

# Bab 13: Keamanan

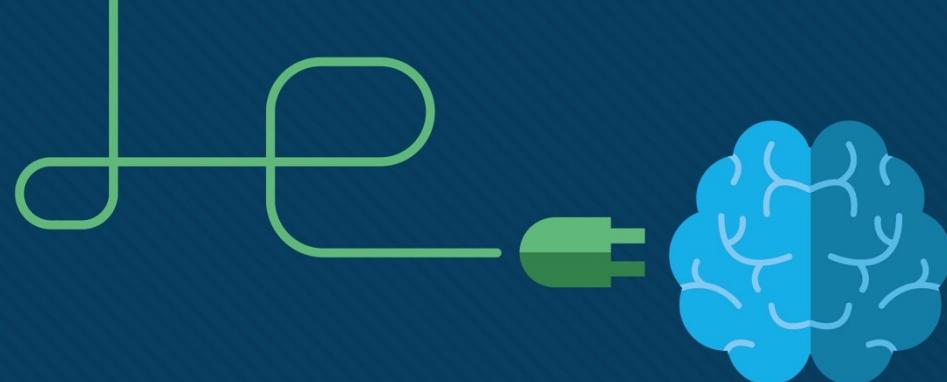
Materi Instruktur



# Bab 13: Keamanan

**Panduan Perencanaan IT Essentials 7.0**





# Bab 13: Keamanan

Dasar-dasar TI v7.0



# Bab 13 - Bagian & Tujuan

## - 13.1 Ancaman Keamanan

- Menjelaskan ancaman keamanan.
- Menjelaskan berbagai jenis malware.
- Menjelaskan tindakan perlindungan terhadap perangkat lunak berbahaya.
- Menjelaskan berbagai jenis serangan jaringan.
- Menjelaskan berbagai serangan rekayasa sosial.

## - 13.2 Prosedur Keamanan

- Menjelaskan prosedur keamanan.
- Jelaskan apa itu kebijakan keamanan.
- Menjelaskan tindakan pengamanan fisik.
- Menjelaskan tindakan yang melindungi data.
- Menjelaskan cara menghancurkan data.

# Bab 13 - Bagian & Tujuan (Lanjutan)

- 13.3 Mengamankan Stasiun Kerja Windows
  - Konfigurasikan pengaturan dan kebijakan keamanan dasar untuk perangkat akhir.
  - Jelaskan cara mengamankan stasiun kerja.
  - Konfigurasikan keamanan menggunakan alat Kebijakan Keamanan Lokal Windows.
  - Mengelola pengguna dan grup Windows.
  - Konfigurasikan keamanan menggunakan alat firewall Windows.
  - Konfigurasikan browser untuk akses aman.
  - Konfigurasikan pemeliharaan keamanan di Windows.
- 13.4 Keamanan Nirkabel
  - Konfigurasikan keamanan nirkabel.
  - Konfigurasikan perangkat nirkabel untuk komunikasi yang aman.

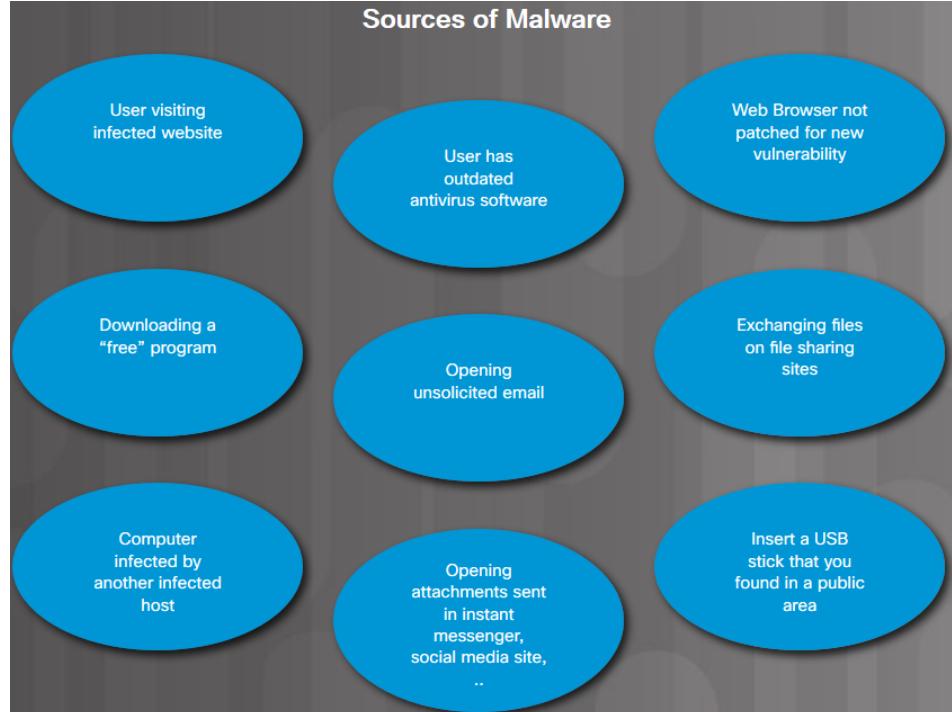
# Bab 13 - Bagian & Tujuan (Lanjutan)

- 13.5 Proses Pemecahan Masalah Dasar untuk Keamanan
  - Menjelaskan cara memecahkan masalah keamanan dasar
  - Jelaskan enam langkah proses pemecahan masalah untuk keamanan.
  - Menjelaskan masalah dan solusi tingkat lanjut untuk keamanan.

# 13.1 Ancaman Keamanan

## Perangkat lunak berbahaya

- Ada banyak jenis ancaman yang dibuat untuk mengganggu komputer dan jaringan.
- Ancaman terbesar dan paling umum bagi komputer dan data di dalamnya adalah malware.
- Malware biasanya dipasang di komputer tanpa sepengetahuan pengguna. Setelah host terinfeksi, malware dapat:
  - Mengubah konfigurasi komputer.
  - Hapus file atau hard drive yang rusak.
  - Mengumpulkan informasi yang disimpan di komputer tanpa persetujuan pengguna.
  - Buka jendela tambahan di komputer atau alihkan browser.



# Virus dan Trojan Horse

- Jenis malware komputer pertama dan paling umum adalah**virus**.
  - Virus memerlukan tindakan manusia untuk berkembang biak dan menginfeksi komputer lain.
  - Virus bersembunyi dengan menempel pada kode komputer, perangkat lunak, atau dokumen di komputer. Saat dibuka, virus akan berjalan dan menginfeksi komputer.
- Penjahat dunia maya juga menggunakan**Kuda Troya**untuk membahayakan tuan rumah.
  - Kuda Troya adalah program yang terlihat berguna tetapi juga membawa kode berbahaya.
  - Kuda Troya sering kali disertakan dalam program daring gratis seperti permainan komputer.

# Jenis-jenis Malware

Adware

Ransomware

Rootkit

Spyware

Worm

- **Perangkat lunak iklan** dapat menampilkan iklan yang tidak diminta menggunakan jendela browser web pop-up, toolbar baru, atau secara tidak terduga mengalihkan halaman web ke situs web lain.
- **Virus Ransomware** biasanya menolak akses pengguna ke berkas mereka dengan mengenkripsi berkas dan kemudian menampilkan pesan yang menuntut tebusan untuk kunci dekripsi.
- **Perangkat Rootkit** sulit dideteksi dan digunakan oleh penjahat dunia maya untuk mendapatkan akses tingkat admin ke komputer.
- **Perangkat lunak mata-mata** mirip dengan adware tetapi digunakan untuk mengumpulkan informasi tentang pengguna dan mengirimkannya kembali ke penjahat dunia maya.
- **Cacing** adalah program yang mereplikasi diri dan menyebar secara otomatis tanpa tindakan pengguna dengan mengeksplorasi kerentanan dalam perangkat lunak.

## Mencegah Malware

# Program Anti-Malware

- Penting bagi Anda untuk melindungi komputer dan perangkat seluler menggunakan perangkat lunak antivirus yang bereputasi baik.
- Saat ini, program antivirus umumnya disebut sebagai program anti-malware
  - Program anti-malware dapat mendeteksi dan memblokir Trojan, rootkit, ransomware, spyware, keylogger, dan program adware.
  - Program anti-malware terus mencari pola yang diketahui terhadap basis data tanda tangan malware yang diketahui.
  - Mereka juga dapat menggunakan teknik identifikasi malware heuristik yang dapat mendeteksi perilaku spesifik yang terkait dengan beberapa jenis malware.



## Mencegah Malware

### Pembaruan File Tanda Tangan

- Malware baru selalu dikembangkan; oleh karena itu, perangkat lunak anti-malware harus diperbarui secara berkala. Proses ini sering kali diaktifkan secara default.
- Selalu unduh file tanda tangan dari situs web produsen untuk memastikan pembaruan tersebut asli dan tidak rusak oleh malware.
  - Untuk menghindari terlalu banyaknya lalu lintas di satu situs web, beberapa produsen mendistribusikan berkas tanda tangan mereka untuk diunduh ke beberapa situs unduhan. Situs unduhan ini disebut mirror.
- **PERINGATAN:** Saat mengunduh berkas tanda tangan dari mirror, pastikan situs mirror tersebut adalah situs yang sah. Selalu tautkan ke situs mirror dari situs web produsen.

# Penjelasan Video – Program Anti-Malware

### Video Demonstration: Protecting Against Malware

In this video demonstration, you will learn how to protect against malware using:

- Windows Security
  - Virus and Threat Protection
  - Firewall
  - App & Browser Control



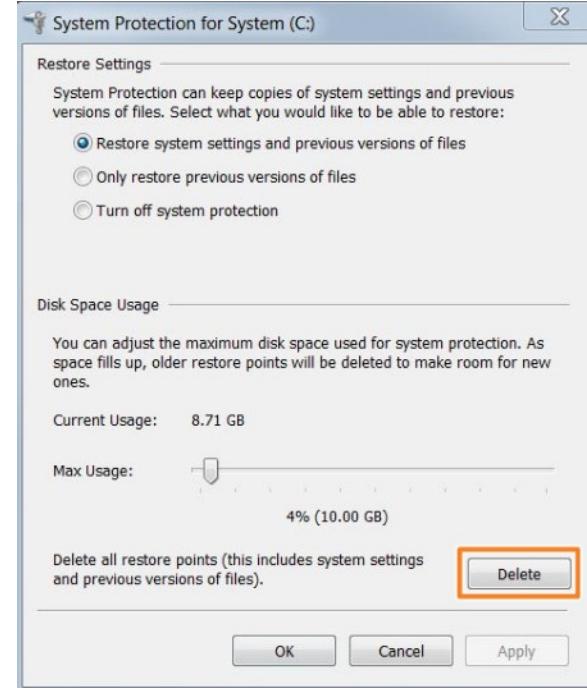
0:01



## Mencegah Malware

# Pemulihan Sistem yang Terinfeksi

- Saat program perlindungan malware mendeteksi bahwa komputer terinfeksi, program tersebut akan menghapus atau mengkarantina ancaman tersebut. Namun, kemungkinan besar komputer masih berisiko.
- Banyak program antimalware yang dapat diatur untuk berjalan saat sistem dimulai sebelum memuat Windows.
- Menghapus malware mungkin mengharuskan komputer di-boot ulang ke Mode Aman.
- Mungkin perlu menghubungi spesialis untuk memastikan komputer telah dibersihkan sepenuhnya. Jika tidak, komputer mungkin perlu diformat ulang, sistem operasi diinstal ulang, dan data Anda dipulihkan dari cadangan terbaru.
- Layanan pemulihan sistem OS dapat menyertakan file yang terinfeksi dalam titik pemulihan. Oleh karena itu, setelah komputer dibersihkan dari malware apa pun, file pemulihan sistem harus dihapus.

