worm ini juga melakukan serangan DDoS (Distributed Denial of Service) ke situs [http://www.sco.com](http://www.sco.com/) dan [http://www.microsoft.com](http://www.microsoft.com/) dan juga memblok beberapa situs antivirus.

**Klarifikasi Virus Komputer**

Virus komputer dan program lain yang membahayakan sistem komputer dapat

diklasifikasikan ke dalam beberapa kelompok menurut bagaimana cara mereka untuk

menjangkiti (infect) sebuah sistem komputer, bagian dari sistem komputer yang mereka

jangkiti, atau kelakuan (behaviour) yang dimiliki oleh mereka. Namun pada dasarnya definisi

dan klasifikasi mengenai kode-kode program berbahaya ini masih rancu dan menjadi

kontroversi bagi banyak orang bahkan bagi orang yang memang mendalami bidang

komputer.

Berikut adalah contoh klasifikasi dari berbagai jenis harmful program (Program Berbahaya).

1. **Malware** : merupakan singkatan dari malicious software , merujuk pada program yang dibuat dengan tujuan membahayakan atau menyerang sebuah sistem komputer. Terdiri atas virus komputer (computer viruses) , computer worms, trojan horses, joke programs dan malicious toolkits .
2. **Computer virus** : merujuk pada program yang memiliki kemampuan untuk bereplikasi dengan sendirinya.
3. **Computer worm** : merujuk pada program independen yang memiliki kemampuan untuk bereplikasi dengan sendirinya. Indepen di sini memiliki makna bahwa worm tidak memiliki host program sebagaimana virus, untuk ditumpangi. Sering kali worm dikelompokan sebagai sub-kelas dari virus komputer.
4. **Trojan horse** : merujuk pada program independen yang dapat mempunyai fungsi yang tampaknya berguna, dan ketika dieksekusi, tanpa sepengetahuan pengguna, juga melaksanakan fungsi-fungsi yang bersifat destruktif.
5. **Malicious toolkits** : merujuk pada program yang didesain untuk membantu menciptakan program-program yang dapat membahyakan sebuah sistem komputer. Contoh dari program jenis ini adalah tool pembuat virus dan program yang dibuat untuk membantu proses hacking.
6. **Joke program** : merujuk pada program yang meniru operasi-operasi yang dapat membahayakan sistem komputer, namun sebenarnya dibuat untuk tujuan lelucon dan tidak mengandung operasi berbahaya apapun.

Lama Waktu Baca

1. 16.30 – 16.50 (Kamis)

- 20.30 – 20.50

2. Jumat

17.40 – 18.00

3. Sabtu

11.40 – 11.55

4. Minggu

12.20 – 12.32

10-55 – 11.12

Sumber

<https://socs.binus.ac.id/2018/12/10/mengenal-virus-komputer-sejarah-jenis-serta-penanggulangannya/>

<https://adoc.pub/tugas-akhir-virus-komputer-sejarah-dan-perkembangannya.html>

<https://phintraco.com/jenis-cyber-threat-intelligence/>

<https://glosarium.org/arti-land-attack-di-komputer/>

<https://www.teknoiot.com/virus-logic-bomb/>

<https://www.niagahoster.co.id/blog/apa-itu-backdoor/>

<http://riofernando112.blogspot.com/2012/10/macam-macam-serangan-pada-komputer.html>

<https://kucingndeso.wordpress.com/2010/11/04/22/>