IDENTITAS BUKU

SISTEM KEAMANAN TEKNOLOGI INFORMASI POLRI

Penyusun:

Tim Penyusun Kurikulum dan Hanjar Dikbangspes
Bintara/Gol. II PNS Polri Tekinfo Dasar
Lemdiklat Polri T.A. 2022

Editor:

1. Kombes Pol. Nirboyo, S.I.K.
2. AKBP Fakhruroji, S.T., M.T.
3. Pembina Drs. Heru Martono, S.Pd.
4. Iptu Sugiarto, S.Kom., M.Kom.
5. Penata TK I Abdul Wahab, S.E.
6. Penata Maisaroh, S.Pd.
7. Briptu Tri Broto Siswoyo, S.Kom.
8. Bripda Aulia Ratu Balqis
9. Bripda Ayudhia Prasastie Dewi

Hanjar Pendidikan Polri
Pendidikan Pengembangan Spesialisasi
Bintara/Gol. II PNS Polri Tekinfo Dasar

Diterbitkan oleh:

Bagian Kurikulum dan Bahan Ajar Pendidikan Pengembangan Spesialisasi
Biro Kurikulum
Lembaga Pendidikan dan Pelatihan Polri
Tahun 2022

DAFTAR ISI

Cover i
Sambutan Kalemdiklat Polri ii
Keputusan Kalemdiklat Polri iv
Lembar Identitas Buku v
Daftar Isi vii

MODUL SISTEM KEAMANAN TEKNOLOGI INFORMASI POLRI

Pendahuluan 1
Standar Kompetensi 1

MODUL 1 KONSEP SISTEM KEAMANAN TEKNOLOGI INFORMASI POLRI

Pengantar 2
Kompetensi Dasar 2
Materi Pelajaran 3
Metode Pembelajaran 3
Alat, Media, Bahan dan Sumber Belajar 3
Kegiatan Pembelajaran 4
Tagihan/Tugas 5
Lembar Kegiatan 5
Bahan Bacaan 6

POKOK BAHASAN 1

KONSEP SISTEM KEAMANAN TEKNOLOGI INFORMASI 6

1. Pengertian Sistem Keamanan TI 6
2. Tujuan Sistem Keamanan TI 6
3. Komponen Sistem Keamanan TI 6
4. Prinsip Kerja Sistem Keamanan TI 11

POKOK BAHASAN 2

GANGGUAN DAN ANCAMAN SISTEM KEAMANAN TEKNOLOGI INFORMASI 15

1. Jenis Gangguan Sistem Keamanan TI 15
2. Ancaman dan Serangan Sistem Keamanan TI 15
3. Jenis-jenis Serangan Sistem Keamanan TI 16

4. Perusak Sistem Keamanan TI 17
5. Resiko Sistem Keamanan TI 17
6. Kerentanan Sistem Keamanan TI 17
Rangkuman 22
Soal Latihan 23

MODUL 2 INSTALASI, PENGOPERASIAN, DAN PERAWATAN SISTEM KEAMANAN TEKNOLOGI INFORMASI POLRI

Pengantar 24
Kompetensi Dasar 24
Materi Pelajaran 25
Metode Pembelajaran 25
Alat, Media, Bahan dan Sumber Belajar 25
Kegiatan Pembelajaran 26
Tagihan/Tugas 28
Lembar Kegiatan 28
Bahan Bacaan 29

POKOK BAHASAN

PROSEDUR INSTALASI, PENGOPERASIAN, DAN PERAWATAN SISTEM KEAMANAN TEKNOLOGI INFORMASI POLRI 29

1. Prosedur Instalasi Sistem Keamanan TI Polri 29
2. Prosedur Pengoperasian Sistem Keamanan TI Polri 45
3. Prosedur Perawatan Sistem Keamanan TI Polri 54

Rangkuman 55
Soal Latihan 55

MODUL	**SISTEM KEAMANAN TEKNOLOGI INFORMASI POLRI**
	40 JP (1800 menit)

PENDAHULUAN

Keamanan Teknologi Informasi adalah aktivitas perlindungan sistem komputer dari serangan orang yang tidak bertanggungjawab. Termasuk di dalamnya pencegahan dari kerusakan pada hardware, software atau data elektronik, juga dari disrupsi atau misdirection dari layanan teknologi informasi. Keamanan teknologi informasi sering dikenal pula dengan istilah cybersecurity, information technology security (IT Security). Bidang ini tumbuh berkembang dengan pesat karena kebutuhan akan pentingoya ketahanan sistem komputer. Hal ini muncul seiring dengan perkembangan pesat dan kompleks teknologi internet, WIFI,bluetooth, handphone, dan perangkat kecil lainnya memanfaatkan platform IoT.

Untuk memberikan pemahaman tentang Sistem Keamanan Teknologi Informasi Polri maka disusun materi konsep sistem keamanan teknologi informasi Polri, instalasi, pengoperasian dan perawatan sistem keamanan teknologi informasi.

STANDAR KOMPETENSI

Memahami keamanan sistem teknologi informasi (TI) dan terampil menginstal, mengoperasikan, serta merawat keamanan sistem teknologi informasi Polri.

MODUL 01

KONSEP SISTEM KEAMANAN TEKNOLOGI INFORMASI POLRI

4 JP (180 menit)

PENGANTAR

Modul *data base* Polri membahas materi tentang: konsep *data base* Polri dan prosedur *keamanan* sistem *TI* (persiapan, pengoperasian, pengakhiran).

Tujuan adalah agar peserta pelatihan memahami konsep sistem keamanan teknologi informasi Polri.

KOMPETENSI DASAR

1. Memahami konsep sistem keamanan TI.

   Indikator Hasil Belajar

   a. Menjelaskan pengertian sistem keamanan TI.
   b. Menjelaskan tujuan sistem keamanan TI.
   c. Menjelaskan komponen-komponen sistem keamanan TI.
   d. Menjelaskan prinsip-prinsip kerja sistem keamanan TI.

2. Memahami gangguan dan ancaman sistem keamanan TI.

   Indikator Hasil Belajar

   a. Menjelaskan jenis gangguan sistem keamanan TI.
   b. Menjelaskan ancaman dan serangan terhadap sistem keamanan TI.
   c. Menjelaskan jenis-jenis serangan sistem keamanan TI.
   d. Menjelaskan perusak sistem keamanan TI.
   e. Menjelaskan kerentanan pada sistem keamanan TI.
   f. Menjelaskan program pengganggu dan perusak sistem keamanan TI.

MATERI PELAJARAN

1. **Pokok Bahasan 1**:

   Konsep sistem keamanan teknologi informasi.

   Subpokok Bahasan:

   a. Pengertian sistem keamanan TI.
   b. Tujuan sistem keamanan TI.
   c. Komponen-komponen sistem keamanan TI.
   d. Prinsip-prinsip kerja sistem keamanan TI.

2. **Pokok Bahasan 2**:

   Gangguan dan ancaman sistem keamanan teknologi informasi.

   Subpokok Bahasan:

   a. Jenis gangguan sistem keamanan TI.
   b. Ancaman dan serangan terhadap sistem keamanan TI.
   c. Jenis-jenis serangan sistem keamanan TI.
   d. Perusak sistem keamanan TI.
   e. Kerentanan pada sistem keamanan TI.
   f. Program pengganggu dan perusak sistem keamanan TI.

METODE PEMBELAJARAN

1. **Metode Ceramah**

   Metode ini digunakan untuk menyampaikan materi tentang konsep sistem keamanan TI dan hal-hal yang mengancam sistem keamanan TI.

2. **Metode Tanya Jawab**

   Metode ini digunakan untuk memperdalam pemahaman materi tentang konsep sistem keamanan TI dan hal-hal yang mengancam sistem keamanan TI.

ALAT, MEDIA, BAHAN DAN SUMBER BELAJAR

1. **Alat, Media dan Bahan:**

   a. *White Board.*
   b. *Laptop.*
   c. LCD.
   d. HVS

e. Alat tulis.
f. Jaringan internet.

2. Sumber Belajar:

a. Peraturan kapolri Nomor 1 tahun 2011 tentang Penyelenggaraan Sistem Telekomunikasi di Lingkungan Polri.
b. Undang-undang Nomor 36 tahun 1999 tentang Telekomunikasi.

KEGIATAN PEMBELAJARAN

1. Tahap Awal: 10 menit

a. Pendidik melaksanakan apersepsi:
   1) Pendidik melaksanakan perkenalan;
   2) Pendidik menyampaikan tujuan pembelajaran dan menyampaikan tugas-tugas yang harus dilaksanakan peserta didik selama pembelajaran;
   3) Pendidik menciptakan suasana pembelajaran yang kondusif.
b. Peserta didik menyimak, menanggapi dan melaksanakan instruksi pendidik.

2. Tahap Inti: 160 menit

a. Pendidik menyampaikan materi tentang sistem keamanan TI Polri.
b. Peserta didik menyimak, mencatat hal-hal yang penting.
c. Pendidik memberikan kesempatan kepada peserta didik untuk bertanya hal-hal yang belum dipahami.
d. Peserta didik bertanya dan menanggapi materi yang disampaikan pendidik.

3. Tahap Akhir: 10 menit

a. Pendidik memberikan kesimpulan materi sistem keamanan TI Polri.
b. Pendidik mengecek penguasaan materi dengan cara bertanya secara lisan dan acak kepada peserta didik.
c. Pendidik melakukan evaluasi pembelajaran dan menutup pembelajaran.

TAGIHAN/TUGAS

Peserta pelatihan mengumpulkan hasil resume materi tentang konsep sistem keamanan teknologi informasi.

LEMBAR KEGIATAN

--

BAHAN BACAAN

POKOK BAHASAN 1

KONSEP SISTEM KEAMANAN TEKNOLOGI INFORMASI

1. Pengertian Sistem Keamanan TI

Sistem keamanan teknologi informasi adalah proses untuk mencegah & mengidentifikasi penggunaan yang tidak sah dari jaringan komputer. Maksudnya penggunaan yang tidak sah yaitu penyusup yang bermaksud untuk mengakses setiap bagian dari sistem teknologi informasi komputer tersebut.

2. Tujuan Sistem Keamanan TI

Tujuan dari sistem keamanan teknologi informasi ialah untuk mengantisipasi resiko jaringan komputer berupa bentuk ancaman fisik maupun logik. Maksudnya ancaman fisik adalah seorang pengganggu yang berniat untuk merusak bagian fisik komputer. Sedangkan ancaman logik adalah ancaman yang berupa pencurian data atau pembobolan terhadap akun seseorang.

3. Komponen Sistem Keamanan TI

a. Jenis jaringan

1) Autentikasi adalah proses pengenalan peralatan, system operasi, kegiatan, aplikasi dan identitas user yang terhubung dengan jaringan komputer dengan cara user memasukkan username dan password pada saat login ke jaringan.
2) Tahapan autentikasi:
   a) Autentikasi untuk mengetahui lokasi melalui data link layer dan network layer.
   b) Autentikasi untuk mengetahui proses yang sedang berjalan yang terjadi pada session dan presentation layer.
   c) Autentikasi untuk mengenal user dan aplikasi yang digunakan (application layer).
3) Enkripsi adalah teknik pengkodean data yang berguna untuk menjaga data atau file. Enkripsi diperlukan untuk menjaga kerahasiaan data.

4) *Virtual Private Network* (VPN) adalah jaringan komunikasi lokal yang terhubung melalui media jaringn. Fungsinya untuk memperoleh komunikasi yang aman (*private*) melalui internet. Kriteria yang harus dipenuhi VPN:

   a) *User authentication*, VPN harus mampu mengklarifikasi identitas klien. VPN mampu memantau aktivitas klien meliputi masalah waktu, kapan, di mana dan berapa lama seorang klien mengakses jaringan serta jenis resource yang diaksesnya.
   b) *Address management*, VPN harus dapat mencantumkan address klien pada intranet dan memastikan alamat tersebut tetap rahasia.
   c) *Data encryption*, data yang melewati jaringan harus dibuat agar tidak dapat dibaca oleh pihak-pihak yang tidak berwenang.
   d) *Key management*, Harus mampu membuat dan memperbaharui encryption key untuk server dan klien.
   e) *Multiprotocol support*, Harus mampu menangani berbagai macam protokol dalam jaringan publik seperti IP atau IPX.

5) DMZ (*De-Militerized Zone*), system untuk server yang berfungsi untuk melindungi system internal dari serangan hacker. DMZ bekerja pada seluruh dasar pelayanan jaringan yang membutuhkan akses terhadap jaringan. Sehingga jika ada yang mencoba melakukan hacking terhadap server yang menggunakan system DMZ maka hacker tersebut hanya akan sampai hostnya.

b. Pengenalan *firewall*

Firewall adalah salah satu aplikasi pada sistem operasi yang dibutuhkan oleh jaringan komputer untuk melindungi intergritas data/sistem jaringan dari serangan-serangan pihak yang tidak bertanggung jawab. Caranya dengan melakukan filterisasi terhadap paket-paket yang melewatinya.

Firewall tersusun dari aturan-aturan yang diterapkan baik terhadap hardware, software ataupun sistem itu sendiri dengan tujuan untuk melindungi jaringan, baik dengan melakukan filterisasi, membatasi, ataupun menolak suatu permintaan koneksi dari jaringan luar lainnya seperti internet.

1) Proses yang terjadi pada *firewall*

Pada *firewall* terjadi beberapa proses yang memungkinkannya melindungi jaringan. Ada tiga macam proses yang terjadi pada *firewall*, yaitu:

a) Modifikasi header paket, digunakan untuk memodifikasi kualitas layanan bit paket TCP sebelum mengalami proses *routing*.
b) Translasi alamat jaringan, translasi yang terjadi dapat berupa translasi satu ke satu (*one to one*), yaitu satu alamat IP privat dipetakan kesatu alamat IP publik atau translasi banyak kesatu (*many to one*) yaitu beberapa alamat IP privat dipetakan kesatu alamat publik.
c) Filter paket, digunakan untuk menentukan nasib paket apakah dapat diteruskan atau tidak.

2) Jenis-jenis *firewall*

Firewall terbagi menjadi 4 jenis yaitu, *packet filtering gateway, application layer gateway, circuit level gateway, dan statefull multilayer inspection firewall*. Adapun penjelasannya sebagai berikut:

a) *Packet filtering gateway*, dapat diartikan sebagai *firewall* yang bertugas melakukan filterisasi terhadap paket-paket yang datang dari luar jaringan yang dilindunginya.
b) *Application layer gateway*, model firewall ini juga dapat disebut *proxy firewall*. Mekanismenya tidak hanya berdasarkan sumber, tujuan dan atribut paket, tapi bisa mencapai isi (content) paket tersebut. Bila kita melihat dari sisi layer TCP/IP, firewall jenis ini akan melakukan filterisasi pada layer aplikasi (*application layer*).
c) *Circuit level gateway*. Model firewall ini bekerja pada bagian Lapisan transport dari model referensi TCP/IP. *Firewall* ini akan melakukan pengawasan terhadap awal hubungan TCP yang biasa disebut sebagai TCP Handshaking, yaitu proses untuk menentukan apakah sesi hubungan tersebut diperbolehkan atau tidak. Bentuknya hampir sama dengan *application layer gateway*, hanya saja bagian yang difilter terdapat ada lapisan yang berbeda, yaitu berada pada layer Transport.
d) *Statefull multilayer inspection firewall*. Model *firewall* ini *merupakan* penggabungan dari ketiga *firewall* sebelumnya. *Firewall* jenis ini akan bekerja pada lapisan Aplikasi, Transport dan Internet.