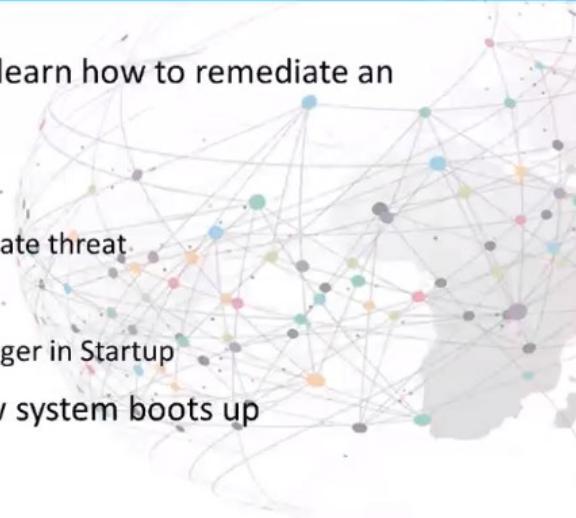


# Penjelasan Video – Memulihkan Sistem yang Terinfeksi

### Video Demonstration: Remediating an Infected System

In this video demonstration, you will learn how to remediate an infected system:

- Use Windows Security
  - Use Virus and Threat Protection to locate threat
  - Run a Full scan
  - Verify no suspicious files in Task Manager in Startup
- Change boot process to control how system boots up



# Jaringan Adalah Target

Perform an information query of a target

Initiate a ping sweep of the target network

Initiate a port scan of active IP addresses

Run Vulnerability Scanners

Run Exploitation tools

- Penyerang mencari informasi jaringan tentang target menggunakan pencarian Google, whois, dan alat lainnya.
- Penyerang memulai pemindaian ping pada alamat jaringan publik target yang ditemukan untuk menentukan alamat IP mana yang aktif.
- Penyerang menentukan layanan mana yang tersedia pada port aktif menggunakan Nmap, SuperScan, dan alat lainnya.
- Penyerang menjalankan pemindai kerentanan untuk menemukan jenis aplikasi dan OS yang berjalan pada host target menggunakan Nipper, Secuna PSI, dan alat lainnya.
- Penyerang mencoba menemukan layanan yang rentan untuk dieksplorasi menggunakan Metasploit, Core Impact, dan alat lainnya.

## Jenis-jenis Serangan TCP/IP

Denial of Service (DoS)

Distributed DoS

DNS Poisoning

Man-in-the-Middle

- **Penolakan Layanan (DoS)** adalah serangan di mana penyerang membanjiri perangkat target dengan permintaan palsu untuk menciptakan penolakan layanan bagi pengguna yang sah.
- **DoS Terdistribusi** adalah serangan DoS yang diperkuat dengan menggunakan banyak host terinfeksi yang disebut zombi untuk mengalahkan target.
- **Keracunan DNS** adalah serangan di mana penyerang berhasil menginfeksi host untuk menerima catatan DNS palsu yang menunjuk ke server jahat.
- **Orang di tengah** adalah serangan di mana penyerang menyadap komunikasi antara dua host.

## Jenis-jenis Serangan TCP/IP (Lanjutan)

Replay

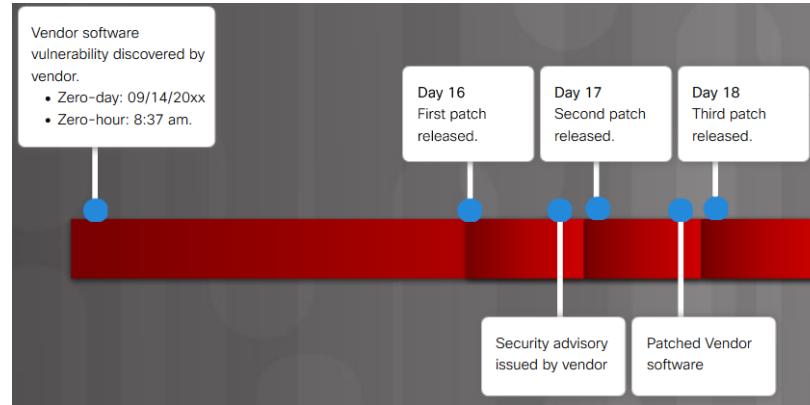
Spoofing

Syn Flood

- **Memutar ulang** adalah jenis serangan spoofing di mana penyerang menangkap paket yang diautentikasi, mengubahnya, dan mengirimkannya ke tujuan asal.
- **Pemalsuan** adalah serangan di mana penyerang memalsukan alamat IP untuk mendapatkan akses ke sumber daya.
- **Banjir Sina** adalah jenis serangan DoS yang mengeksloitasi jabat tangan tiga arah TCP.

# Hari Nol

- Dua istilah berikut umumnya digunakan untuk menggambarkan saat ancaman terdeteksi:
  - **Hari nol**-Kadang-kadang juga disebut sebagai serangan zero-day, ancaman zero-day, atau eksloitasi zero-day. Ini adalah hari ketika kerentanan yang tidak diketahui telah ditemukan oleh vendor. Istilah ini merujuk pada jumlah waktu yang dimiliki vendor untuk mengatasi kerentanan tersebut.
  - **Jam nol**-Inilah saatnya eksloitasi itu ditemukan.
- Perangkat lunak tersebut dapat dieksloitasi hingga patch yang mengatasi kerentanan tersedia.



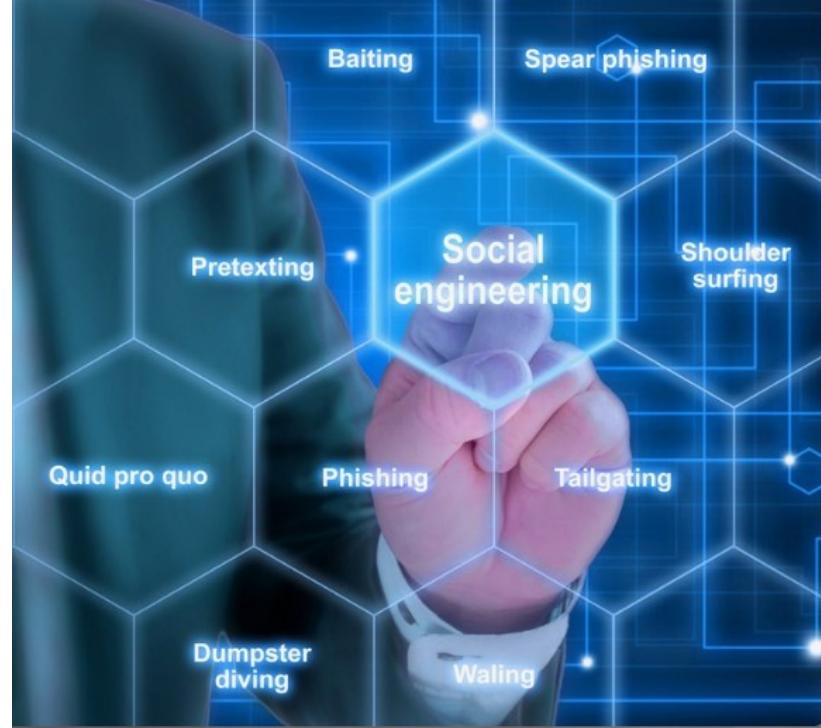
## Melindungi Terhadap Serangan Jaringan

- Tidak ada solusi tunggal untuk melindungi terhadap semua serangan TCP/IP atau zero-day.
- Salah satu solusinya adalah menggunakan pendekatan pertahanan berlapis, yang juga dikenal sebagai pendekatan berlapis, terhadap keamanan.
  - Hal ini memerlukan kombinasi perangkat jaringan dan layanan yang bekerja bersama-sama.
- Semua perangkat jaringan termasuk router dan switch harus diamankan untuk mencegah penyerang merusak perangkat.

# Serangan Rekayasa Sosial

## Rekayasa Sosial

- Penjahat dunia maya menggunakan teknik rekayasa sosial untuk menipu target yang tidak menaruh curiga agar mengungkapkan informasi rahasia.
- Rekayasa sosial adalah serangan akses yang mencoba memanipulasi individu agar melakukan tindakan atau membocorkan informasi rahasia.
- Insinyur sosial sering kali mengandalkan sifat manusia dan kemauan orang untuk membantu.
- **Catatan:** Rekayasa sosial sering digunakan bersama dengan serangan jaringan lainnya.



# Teknik Rekayasa Sosial

- **Dalih**-Seorang penyerang berpura-pura membutuhkan data pribadi untuk mengonfirmasi identitas penerima.
- **Penipuan**-Seorang penyerang mengirim email penipuan yang disamarkan berasal dari sumber tepercaya.
- **Penipuan Tombak**-Penyerang membuat serangan phishing yang ditargetkan untuk individu atau organisasi tertentu.
- **Spam**-Email yang tidak diminta yang sering kali berisi tautan berbahaya, malware, atau konten yang menipu.
- **Sesuatu untuk Sesuatu**-Ketika penyerang meminta informasi pribadi dengan imbalan sesuatu.
- **Umpam**-Seorang penyerang meninggalkan flash drive yang terinfeksi malware di lokasi umum.
- **Peniruan**-Penyerang berpura-pura menjadi seseorang yang bukan dirinya.
- **Mengintai dari belakang**-Penyerang mengikuti orang yang berwenang ke area aman.
- **Berselancar di bahu**-Seorang penyerang melihat dari balik bahu seseorang untuk mencuri informasi.
- **Menyelam di Tempat Pembuangan Sampah**-Seorang penyerang menelusuri sampah untuk mencari informasi rahasia.

# Melindungi Diri dari Rekayasa Sosial



## 13.2 Prosedur Keamanan

# Apa itu Kebijakan Keamanan

- Kebijakan keamanan adalah:
  - serangkaian tujuan keamanan yang memastikan keamanan jaringan, data, dan komputer dalam suatu organisasi.
  - dokumen yang terus berkembang berdasarkan perubahan dalam teknologi, bisnis, dan persyaratan karyawan.
  - biasanya dibuat oleh suatu komite yang anggotanya terdiri atas manajemen dan staf IT.
- Terserah kepada staf TI untuk menerapkan spesifikasi kebijakan keamanan dalam jaringan.

## Security Policy Identifies

- Which assets require protection?
- What are the possible threats?
- What to do in the event of a security breach?
- What training will be in place to educate the end users?

## Security Policy

- Identification and Authentication Policies
- Password Policies
- Acceptable Use Policies
- Remote Access Policies
- Network Maintenance Policies
- Incident Handling Policies

## Kategori Kebijakan Keamanan

Identification and Authentication Policies

Password Policies

Acceptable Use Policies

Remote Access Policies

Network Maintenance Policies

Incident Handling Policies

- **Kebijakan Identifikasi dan Autentikasi**–Menguraikan prosedur verifikasi dan menentukan orang yang berwenang yang dapat memiliki akses ke sumber daya jaringan.
- **Kebijakan Kata Sandi**–Memastikan kata sandi memenuhi persyaratan minimum dan diubah secara berkala.
- **Kebijakan Penggunaan yang Dapat Diterima**–Mengidentifikasi sumber daya dan penggunaan jaringan yang dapat diterima oleh organisasi dan dapat mencakup konsekuensi pelanggaran kebijakan.
- **Kebijakan Akses Jarak Jauh**–Mengidentifikasi bagaimana pengguna jarak jauh mengakses jaringan dan apa yang dapat diakses?
- **Kebijakan Pemeliharaan Jaringan**–Menentukan sistem operasi perangkat jaringan dan prosedur pembaruan aplikasi pengguna akhir.
- **Kebijakan Penanganan Insiden**–Menjelaskan bagaimana insiden keamanan ditangani.

