MODUL 1

PENGENALAN *CYBER SECURITY* DAN SISTEM OPERASI LINUX

1.1 Tujuan Praktikum

1. Mengetahui pengertian *cyber security*.
2. Mengetahui ap aitu sistem operasi linux.
3. Mengetahui perintah-perintah dasar dari linux.
4. Mengetahui dan memahami cara kerja dari linux.

1.2 Alat dan Bahan

1. Laptop
2. Mouse
3. VirtualBox
4. Linux OS

1.3 Dasar Teori

1.3.1 Pengenalan *Cyber Security*

Cyber Security adalah bidang keamanan siber yang berfokus pada perlindungan jaringan komputer dari ancaman siber. *Cyber Security* memiliki tiga tujuan utama; mencegah akses illegal ke sumber daya jaringan, mendeteksi dan menghentikan serangan siber dan pelanggaran keamanan yang sedang berlangsung, dan memastikan bahwa pengguna yang berwenang memiliki akses yang aman ke sumber daya jaringan yang mereka butuhkan saat mereka membutuhkannya.

Seiring dengan bertambahnya ukuran dan kompleksitas jaringan, begitu pula dengan risiko serangan siber. Sebagai contoh, menurut laporan *Cost of Data Breach* 2022 dari IBM, 83% organisasi yang disurvei mengalami lebih dari satu kali pelanggaran data (pelanggaran keamanan yang mengakibatkan akses illegal ke informasi sensitif atau rahasia). Serang-serangan ini sangat mahal: Biaya rata-rata global untuk pelanggaran data adalah USD 4,35 juta, dan

biaya rata-rata pelanggaran data di Amerika Serikat lebih dari dua kali lipatnya, yaitu USD 9,44 juta.

Sistem cyber security bekerja pada dua tingkat; di parameter dan di dalam jaringan. Di parameter, kontrol keamanan mencoba menghentikan ancaman siber agar tidak masuk ke dalam jaringan. Namun penyerangan jaringan terkadang menerobos masuk, sehingga tim keamanan IT juga menempatkan kontrol di sekitar sumber daya di dalam jaringan, seperti laptop dan data. Bahkan jika penyerangan berhasil masuk, mereka tidak akan bebas berkuasa. Strategi ini meletakkan beberapa kontrol antara peretas dan potensi kerentanan, disebut "*defense in depth*".

1.3.2 Konsep CIA Triad dalam Cyber Security

CIA Triad adalah model penting dalam menjaga keamanan informasi, yang telah digunakan oleh banyak perusahaan untuk membangun sistem keamanan yang kuat dan menyeluruh. Model ini terdiri dari 3 aspek utama yang akan menjadi komponen penting dari *cyber security* yaitu:

1. ***Confidentiality* (Kerahasiaan)** berkaitan dengan menjaga informasi agar hanya diakses oleh pihak yang berwenang, dengan tujuan melindungi data sensitif dari pihak yang tidak berhak.
2. ***Integrity* (Integritas)** berfokus pada memastikan bahwa informasi tetap akurat dan tidak diubah secara tidak sah selama penyimpanan, transmisi, atau pemrosesan, untuk mencegah manipulasi data.
3. ***Availability* (Ketersediaan)** memastikan bahwa informasi selalu tersedia dan dapat diakses oleh pihak yang berhak saat diperlukan, dengan menjaga sistem tetap operasional tanpa gangguan.

Berikut adalah beberapa contoh kontrol keamanan yang digunakan dalam CIA Triad model:

1. ***Confidentiality policies***: Perusahaan dapat menetapkan aturan terkait akses dan penggunaan informasi sensitif, serta menentukan siapa yang berhak mengaksesnya.