Dengan penggabungan ketiga model *firewall* yaitu *packet filtering gateway*, application layer gateway dan *circuit level gateway*, *mungkin* dapat dikatakan *firewall* jenis ini merupakan *firewall* yang, memberikan fitur terbanyak dan memeberikan tingkat keamanan yang paling tinggi.

3) Sistem *firewall*

Aplikasi pengendalian jaringan dengan menggunakan firewall dapat diimplementasikan dengan menerapkan sejumlah aturan (chains) pada topologi yang sudah ada. Dalam hal pengendalian jaringan dengan menggunakan iptables, ada dua hal yang harus diperhatikan yaitu:

a) Koneksi paket yang menerapkan *firewall* yang digunakan.
b) Konsep *firewall* yang diterapkan.
c) Penerapan *firewall*.

4) Istilah pada penerapan *Firewall*

a) *Host*

Suatu sistem komputer yang terhubung pada suatu network.

b) *Bastion host*

Sistem komputer yang harus memiliki tingkat sekuritas yang tinggi karena sistem ini rawan sekali terhadap serangan *hacker* dan *cracker*, karena biasanya mesin ini diekspos ke network luar (internet) dan merupakan titik kontak utama para user dari internal network.

c) *Packet filtering*

Aksi dari suatu devais untuk mengatur secara selektif alur data yang melintasi suatu network. *Packet filter* dapat memblok atau memperbolehkan suatu paket data yang melintasi network tersebut sesuai dengan kebijaksanaan alur data yang digunakan (*security policy*).

d) *Perimeter network*

Suatu *network* tambahan yang terdapat di antara network yang dilindungi dengan network eksternal, untuk menyediakan layer tambahan dari suatu sistem security. Perimeter network juga sering disebut dengan DMZ (*De-Millitarized Zone*).

5) Keuntungan *firewall*

a) *Firewall* merupakan fokus dari segala keputusan *sekuritas*. Hal ini disebabkan karena *firewall* merupakan satu titik tempat keluar masuknya trafik internet pada suatu jaringan.

b) *Firewall* dapat menerapkan suatu kebijaksanaan sekuritas. Banyak sekali service-service yang digunakan di internet. Tidak semua service tersebut aman digunakan, oleh karenanya *firewall* dapat berfungsi sebagai penjaga untuk mengawasi service-service mana yang dapat digunakan untuk menuju dan meninggalkan suatu network.

c) *Firewall* dapat mencatat segala aktivitas yang berkaitan dengan alur data secara efisien. Semua trafik yang melalui firewall dapat diamati dan dicatat segala aktivitas yang berkenaan dengan alur data tersebut. Dengan demikian *network administrator* dapat segera mengetahui jika terdapat aktivitas aktivitas yang berusaha untuk menyerang internal network mereka.

d) *Firewall dapat* digunakan untuk membatasi pengunaan *sumberdaya* informasi. Mesin yang menggunakan *firewall* merupakan mesin yang terhubung pada beberapa network yang berbeda, sehingga kita dapat membatasi network mana saja yang dapat mengakses suatu service yang terdapat pada network lainnya.

6) Kelemahan *firewall*

a) *Firewall* tidak dapat melindungi network dari serangan koneksi yang tidak melewatinya (terdapat pintu lain menuju *network* tersebut).

b) *Firewall* tidak dapat melindungi dari serangan dengan metoda baru yang belum dikenal oleh *firewall.*

c) *Firewall tidak* dapat melindungi dari serangan virus.

7) Kemampuan *firewall* dalam penerapannya pada VPN

a) IP *hiding/mapping*. Kemampuan ini mengakibatkan IP address dalam jaringan dipetakan atau ditranslasikan ke suatu IP address baru. Dengan demikian IP address dalam jaringan tidak akan dikenali di Internet.

b) *Privilege limitation*. Dengan kemampuan ini kita dapat membatasi para user dalam jaringan sesuai dengan otorisasi atau hak yang diberikan kepadanya. Misalnya, User A hanya boleh

mengakses homepage, user B boleh mengakses home page, e-mail dan news, sedangkan user C hanya boleh mengakses e-mail.

c) *Outside limitation*. Dengan kemampuan ini kita dapat membatasi para user dalam jaringan untuk hanya mengakses ke alamat-alamat tertentu di Internet di luar dari jaringan kita.

d) *Inside limitation*. Kadang-kadang kita masih memperbolehkan orang luar untuk mengakses informasi yang tersedia dalam salah satu komputer (misalnya Web Server) dalam jaringan kita. Selain itu, tidak diperbolehkan, atau memang sama sekali tidak dizinkan untuk mengakses seluruh komputer yang terhubung ke jaringan kita.

e) *Password and encrypted authentication*. Beberapa user di luar jaringan memang diizinkan untuk masuk ke jaringan kita untuk mengakses data dan sebagainya, dengan terlebih dahulu harus memasukkan password khusus yang sudah terenkripsi.

c. Security *Information* and *Event Management (*SIEM).

SIEM merupakan sistem yang membantu untuk memonitor lalu lintas jaringan dan memberikan analisa secara real-time dari log yang dihasilkan oleh aplikasi ataupun perangkat keamanan. SIEM merupakan juga sistem manajemen log yang mengumpulkan log dari berbagai aplikasi dan perangkat keamanan seperti server, network, database, firewall dll.

4. Prinsip Kerja Sistem Keamanan TI

a. Perencanaan sistem keamanan TI

1) Pembatasan akses jaringan komputer

a) *Internal password autenthication*

Password yang baik menjadi penting dalam suatu keamanan jaringan. Password yang baik adalah kombinasi dari angka dan huruf sehingga lebih sulit untuk terkena hack. Kebanyakan masalah dalam keamanan jaringan disebabkan karena password yang kurang baik.

b) *Server-based password autenthication*

Sebuah computer server juga perlu kunci atau password agar data yang disimpan didalamnya dapat terjaga dengan aman. Dalam keamanan

jaringan password dalam server merupakan kebutuhan yang harus ada.

c) *Firewall and routing control*

Firewall sangat penting pada jaringan untuk meminimalisir pencurian data computer tersebut. Karena itu pada saat instalasi jaringan firewall dan konfigurasi *routing* harus tepat agar tidak terja dikendala pada kedepannya.

d) Monitoring terjadwal dalam jaringan

Untuk sebuah admin dalam sebuah jaringan, monitoring itu sangat perlu dilakukan agar mengetahui kondisi dan keadaan jaringan tersebut agar tidak sampai down.

e) Menggunakan metode enkripsi tertentu

Dasar enkripsi cukup sederhana. Pengirim menjalankan fungsi enkripsi pada pesan *plaintext*, *ciphertext* yang dihasilkan kemudian dikirimkan lewat jaringan, dan penerima menjalankan fungsi dekripsi (*decryption*) untuk mendapatkan plaintext semula.

f) Proses enkripsi/dekripsi

Proses ini tergantung pada kunci (key) rahasia yang hanya diketahui oleh pengirim dan penerima. Ketika kunci dan enkripsi ini digunakan, sulit bagi penyadap untuk mematahkan ciphertext, sehingga komunikasi data antara pengirim dan penerima aman.

2) Password

Akun administrator pada suatu server sebaiknya diubah namanya dan sebaiknya hanya satu akun saja yang dapat mengakses. Untuk melakukan pengujian password yang dibuat. Ada utilitas yang dapat digunakan untuk mengetes kehandalan password, yaitu dengan menggunakan software seperti avior yang bertujuan untuk melakukan *brute-force password*.

3) Memonitor jaringan

Untuk meminimalisir penyerangan terhadap keamanan jaringan, hal yang dapat dilakukan administrator dalam memonitoring jaringan sebaiknya adalah dengan membatasi user yang dapat melakukan full-access kedalam suatu server.

Cara paling sederhana adalah dengan memberlakukan wewenang read only untuk semua user. Pemonitoran juga dapat dilakukan dengan melakukan pengauditan sistem log pada server tertentu oleh administrator jaringan.

Tujuannya adalah mengidentifikasi gangguan dan ancaman keamanan yang akan terjadi pada jaringan.

4) Penggunaan AntiVirus

Penggunaan AntiVirus merupakan hal ini yang paling penting. Antivirus yang akan mencegah berbagai macam virus komputer. Antivirus yang digunakan harus sesuai dengan spesifikasi pada jaringan komputer. Selain itu proses update antivirus harus dilakukan secara berkala agar antivirus dapat melakukan pendeteksian virus-virus baru secara efektif.

5) Update komputer

Pentingnya untuk selalu mengupdate apapun demi keamanan komputer. Bukan hanya antivirus saja yang perlu diupdate melainkan *operating system*, *software* yang terinstal, serta driver perlu dilakukan proses update.

b. Pengamanan saluran terbuka

Protokol TCP/IP merupakan protocol dalam set standar yang terbuka dalam pengiriman data, untuk itulah perlu dilakukan enkripsi dalam rangka penanganan keamanan data yang diterapkan pada protocol tersebut, yang meliputi:

1) Keamanan pada lapisan aplikasi

a) SET (*Secure Electronics Transaction*)

(1) Menentukan bagaimana transaksi mengalir antara pemakai, pedagang dan bank.
(2) Menentukan fungsi keamanan: digital signature, hash dan enkripsi.
(3) Produk dari Mastercard dan VISA International.

b) Secure HTTP

(1) Produk dari workgroup IETF, diimplementasikan pada webserver mulai 1995.
(2) Menentukan mekanisme kriptografi standar untuk mengenkripsikan pengiriman data http.

c) *Pretty Good Privacy* (PGP)

(1) Standarisasi RFC 1991

(2) Membuat dan memastikan digital signature, mengenkripsi--deskripsi dan mengkompresi data.

d) *Secure MIME* (S/MIME)

(1) Standarisasi RFC 1521.
(2) MIME (*Multipurpose Internet Mail Extension*).
(3) Menentukan cara menempelkan file untuk dikirim ke internet dengan menggunakan.
(4) Metode hirarki dalm pendefenisian user remi dan sertfikat digitalnya.

e) *Cybercash*

(1) Standarisasi RFC 1898.
(2) Memproses kartu kredit di internet dengan mengenkripsi dan menandatangani transaksi secara digital.

2) Keamanan dalam lapisan transport

Secure Socket Layer (SSL) yang meliputi:

a) Produk *netscape*
b) *Protocol* yang menegoisasikan hubungan yang aman antara client dan server, dengan
c) menggunakan kunci enkripsi 40-bit.

3) Keamanan dalam lapisan *network*

a) *IP security Protocol*: melindungi *protocol client IP* pada *network* layer.
b) *IP Authentication header.*

(1) *IP Encapsulating Security protocol.*
(2) *Simple-key management for Internet protocol* (SKIP).
(3) *Internet security Association and key management protocol* (ISAKMP).

c) *Internet key management protocol* (IKMP).

c. Penanggulangan resiko

Untuk menanggulangi resiko (*Risk*) tersebut dilakukan apa yang disebut countermeasures" yang dapat berupa:

1) Usaha untuk mengurangi *threat*;
2) Usaha untuk mengurangi *vulnerabilit;*
3) Usaha untuk mengurangi impak (*impact*);
4) Mendeteksi kejadian yang tidak bersahabat (*hostile event*);
5) Kembali (*recover*) dari kejadian.

POKOK BAHASAN 2

GANGGUAN DAN ANCAMAN SISTEM KEAMANAN TEKNOLOGI INFORMASI

1. Jenis Gangguan Sistem Keamanan TI

a. *Hacking*, berupa pengrusakan pada infrastruktur jaringan yang sudah ada, misalnya pengrusakan pada sistem dari suatu server.
b. *Physing*, berupa pemalsuan terhadap data resmi dilakukan untuk hal yang berkaitan dengan pemanfaataanya.
c. *Deface*, perubahan terhadap tampilan suatu website secara illegal. *Carding*, pencurian data terhadap identitas perbankan seseorang, misalnya pencurian nomor kartu kredit, digunakan untuk memanfaatkan saldo yang terdapat pada rekening tersebut untuk keperluan belanja online.
d. *Carding*, pencurian data terhadap identitas perbankan seseorang, misalnya pencurian nomor kartu kredit, digunakan untuk memanfaatkan saldo yang terdapat pada rekening tersebut untuk keperluan belanja online.

2. Ancaman dan Serangan Terhadap Sistem Keamanan TI

a. Serangan fisik terhadap keamanan jaringan.
b. Terjadi gangguan pada kabel.
c. Kerusakan harddisk.
d. Konsleting.
e. Data tak tersalur dengan baik.
f. Koneksi tak terdeteksi.
g. Akses bukan pengguna.
h. Serangan logik terhadap keamanan jaringan.
i. SQL Injection adalah hacking pada sistem komputer dengan mendapat akses basis data pada sistem.
j. DoS (*Denial of Service*) adalah Serangan pada Sistem dengan mengabiskan Resource pada Sistem.
k. Request *Flooding* adalah serangan dengan membanjiri banyak request pada sistem yang dilayani host sehingga request banyak dari pengguna tak terdaftar dilayani oleh layanan tersebut.
l. *Deface* adalah adalah serangan pada perubahan tampilan.
m. *Social Engineering* adalah serangan pada sisi sosial dengan memanfaatkan kepercayaan pengguna. hal ini seperti fake login hingga memanfaatkan kelemahan pengguna dalam social media.

n. *Malicious Code* adalah serangan dengan menggunakan kode berbahaya dengan menyisipkan virus, worm atau trojan horse.

o. *Packet Sniffer* adalah serangan menangkap paket yang lewat dalam sebuah jaringan.

3. Jenis-jenis Serangan Sistem Keamanan TI

Scanning adalah metode bagaimana caranya mendapatkan informasi sebanyak-banyaknya dari IP/Network korban. Biasanya scanning dijalankan secara otomatis mengingat scanning pada multiple-host sangat menyita waktu. Hackers biasanya mengumpulkan informasi dari hasil scanning ini.

Dengan mengumpulkan informasi yang dibutuhkan maka hackers dapat menyiapkan serangan yang akan dilancarkannya. Nmap adalah sebuah network scanner yang banyak digunakan oleh para professional di bidang network security, walaupun ada tool khusus dibuat untuk tujuan hacking, tetap belum dapat mengalahkan kepopuleran Nmap. Nessus juga merupakan network scanner tapi dapat melaporkan apabila terdapat celah keamanan pada target yang diperiksanya. Hacker biasanya menggunakan Nessus untuk pengumpulan informasi sebelum benar-benar meluncurkan serangan.

Untungnya beberapa scanner meninggalkan jejak unik yang memungkinkan para *System Administrator* untuk mengetahui bahwa sistem mereka telah di-scanning sehingga mereka bisa segera membaca artikel terbaru yang berhubungan dengan informasi log.

a. *Password cracking*

Brute-force adalah sebuah teknik di mana akan dicobakan semua kemungkinan kata kunci (password) untuk bisa ditebak untuk akses ke dalam sebuah sistem. Membongkar kata kunci dengan teknik ini sangat lambat tapi efisien, semua kata kunci dapat ditebak asalkan waktu tersedia. Membalikkan hash pada kata kunci merupakan hal yang mustahil, tapi ada beberapa cara untuk membongkar kata kunci tersebut walaupun tingkat keberhasilannya tergantung dari kuat-lemahnya pemilihan kata kunci oleh pengguna. Bila seseorang dapat mengambil data hash yang menyimpan kata kunci, cara yang lumayan efisien adalah menggunakan metode dictionary attack yang dapat dilakukan oleh utility John The Ripper.

b. *Rootkit*

Rootkit adalah alat untuk menghilangkan jejak apabila telah dilakukan penyusupan Rootkit biasanya mengikutkan beberapa tool yang dipakai oleh sistem dengan sudah dimodifikasi sehingga dapat menutupi jejak. Sebagai contoh,

memodifikasi PS di Linux atau Unix sehingga tidak dapat melihat background process yang berjalan.