## Mengamankan Perangkat dan Data

- Sasaran kebijakan keamanan adalah untuk memastikan lingkungan jaringan yang aman dan melindungi aset.
- Aset suatu organisasi meliputi data, karyawan, dan perangkat fisik seperti komputer dan peralatan jaringan.
- Kebijakan keamanan harus mengidentifikasi perangkat keras dan peralatan yang dapat digunakan untuk mencegah pencurian, vandalisme, dan kehilangan data.

# Melindungi Peralatan Fisik

## Keamanan Fisik

- Keamanan fisik sama pentingnya dengan keamanan data.
  - Misalnya, jika komputer diambil dari suatu organisasi, datanya juga dicuri atau lebih buruk lagi, hilang.
- Keamanan fisik melibatkan pengamanan:
  - Akses ke tempat organisasi
  - Akses ke area terbatas
  - Infrastruktur komputasi dan jaringan



## Kategori Kebijakan Keamanan



- **Kunci konvensional**—Dibuka dengan memasukkan kunci yang diperlukan ke mekanisme gagang pintu.
- **Kunci baut mati**—Dibuka dengan memasukkan kunci yang diperlukan ke dalam kunci yang terpisah dari mekanisme gagang pintu.
- **Kunci elektronik**—Dibuka dengan memasukkan kode kombinasi rahasia atau PIN ke papan tombol.
- **Kunci berbasis token**—Dibuka dengan menggesek kartu aman atau dengan menggunakan pembaca jarak dekat untuk mendeteksi kartu pintar atau kunci fob nirkabel.
- **Kunci biometrik**—Dibuka dengan menggunakan pemindai biometrik seperti pembaca sidik jari.
- **Kunci multifaktor**—Kunci yang menggunakan kombinasi mekanisme di atas.

# Melindungi Peralatan Fisik mantra

- Di lingkungan dengan keamanan tinggi, mantra sering digunakan untuk membatasi akses ke area terlarang dan mencegah tindak membuntuti.
- Mantrap adalah ruangan kecil dengan dua pintu, yang satu harus ditutup sebelum yang lain dapat dibuka.
- Biasanya, seseorang memasuki mantrap dengan membuka satu pintu. Begitu berada di dalam mantrap, pintu pertama akan tertutup dan kemudian pengguna harus membuka pintu kedua untuk memasuki area terlarang.



## Melindungi Peralatan Fisik

# Mengamankan Komputer dan Perangkat Keras Jaringan

- Organisasi harus melindungi infrastruktur komputasi dan jaringan mereka.
  - Ini termasuk kabel, peralatan telekomunikasi, dan perangkat jaringan.
- Ada beberapa metode untuk melindungi peralatan komputer dan jaringan secara fisik.
- Peralatan jaringan hanya boleh dipasang di area yang aman. Selain itu, semua kabel harus ditutup dalam saluran atau diarahkan ke dalam dinding untuk mencegah akses atau gangguan yang tidak sah.

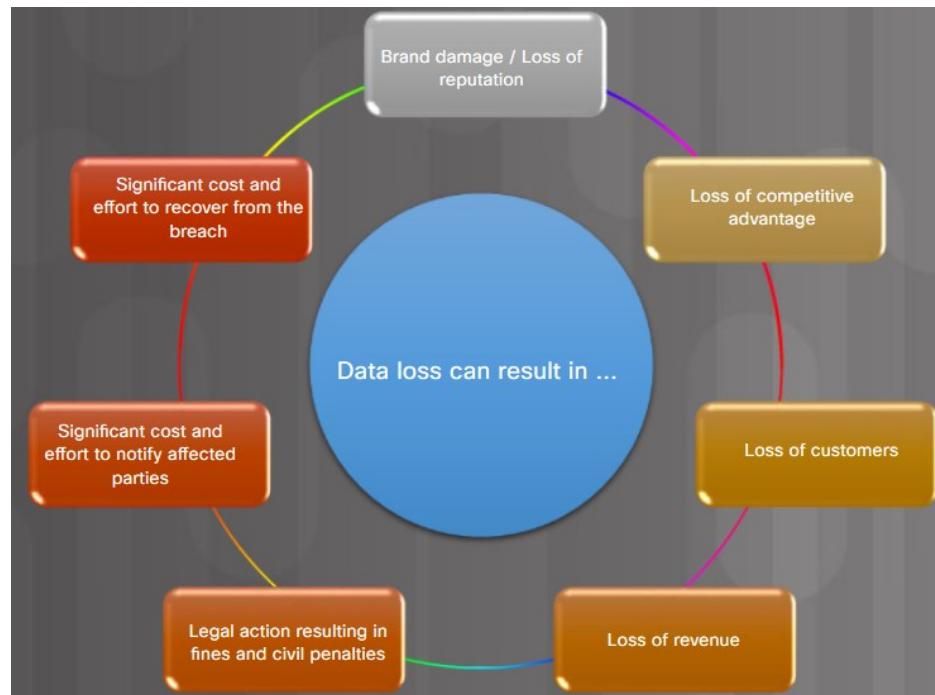
## Melindungi Peralatan Fisik

# Mengamankan Komputer dan Perangkat Keras Jaringan (Lanjutan)

- Faktor-faktor yang menentukan peralatan paling efektif untuk digunakan untuk mengamankan peralatan dan data meliputi:
  - Bagaimana peralatan tersebut digunakan
  - Dimana peralatan komputer berada
  - Jenis akses pengguna apa yang diperlukan terhadap data
- Misalnya:
  - Komputer di tempat umum yang ramai memerlukan perlindungan tambahan dari pencurian dan vandalisme.
  - Di pusat panggilan yang sibuk, server mungkin perlu diamankan di ruang peralatan yang terkunci.
  - Saat menggunakan laptop di tempat umum, dongle keamanan dan fob kunci memastikan bahwa komputer terkunci jika pengguna dan laptop dipisahkan.

# Data – Aset Terbesar Anda

- Data kemungkinan besar merupakan aset paling berharga bagi suatu organisasi. Data organisasi dapat mencakup data penelitian dan pengembangan, penjualan, keuangan, sumber daya manusia, karyawan, dan pelanggan.
- Data dapat hilang atau rusak dalam keadaan seperti pencurian, kegagalan peralatan, atau bencana.
- Kehilangan atau eksfiltrasi data adalah istilah yang digunakan untuk menggambarkan saat data hilang, dicuri, atau bocor ke publik.
- Data dapat dilindungi dari kehilangan data menggunakan pencadangan data, enkripsi file/folder, dan izin.



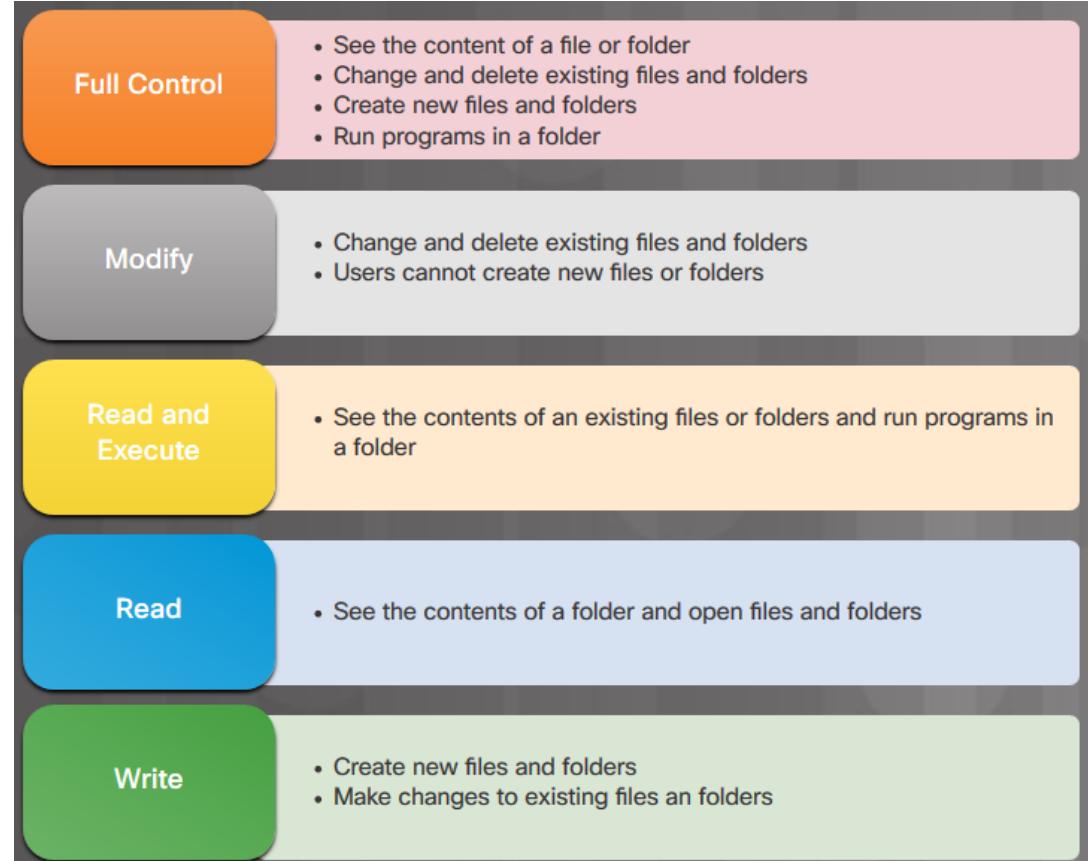
## Melindungi Data

### Pencadangan Data

- Mencadangkan data adalah salah satu cara paling efektif untuk melindungi dari kehilangan data.
  - Pencadangan data menyimpan salinan informasi pada komputer ke media cadangan yang dapat dilepas
  - Pencadangan data harus dilakukan secara berkala seperti yang ditetapkan dalam kebijakan keamanan.
  - Cadangan data biasanya disimpan di luar lokasi untuk melindungi media cadangan jika terjadi sesuatu pada fasilitas utama.
- Host Windows memiliki utilitas pencadangan dan pemulihan.
- Host macOS memiliki **Mesin Waktu** utilitas untuk melakukan fungsi pencadangan dan pemulihan.

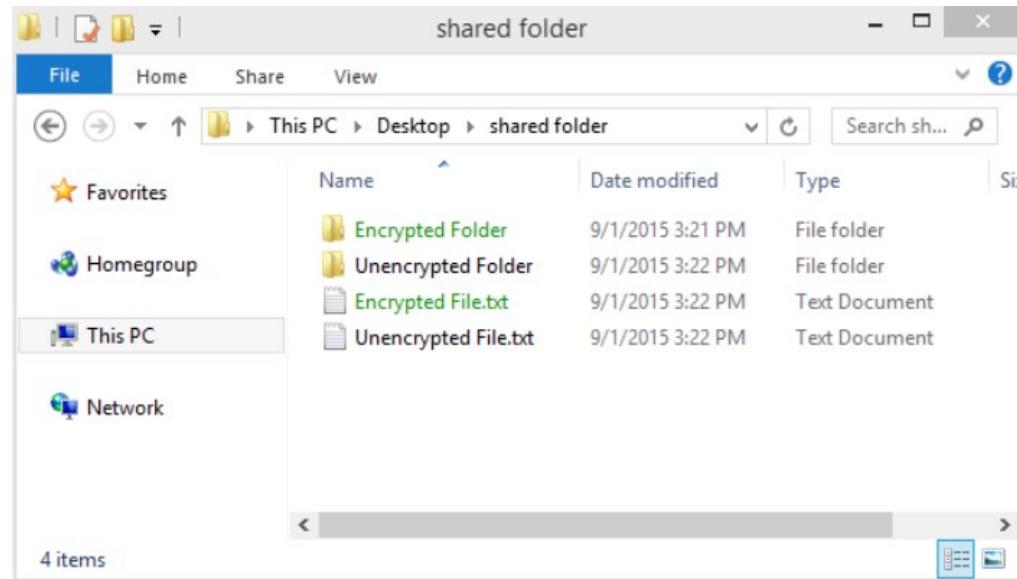
# Izin File dan Folder

- Izin adalah aturan yang Anda konfigurasikan untuk membatasi akses folder atau file untuk suatu tujuan individu atau untuk sekelompok pengguna.
- Pengguna hendaknya dibatasi hanya pada sumber daya yang mereka perlukan di komputer atau jaringan.
- Hal ini dikenal sebagai prinsip hak istimewa paling sedikit.