2. ***Data retention policies***: Menetapkan kebijakan retensi data memungkinkan perusahaan menyimpan informasi untuk jangka waktu yang sesuai dengan kebutuhan bisnis dan regulasi yang berlaku.
3. ***Strong passwords***: Mewajibkan pengguna untuk menggunakan kata sandi yang rumit dan kuat membantu melindungi data dari akses yang tidak sah.
4. ***Data encryptions***: Menggunakan enkripsi untuk melindungi data baik saat disimpan maupun selama pengiriman antar perangkat.
5. ***IT security solutions***: Mengimplementasikan solusi keamanan TI yang tangguh untuk melindungi perusahaan dari berbagai ancaman keamanan.

1.3.3 Tim Keamanan pada Bidang Cyber Security

Semakin berkembangnya teknologi, ancaman siber pun semakin canggih dan kompleks. Oleh karena itu, perusahaan dan organisasi memerlukan strategi yang efektif untuk melindungi sistem mereka dari serangan dan memastikan informasi tetap aman. Salah satu pendekatan yang banyak diterapkan dalam bidang keamanan siber adalah melalui penggunaan tim keamanan yang terstruktur dengan baik, yakni:

1. ***Red Team***

Red Team adalah tim yang bertugas mengevaluasi keamanan suatu sistem atau organisasi melalui simulasi serangan. Tujuan utama mereka adalah untuk mengidentifikasi kelemahan dan celah dalam infrastruktur, aplikasi, dan kebijakan keamanan. *Red Team* berperan sebagai penyerang yang mencoba menguji keefektifan sistem pertahanan dan mendapatkan wawasan tentang metode serangan dari sudut pandang penyerang. Tugas mereka mencakup

melakukan *penetration testing, social engineering*, dan pengujian keamanan yang lainnya.

2. *Blue Team*

Blue Team adalah bertanggung jawab untuk mempertahankan dan melindungi sistem atau organisasi dari serangan *cyber*. Mereka bertugas me-*monitor* dan mendeteksi ancaman keamanan, serta merespons serangan secara cepat. Fokus utama mereka adalah memastikan keberlanjutan operasional dan memperkuat sistem pertahanan. Tugas mereka meliputi konfigurasi keamanan, pemantauan kegiatan jaringan, analisis log, dan pemulihan sistem setelah serangan.

3. *Purple Team*

Purple Team adalah gabungan dari *Red Team* dan *Blue Team*, dengan fokus pada kolaborasi antara kedua tim untuk meningkatkan keamanan secara menyeluruh. Tim ini bekerja sama dalam menganalisis temuan dari serangan simulasi *Red Team* dan memperbaiki kelemahan yang teridentifikasi. *Purple Team* juga berperan sebagai *platform* untuk berbagi pengetahuan, pengalaman, dan praktik terbaik antara kedua tim. Tugas mereka meliputi *debriefing* setelah serangan simulasi, mengidentifikasi tindakan perbaikan, dan mengimplementasikan solusi keamanan yang lebih efektif.

1.3.4 Sejarah Linux

Kernel Linux pada mulanya berasal dari proyek hobi mahasiswa Universitas Helsinki di Finlandia, Bernama Linus Torvalds. Bermula dari ketidakpuasan Linus terhadap kernel Minix yang dipakai di kampusnya. Orang yang memplubikasikan Linux di Indonesia adalah Paulus Suryono Adisoemarta (Bung Yono). Tahun 1992-1994 adalah masa vakum perkembangan Linux. Masuknya Distro Slackware (Kernel 1.0.8) ke Indonesia memicu tumbuhnya komunitas GNU/LINUX di lingkungan Universitas Indonesia.

1.3.5 Pengertian Linux

Linux adalah sistem operasi komputer yang bertipe Unix. Linux merupakan salah satu contoh hasil pengembangan perangkat lunak bebas dan sumber terbuka utama. Seperti perangkat lunak dan sumber terbuka lainnya pada umumnya, kode sumber linux dapat dimodifikasi, digunakan dan didistribusikan kembali secara bebas oleh siapa saja. Linux juga merupakan sistem operasi *open-source* yang terkenal karena keamanan, stabilitas, dan fleksibelitasnya. Linux memiliki lisensi *General Public License* (GNU). GNU merupakan lisensi *copyleft* bebas untuk perangkat lunak yang menjamin kebebasan untuk mendistribusikan dan mengubah semua versi dari sebuah program untuk membuat program baru dengan syarat kode program yang asli harus disertakan, Linux bersifat terbuka (*open source*) siapapun individu.