4. Perusak Sistem Keamanan TI

a. *Hacker and cracker*

Hacker dengan keahliannya dapat melihat & memperbaiki kelemahan perangkat lunak di komputer; biasanya kemudian di publikasikan secara terbuka di Internet agar sistem menjadi lebih baik. Sialnya, segelintir manusia berhati jahat menggunakan informasi tersebut untuk kejahatan mereka biasanya disebut cracker.

b. *Program bug*

Program biasa yang mempunyai kesalahan (bug) dalam pemrogramannya akibat keteledoran sang pembuat. Salah satu akibatnya adalah terjadinya hang.

5. Resiko Sistem Keamanan TI

Ada tiga komponen yang memberikan kontribusi kepada *risk*, yaitu *asset*, *vulnerabilities*, dan *threats*.

a. Assets (aset), terdiri dari *hardware*, *software*, dokumentasi, data, komunikasi, lingkungan, dan manusia.
b. Threats (ancaman), terdiri dari pemakai (*users*), *teroris*, kecelakaan (*accidents*), *crackers*, penjahat kriminal, nasib (*acts of God*), intel luar negeri (*foreign intelligence*)
c. *Vulnerabilities* (kelemahan), terdiri dari *software bugs*, *hardware bugs*, radiasi (dari layar, transmisi), *tapping*, *crosstalk*, *unauthorized users*, cetakan, *hardcopy* atau *print out*, keteledoran (*oversight*), *cracker* via telepon, dan *storage* media.

6. Kerentanan Sistem Keamanan TI

Jaringan komputer adalah sebuah kumpulan komputer, printer dan peralatan lainnya yang terhubung dalam satu kesatuan. Informasi dan data bergerak melalui kabel-kabel atau tanpa kabel sehingga memungkinkan pengguna jaringan komputer dapat saling bertukar dokumen dan data, mencetak pada printer yang sama dan bersama-sama menggunakan *hardware/software* yang terhubung dengan jaringan. Setiap komputer, printer atau periferal yang terhubung dengan jaringan disebut node. Sebuah jaringan komputer dapat memiliki dua, puluhan, ribuan atau bahkan jutaan node

Beberapa titik rentan yang sering terjadi pada jaringan IT adalah sebagai berikut:

a. *Weak protocols*

Komunikasi jaringan komputer menggunakan protokol antara client dan server. Kebanyakan dari protokol yang digunakan saat ini merupakan protocol yang telah digunakan beberapa dasawarsa belakangan. Protokol lama ini, seperti File *Transmission Protocol* (FTP), TFTP ataupun telnet, tidak didesain untuk menjadi benar-benar aman. Malahan faktanya kebanyakan dari protokol ini sudah seharusnya digantikan dengan protokol yang jauh lebih aman, dikarenakan banyak titik rawan yang dapat menyebabkan pengguna yang tidak bertanggung jawab dapat melakukan eksploitasi. Sebagai contoh, seseorang dengan mudah dapat mengawasi *traffic* dari telnet dan dapat mencari tahu nama *user* dan *password*.

b. *Software issue*

Menjadi sesuatu yang mudah untuk melakukan eksploitasi celah pada perangkat lunak. Celah ini biasanya tidak secara sengaja dibuat tapi kebanyakan semua orang mengalami kerugian dari kelemahan seperti ini. Celah ini biasanya dibakukan bahwa apapun yang dijalankan oleh root pasti mempunyai akses root, yaitu kemampuan untuk melakukan segalanya di dalam sistem tersebut. Eksploitasi yang sebenarnya mengambil keuntungan dari lemahnya penanganan data yang tidak diduga oleh pengguna, sebagai contoh, *buffer overflow* dari celah keamanan format string merupakan hal yang biasa saat ini. Eksploitasi terhadap celah tersebut akan menuju kepada situasi di mana hak akses pengguna akan dapat dinaikkan ke tingkat akses yang lebih tinggi. Ini disebut juga dengan rooting sebuah host dikarenakan penyerang biasanya membidik untuk mendapatkan hak akses *root*.

c. *Buffer overflow*

"*Buffer overflow*" mempunyai arti sama dengan istilahnya. Programmer telah mengalokasikan sekian besar memory untuk beberapa variabel spesifik. Bagaimanapun juga, dengan celah keamanan ini, variabel ini dapat dipaksa menuliskan ke dalam stack tanpa harus melakukan pengecekan kembali bila panjang variabel tersebut diizinkan. Jika data yang berada di dalam buffer ternyata lebih panjang daripada yang diharapkan, kemungkinan akan melakukan penulisan kembali stack frame dari return address sehingga alamat dari proses eksekusi program dapat dirubah. Penulis *malicious code* biasanya akan akan melakukan eksploitasi terhadap penulisan kembali *return address* dengan merubah

return address kepada *shell code* pilihan mereka sendiri untuk melakukan pembatalan akses shell dengan menggunakan hak akses dari *user-id* dari program yang tereksploitasi tersebut. *Shell code* ini tidak harus disertakan dalam program yang tereksploitasi, tetapi biasanya dituliskan ke dalam bagian celah dari buffer. Ini merupakan trik yang biasa digunakan pada *variabel environment* seperti ini. *Buffer overflow* adalah masalah fundamental berdasarkan dari arsitektur komputasi modern. Ruang untuk variabel dan kode itu sendiri tidak dapat dipisahkan ke dalam blok yang berbeda di dalam memory. Sebuah perubahan di dalam arsitektur dapat dengan mudah menyelesaikan masalah ini, tapi perubahan bukan sesuatu yang mudah untuk dilakukan dikarenakan arsitektur yang digunakan saat ini sudah sangat banyak digunakan.

d. *Format string*

Celah *format string* tercipta karena kemalasan (*laziness*), ketidakpedulian (*ignorance*), atau *programmer* yang mempunyai skill pas-pasan. Celah format string biasanya disebabkan oleh kurangnya format string seperti %s di beberapa bagian dari program yang menciptakan output, sebagai contoh fungsi printf() di C/C++. Bila input diberikan dengan melewatkan format string seperti %d dan %s kepada program, dengan mudah melihat *stack dump* atau penggunaan teknik seperti pada *buffer overflow*. Celah ini berdasarkan pada truncated *format string* dari *input*. Ini merujuk kepada situasi di mana secara external, data yang disuplai yang diinterpretasikan sebagai bagian dari format *string argument*, secara khusus membuat suatu input dapat menyebabkan program yang bermasalah menunjukkan isi memory dan juga kontrol kepada eksekusi program dengan menuliskan apa saja kepada lokasi pilihan sama seperti pada eksploitasi *overflow*.

e. *Hardware issue*

Biasanya perangkat keras tidak mempunyai masalah pada penyerangan yang terjadi. Perangkat lunak yang dijalankan oleh perangkat keras dan kemungkinan kurangnya dokumentasi spesifikasi teknis merupakan suatu titik lemah. Misconfiguration Kesalahan konfigurasi pada server dan perangkat keras (*hardware*) sangat sering membuat para penyusup dapat masuk ke dalam suatu sistem dengan mudah. Sebagai contoh, penggantian halaman depan suatu situs karena kesalahan konfigurasi pada perangkat lunak www-server atapun modulnya. Konfigurasi yang tidak hati-hati dapat menyebabkan usaha penyusupan menjadi jauh lebih mudah terlebih jika ada pilihan lain yang dapat diambil oleh para penyusup. Sebagai contoh, sebuah server yang

menjalankan beberapa layanan SSH dapat dengan mudah disusupi apabila mengijinkan penggunaan protokol versi 1 atau remote root login (RLOGIN).
Kesalahan konfigurasi yang jelas ini menyebabkan terbukanya celah keamanan dengan penggunaan protokol versi 1, seperti *buffer overflow* yang dapat menyebabkan penyusup dapat mengambil hak akses root atau dengan menggunakan metode brute-force password untuk dapat menebak password root.

f. DoS, DDoS

Serangan Denial of Service (DoS) adalah serangan yang mengakibatkan setiap korbannya akan berhenti merespon atau berlaku tidak lazim. Contoh serangan klasik DoS adalah Ping of Death dan Syn Flood yang untungnya sudah hampir tidak dapat dijumpai pada saat sekarang. Biasanya serangan DoS menyerang celah yang terdapat pada layanan sistem atau pada protokol jaringan kerja untuk menyebabkan layanan tidak dapat digunakan. Teknik yang lainnya adalah menyebabkan system korban tersedak dikarenakan banyaknya paket yang diterima yang harus diproses melebihi kemampuan dari sistem itu sendiri atau menyebabkan terjadinya bottleneck pada bandwidth yang dipakai oleh sistem. Serangan Distributed Denial of Service (DDoS) merupakan tipe serangan yang lebih terorganisasi. Jenis serangan ini biasanya membutuhkan persiapan dan juga taktik untuk dapat menjatuhkan korbannya dengan cepat dan sebelumnya biasanya para penyerang akan mencari system kecil yang dapat dikuasai. Setelah mendapat banyak sistem kecil, penyerang akan menyerang system yang besar dengan menjalankan ribuan bahkan puluhan ribu sistem kecil secara bersamaan untuk menjatuhkan sebuah sistem besar.

g. Virus

Salah satu definisi dari program virus adalah menyisipkan dirinya kepada objek lain seperti file *executable* dan beberapa jenis dokumen yang banyak dipakai orang. Selain kemampuan untuk mereplikasi dirinya sendiri, virus dapat menyimpan dan menjalankan sebuah tugas spesifik. Tugas tersebut bisa bersifat menghancurkan atau sekedar menampilkan sesuatu ke layar monitor korban dan bisa saja bertugas untuk mencari suatu jenis file untuk dikirimkan secara acak ke internet bahkan dapat melakukan format pada hard disk korban. Virus yang tersebar di internet dan belum dikenali tidak akan dapat ditangkap oleh program antivirus ataupun semacamnya, sehingga apabila korban telah terjangkit, tetap tidak mengetahuinya. Perangkat lunak antivirus biasanya mengenali virus atau calon virus melalui

tanda yang spesifik yang terdapat pada bagian inti virus itu sendiri. Beberapa virus menggunakan teknik polymorphic agar luput terdeteksi oleh antivirus. Kebiasaan virus *polymorphic* adalah merubah dirinya pada setiap infeksi yang terjadi yang menyebabkan pendeteksian menjadi jauh lebih sulit. Praktisnya setiap *platform* komputer mempunyai virus masing-masing dan ada beberapa virus yang mempunyai kemampuan menjangkiti beberapa platform yang berbeda (*multi-platform*). Virus multi-platform biasanya menyerang *executable* ataupun dokumen pada Windows dikarenakan kepopuleran oleh sistem operasi Microsoft Windows dan Microsoft Office sehingga banyak ditemukan virus yang bertujuan untuk menghancurkan kerajaan Microsoft Corp.
Secara garis beras kriteria virus yaitu memiliki kemampuan untuk mendapatkan informasi, memeriksa suatu file, menggandakan diri dan menularkan diri, melakukan manipulasi, serta menyembunyikan diri. Adapun jenis jenis virus antara lain *Virus Boot Sector / Boot Record / Partisi, Virus File, Virus Hybrid, Virus FAT, Virus Macro*. Sedangkan siklus hidup virus sebagai berikut:

1) *Dormant phase* (fase istirahat/tidur).
2) *Propagation phase* (fase penyebaran).
3) *Trigerring phase* (fase aktif).
4) *Execution phase* (fase eksekusi).

Cara penyebaran virus dapat melalui disket, media storage yang lain, jaringan (LAN, WAN, dsb), WWW (internet) serta *Software* yang *Freeware*, *Shareware* atau bahkan Bajakan. Adapun langkah-langkah yang dapat dilakukan untuk pencegahan virus sebagai berikut:

1) Gunakan antivirus yang anda percayai dengan update terbaru.
2) Selalu scanning semua media penyimpanan eksternal yang akan digunakan, mungkin hal ini agak merepotkan tetapi jika auto-protect antivirus anda bekerja maka prosedur ini dapat dilewatkan.
3) Jangan biarkan sembarang orang untuk memakai komputer Anda.
4) Jika anda terhubung langsung ke Internet cobalah untuk mengkombinasikan antivirus anda dengan Firewall, Anti-spamming, dsb.
5) Selalu waspada terhadap fle-file yang mencurigakan, contoh: file dengan 2 buah exstension atau file executable yang terlihat mencurigakan.
6) Untuk software freeware + shareware, ada baiknya anda mengambilnya dari situs resminya.

Sedangkan langkah-langkah yang dapat dilakukan apabila telah terinfeksi virus sebagai berikut:

1) Deteksi dan tentukan dimanakah kira-kira sumber virus tersebut apakah di disket, jaringan, email dsb. Jika anda terhubung ke jaringan maka ada baiknya anda mengisolasi komputer anda dulu (baik dengan melepas kabel atau mendisable sambungan internet dari control panel).
2) Identifikasi dan klasifikasikan jenis virus apa yang menyerang pc anda, dengan cara: Gejala yang timbul, misal: pesan, file yang corrupt atau hilang dsb; Scan dengan antivirus anda.
3) Bersihkan virus tersebut.
4) Langkah terburuk. Jika semua hal diatas tidak berhasil adalah memformat ulang komputer anda.

h. *Worms*

Sebuah worm komputer merupakan program yang menyebar sendiri dengan cara mengirimkan dirinya sendiri ke sistem yang lainnya. Worm tidak akan menyisipkan dirinya kepada objek lain. Pada saat sekarang banyak terjadi penyebaran Worm dikarenakan para pengguna komputer tidak melakukan update pada perangkat lunak yang mereka gunakan, sebagai contoh, *Outlook Express* mempunyai fungsi yang dapat mengizinkan eksekusi pada file sisipan (*attachment*) email tanpa campur tangan dari pengguna komputer itu sendiri.

RANGKUMAN

1. Sistem keamanan teknologi informasi adalah proses untuk mencegah & mengidentifikasi penggunaan yang tidak sah dari jaringan komputer. Sistem keamanan TI ini bertujuan untuk mengantisipasi resiko jaringan komputer berupa bentuk ancaman fisik maupun logik. Komponen sistem keamanan TI terdiri dari jenis-jenis jaringan, *Firewall* dan *Security Information* and *Event Management* (SIEM). Adapun prinsip-prinsip kerja sistem keamanan TI terdiri atas perencanaan sistem keamanan TI, pengamanan saluran terbuka serta penanggulangan resiko.

2. Hal-hal yang mengancam sistem keamanan teknologi informasi Polri terdiri dari jenis gangguan sistem keamanan TI, kemungkinan ancaman dan serangan terhadap sistem keamanan TI, jenis-jenis serangan yang sering terjadi melalui sistem keamanan TI, perusak sistem keamanan TI, kerentanan yang dapat terjadi pada sistem keamanan TI, serta program pengganggu dan perusak sistem keamanan TI.

SOAL LATIHAN

1. Jelaskan pengertian sistem keamanan TI!
2. Jelaskan tujuan sistem keamanan TI!
3. Jelaskan komponen-komponen sistem keamanan TI!
4. Jelaskan prinsip-prinsip kerja sistem keamanan TI!
5. Jelaskan jenis-jenis serangan yang sering terjadi melalui sistem keamanan TI!
6. Jelaskan program pengganggu dan perusak sistem keamanan TI.

MODUL 02	**INSTALASI, PENGOPERASIAN, DAN PERAWATAN SISTEM KEAMANAN TEKNOLOGI INFORMASI**
	36 JP (1620 menit)

PENGANTAR

Modul *data base* Polri membahas materi tentang: konsep *data base* Polri dan prosedur *keamanan* sistem *TI* (persiapan, pengoperasian, pengakhiran).