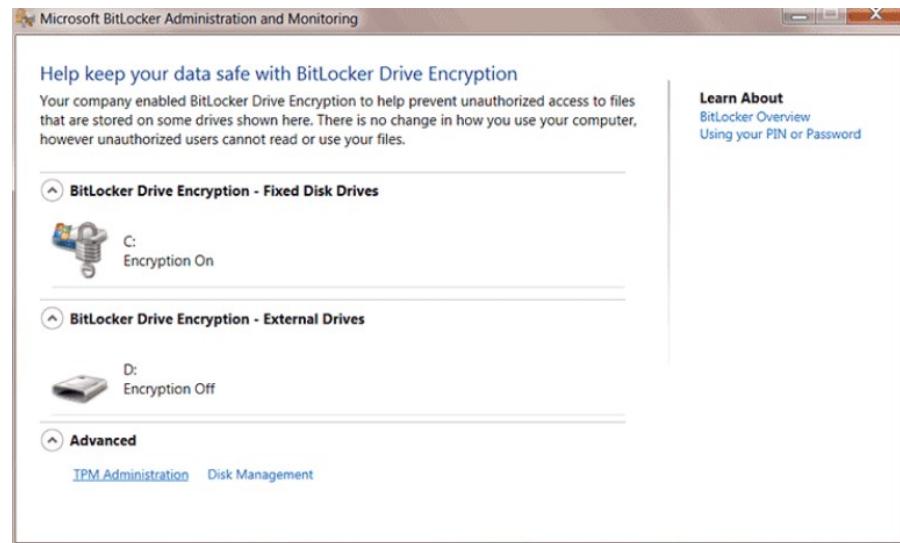
# Enkripsi File dan Folder

- Enkripsi sering digunakan untuk melindungi data.
  - Enkripsi adalah proses mengubah data menggunakan algoritma rumit untuk membuatnya tidak dapat dibaca.
  - Kunci khusus harus digunakan untuk mengembalikan informasi yang tidak dapat dibaca menjadi data yang dapat dibaca.
- Encrypting File System (EFS) adalah fitur Windows yang dapat mengenkripsi data.
  - EFS terhubung langsung ke akun pengguna tertentu.
  - Hanya pengguna yang mengenkripsi data yang akan dapat mengaksesnya setelah data dienkripsi.



# Windows BitLocker dan BitLocker untuk Go

- Anda dapat mengenkripsi seluruh hard drive menggunakan fitur yang disebut BitLocker.
- Untuk menggunakan BitLocker:
  - Setidaknya dua volume harus ada pada hard disk.
  - Trusted Platform Module (TPM) harus diaktifkan di BIOS.
    - TPM adalah chip khusus yang dipasang pada motherboard yang menyimpan kunci enkripsi, sertifikat digital, dan kata sandi.
- Enkripsi BitLocker juga dapat digunakan dengan drive yang dapat dilepas dengan menggunakan BitLocker To Go.
  - BitLocker To Go tidak menggunakan chip TPM, tetapi tetap menyediakan enkripsi dan memerlukan kata sandi.

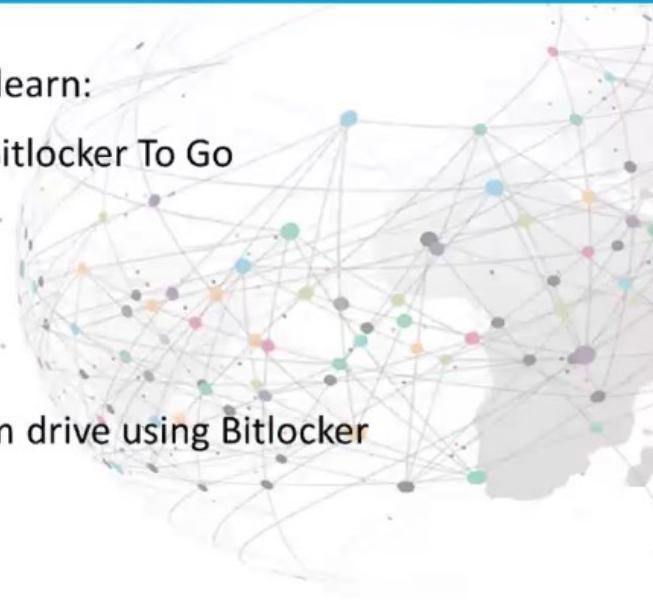


# Demonstrasi Video – BitLocker dan BitLocker To Go

## Video Demonstration: Bitlocker and Bitlocker To Go

In this video demonstration, you will learn:

- How to encrypt a flash drive using Bitlocker To Go
- Options for encrypting a drive
- Options for Bitlocker To Go
- How to unlock an encrypted drive
- How to encrypt an Operating System drive using Bitlocker



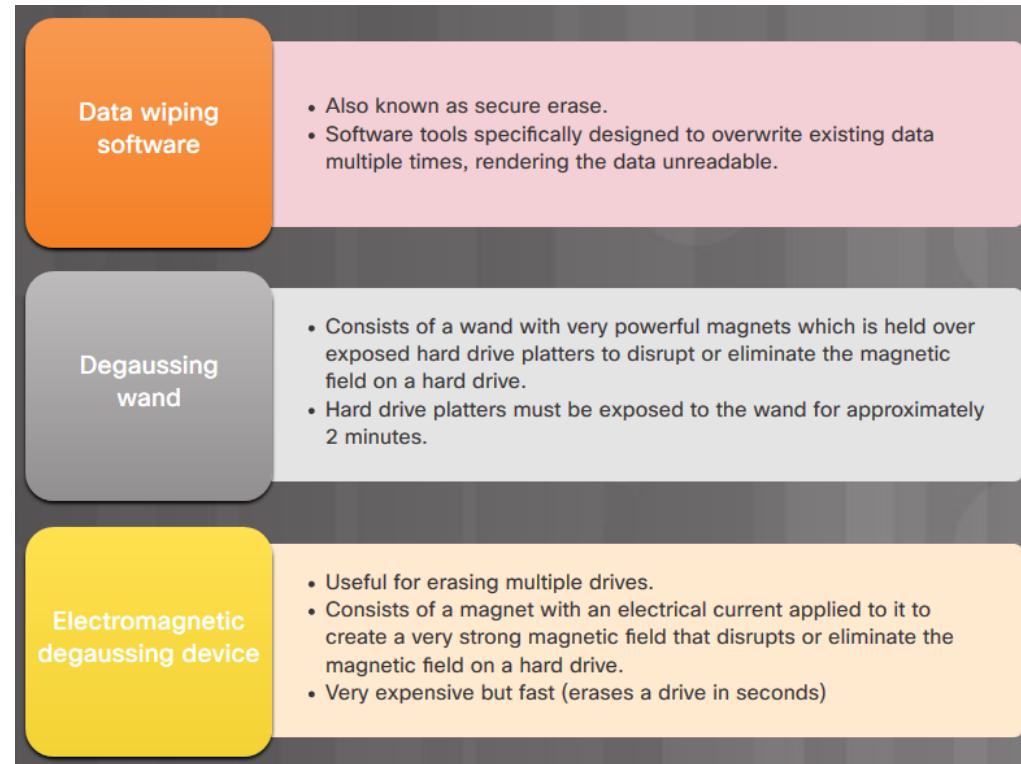
## Mencegah Malware

# Lab – Bitlocker dan Bitlocker To Go

Di lab ini, Anda akan mengaktifkan enkripsi BitLocker pada drive data yang dapat dilepas dan pada drive sistem komputer.

# Penghapusan Data Media Magnetik

- Melindungi data juga mencakup menghapus file dari perangkat penyimpanan saat tidak lagi diperlukan.
- Sekadar menghapus file atau memformat ulang drive mungkin tidak cukup untuk menjamin privasi Anda.
- Alat perangkat lunak dapat digunakan untuk memulihkan folder, file, dan bahkan seluruh partisi.
- Karena alasan ini, media penyimpanan harus dihapus sepenuhnya menggunakan satu atau lebih metode yang tercantum dalam gambar.

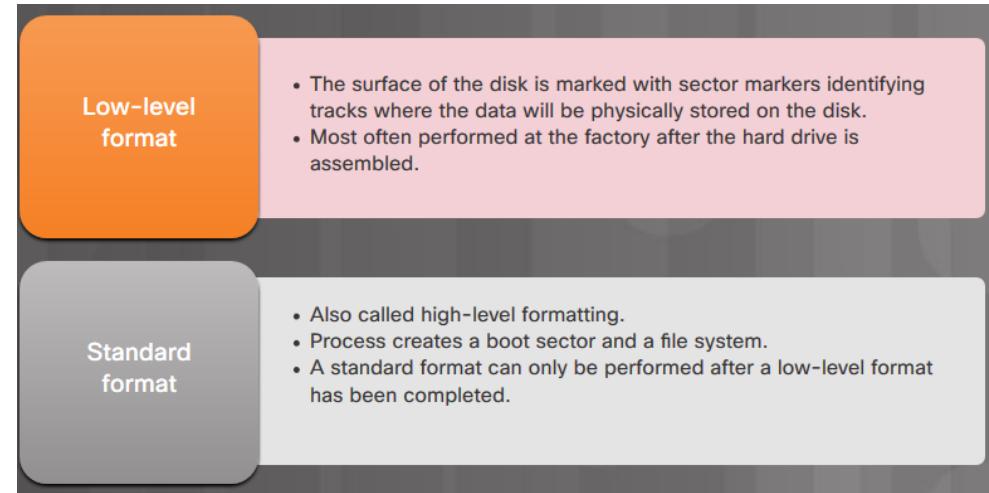


## Penghapusan Data Media Lain

- SSD terdiri dari memori flash, bukan piringan magnetik.
  - Teknik umum yang digunakan untuk menghapus data seperti degaussing tidak efektif dengan memori flash.
  - Lakukan penghapusan aman untuk memastikan sepenuhnya bahwa data tidak dapat dipulihkan dari SSD dan SSD hibrid.
- Media penyimpanan dan dokumen lainnya (misalnya, cakram optik, eMMC, stik USB) juga harus dimusnahkan.
  - Gunakan mesin penghancur atau insinerator yang dirancang untuk menghancurkan dokumen dan setiap jenis media.
- Saat memikirkan perangkat apa yang harus dihapus atau dimusnahkan, ingatlah bahwa perangkat selain komputer dan perangkat seluler juga menyimpan data.
  - Printer dan perangkat multifungsi juga dapat berisi hard drive yang menyimpan dokumen yang dicetak atau dipindai. Fitur penyimpanan ini dapat dimatikan dalam beberapa kasus, atau perangkat perlu dihapus secara berkala.