1.3.6 Jenis-jenis Distro Linux

Beberapa jenis Distro Linux beserta contoh Distro turunannya, yaitu:

1. Debian, mengutamakan kestabilan dan kehandalan meskipun mengorbankan aspek kemudahan dan kemutakhiran program. Debian menggunakan *.deb dalam paket instalasi programnya. Distro turunannya: Debian, Kali Linux, Ubuntu, gOs Linux, Dream Linux, Linux Mint, Xandros Linux, BlankON Linux, Dewalinux, dll.

2. *RedHat*, merupakan distro pertama yang instalasi dan pemrogramannya mudah. Distro berbasis *RedHat* menggunakan binary RPM (*RedHat Package Management*). Contoh distro dari varian ini adalah RedHat, Mandrake, Mandriva, PCLinuxOS, centOS, Fedora, Core, IGOS, dll.

3. *Slackware*, bisa dikatakan Linux untuk *advanced*, hampir semua dokumentasi Linux disusun berdasarkan slackware. Semua isinya (kernel, library ataupun aplikasinya) sudah teruji. *Slackware* menganjurkan untuk menginstall dari *source* sehingga setiap program yang di-*install* teroptimasi dengan sistem kita. Slackware menggunakan libc5 dalam *binary/library*-nya dan filenya menggunakan.tgz. contoh distro; Slackware, Slax, Zenwalk, Vektor Linux, Backtrack, KateOS, Puppy Linux, dll.

4. SuSE distribusi dari YaST (*Yet Another Setup Tools*) untuk mengkonfigurasi sistem merupakan distribusi Linux yang peng- install-nya menggunakan bahasa Indonesia. Contoh distro; SuSE Linux Enterprise, OpenSuse, dll.

5. Ubuntu adalah salah satu distribusi Linux yang berbasiskan pada Debian dan memiliki *interface* desktop. Proyek Ubuntu disponsori oleh *Canocical Ltd* (Perusahaan milik Mark Shuttleworth).

6. Kali Linux merupakan sebuah sistem Operasi yang dibangun berbasis Debian yang merupakan distribusi dari induknya, yaitu Linux. Kali Linux sendiri dikembangkan oleh Lembaga yang Bernama *Offensive Security*. Bukan dibangun dari dasar, Kali sendiri merupakan *development project* dari raksasa besar *Penetration Tool OS*, yaitu *BackTrack*. Sebelum Kali Linux, *Backtrack* sudah digunakan sebagai alat penetrasi keamanan komputer terbaik yang pernah ada. Walaupun ada juga beberapa OS yang memiliki fungsi yang sama seperti *BlackArch, BAckBox*, dll.

7. BSD, beberapa distro BSD dikembangkan berdasarkan *source code* yang dikenal sebagai 4,4BSD-Lite. Contoh distro; FreeBSD, OpenBSD, NetBSD, DragonflyBSD, PcBSD.

1.3.7 Kelebihan dan Kekurangan Kali Linux

Kelebihan Kali Linux:

1. *Streaming Security* serta *update package* dari repositori Debian Sinkronisasi dengan repositori Debian 4 kali sehari, terus memberikan update paket terbaru dan perbaikan keamanan yang tersedia.
2. *Packaging* File Debian dari masing-masing *tool* di kali, jadi *tools* di Kali Linux bisa digunakan oleh distro yang lain yang masih turunan dari Linux Debian, seperti Ubuntu, Blankon, dll.
3. Pemaketan/packaging jangka Panjang & sering maintenance pada bug di *tools*-nya.
4. Bisa menggunakan banyak desktop environment misal KDE, LXDE, XFCE.
5. Kemudahan update untuk versi Kali Linux terbaru.