Tujuan adalah agar peserta pelatihan memahami dan terampil menginstalasi tool keamanan sistem TI dan mengoperasionalkan keamanan sistem TI.

KOMPETENSI DASAR

1. Memahami prosedur instalasi, pengoperasian, dan perawatan sistem keamanan TI Polri.

   Indikator Hasil Belajar:

   a. Menjelaskan prosedur instalasi sistem keamanan TI Polri.
   b. Menjelaskan prosedur pengoperasian sistem keamanan TI Polri.
   c. Menjelaskan prosedur perawatan sistem keamanan TI Polri.

2. Terampil melakukan instalasi, pengoperasian, dan perawatan sistem keamanan TI Polri.

   Indikator Hasil Belajar:

   a. Mempraktikan instalasi sistem keamanan TI Polri.
   b. Mempraktikan pengoperasian sistem keamanan TI Polri.
   c. Mempraktikan perawatan sistem keamanan TI Polri.

MATERI PELAJARAN

Pokok Bahasan:

Prosedur instalasi, pengoperasian, dan perawatan sistem keamanan TI Polri.

Subpokok Bahasan:

1. Prosedur instalasi sistem keamanan TI Polri.
2. Prosedur pengoperasian sistem keamanan TI Polri.
3. Prosedur perawatan sistem keamanan TI Polri.

METODE PEMBELAJARAN

1. **Metode Ceramah**

   Metode ini digunakan untuk menyampaikan materi tentang prosedur instalasi, pengoperasian, dan perawatan sistem keamanan TI Polri.

2. **Metode Tanya Jawab**

   Metode ini digunakan untuk memperdalam pemahaman materi tentang prosedur instalasi, pengoperasian, dan perawatan sistem keamanan TI Polri.

3. **Metode Praktik**

   Metode ini digunakan untuk mempraktikkan prosedur instalasi, pengoperasian, dan perawatan sistem keamanan TI Polri.

ALAT, MEDIA, BAHAN DAN SUMBER BELAJAR

1. **Alat, Media dan Bahan:**

   a. *White board*.
   b. Laptop.
   c. LCD.
   d. HVS.
   e. Alat tulis.
   f. Jaringan internet.

2. **Sumber Belajar**

   a. Peraturan Kapolri Nomor 1 tahun 2011 tentang Penyelenggaraan Sistem Telekomunikasi di Lingkungan Polri.

	b. Undang-undang Nomor 36 tahun 1999 tentang Telekomunikasi.

KEGIATAN PEMBELAJARAN

1. Tahap Awal: 10 menit

a. Pendidik melaksanakan apersepsi:

1) Pendidik melaksanakan perkenalan;
2) Pendidik menyampaikan tujuan pembelajaran dan menyampaikan tugas-tugas yang harus dilaksanakan peserta didik selama pembelajaran;
3) Pendidik menciptakan suasana pembelajaran yang kondusif.

b. Peserta didik menyimak, menanggapi dan melaksanakan instruksi pendidik.

2. Tahap Inti: 1.510 menit

Tahap inti 1: penyampaian materi (270 menit)

a. Pendidik menyampaikan materi tentang prosedur instalasi, pengoperasian dan perawatan sistem keamanan TI Polri.
b. Peserta didik menyimak, mencatat hal-hal yang penting.
c. Pendidik memberikan contoh pelaksanaan prosedur instalasi, operasional dan perawatan sistem keamanan TI Polri.
d. Pendidik memberikan kesempatan kepada peserta didik untuk bertanya hal-hal yang belum dipahami.
e. Peserta didik bertanya dan menanggapi materi yang disampaikan pendidik.

Tahap inti 2: praktik menginstal sistem keamanan teknologi informasi Polri (790 menit)

a. Pendidik membagi peserta didik menjadi beberapa kelompok, satu kelompok terdiri dari dua orang.
b. Pendidik menugaskan masing-masing kelompok untuk menginstal sistem keamanan TI Polri.
c. Pendidik memfasilitasi jalannya praktik.
d. Masing-masing kelompok mempraktikkan penginstalan sistem keamanan TI Polri.
e. Masing-masing kelompok membuat laporan hasil praktik dan ditanggapi oleh pendidik.
f. Pendidik memberikan tanggapan laporan hasil praktik masing-masing kelompok.
g. Peserta didik mengumpulkan laporan hasil praktik.

Tahap inti 3: praktik pengoperasian sistem keamanan TI Polri (270 menit)

a. Pendidik membagi peserta didik menjadi beberapa kelompok, satu kelompok terdiri dari dua orang.
b. Pendidik menugaskan masing-masing kelompok untuk mengoperasikan sistem keamanan TI Polri, yang terdiri dari:
   1) Mengoperasikan sistem keamanan TI *pantest*.
   2) Mengoperasikan sistem keamanan TI *monitoring*.
c. Pendidik memfasilitasi jalannya praktik.
d. Masing-masing kelompok mempraktikkan:
   1) Mengoperasikan sistem keamanan TI *pantest*.
   2) Mengoperasikan sistem keamanan TI monitoring.
e. Masing-masing kelompok membuat laporan hasil praktik dan ditanggapi oleh pendidik.
f. Pendidik memberikan tanggapan laporan hasil praktik masing-masing kelompok.
g. Peserta didik mengumpulkan laporan hasil praktik.

Tahap inti 4: praktik merawat sistem keamanan teknologi informasi Polri (180 menit) (4 jp)

a. Pendidik membagi peserta didik menjadi beberapa kelompok, satu kelompok terdiri dari dua orang.
b. Pendidik menugaskan masing-masing kelompok untuk merawat sistem keamanan TI Polri.
c. Pendidik memfasilitasi jalannya praktik.
d. Masing-masing kelompok mempraktikkan sistem perawatan keamanan TI Polri.
e. Masing-masing kelompok membuat laporan hasil praktik dan ditanggapi oleh pendidik.
f. Pendidik memberikan tanggapan laporan hasil praktik masing-masing kelompok.
g. Peserta didik mengumpulkan laporan hasil praktik.

3. Tahap Akhir: 10 menit

a. Pendidik memberikan kesimpulan materi prosedur instalasi, pengoperasian dan perawatan sistem keamanan TI Polri.
b. Pendidik mengecek penguasaan materi dengan cara bertanya secara lisan dan acak kepada peserta didik.
c. Pendidik melakukan evaluasi pembelajaran dan menutup pembelajaran.

4. Tes Capaian Kompetensi: 90 menit

Tes tertulis dalam bentuk objektif tes (pilihan ganda dan jawaban singkat) dan subjektif tes (uraian).

TAGIHAN/TUGAS

1. Peserta didik mengumpulkan tugas resume paling lama dua hari setelah pemberian materi.
2. Masing-masing kelompok mengumpulkan laporan hasil praktik berupa file atau program.

LEMBAR KEGIATAN

BAHAN BACAAN

POKOK BAHASAN

PROSEDUR INSTALASI, PENGOPERASIAN, DAN PERAWATAN SISTEM KEAMANAN TI POLRI

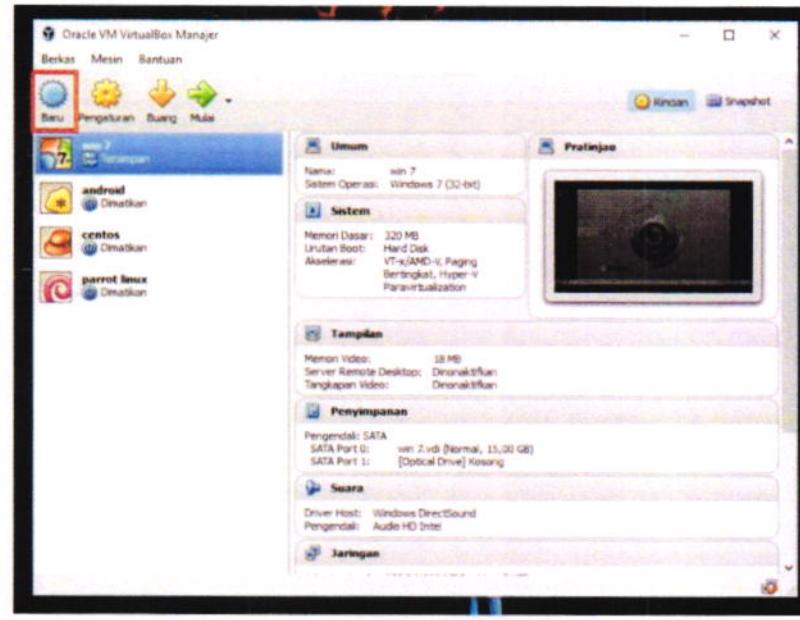
1. Prosedur Instalasi Sistem Keamanan TI Polri

Aplikasi Kali Linux 2.0 di VirtualBox merupakan salah satu distribusi/distro yang diciptakan khusus untuk penetrating dan keamanan terpopuler di dunia. Bagi yang mengenal Backtrack pasti sudah tidak asing pula dengan Kali Linux. Bisa di bilang Kali linux merupakan reinkarnasi/versi terbaru dari Backtrack.

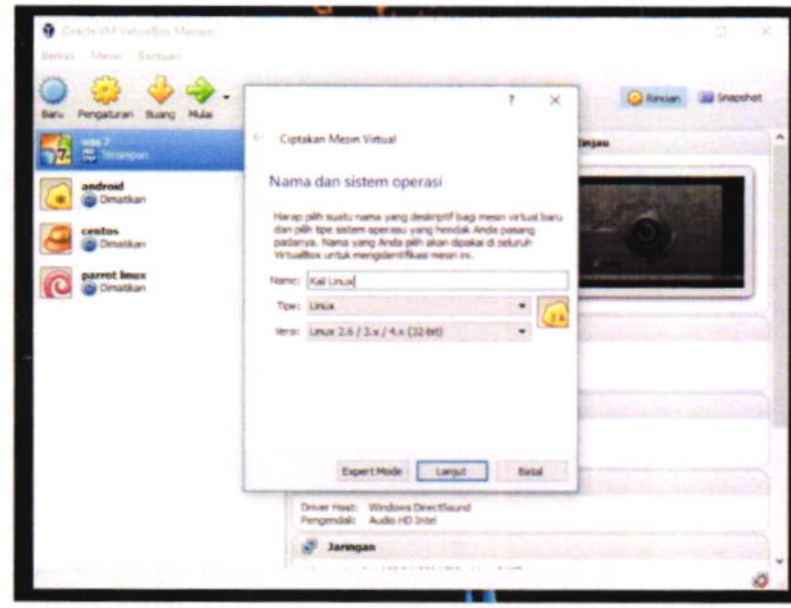
Adapun cara menginstall Kali Linux 2.0 di VirtualBox sebagai berikut:

a. Pertama, sebelum dapat mengintall kali linux, pastikan sudah mendownload kali linux dan sudah menginstal VirtualBox tentunya. dapat mendownloadnya di situs resmi Kali Linux: https://www.kali.org/downloads/

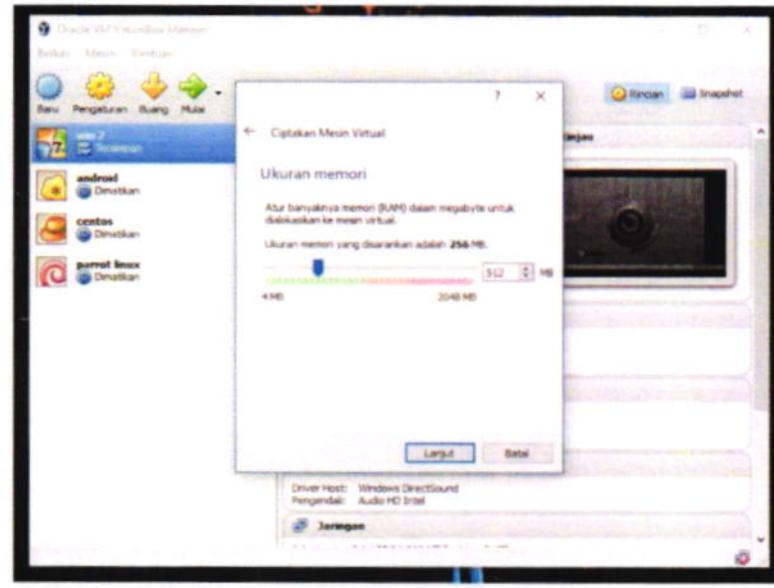
b. Buka VirtualBox. Karena akan menggunakan VirtualBox berbahasa Indonesia, tekan add untuk menambahkan komputer virtual.



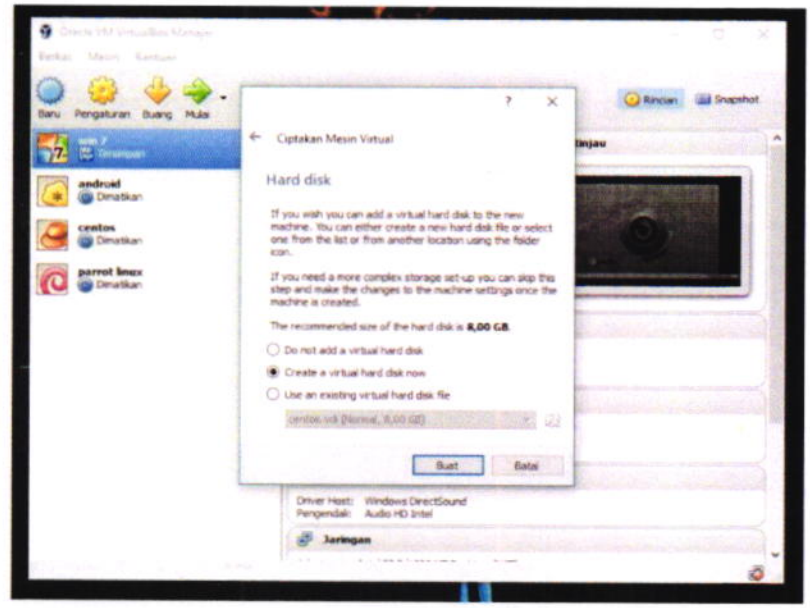
c. Kemudian isikan perintah seperti dibawah ini lalu tekan Lanjut.



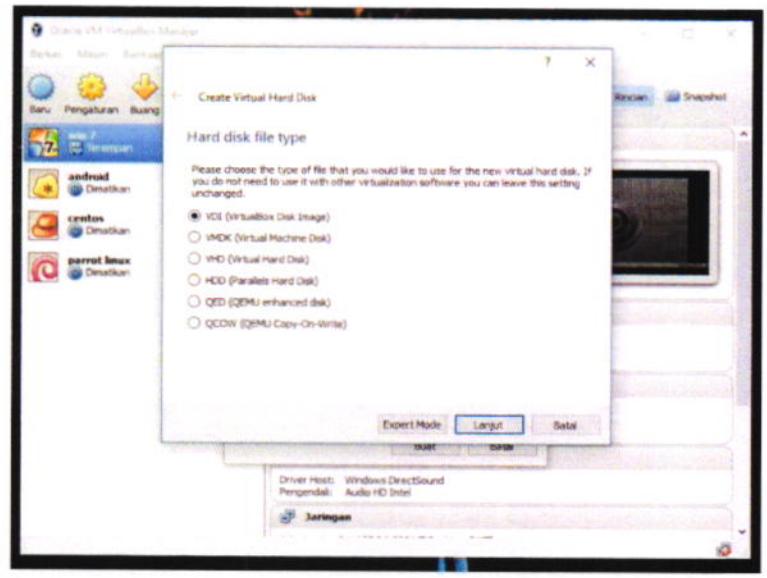
d. Setelah itu tentukan kapasitas RAM yang ingin pasang pada mesin virtual . Dalam kasus ini saya menggunakan kapasitas 512MB.