# Daur Ulang dan Pemusnahan Hard Drive

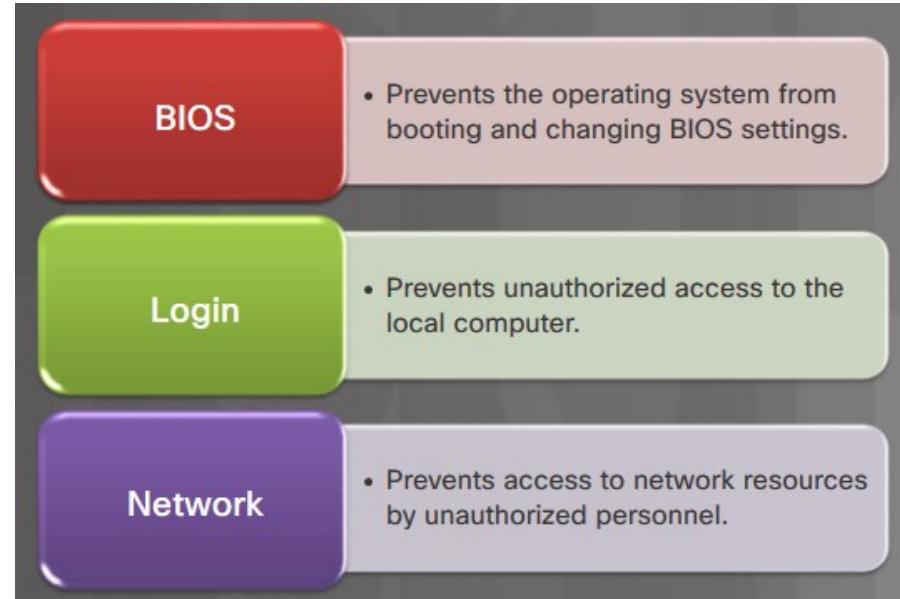
- Ketika media penyimpanan tidak lagi diperlukan, media tersebut dapat berupa:
  - **Hancur**-Menghancurkan hard drive sepenuhnya memastikan bahwa data tidak dapat dipulihkan dari hard drive.
  - **Didaur ulang**-Hard drive yang telah dihapus dapat digunakan kembali di komputer lain. Drive dapat diformat ulang dan sistem operasi baru dapat diinstal.



# 13.3 Mengamankan Jendela Stasiun kerja

## Mengamankan Komputer

- Komputer dan stasiun kerja harus diamankan dari pencurian.
  - Kunci stasiun kerja Anda saat Anda tidak hadir untuk mencegah pengguna yang tidak berwenang mencuri atau mengakses komputer lokal dan sumber daya jaringan.
  - Jika Anda harus meninggalkan komputer di tempat umum yang terbuka, kunci kabel harus digunakan untuk mencegah pencurian.
  - Gunakan layar privasi untuk melindungi informasi yang ditampilkan di layar Anda dari mata-mata
- Akses ke komputer Anda juga harus dilindungi.
  - Ada tiga tingkat perlindungan kata sandi yang dapat digunakan pada komputer.



## Mengamankan BIOS

- Kata sandi login Windows, Linux, atau Mac dapat dilewati.
- Menetapkan kata sandi BIOS atau UEFI mencegah seseorang mengubah pengaturan yang dikonfigurasi dan juga dapat mencegah seseorang mem-boot komputer.
- Semua pengguna, apa pun akun penggunanya, berbagi kata sandi BIOS.
- Kata sandi UEFI dapat diatur berdasarkan per pengguna, namun diperlukan server autentikasi.

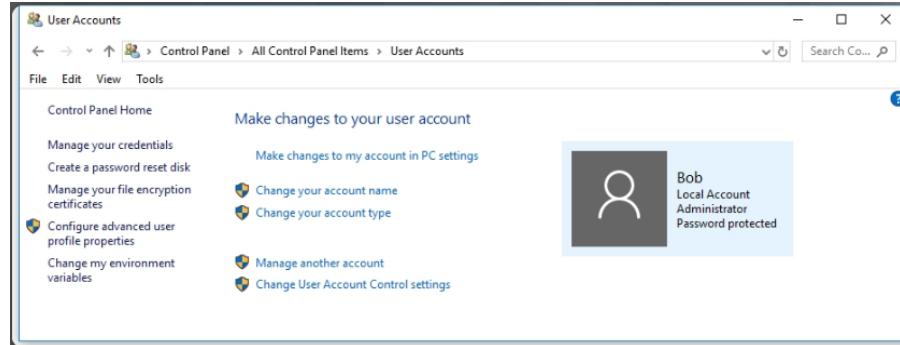


## Mengamankan Login Windows

- Jenis perlindungan kata sandi yang paling umum adalah login komputer.
- Bergantung pada sistem komputer Anda, Windows 10 mungkin juga mendukung opsi masuk lainnya. Secara khusus, Windows 10 mendukung opsi masuk berikut:
  - **Jendela Halo**-Fitur yang memungkinkan Windows menggunakan pengenalan wajah atau menggunakan sidik jari Anda untuk mengakses Windows.
  - **PIN**-Masukkan nomor PIN yang telah dikonfigurasikan sebelumnya untuk mengakses Windows.
  - **Kata sandi gambar**-Anda memilih gambar dan gerakan untuk digunakan dengan gambar tersebut guna membuat kata sandi yang unik.
  - **Kunci dinamis**-Fitur ini membuat Windows terkunci saat perangkat yang telah dipasangkan sebelumnya seperti telepon seluler berada di luar jangkauan PC.

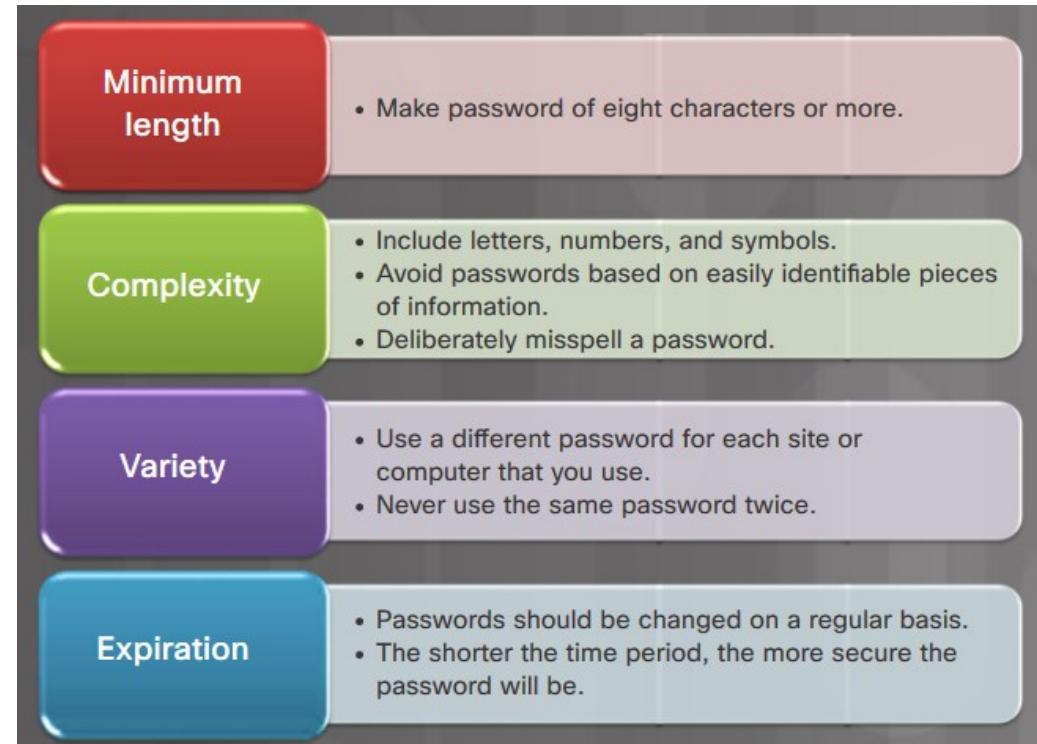
# Manajemen Kata Sandi Lokal

- Manajemen kata sandi untuk komputer Windows mandiri dapat diatur secara lokal menggunakan Windows **Akun Pengguna** alat.
  - Untuk membuat, menghapus, atau mengubah kata sandi di Windows, gunakan **Panel Kontrol > Akun Pengguna**
- Penting juga untuk memastikan komputer aman saat pengguna sedang bepergian.
  - Kebijakan keamanan seharusnya berisi aturan tentang keharusan komputer terkunci saat screensaver dimulai.
  - Di semua versi Windows, gunakan **Panel Kontrol > Personalisasi > Pengaman Layar**
    - Pilih screen saver dan waktu tunggu, lalu pilih **Saat melanjutkan, tampilkan layar logon** pilihan.



## Nama Pengguna dan Kata Sandi

- Nama pengguna, seperti kata sandi, adalah bagian informasi penting dan tidak boleh diungkapkan.
- Pedoman kata sandi merupakan komponen penting dari kebijakan keamanan.
- Setiap pengguna yang harus masuk ke komputer atau terhubung ke sumber daya jaringan harus diharuskan memiliki kata sandi.
- Kata sandi membantu mencegah pencurian data dan tindakan jahat.
- Kata sandi juga membantu mengonfirmasi bahwa pencatatan peristiwa valid dengan memastikan bahwa pengguna adalah orang yang tepat.



# Kebijakan Keamanan Lokal Windows

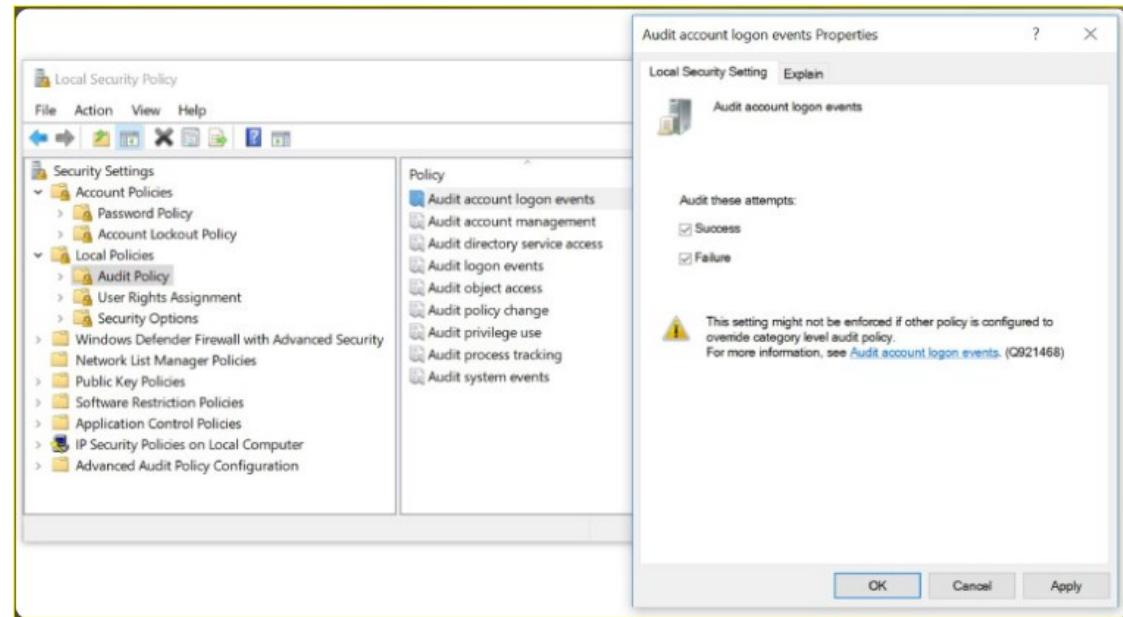
- Di sebagian besar jaringan yang menggunakan komputer Windows, Direktori Aktif dikonfigurasi dengan Domain di Windows Server.
  - Komputer Windows adalah anggota suatu domain.
  - Administrator mengonfigurasi Kebijakan Keamanan Domain yang berlaku untuk semua komputer yang bergabung.
  - Kebijakan akun ditetapkan secara otomatis saat pengguna masuk ke Windows.
- Untuk komputer mandiri yang bukan bagian dari domain Direktori Aktif, Kebijakan Keamanan Lokal Windows dapat digunakan untuk menegakkan pengaturan keamanan.
  - Untuk mengakses Kebijakan Keamanan Lokal di Windows 7 dan Vista, gunakan**Mulai > Panel Kontrol > Alat Administratif > Kebijakan Keamanan Lokal**.
  - Di Windows 8, 8.1, dan Windows 10, gunakan**Pencarian > secpol.msc** dan kemudian klik**polisi**.
- **Catatan:** Di semua versi Windows, Anda dapat menggunakan**Berlari** memerintah**secpol.msc** untuk membuka alat Kebijakan Keamanan Lokal.