6. Support jangka panjang pada pengembangan jangka panjang pada ARM *Hardware*
7. Automatis Instalasi pada Kali
8. Kustomisasi ISO & Boostraps

Kekurangan Kali Linux:

1. Sistem operasi Kali Linux sulit untuk dipelajari, terutama yang belum mempunyai kemampuan komputer sama sekali.
2. Belum banyak aplikasi yang mendukung Linux.
3. Tampilan dari sistem operasi ini kurang menarik.
4. Tidak banyak dukungan dari *Hardware* tertentu.

1.3.8 Alasan Memilih Kali Linux

1. Kali Linux merupakan sistem operasi yang bersifat *free license* alias gratis. Tidak perlu membayar untuk mendapatkan Linux, bukan bajakan. Siapa saja bisa mengembangkannya secara bebas.
2. Keamanan menggunakan Kali Linux lebih terjamin dibandingkan Windows. Virus pun tidak mudah tersebar karena sifatnya yang multiuser, sehingga virus tidak mampu menyebar dari *user* satu pada *user* lainnya.

1.3.9 Fitur-fitur Kali Linux

Sistem operasi Kali Linux merupakan pengembangan dari sistem operasi *BackTrack* Linux yang sudah disempurnakan, berikut beberapa fitur Kali Linux yang akan dirangkum dalam beberapa poin, yaitu:

1. **Gratis**

   Kali Linux akan selalu gratis dipakai oleh siapapun, dan kapanpun.
2. ***Package* yang dapat diubah sepenuhnya**

   Yaitu dapat diubah isi dari Kali Linux sendiri, seperti tampilan *User Interface, package* aplikasi, dan lain-lain.
3. **FHS *Compliant System***

Pada FHS *Compliant System*, untuk menjalankan suatu aplikasi tidak perlu melalui direktori asal, misalnya pada terminal *console* cukup menuliskan aplikasi apa yang ingin dijalankan.

4. **Lebih dari 300 *tool Penetration Tester***

   Tools Penetration Tester seperti *Aircrack, Asleap, Bluelog, Bluemaho* yang digunakan untuk wireless attack, seperti penyadapan *wifi, traffic monitoring, man in the middle*, dan lain-lain.

5. **Merupakan yang terbaik untuk *hacking* dan keamanan**

   Muncul pada saat 2006, Kali Linux dinobatkan menjadi sistem operasi terbaik untuk kebutuhan hacking dan keamanan.

6. **Mempunyai banyak bahasa yang bisa digunakan**

   Meskipun mayoritas petunjuk ditulis dengan bahasa Inggris, tetapi pengguna dapat memilih bahsa lain yang sesuai dengan bahsa yang mereka gunakan, seperti Bahasa Indonesia.

7. **Berjalan pada Kernel Linux 4.0**

   Berfungsi sebagai *task switching, multitasking*, melakukan tugas-tugas network serta mengatur penggunaan memori, dengan versi 4.0 merupakan Kernel yang lebih efesien dan lebih terbaru.

8. **Menggunakan desktop GNOME 3, bukan GNOME fallback**

   GNOME (*GNU Network Model Environment*) adalah versi terbaru dari GNOME yang dijalankan pada versi Ubuntu 11.10 yang mana lebih *user-friendly* dibandingkan dengan GNOME versi sebelumnya.

9. ***In-built screencasting tool***

   Pada versi *BackTrack* tidak ada fitur ini, fitur ini dapat digunakan untuk merekam desktop, sehingga tidak perlu rumit untuk merekam apa yang ditampilkan di *desktop* dan repot-repot mencari *tool* yang lain.

10. **Dukungan Ruby 2.0**

    Dengan dukungan Ruby 2.0, membuat Metasploit memuat lebih cepat.

11. **Dukungan perangkat yang luas**

    Kompatibilitas terhadap perangkat-perangkat eksternal seperti SS (*Solid-State Drive*), USB (*Universal Serial Bus*), *Keyboard* eksternal, dan lain-lain.