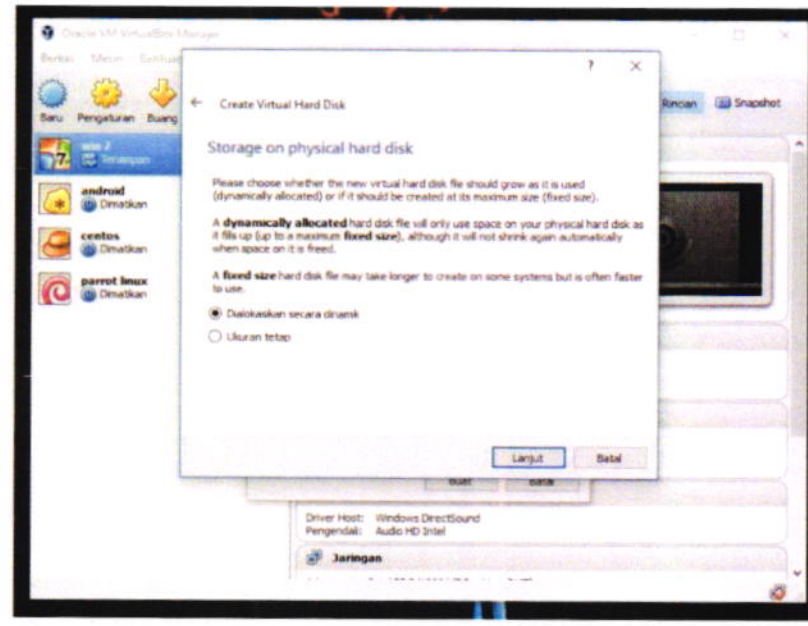
e. Lalu klik "Create a virtual hardisk now" dimana itu adalah tempat untuk menyimpan data (hardisk virtual) kali linux



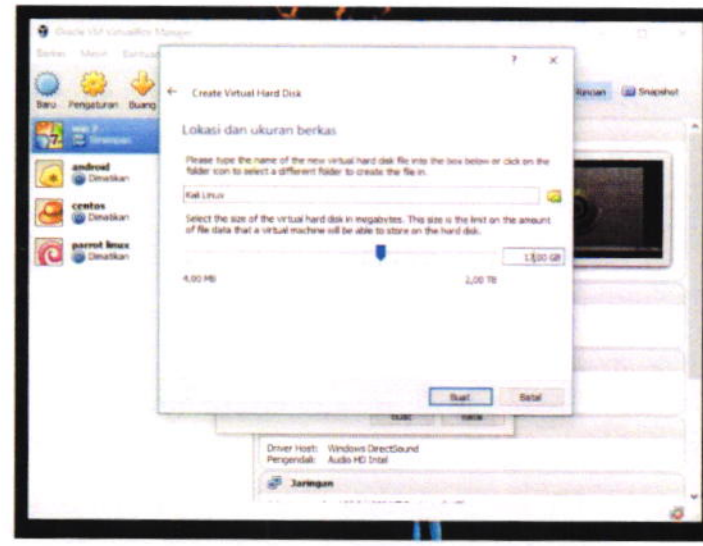
f. Selanjutnya akan diminta untuk memilih tipe hard drive. Pilih saja tipe VDI (VirtualBox Disk Image) agar tidak terlalu ribet nantinya.



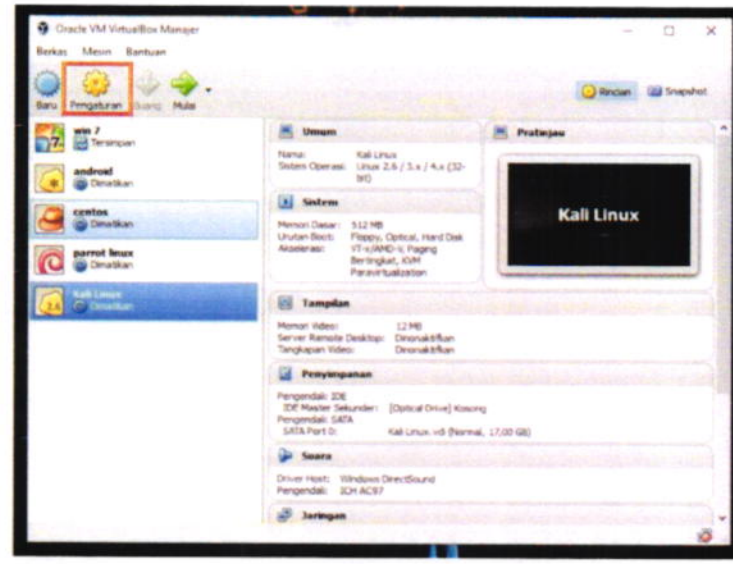
g. Lalu akan mendapati pilihan seperti dibawah ini. Untuk yang satu ini pilih "Dialokasikan secara dinamik" agar file tersebut dapat di ubah-ubah ukurannya.



h. Setelah itu akan diminta untuk mengisi besaran kapasitas Hardisk pada mesin virtual. Dalam kasus ini saya mengisi 17GB karena Kali linux membutuhkan resource setidaknya minimal 16GB

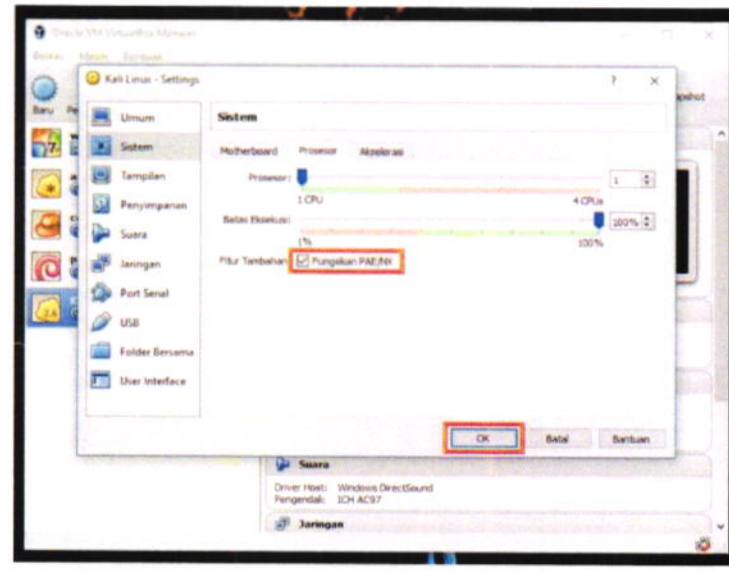


i. Selanjutnya klik pengaturan / setting.

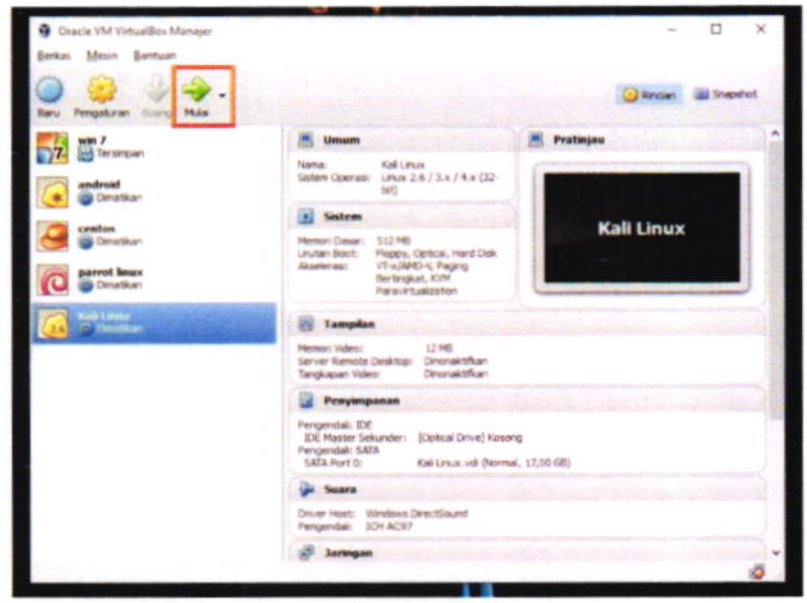


j. Kemudian klik pada sistem dan centang pada Fungsikan PAE/NX lalu tekan OK.

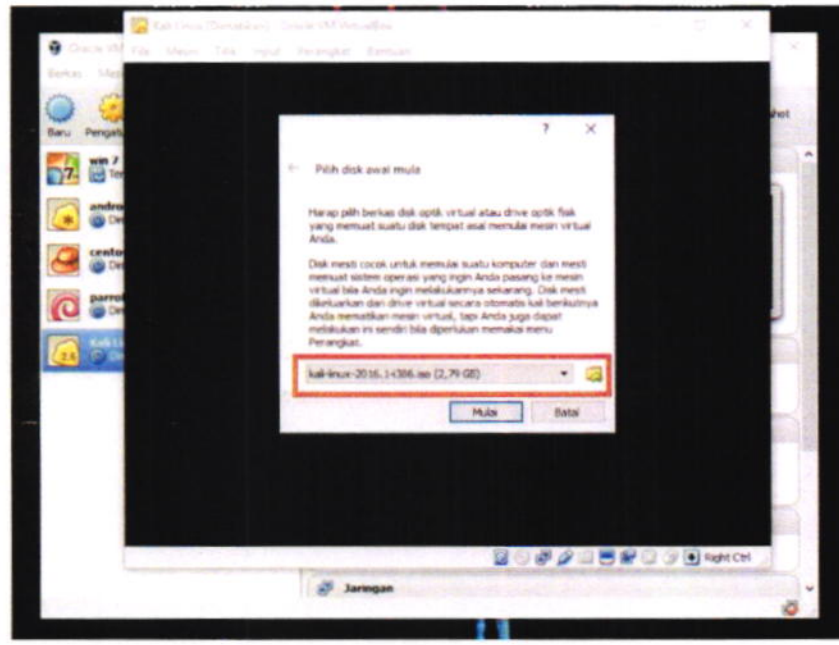
k. Kemudian klik pada sistem dan centang pada Fungsikan PAE/NX lalu tekan OK.



l. Pada tahap ini, semua setting pada virtualbox telah selesai, selanjutkan tekan "Mulai" untuk memulai instalasi.

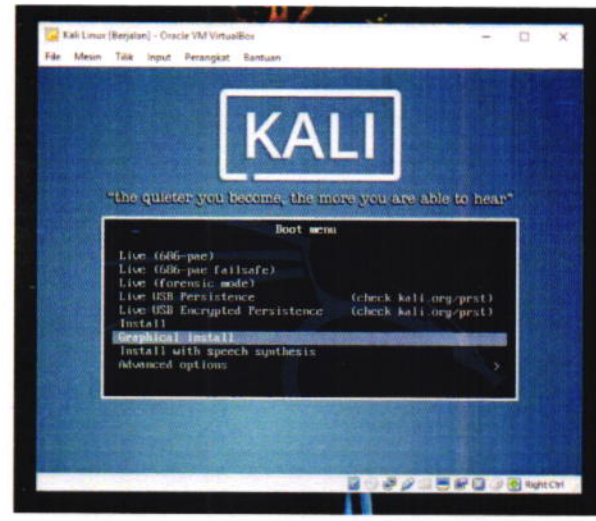


m. Setelah itu akan diminta untuk memasukkan iso kali linux yang sudah persiapkan diawal. Caranya klik Choose, kemudian browse file .iso Kali Kinux , kemudian klik Mulai!

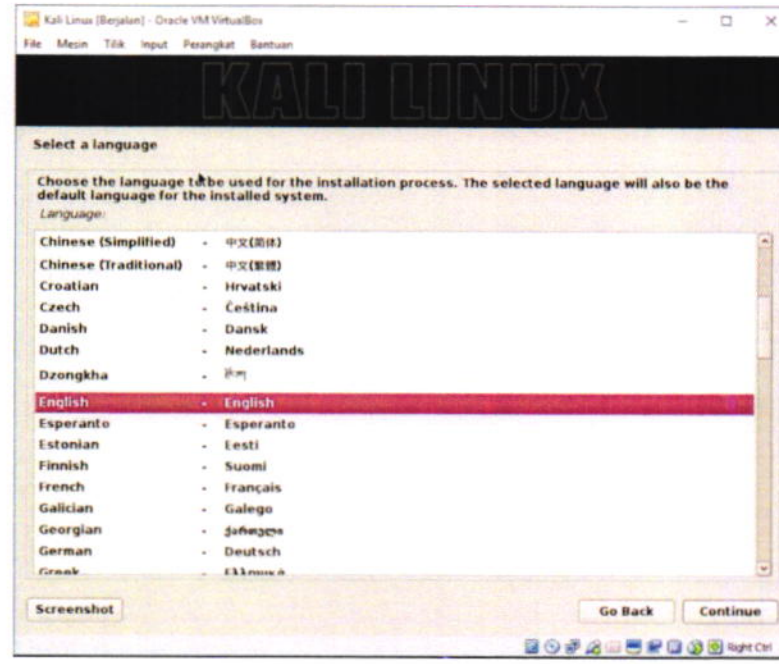


n. Setelah semua selesai, akan dihadapkan pada option seperti dibawah ini. Pada kasus ini saya menggunakan opsi Graphical Install.
Keterangan:

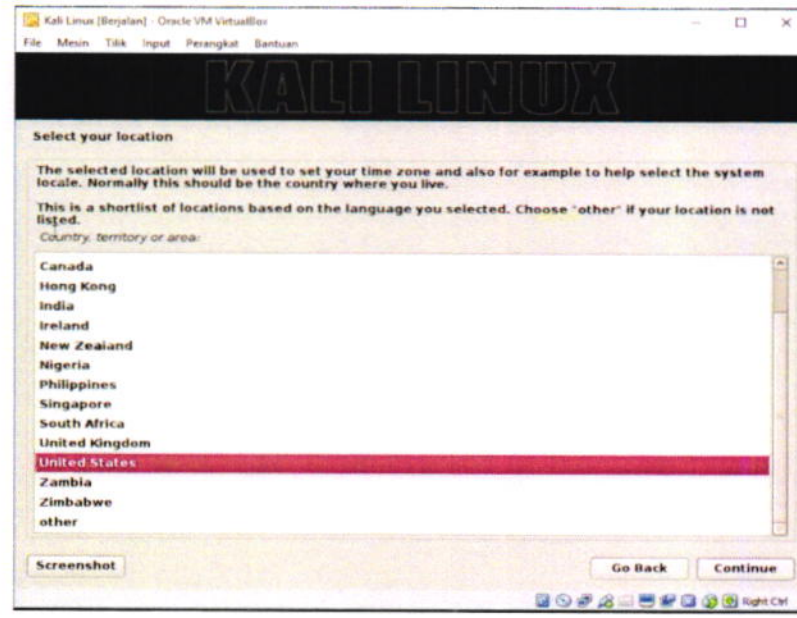
1) Live pae (686 pae): Untuk booting Kali linux tanpa harus menginstallnya.
2) Install: Untukmenginstall kali linux menggunakan modetext.
3) Graphical Install: Untuk menginstall kali linux menggunakan mode**Grafis**.