## Kebijakan Akun Pengaturan Keamanan

- Kebijakan keamanan akan mengidentifikasi kebijakan kata sandi yang diperlukan.
- Kebijakan keamanan lokal Windows dapat digunakan untuk menerapkan kebijakan kata sandi.
  - Menggunakan**Kebijakan Akun > Kebijakan Kata Sandi**untuk menegakkan persyaratan kata sandi
  - Menggunakan**Kebijakan Akun > Kebijakan Penguncian Akun**untuk mencegah serangan brute-force
    - Kebijakan Penguncian Akun ini juga akan melindungi dari serangan kamus. Ini adalah jenis serangan brute-force yang mencoba setiap kata dalam kamus dengan harapan mendapatkan akses.

# Pengaturan Keamanan Kebijakan Lokal

- Kebijakan Lokal dalam Kebijakan Keamanan Lokal digunakan untuk mengkonfigurasi kebijakan audit, kebijakan hak pengguna, dan kebijakan keamanan.
  - Ini juga dapat digunakan untuk mencatat upaya login yang berhasil dan tidak berhasil.
- Gunakan **Kebijakan Lokal > Kebijakan Audit** untuk mengaktifkan audit.



## Mengekspor Kebijakan Keamanan Lokal

- Seorang administrator mungkin perlu menerapkan kebijakan lokal yang luas untuk hak pengguna dan opsi keamanan. Kebijakan ini kemungkinan besar perlu direplikasi pada setiap sistem.
- Untuk membantu menyederhanakan proses ini, **Kebijakan Keamanan Lokal** dapat diekspor dan disalin ke host Windows lainnya.
- Langkah-langkah untuk mereplikasi Kebijakan Keamanan Lokal di komputer lain adalah:
  1. Gunakan **Tindakan > Eksport Daftar...** fitur untuk mengekspor kebijakan host yang aman.
  2. Simpan kebijakan dengan nama, seperti **tasiun\_kerja.inf**. ke media eksternal.
  3. Kemudian impor berkas Kebijakan Keamanan Lokal ke komputer mandiri lainnya.

# Lab – Konfigurasi Kebijakan Keamanan Lokal Windows

Di lab ini, Anda akan mengonfigurasi Kebijakan Keamanan Lokal Windows. Anda akan mengubah persyaratan kata sandi, mengaktifkan audit, mengonfigurasi beberapa hak pengguna, dan menetapkan beberapa opsi keamanan. Anda kemudian akan menggunakan Pengelola Peristiwa untuk melihat informasi yang dicatat.

# Memelihara Akun

- **Mengakhiri Akses Karyawan**—Ketika seorang karyawan meninggalkan organisasi, segera nonaktifkan akun, atau ubah kredensial login.
- **Akses Tamu**—Akun tamu khusus untuk pekerja sementara dan tamu dengan hak istimewa tambahan dapat dibuat dan dinonaktifkan sesuai kebutuhan.
- **Lacak Waktu Login**—Izinkan karyawan login hanya selama jam-jam tertentu dalam sehari, dan blokir login pada sisa hari itu.
- **Log Upaya Login yang Gagal**—Konfigurasikan sejumlah waktu tertentu di mana pengguna dapat mencoba masuk.
- **Waktu Habis Diam dan Kunci Layar**—Konfigurasikan pengatur waktu siaga untuk secara otomatis mengeluarkan pengguna dari akun. Pengguna harus masuk kembali untuk membuka kunci layar.

# Mengelola Alat Akun Pengguna dan Tugas Akun Pengguna

## User Account Control (UAC)

- Control Panel > User Accounts > Manage another account
- Use this to add, remove, or change attributes of individual users.
- When logged in as an administrator, use the UAC to configure settings to prevent malicious code from gaining administrative privileges.

## Local Users and Groups Manager

- Control Panel > Administrative Tools > Computer Management > Local Users and Groups
- Can be used to create and manage users and groups that are stored locally on a computer.

## Manajer Pengguna dan Grup Lokal

- Alat Pengguna dan Grup Lokal dapat membatasi kemampuan pengguna dan grup untuk melakukan tindakan tertentu dengan menetapkan hak dan izin
- Untuk mengkonfigurasi semua pengguna dan grup di komputer menggunakan**Manajer Pengguna dan Grup Lokal** alat, ketik **lusrmgr.msc** di kotak Pencarian, atau utilitas Jalankan Baris.
  - Itu **Pengguna dan Grup Lokal > Pengguna** jendela menampilkan akun pengguna saat ini pada komputer.
- Klik dua kali pada pengguna atau klik kanan dan pilih **Properti** membuka jendela properti pengguna:
  - mengubah opsi pengguna yang ditentukan saat pengguna dibuat
  - mengunci akun
  - menetapkan pengguna ke dalam grup
  - mengontrol folder mana yang dapat diakses pengguna.
- Untuk menambahkan pengguna, klik **Tindakan** menu dan pilih **Pengguna Baru**.
- Di sini Anda dapat menetapkan nama pengguna, nama lengkap, deskripsi, dan opsi akun.

# Mengelola Grup

- Pengguna dapat dimasukkan ke dalam grup untuk memudahkan pengelolaan.
- Alat Manajer Pengguna dan Grup Lokal digunakan untuk mengelola grup lokal pada komputer Windows.
  - Menggunakan **Panel Kontrol > Alat Administratif > Manajemen Komputer > Pengguna dan Grup Lokal** untuk membuka Manajer Pengguna dan Grup Lokal.
  - Dari jendela Pengguna dan Grup Lokal, klik dua kali **Kelompok** untuk mencantumkan semua grup lokal pada komputer.
- Klik dua kali grup untuk melihat propertiya.
- Untuk membuat grup baru, klik **Aksi > Grup Baru** untuk membuka **Grup Baru** jendela
  - Di sini Anda dapat membuat grup baru dan menetapkan pengguna ke dalamnya.

## Pengguna dan Komputer Direktori Aktif

- Sementara akun lokal disimpan dalam database Akun Keamanan Lokal di komputer lokal, akun domain disimpan di Direktori Aktif pada Pengontrol Domain (DC) Windows Server.
- Hanya administrator domain yang diizinkan membuat akun domain di Pengendali Domain.
  - Akun domain dapat diakses dari komputer mana pun yang terhubung ke domain.
- Direktori Aktif adalah basis data semua komputer, pengguna, dan layanan dalam domain Direktori Aktif.
  - Konsol Pengguna dan Komputer Direktori Aktif di server Windows digunakan untuk mengelola pengguna, grup, dan Unit Organisasi (OU) Direktori Aktif.
    - Unit organisasi menyediakan cara untuk membagi domain menjadi unit administratif yang lebih kecil.
- Membuat akun grup baru di direktori aktif mirip dengan membuat pengguna baru.
  - Buka Pengguna dan Komputer Direktori Aktif dan pilih wadah yang akan menampung grup, klik **Tindakan**, klik **Baru** dan kemudian klik **Kelompok** dan isi detail grup dan klik **OKE**.

## Lab – Konfigurasi Pengguna dan Grup di Windows

Di lab ini, Anda akan membuat pengguna dan grup serta menghapus pengguna menggunakan Pengelola Pengguna dan Grup Lokal. Anda juga akan menetapkan izin grup dan pengguna ke folder.

## Tembok Api

- Firewall melindungi komputer dan jaringan dengan mencegah lalu lintas yang tidak diinginkan memasuki jaringan internal.
- Firewall dapat mengizinkan pengguna luar mengontrol akses ke layanan tertentu.
- Layanan firewall dapat disediakan sebagai berikut:
  - **Firewall berbasis host**-Menggunakan perangkat lunak seperti Windows Defender Firewall.
  - **Kantor rumah kantor kecil (SOHO)**-Solusi berbasis jaringan menggunakan router nirkabel rumah atau kantor kecil.
  - **Organisasi kecil hingga menengah**-Solusi berbasis jaringan menggunakan perangkat khusus seperti Cisco Adaptive Security Appliance (ASA) atau diaktifkan pada Cisco Integrated Services Router (ISR).
  - Fokus bagian ini adalah pada solusi firewall berbasis host menggunakan Windows Firewall.

## Firewall Perangkat Lunak

- Firewall perangkat lunak adalah program yang menyediakan layanan firewall pada komputer untuk mengizinkan atau menolak lalu lintas ke komputer.
  - Firewall perangkat lunak menerapkan serangkaian aturan pada transmisi data melalui pemeriksaan dan penyaringan paket data.
- Windows Firewall adalah contoh firewall perangkat lunak yang membantu mencegah penjahat dunia maya dan malware mendapatkan akses ke komputer Anda.
  - Ini terinstal secara default ketika OS Windows diinstal.
    - **Catatan:** Pada Windows 10, Windows Firewall diubah namanya menjadi Windows Defender Firewall. Di bagian ini, Windows Firewall mencakup Windows Defender Firewall.
- Pengaturan Windows Firewall dikonfigurasi menggunakan jendela Windows Firewall.
  - Untuk mengubah pengaturan Windows Firewall, Anda harus memiliki hak administrator untuk membuka jendela Windows Firewall.
  - Untuk membuka jendela Windows Firewall, gunakan**Panel Kontrol > Firewall Windows**.

## Tembok Api Windows

- Windows Firewall memiliki seperangkat aturan masuk dan keluar standar yang diaktifkan tergantung pada lokasi jaringan yang terhubung.
  - Aturan firewall dapat diaktifkan untuk jaringan pribadi, jaringan tamu atau publik, atau jaringan domain perusahaan.
- Dari jendela Windows Firewall, Anda dapat mengaktifkan atau menonaktifkan Windows Firewall, mengubah pengaturan notifikasi, mengizinkan aplikasi melewati firewall, mengkonfigurasi pengaturan lanjutan, atau mengembalikan default firewall.
- Jika Anda ingin menggunakan firewall perangkat lunak yang berbeda, Anda harus menonaktifkan Windows Firewall.

## Mengonfigurasi Pengecualian di Windows Firewall

- Anda dapat mengizinkan atau menolak akses ke program atau port tertentu dari jendela Windows Firewall.
- Untuk mengonfigurasi pengecualian dan mengizinkan atau memblokir aplikasi atau port, klik**Izinkan aplikasi atau fitur melalui Windows Firewall**untuk membuka jendela aplikasi yang diizinkan dan dapat:
  - Tambahkan program atau port yang diizinkan
  - Mengubah program atau port yang diizinkan
  - Hapus program atau port yang diizinkan

## Firewall Windows dengan Keamanan Tingkat Lanjut

- Alat Windows lain yang tersedia untuk menyediakan kontrol akses lebih besar dengan kebijakan Windows Firewall adalah Windows Firewall dengan Keamanan Lanjut.
  - Ini disebut Windows Defender Firewall dengan Keamanan Lanjut di Windows 10.
- Untuk membukanya, dari jendela Windows Firewall, klik **Pengaturan lanjutan** untuk membukanya.
  - **Catatan:** Atau, masukkan **wf.msc** di kotak pencarian dan tekan enter.
- Windows Defender Firewall dengan Keamanan Lanjut menyediakan fitur-fitur berikut:
  - **Aturan Masuk dan Keluar**—Konfigurasikan aturan masuk yang diterapkan pada lalu lintas internet masuk dan aturan keluar yang diterapkan pada lalu lintas yang meninggalkan komputer Anda.
  - **Aturan Keamanan Koneksi**—Mengamankan lalu lintas antara dua komputer dan mengharuskan kedua komputer memiliki aturan yang sama yang ditetapkan dan diaktifkan.
  - **Pemantauan**—Menampilkan aturan aktif masuk atau keluar firewall atau aturan keamanan koneksi aktif.