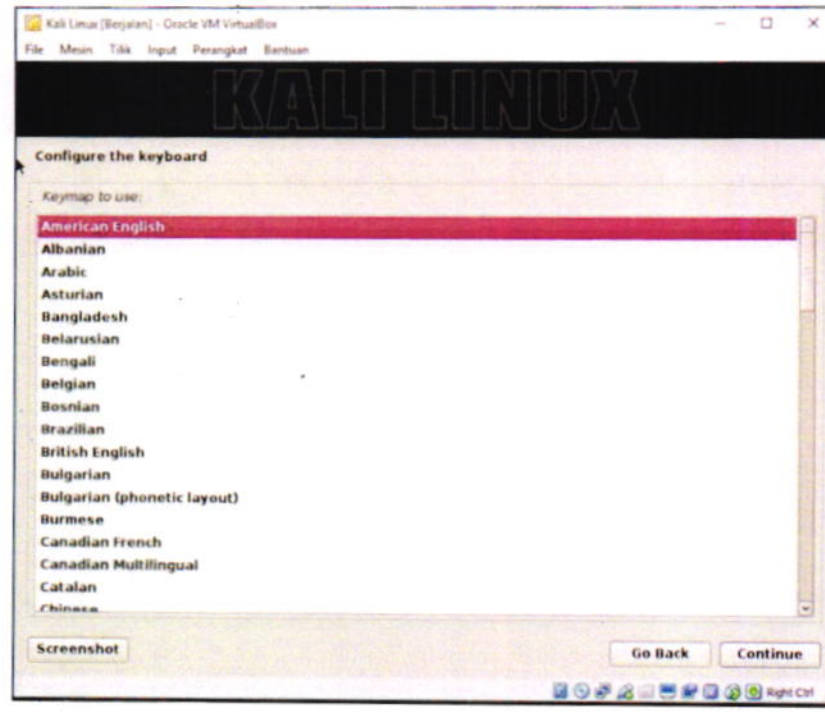
o. Lalu pilih bahasa yang ingin diinstal pada kali linux. Seperti biasa saya menggunakan bahasa default English tanpa ada perubahan.



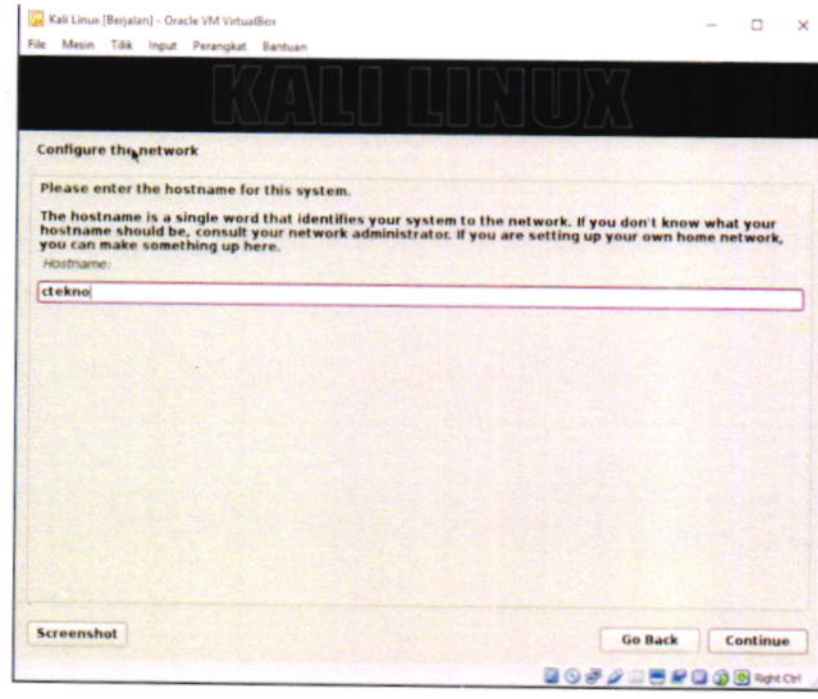
p. Selanjutnya pilih lokasi, disini saya menggunakan lokasi default tanpa ada perubahan.



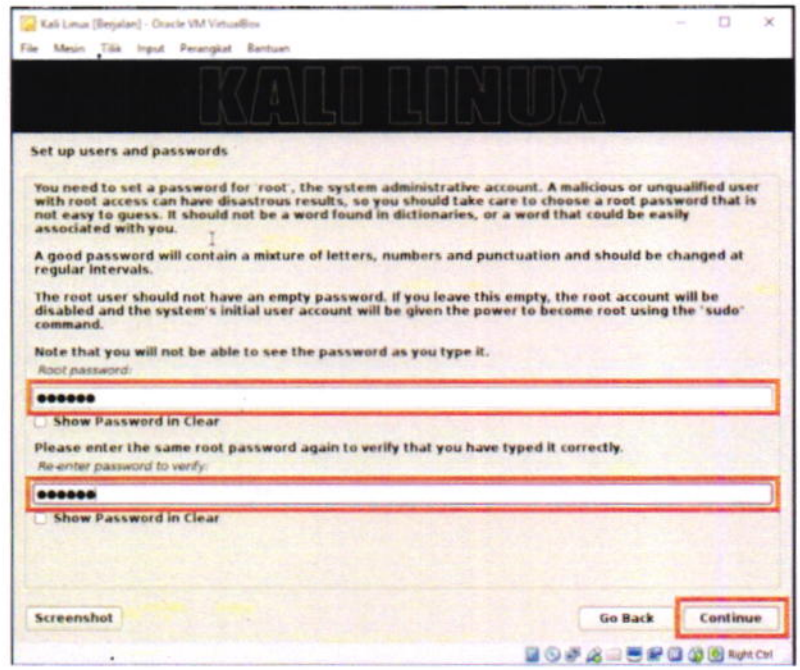
q. Berikutnya pilih keyboard untuk sistem Kali linux. Disini juga membiarkannya default.



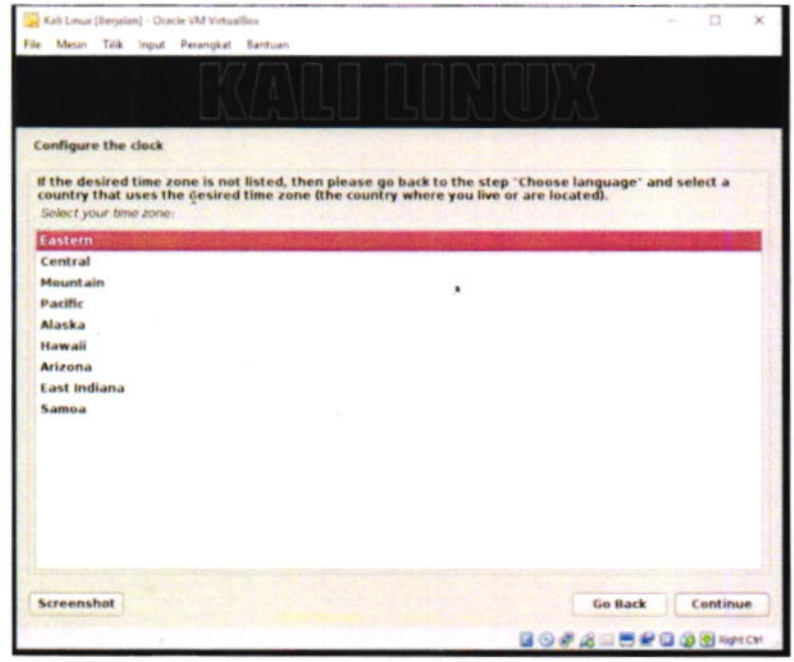
r. Lalu akan diminta untuk mengisi hostname. dapat membiarkan default atau mengisinya sesuka hatimu.



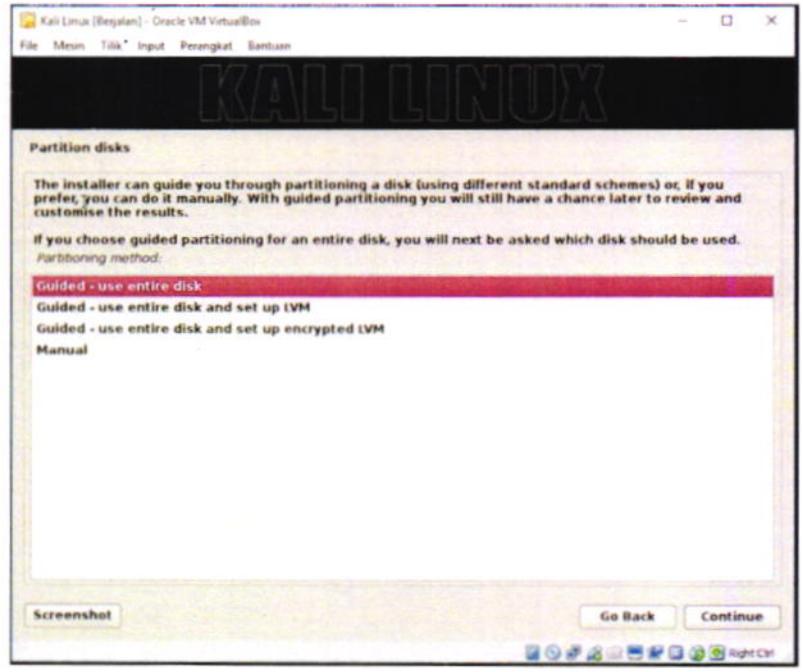
s. Selanjutnya pengisian password. Password inilah yang nanti akan kita gunakan untuk login di kali linux. Jadi sebaiknya pilih pasword yang mudah di ingat.



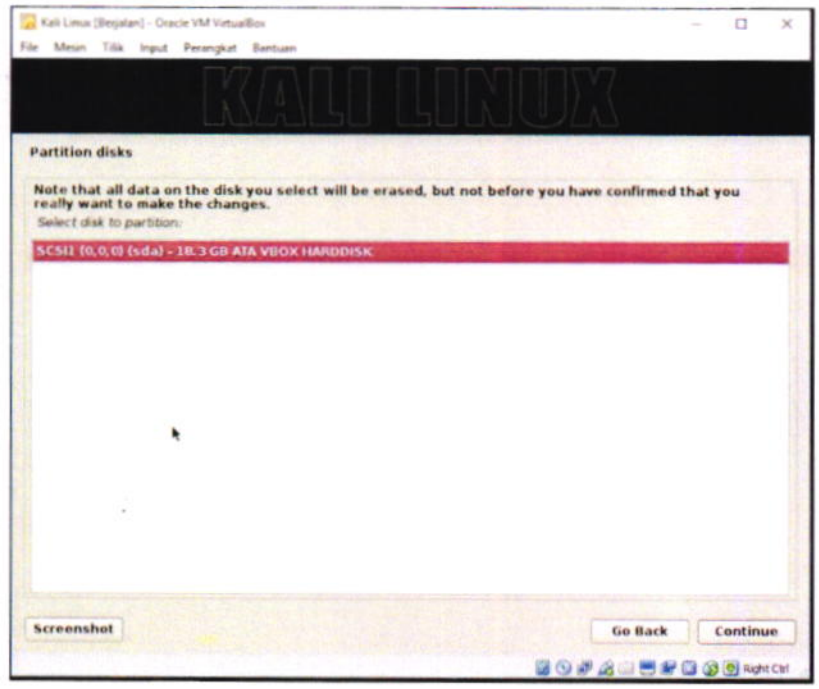
t. Lalu konfigurasi time



u. Berikutnya pilih "Guided - use entire disk" lalu tekan continue.

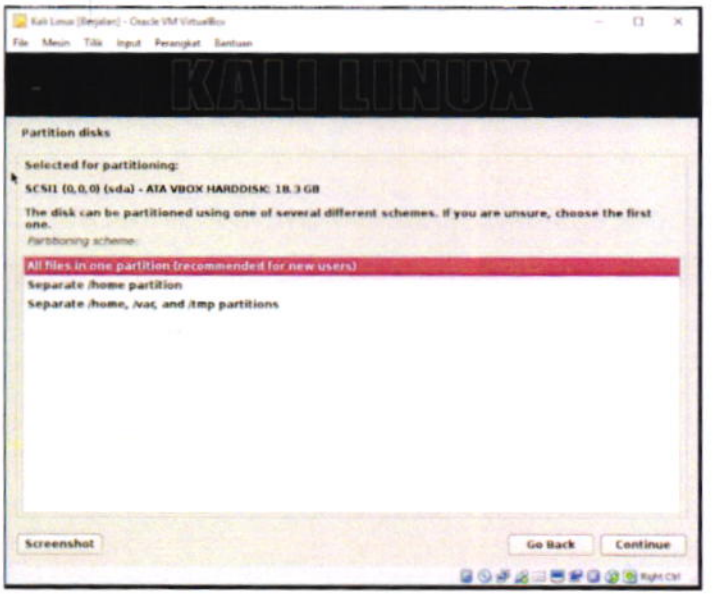


v. Selanjutnya pilih "ATA VBOX HARDISK" lalu tekan continue. Hardisk ini adalah hardisk dari settingan virtual box yang telah di buat tadi.

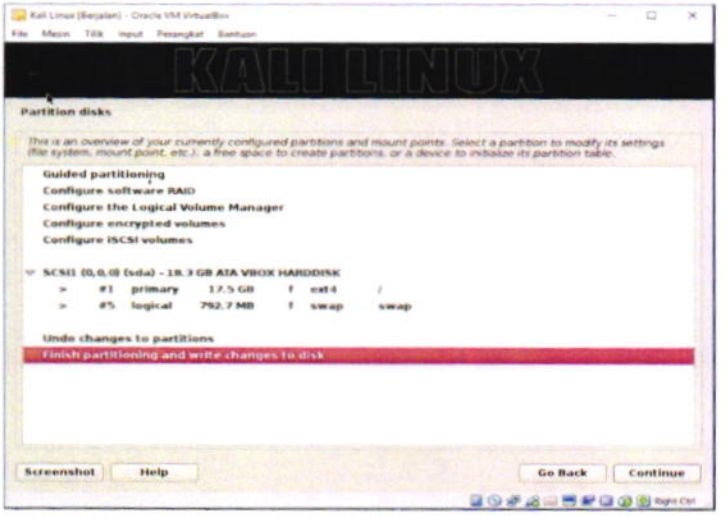


w. Selanjutnya akan dihadapkan 3 opsi partisi yang akan di gunakan untuk instalasi Kali linux. Keterangan:

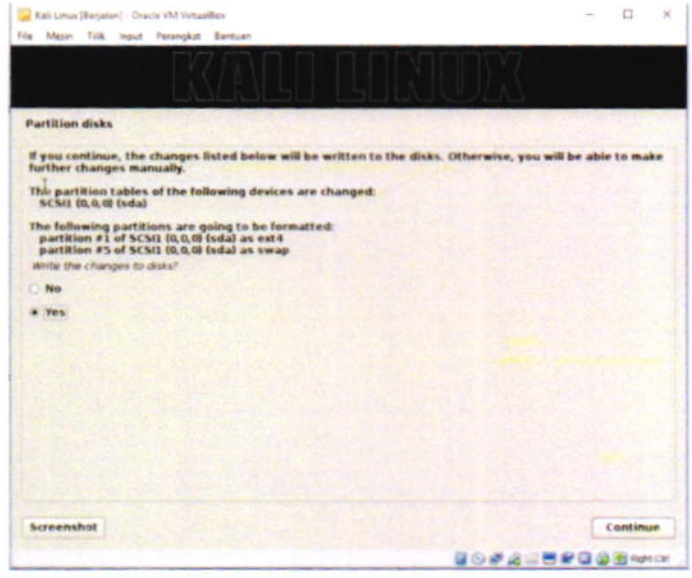
1) All files in one partition : untuk menginstal kali pada satu partisi
2) Separatee /home partition : untuk mengintsal kali dengan memisahkan partisi /home
3) Separatee /home, /var, and /tmp partitions : untuk mengintsal kali dengan memisahkan partisi /home, /var, and /tmp partitions.



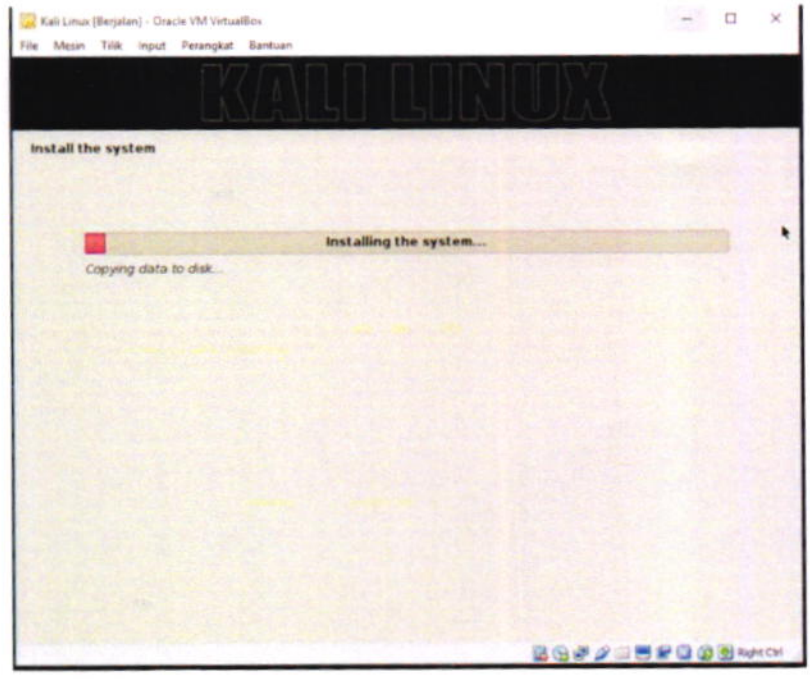
x. Selanjutnya tekan "Finish partitioning and write changes to disk" lalu tekan continue.



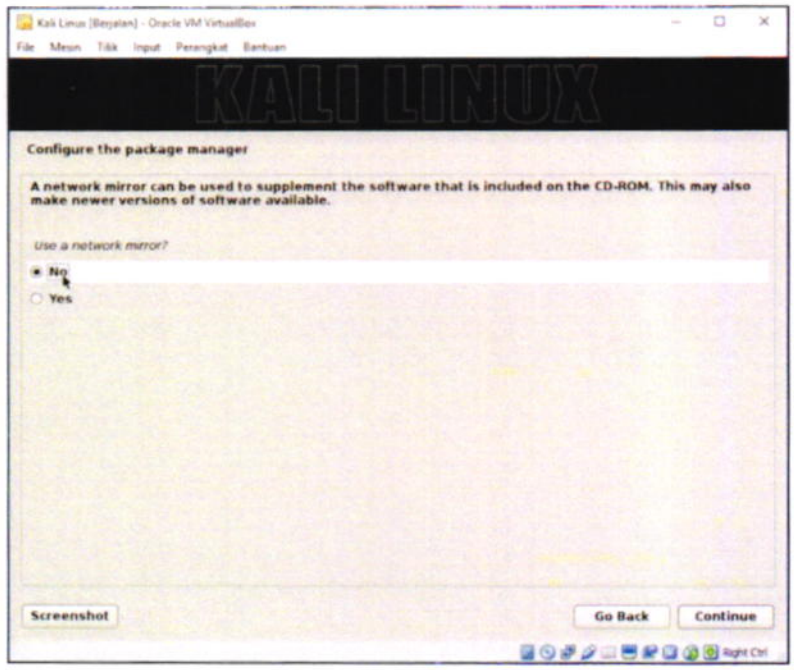
y. Lalu akan ditampilkan peringatan untuk memformat semua hardisk virtual. Klik yes lalu tekan continue.



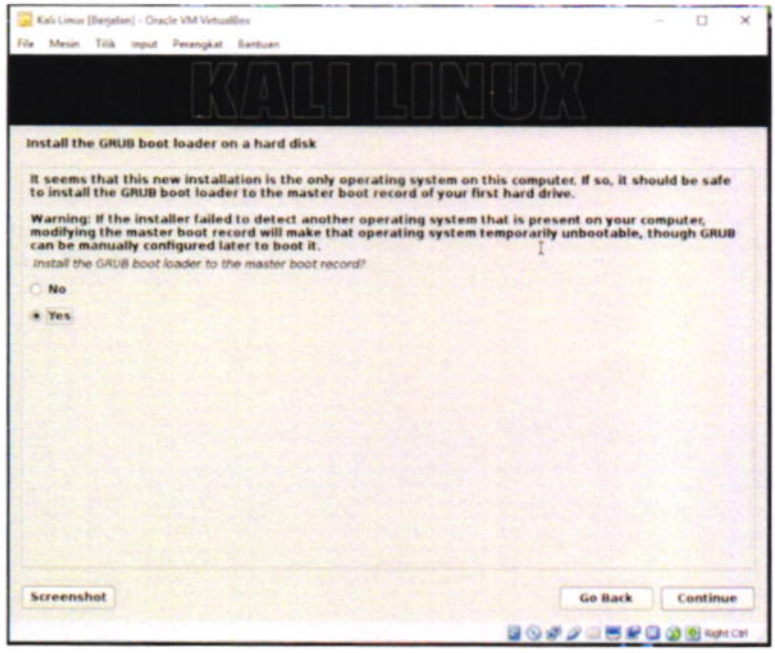
z. Selanjutnya adalah proses install system pada hardisk virtual dan tunggu hingga selesai.



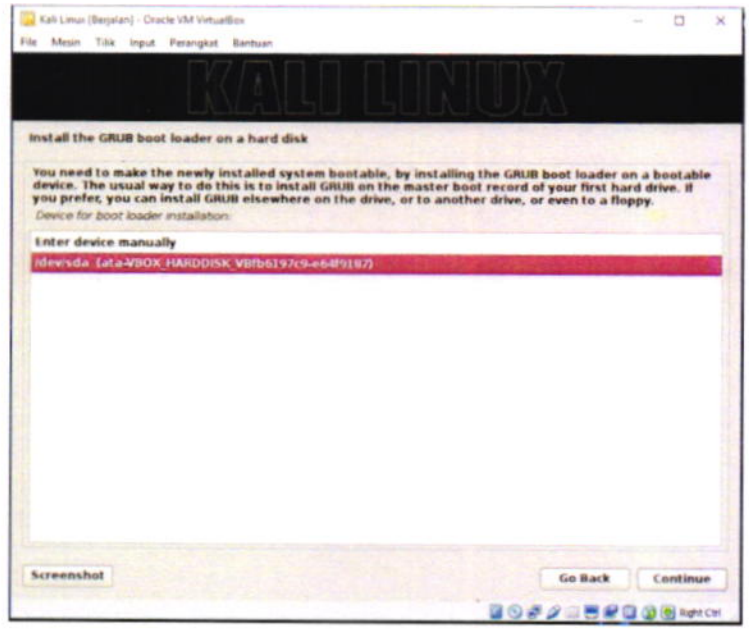
aa. Berikutnya akan mendapati notifikasi apakah ingin menginstal mirror.



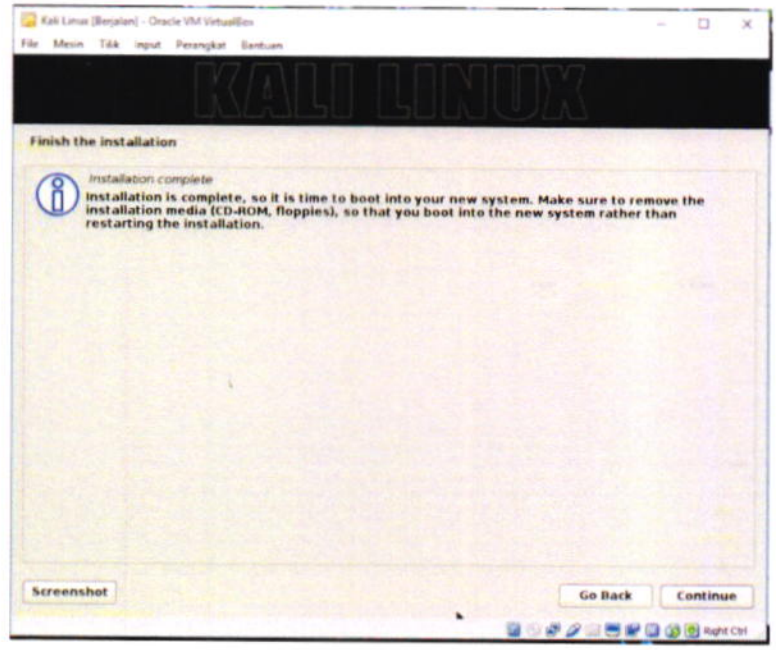
bb. Tunggu hingga proses selesai. Setelah itu akan ditanya lagi "Apakah ingin menginstal Grub boot loader." Pada Opsi ini pilih YES.



cc. Selanjutnya akan mendapat notifikasi "dimana ingin menginstal grub loader?" Pilih saja /dev/sda (ata-VBOX_HARDISK).



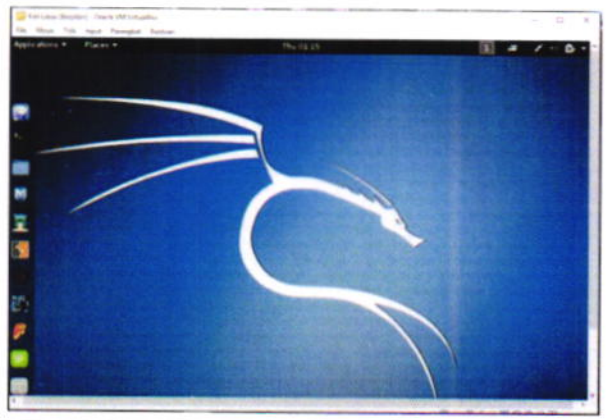
dd. Kemudian tunggu lagi hingga semua proses selesai. Setelah proses instalasi selesai maka akan muncul gambar seperti dibawah ini. Selanjutnya klik Continue lalu virtualbox akan merestart dengan sendirinya.



ee. Setelah itu dapat login dengan username "root".

ff. Kemudian masukkan password yang isi pada saat proses instalasi tadi.

gg. Done! sekarang Kali linux sudah berhasil terinstal di dalam virtual box.



2. Prosedur Pengoperasian Sistem Keamanan TI Polri

Prosedur pengoperasian sistem keamanan Teknologi Informasi Polri terdiri dari prosedur operasional *pantest* dan prosedur operasional *monitoring*. Adapun penjelasannya sebagai berikut:

a. Prosedur operasional *pantest (penetration testing)*

Dalam menjalankan prosedur operasional *penetration testing,* terdapat 2 cara yang dapat dilakukan yaitu:

1) Cara 1

a) Tahap persiapan

Prosedur operasional ini adalah untuk melakukan penetration testing terhadap kemungkinan kerentanan pada aplikasi web. sebelum memulai pelaksanaan operasional, lakukan persiapan berikut:

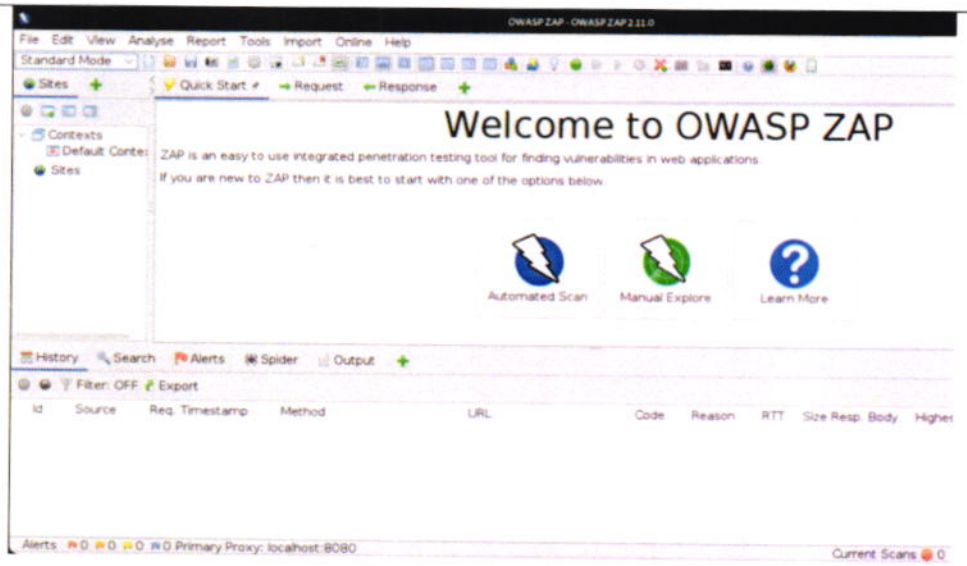
(1) Memiliki username dan password valid untuk OS Kali linux.
(2) memastikan pada OS kali linux sudah terdapat aplikasi Owasp Zap.
(3) mengetahui alamat web dari aplikasi yang akan dilakukan pentest.

b) Tahap pelaksanaan:

(1) Login ke OS Kali Linux menggunakan username dan password.
(2) Buka terminal, jalankan perintah "owasp-zap".

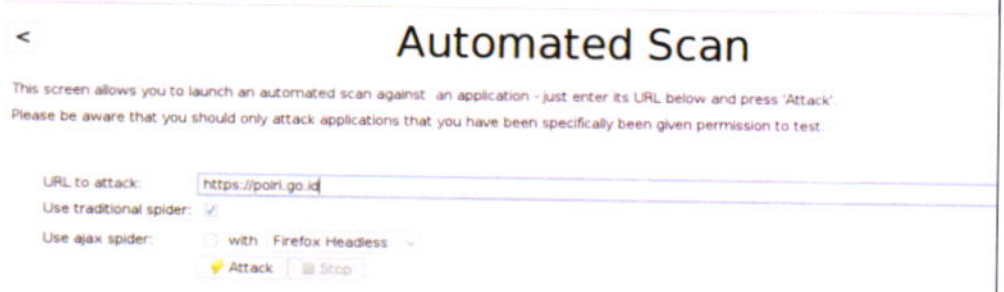
```
┌──(root💀 pentester)-[~]
└─# owasp-zap
```

(3) Maka akan muncul aplikasi Zap.

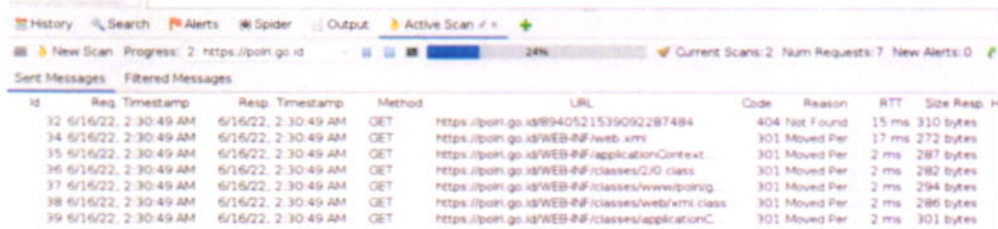


(4) Rubah standart menjadi attack mode.
(5) Pilih automated scan.