# Lab – Konfigurasi Windows Firewall

Di lab ini, Anda akan menjelajahi Windows Firewall dan mengonfigurasi beberapa pengaturan lanjutan.

## Keamanan Web

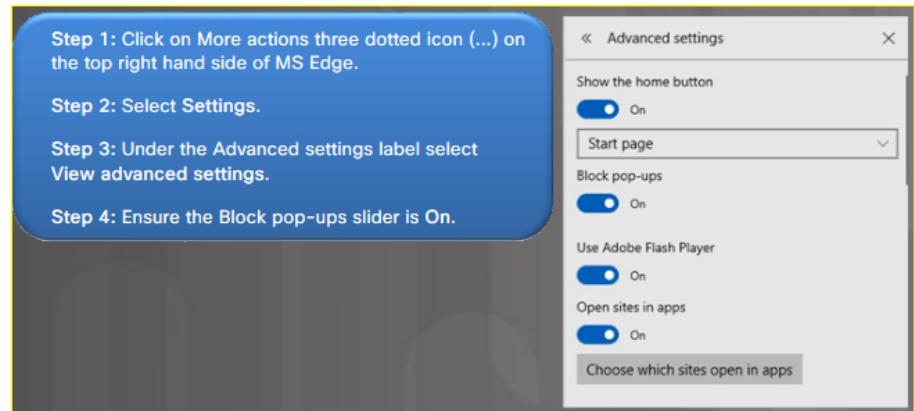
- Peramban web tidak hanya digunakan untuk menjelajah web, tetapi sekarang juga digunakan untuk menjalankan aplikasi lain termasuk Microsoft 365, Google Docs, antarmuka untuk pengguna SSL akses jarak jauh, dan banyak lagi.
- Untuk membantu mendukung fitur-fitur tambahan ini, browser menggunakan plug-in untuk mendukung konten lainnya.
  - Akan tetapi, beberapa plug-in ini juga dapat menimbulkan masalah keamanan.
- Peramban adalah target dan harus diamankan.

## Penjelajahan InPrivate

- Peramban web menyimpan informasi tentang halaman web yang Anda kunjungi, pencarian yang Anda lakukan, dan informasi identitas lainnya termasuk nama pengguna, kata sandi, dan lainnya.
- Informasi yang disimpan oleh peramban web dapat dipulihkan dan dimanfaatkan untuk mencuri identitas Anda, uang Anda, atau mengubah kata sandi pada akun penting.
- Untuk meningkatkan keamanan saat menggunakan komputer publik, selalu:
  - **Hapus riwayat penelusuran Anda**—Semua peramban web memiliki cara untuk menghapus riwayat penelusuran, cookie, file, dan banyak lagi.
  - **Gunakan mode InPrivate**—Menggunakan browser InPrivate akan menyimpan file dan cookie sementara dan menghapusnya ketika sesi InPrivate berakhir.
- Untuk Internet Explorer 11, gunakan**Alat > Penjelajahan InPrivate**
  - **Catatan:**Sebagai pers alternatif**Ctrl+Shift+P**untuk membuka jendela InPrivate.

## Pemblokir Pop-up

- Pop-up dimulai saat menjelajah, seperti tautan pada halaman yang membuka pop-up untuk menyampaikan informasi tambahan atau gambar close-up.
- Beberapa pop-up dimulai oleh situs web atau pengiklan dan sering kali tidak diinginkan atau mengganggu.
- Sebagian besar peramban web menawarkan kemampuan untuk memblokir jendela pop-up.
  - Hal ini memungkinkan pengguna untuk membatasi atau memblokir sebagian besar pop-up yang muncul saat menjelajah web.
  - Untuk mengaktifkan fitur Pemblokir Pop-up Internet Explorer 11, gunakan **Alat > Pemblokir Pop-up > Aktifkan Pemblokir Pop-up.**



# Filter Layar Pintar

**Step 1:** Click on More actions three dotted icon (...) on the top right hand side of MS Edge.

**Step 2:** Select Settings.

**Step 3:** Under the Advanced settings label select View advanced settings.

**Step 4:** Scroll to the bottom of this list to the Help protect me from malicious sites and downloads with Windows Defender SmartScreen and ensure the slider is On.

Let sites save protected media licenses on my device

On

Use page prediction to speed up browsing, improve reading, and make my overall experience better

On

Help protect me from malicious sites and downloads with Windows Defender SmartScreen

On

## Penyaringan ActiveX

- Beberapa peramban web mungkin mengharuskan Anda memasang kontrol ActiveX.
  - Kontrol ActiveX dapat digunakan untuk tujuan jahat.
- Ketika penyaringan ActiveX diaktifkan, Anda dapat memilih situs web mana yang diizinkan untuk menjalankan kontrol ActiveX.
  - Situs yang tidak disetujui tidak dapat menjalankan kontrol ini, dan browser tidak menampilkan pemberitahuan bagi Anda untuk memasang atau mengaktifkannya.
- Untuk mengaktifkan penyaringan ActiveX di Internet Explorer 11, gunakan**Alat > Penyaringan ActiveX**.
- Untuk melihat situs web yang berisi konten ActiveX saat pemfilteran ActiveX diaktifkan, klik tombol biru **Penyaringan ActiveX** ikon di bilah alamat, dan klik**Matikan Penyaringan ActiveX**.
  - Setelah melihat konten, Anda dapat mengaktifkan kembali penyaringan ActiveX untuk situs web tersebut dengan mengikuti langkah yang sama.

# Pengaturan Terbatas

- Perangkat sering kali dilengkapi dengan fitur keamanan yang tidak diaktifkan atau fitur keamanan menggunakan pengaturan default.
  - Pengaturan permisif default dapat membuat perangkat rentan terhadap penyerang.
- Banyak perangkat sekarang dikirimkan dengan pengaturan terbatas dan harus dikonfigurasi untuk mengaktifkan akses.
- Merupakan tanggung jawab Anda untuk mengamankan perangkat dan mengonfigurasi pengaturan pembatasan bila memungkinkan.

### Nonaktifkan Putar Otomatis

- Host Windows lama menggunakan AutoRun untuk menyederhanakan pengalaman pengguna.
  - Ketika media baru (misalnya, flash drive, CD, atau DVD drive) dimasukkan ke dalam komputer, AutoRun akan secara otomatis mencari file bernama **autorun.inf** dan mengeksekusinya.
  - Pengguna jahat menggunakan fitur ini untuk menginfeksi host.
- Host Windows yang lebih baru sekarang menggunakan AutoPlay.
- AutoPlay menyediakan kontrol tambahan dan dapat meminta pengguna untuk memilih tindakan berdasarkan konten media baru.
  - Gunakan **Panel Kontrol > Putar Otomatis** jendela, untuk membuka jendela Putar Otomatis dan mengonfigurasi tindakan yang terkait dengan media tertentu.
- Solusi yang paling aman adalah mematikan AutoPlay.

# Paket Layanan dan Patch Keamanan Sistem Operasi

- Patch merupakan pembaruan kode yang disediakan produsen untuk mencegah virus atau worm yang baru ditemukan agar tidak berhasil melakukan serangan.
  - Produsen dapat menggabungkan patch dan pemutakhiran menjadi aplikasi pemutakhiran komprehensif yang disebut paket layanan.
- Sangat penting untuk menerapkan patch keamanan dan pembaruan OS bila memungkinkan.
- Windows secara rutin memeriksa situs web Pembaruan Windows untuk pembaruan berprioritas tinggi yang dapat membantu melindungi komputer dari ancaman keamanan terkini.
  - Bergantung pada pengaturan yang Anda pilih, Windows secara otomatis mengunduh dan menginstal pembaruan berprioritas tinggi yang dibutuhkan komputer Anda atau memberitahukan Anda saat pembaruan tersebut tersedia.

# 13.4 Konfigurasi Keamanan Nirkabel

# Jenis Enkripsi Komunikasi Umum

- Komunikasi antara dua komputer mungkin memerlukan komunikasi yang aman.
- Ada dua persyaratan utama:
  - Persyaratan pertama adalah bahwa informasi yang diterima belum diubah oleh seseorang yang telah menyadap pesan tersebut.
  - Yang kedua adalah siapa pun yang dapat menyadap pesan tersebut tidak dapat membacanya.
- Teknologi berikut ini memenuhi persyaratan tersebut:
  - Pengkodean hash
  - Enkripsi simetris
  - Enkripsi asimetris

# Jenis Enkripsi Komunikasi Umum (Lanjutan)

- Pengkodean hash, atau hashing, memastikan integritas pesan.
  - Ini berarti pesan tersebut tidak rusak atau diutak-atik selama pengiriman.
  - Hashing menggunakan fungsi matematika untuk membuat nilai numerik, yang disebut intisari pesan yang unik untuk data tersebut
  - Algoritma hashing yang paling populer adalah Secure Hash Algorithm (SHA), yang menggantikan algoritma Message Digest 5 (MD5) yang lama.

# Jenis Enkripsi Komunikasi Umum (Lanjutan)

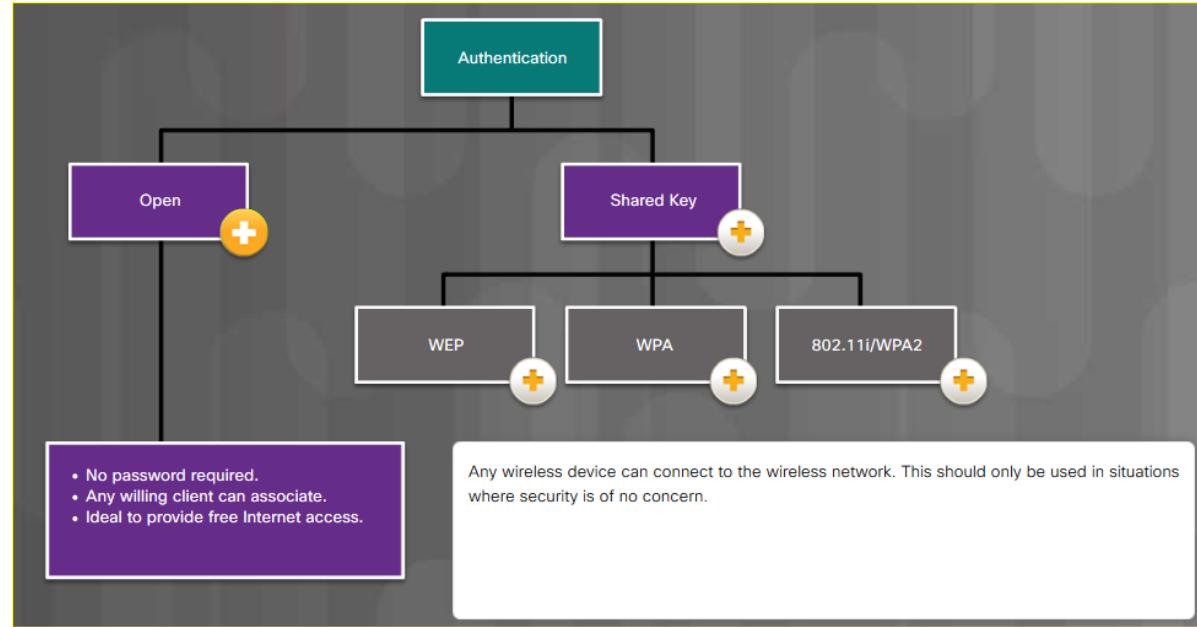
- Enkripsi simetris memastikan kerahasiaan pesan.
  - Jika pesan terenkripsi dicegat, pesan tersebut tidak dapat dipahami. Pesan tersebut hanya dapat didekripsi (yaitu, dibaca) menggunakan kata sandi (yaitu, kunci) yang digunakan untuk mengenkripsinya.
  - Enkripsi simetris mengharuskan kedua sisi percakapan terenkripsi menggunakan kunci enkripsi yang identik untuk mengodekan dan mendekodekan data.
  - Advanced Encryption Standard (AES) dan Triple Data Encryption Algorithm (3DES) yang lebih lama adalah contoh enkripsi simetris.
- Enkripsi asimetris juga memastikan kerahasiaan pesan.
  - Dibutuhkan dua kunci, kunci pribadi dan kunci publik.
  - Kunci publik dapat didistribusikan secara luas, termasuk mengirim email dalam bentuk teks biasa atau memposting di web.
  - Kunci pribadi disimpan oleh seorang individu dan tidak boleh diungkapkan kepada pihak lain mana pun.
  - RSA adalah contoh enkripsi asimetris yang paling populer.