(6) Masukkan alamat url website, kemudian kik start

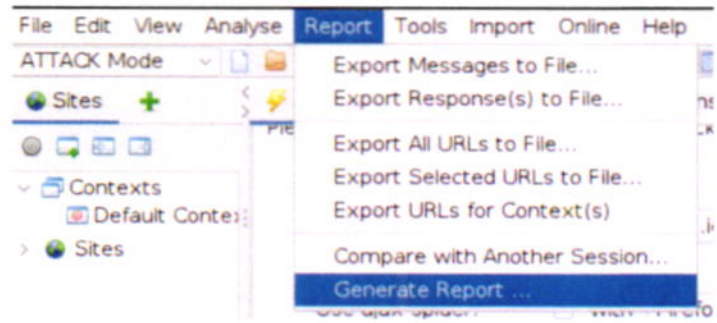


(7) Maka scanning akan berjalan seperti tampilan berikut;

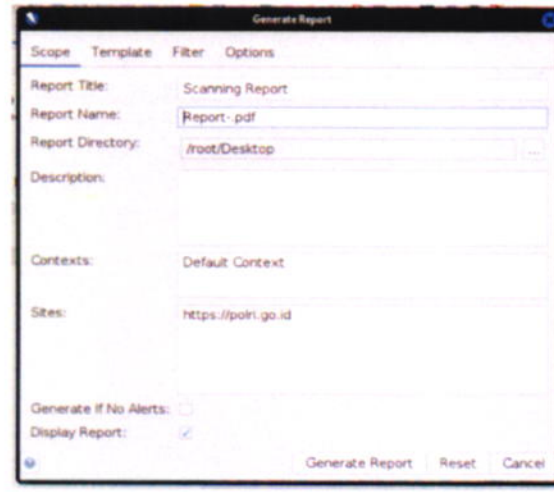


c) Tahap pengakhiran

1) Eksport laporan dengan cara klik report, kemudian klik ekport.



2) Kemudian muncul dialog box berikut, isi sesuai kebutuhan, kemudian klik "Generate Report".



2) Cara 2

a) Tahap persiapan

(1) Kesehatan dan keselamatan kerja diperiksa sesuai ketentuan.
(2) Peralatan dan perlengkapan disiapkan sesuai kebutuhan.
(3) Dokumen teknis dan SOP terkait sistem disiapkan sesuai kebutuhan.
(4) Praktik keamanan sistem menggunakan 2 software yaitu virtual box dan kali linux.

b) Tahap pelaksanaan

(1) Tahapan hacking dibagi menjadi 5 tahap yaitu:

(a) Reconnaissance atau pengintaian.
(b) Scanning atau pemindaian.
(c) Gaining access atau mendapatkan akses.
(d) Maintaining access atau mempertahankan akses.
(e) Clearing tracks atau membersihkan jejak.

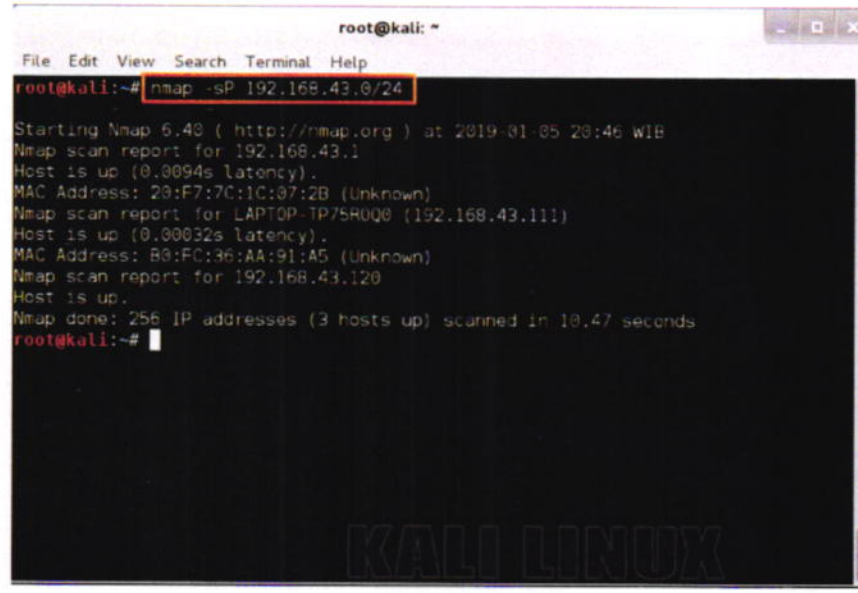
Namun dalam praktikum ini hanya akan belajar sampai tahap dua yaitu scanning atau pemindaian.

(2) NMAP *(Network Mapper)* adalah sebuah aplikasi atau tool yang berfungsi untuk melakukan port scanning. Nmap dibuat oleh Gordon Lyon, atau lebih dikenal dengan nama Fyodor Vaskovich. Aplikasi ini digunakan untuk meng-audit jaringan yang ada, antara lain:

(a) Mengidentifikasi komputer yang sedang aktif (active machine).
(b) Menemukan port yang terbuka.
(c) Mendapatkan informasi tentang sistem operasi (OS fingerprinting).
(d) Mendapatkan informasi layanan yang sedang berjalan (Service fingerprinting).

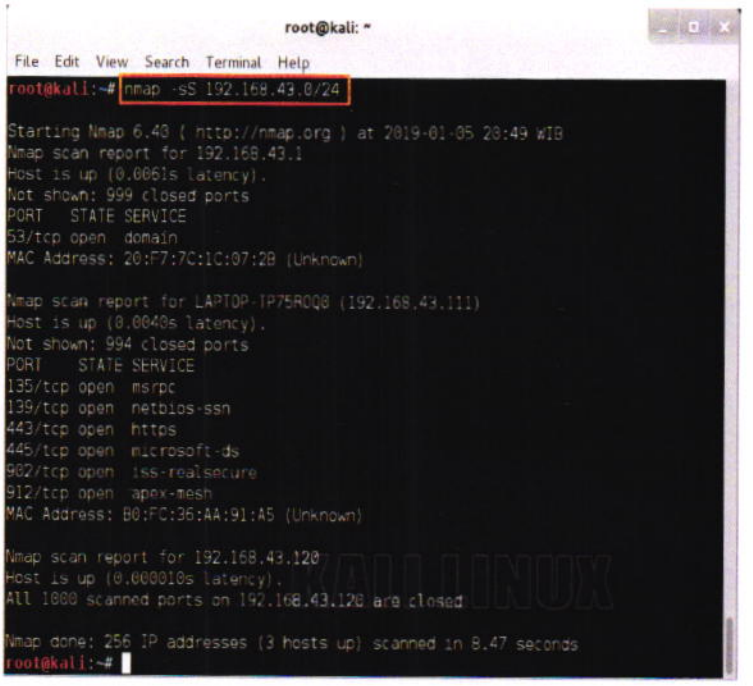
(3) Mengidentifikasi komputer yang sedang aktif (*active machine*)

Sebelum melakukan test security, pertama kita perlu mengidentifikasi mesin yang aktif pada range network yang dijadikan target. Oleh karna itu kita bisa menggunakan nmap dengan option "-sP". Yaitu melakukan scanning range ip pada segment 56 dan mengidentifikasi mesin yang aktif.



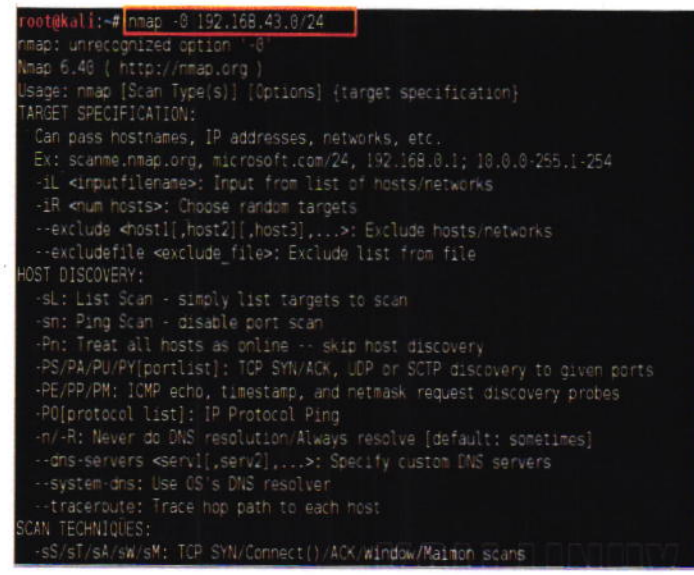
(4) Menemukan port yang terbuka

Dengan informasi range network target dan mesin yang aktif, proses selanjutnya adalah scanning port pada mesin yang aktif untuk melihat port yang terbuka. Pada step ini menggunakan option "-sS" dan option "-p", dan pilih salah satu ip/mesin yang aktif untuk di-scan.



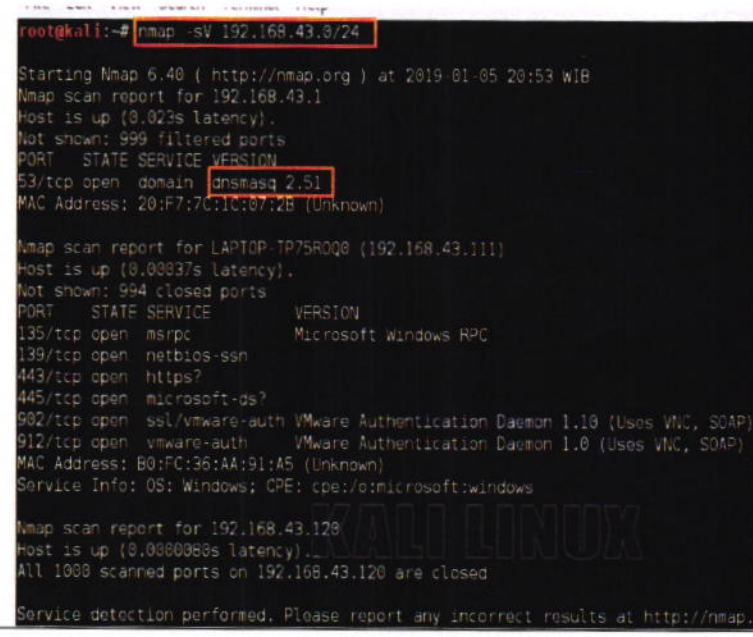
(5) Mendapatkan informasi tentang sistem operasi (OS fingerprinting)

Pada bagian proses pengumpulan informasi ini, adalah menentukan sistem operasi apa yang berjalan pada mesin yang aktif untuk mengetahui tipe sistem yang sedang ditest security nya. Menggunakan option "-O" untuk mendeteksi OS yang berjalan. Ketika Nmap tidak dapat mendeteksi OS secara tepat, ia terkadang memberikan kemungkinan terdekat. Tebakan yang cocok akan dilakukan oleh Nmap. Dengan option ini membuat Nmap menduga dengan lebih agresif. Nmap tetap akan memberitahu anda ketika kecocokan tidak sempurna, dicetak dan menampilkan tingkat kepercayaan (persentase) untuk setiap dugaan.



(6) Mendapatkan informasi layanan yang sedang berjalan (*service fingerprinting*)

Setelah port yang open diketahui dengan menggunakan salah satu metode scan diatas, hal selanjutnya adalah deteksi versi dari service yang sedang berjalan. Nmap akan berusaha menentukan nama protokol layanan serta versi dari layananan tersebut. Dan untuk mendeteksi versi dari service tersebut menggunakan option "-sV".



c) Tahap pengakhiran

1) Hasil instalasi, konfigurasi, dan operasionalisasi dicatat sesuai ketentuan.
2) Peralatan dan perlengkapan di cek kelengkapannya dan disimpan kembali sesuai ketentuan.
3) Laporan hasil kegiatan disusun dan dilaporkan kepada Pimpinan.

b. Prosedur operasional *monitoring*

1) Update sistem dan install requirement untuk wazuh agent

```
apt-get update
apt-get install make gcc libc6-dev curl automake autoconf libtool
```

2) Download dan ekstrak file yang di download

```
curl -Ls https://github.com/wazuh/wazuh/archive/v3.13.0.tar.gz | tar zx
```

3) Setelah selesai di download, lakukan install *wazuh agent*

```
cd wazuh-3.13.0
./install.sh
```

4) Pilih agent untuk menu installasinya

```
What kind of installation do you want (manager, agent, local, hybrid or
help)? agent
```

5) Jika sebelumnya anda telah mengkompile untuk platform lain, maka ada step dimana anda harus membersihkan build menggunakan Makefile src :

```
cd wazuh-3.13.0
make -C src clean
make -C src clean-deps
```

6) Register *wazuh agent*

```
/var/ossec/bin/agent-auth -m <manager_IP>
```

7) Untuk mengaktifkan komunikasi antara agent dan server *wazuh* bisa merubah konfigurasi di /var/ossec/etc/ossec.conf

```
<client>
  <server>
    <address>MANAGER_IP</address>
    ...
  </server>
</client>
```

8) Restart *wazuh agent*

```
/var/ossec/bin/ossec-control restart
Killing wazuh-modulesd...
Killing ossec-logcollector...
Killing ossec-syscheckd...
Killing ossec-agentd...
Killing ossec-execd...
Wazuh v3.13.0 Stopped
Starting Wazuh v3.13.0...
Started ossec-execd...
Started ossec-agentd...
Started ossec-syscheckd...
Started ossec-logcollector...
Started wazuh-modulesd...
Completed.
```

9) *Wazuh* agent siap dijalankan untuk monitoring kemanan sistem TIK

3. Prosedur Perawatan Sistem Keamanan TI Polri

a. Tahap persiapan

Menyiapkan peralatan pekerjaan antara lain obeng, vacuum cleaner, sarung tangan, gelang anti statis, dan lain-lain.

b. Tahap pelaksanaan

1) Perawatan fisik perangkat keamanan dengan membersihkan dan pengecekan suhu perangkat secara berkala berkisar 20-25 derajat celcius dengan rentang suhu toleransi 15-32 derajat celcius.
2) Melakukan update sistem operasi dan patch terbaru.
3) Melakukan backup (penyalinan) data sebagai tindakan pencegahan kehilangan data.
4) Pastikan Ruangan harus dalam keadaan bersih dan terus memperhatikan.
5) Listrik harus standby 24 jam secara terus menerus karena sistem harus bisa diakses setiap saat.
6) Untuk monitor tipe CRT (Cathode Ray Tube) semprotkan cairan pembersih langsung ke layar, karena monitor terbuat dari kaca jadi aman, kemudian lap dengan menggunakan lap halus, untuk monitor tipe LCD dan LED dilarang karena bisa membuat layar rusak dan kekuningan.
7) Jangan menutup atau memasukan benda ke ventilasi udara pada monitor.
8) Jika hendak dibersihkan, komputer dalam keadaan mati.
9) Proses pengelapan harus searah agar tidak terjadi goresan.
10) Jangan dekatkan monitor ke alat yang mengandung elektromagnetik, karena bisa merusak komponen, dan membuat layar menjadi hijau.
11) Melakukan penggantian password perangkat secara berkala untuk mengurangi resiko peretasan.
12) Hilangkan akses yang tidak perlu ke hardware maupun software.
13) Membatasi jumlah user yang melakukan login.

c. Tahap pengakhiran

1) Hasil instalasi, konfigurasi, dan operasionalisasi dicatat sesuai ketentuan.
2) Peralatan dan perlengkapan pendukung di cek kelengkapannya dan disimpan kembali sesuai ketentuan
3) Laporan hasil kegiatan disusun dan dilaporkan kepada Pimpinan.

RANGKUMAN

Proses Instalasi Sistem Keamanan TI Polri menggunakan aplikasi Kali Linux 2.0 di VirtualBox yang merupakan salah satu distribusi/distro yang diciptakan untuk kepentingan *penetrating* dan keamanan. Prosedur pengoperasian sistem keamanan Teknologi Informasi Polri terdiri dari prosedur operasional pantest dan prosedur operasional monitoring. Serta mengenai prosedur perawatan sistem keamanan TI Polri terdiri dari tahap persiapan, tahap pengoperasian, dan tahap pengakhiran.

SOAL LATIHAN

1. Jelaskan prosedur instalasi sistem keamanan TI Polri!
2. Jelaskan prosedur pengoperasian sistem keamanan TI Polri!
3. Jelaskan prosedur perawatan sistem keamanan TI Polri!