## Pengidentifikasi Set Layanan

- Service Set Identifier (SSID) adalah nama jaringan nirkabel.
  - Router nirkabel atau titik akses menyiaran SSID secara default sehingga perangkat dapat mendeteksi jaringan nirkabel.
- Jika pengaturan siaran SSID telah dinonaktifkan pada router nirkabel atau titik akses, pengguna harus memasukkan SSID secara manual pada klien nirkabel untuk terhubung ke jaringan nirkabel.
  - Menonaktifkan siaran SSID memberikan sedikit keamanan:
    - Seseorang yang mengetahui SSID jaringan nirkabel dapat memasukkannya secara manual.
    - Jaringan nirkabel juga akan menyiaran SSID selama pemindaian komputer.
    - SSID juga dapat dicegat saat transit.

# Metode Autentikasi

- Kunci Bersama menyediakan mekanisme untuk mengautentikasi dan mendekripsi data antara klien nirkabel dan AP router nirkabel.
- WEP adalah singkatan dari Wired Equivalent Privacy.
- WPA adalah singkatan dari Wi-Fi Protected Access.
- IEEE 802.11i/WPA2 adalah standar industri terkini untuk mengamankan WLAN. Keduanya menggunakan Advanced Encryption Standard (AES).



# Mode Keamanan Nirkabel

### Wireless Security Modes

Instructions

Click each of the buttons for more information on wireless security modes.

**WPA2**

Use a wireless encryption system to encode the information being sent to prevent unwanted capture and use of data. Most wireless access points support several different security modes. As discussed in a previous chapter, always implement the strongest security mode (WPA2) possible.

Firmware Version: v0.93.3

Wireless-N Broadband Router WRT300N

Wireless Setup Wireless Security Access Restrictions Applications & Gaming Administration Status

Basic Wireless Settings Wireless Security Wireless MAC Filter Advanced Wireless Settings

Wireless Security

Security Mode:

- Disabled
- Disabled
- WEP
- WPA Personal
- WPA Enterprise
- WPA2 Personal**
- WPA2 Enterprise

WPS

# Mode Keamanan Nirkabel (Lanjutan)

### Wireless Security Modes

Instructions

Click each of the buttons for more information on wireless security modes.

### WPS

Many routers offer Wi-Fi Protected Setup (WPS). With WPS, both the router and the wireless device will have a button that, when both are pressed, automatically configures Wi-Fi security between the devices. A software solution using a PIN is also common. It is important to know that WPS is not entirely secure. It is vulnerable to brute-force attack. WPS should be turned off as a security best practice.

 CISCO

© 2016 Cisco dan/atau afiliasinya. Semua hak dilindungi undang-undang. Cisco Confidential

92

## Pembaruan Firmware

- Sebagian besar router nirkabel menawarkan firmware yang dapat dimutakhirkan.
  - Rilis firmware mungkin berisi perbaikan untuk masalah umum yang dilaporkan oleh pelanggan serta kerentanan keamanan.
- Penting untuk memeriksa situs web produsen secara berkala guna mengetahui firmware terkini.
- Umumnya, GUI digunakan untuk mengunggah firmware ke router nirkabel.

## Tembok Api

- Firewall perangkat keras memeriksa paket data dari jaringan sebelum mencapai perangkat di dalam jaringan.
  - Firewall dapat dikonfigurasi untuk memblokir port individual, serangkaian port, atau lalu lintas aplikasi tertentu.
- Sebagian besar router nirkabel juga menyertakan firewall perangkat keras terintegrasi.
- Mereka dapat dikonfigurasi untuk mengizinkan dua jenis lalu lintas berbeda ke jaringan Anda:
  - Respons terhadap lalu lintas yang berasal dari dalam jaringan Anda
  - Lalu lintas yang ditujukan ke pelabuhan yang sengaja Anda biarkan terbuka

# Penerusan Port dan Pemicu Port

- Firewall perangkat keras dapat digunakan untuk memblokir port guna mencegah akses tidak sah masuk dan keluar LAN.
- Namun, ada situasi ketika port tertentu harus dibuka agar program dan aplikasi tertentu dapat berkomunikasi dengan perangkat di jaringan berbeda.
- Penerusan port adalah metode berbasis aturan untuk mengarahkan lalu lintas antara perangkat di jaringan terpisah.

## Pasang dan Mainkan Universal

- Universal Plug and Play (UPnP) adalah protokol yang memungkinkan perangkat untuk meneruskan lalu lintas secara dinamis melalui port jaringan tanpa memerlukan campur tangan atau konfigurasi pengguna.
- Penerusan port sering digunakan untuk:
  - Media streaming
  - Menjadi tuan rumah pertandingan
  - Menyediakan layanan dari komputer rumah dan bisnis kecil hingga internet.

# Packet Tracer – Konfigurasi Keamanan Nirkabel

Dalam aktivitas ini, Anda akan mengonfigurasi router nirkabel untuk:

- Gunakan WPA2 Personal sebagai metode keamanan
- Mengandalkan penyaringan MAC untuk meningkatkan keamanan
- Mendukung Penerusan Port Tunggal

# 13.5 Proses Pemecahan Masalah Dasar untuk Keamanan

# Proses Pemecahan Masalah

Step 1. Identify the problem.

Step 2. Establish a theory of probable cause.

Step 3. Test the theory to determine the cause.

Step 4. Establish a plan of action to resolve the problem and implement the solution.

Step 5. Verify full system functionality and if applicable, implement preventive measures.

Step 6. Document findings, actions, and outcomes.

## Mengidentifikasi Masalah

### Step 1 - Identify the Problem

Open-ended questions	<ul style="list-style-type: none"><li>• When did the problem start?</li><li>• What problems are you experiencing?</li><li>• What websites have you visited recently?</li><li>• What security software is installed on your computer?</li><li>• Who else has used your computer recently?</li></ul>
Closed-ended questions	<ul style="list-style-type: none"><li>• Is your security software up to date?</li><li>• Have you scanned your computer recently for viruses?</li><li>• Did you open any attachments from a suspicious email?</li><li>• Have you changed your password recently?</li><li>• Have you shared your password?</li></ul>

## Menetapkan Teori Penyebab yang Mungkin

### Step 2: Establish a Theory of Probable Cause

Common causes of security problems

- Virus
- Trojan Horse
- Worm
- Spyware
- Adware
- Grayware or Malware
- Phishing scheme
- Password compromised
- Unprotected equipment rooms
- Unsecured work environment

## Uji Teori untuk Menentukan Penyebabnya

### Step 3. Test the Theory to Determine Cause

#### Common steps to determine cause

- Disconnect from the network.
- Update antivirus and spyware signatures.
- Scan computer with protection software.
- Check computer for the latest OS patches and updates.
- Reboot the computer or network device.
- Login as an administrative user to change a user's password.
- Secure equipment rooms.
- Secure work environment.
- Enforce security policy.

## Tetapkan Rencana Aksi untuk Menyelesaikan Masalah dan Menerapkan Solusinya

### Step 4: Establish a Plan of Action to Resolve the Problem and Implement the Solution

If no solution is achieved in the previous step, further research is needed to implement the solution.

- Helpdesk repair logs
- Other technicians
- Manufacturer FAQ websites
- Technical websites
- News groups
- Computer manuals
- Device manuals
- Online forums
- Internet search

## Verifikasi Fungsionalitas Sistem Penuh dan jika Berlaku Terapkan Tindakan Pencegahan

### Step 5: Verify Full System Functionality and if Applicable Implement Preventive Measures

Verify solution and full system functionality for laptops

- Re-scan computer to ensure no viruses remain.
- Re-scan computer to ensure no spyware remains.
- Check the security software logs to ensure no problems remain.
- Check computer for the latest OS patches and updates.
- Test network and Internet connectivity.
- Ensure all applications are working.
- Verify access to authorized resources such as shared printers and databases.
- Make sure entries are secured.
- Ensure security policy is enforced.

# Temuan, Tindakan, dan Hasil Dokumen

## Step 6: Document Findings, Actions, and Outcomes

Document your findings, actions, and outcomes

- Discuss the solution implemented with the customer.
- Have the customer verify problem has been solved.
- Provide the customer with all paperwork.
- Document the steps taken to solve the problem in the work order and technician's journal.
- Document any components used in the repair.
- Document the time spent to solve the problem.

# Masalah Umum dan Solusi Keamanan

## Mengidentifikasi Masalah Umum dan Solusinya

### Identify Common Problems and Solutions

#### Symptoms

A security alert is displayed.

An authorized wireless access point is discovered on the network.

System files have been renamed, applications crash, files are disappearing, or file permissions have changed.

Windows update fails.

Your wireless network is compromised even though 128-bit WEP encryption is used.

A user is receiving hundreds or thousands of junk emails each day.

An unknown printer repair person is observed looking under keyboards and on desktops.

Users with flash drives are infecting computers on the network with viruses.

Your email contacts report spam coming from you.

#### Instructions

Security problems can be attributed to a number of reasons. You will resolve some types of security problems more often than others.

Click on a symptom to see possible causes and solutions. At any time, click another symptom on the left side of the screen. To see a PDF of the entire table, click the PDF of Table button on the lower right corner of the screen.

#### A security alert is displayed.

Probable Causes	Possible Solutions
<ul style="list-style-type: none"><li>The windows firewall is disabled.</li></ul>	<ul style="list-style-type: none"><li>Enable the Windows Firewall.</li></ul>
<ul style="list-style-type: none"><li>Virus definitions are out-of-date.</li></ul>	<ul style="list-style-type: none"><li>Update virus definitions.</li></ul>
<ul style="list-style-type: none"><li>Malware has been detected.</li></ul>	<ul style="list-style-type: none"><li>Scan for malware.</li></ul>

Show PDF

## Masalah Umum dan Solusi Keamanan

### Lab – Mendokumentasikan Informasi Pelanggan dalam Perintah Kerja

Di lab ini, Anda akan mendokumentasikan informasi pelanggan dalam perintah kerja.

# 13.6 Ringkasan Bab

## Bab 13: Keamanan

- Menjelaskan ancaman keamanan umum dan cara mencegah dan memulihkan dari ancaman.
- Identifikasi tujuan dan penggunaan prosedur keamanan dalam melindungi peralatan fisik dan data.
- Amankan stasiun kerja Windows dalam BIOS, Sistem Operasi, dan firewall.
- Konfigurasikan pengaturan keamanan nirkabel pada router kantor kecil/kantor rumah.
- Pecahkan masalah umum untuk keamanan

