Computer and Network Security
Security in Operating System

VER 2020

KEAMANAN SISTEM OPERASI LINUX

Account Pemakai (user account)

- Keuntungan :
  - Kekuasaan dalam satu account yaitu root, sehingga mudah dalam administrasi system.
  - Kecerobohan salah satu user tidak berpengaruh kepada system secara keseluruhan.
  - Masing-masing user memiliki privacy yang ketat
- Macam-macam User :
  - Root : kontrol system file, user, sumber daya (devices) dan akses jaringan
  - User : account dengan kekuasaan yang diatur oleh root dalam melakukan aktifitas dalam system.
  - Group : kumpulan user yang memiliki hak sharing yang sejenis terhadap suatu devices tertentu.

Kontrol Akses secara Diskresi (Discretionary Access control)

Discretionary Access control (DAC) adalah metode pembatasan yang ketat, meliputi :

- Setiap account memiliki username dan password sendiri.
- Setiap file/device memiliki atribut (read/write/execution) kepemilikan, group, dan uses umum.

Discretionary Access control

Jika dilakukan list secara detail menggunakan $ls-l, sehingga dapat melihat penerapan DAC pada file system Linux :

```
d rw- --x --- 5 fade users 1024 Feb 8 12:30 Desktop
-rw- r-- r-- 9 Goh hack 318 Mar 30 09:05 borg.dead.letter
```

Perbedaan Permission pada Directory dan File

Access Type	File	Directory
Read	If the file contents can be read	If the directory listing can be obtained
Write	If user or process can write to the file (change its contents)	If user or process can change directory contents somehow: create new or delete existing files in the directory or rename files.
Execute	If the file can be executed	If user or process can access the directory, that is, go to it (make it to be the current working directory)

Discretionary Access control

```
d  rw-  - -x   - - -  5  fade  users  1024  Feb   8  12:30  Desktop
- rw-  r - -   r - -  9  Goh   hack    318  Mar  30  09:05  borg.dead.letter
```

-	rw-	r - -	r - -	9	Goh	hack	318	Mar	30	09:05	borg.dead.letter
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**		**11**

Keterangan :

1 = tipe dari file ; tanda dash (-) berarti file biasa, d berarti directory, l berarti file link, dsb

2 = Izin akses untuk owner (pemilik), r=read/baca, w=write/tulis, x=execute/eksekusi

3 = Izin akses untuk group

4 = Izin akses untuk other (user lain yang berada di luar group yang didefinisikan sebelumnya)

5 = Jumlah link file

6 = Nama pemilik (owner)

7 = Nama Group

8 = Besar file dalam byte

9 = Bulan dan tanggal update terakhir

10 = Waktu update terakhir

11 = Nama file/device

Perintah-perintah penting pada DAC

- Mengubah izin akses file :

1. bu : **chmod < u | g | o > < + | - > < r | w | e > nama file**,
   contoh :
   chmod u+x g+w o-r borg.dead.letter ; tambahkan akses eksekusi(e) untuk user (u), tambahkan juga akses write(w) untuk group (g) dan kurangi izin akses read(r) untuk other(o) user.
2. chmod metode octal, bu: **chmod** - - - **namafile** , digit dash (-) pertama untuk izin akses user, digit ke-2 untuk izin akses group dan digit ke-3 untuk izin akses other, berlaku ketentuan : r(read) = 4, w(write) = 2, x (execute) = 1 dan tanpa izin akses = 0.
   Contoh :
   Chmod 740 borg.dead.letter
   Berarti : bagi file *borg.dead.letter* berlaku
   digit ke-1 → 7=4+2+1=izin akses r,w,x penuh untuk user.
   digit ke-2 → 4=4+0+0=izin akses r untuk group
   digit ke-3 → 0=0+0+0=tanpa izin akses untuk other user.

Perintah-perintah penting pada DAC

- Mengubah kepemilikan : chown <owner/pemilik><nama file>
- Mengubah kepemilikan group : chgrp <group owner><nama file>
- Menggunakan account root untuk sementara :

  ~$su ; system akan meminta password
  password : **** ; prompt akan berubah jadi pagar, tanda login sebagai root
  ~#

- Mengaktifkan shadow password, yaitu membuat file **/etc/passwd** menjadi dapat dibaca (readable) tetapi tidak lagi berisi password, karena sudah dipindahkan ke **/etc/shadow**

Contoh tipikal file **/etc/passwd** setelah diaktifkan shadow:

```
...
root:x:0:0::/root:/bin/bash
fade:x:1000:103: , , , :/home/fade:/bin/bash
...
```

SELinux (1)

- Security Enhanced Linux or **SELinux** is a set of modifications developed by the United States National Security Agency (NSA) to provide a variety of security policies for Linux. SELinux was released as open source at the end of 2000. Since kernel version 2.6 it is an integrated part of Linux.
- SELinux offers security. SELinux can control what kind of access users have to files and processes. Even when a file received **chmod 777**, SELinux can still prevent applications from accessing it (Unix file permissions are checked first!). SELinux does this by placing users in **roles** that represent a security context. Administrators have very strict control on access permissions granted to roles.
- SELinux is present in the latest versions of Red Hat Enterprise Linux, Debian, CentOS, Fedora, and many other distributions.

SELinux (2)

selinux knows three modes: enforcing, permissive and disabled. The **enforcing** mode will enforce policies, and may deny access based on **selinux rules**. The **permissive** mode will not enforce policies, but can still log actions that would have been denied in **enforcing** mode. The **disabled** mode disables **selinux**.

```
root@deb503:~# selinux-activate
Activating SE Linux
Searching for GRUB installation directory ... found: /boot/grub
Searching for default file ... found: /boot/grub/default
Testing for an existing GRUB menu.lst file ... found: /boot/grub/menu.lst
Searching for splash image ... none found, skipping ...
Found kernel: /boot/vmlinuz-2.6.26-2-686
Updating /boot/grub/menu.lst ... done

SE Linux is activated.  You may need to reboot now.
```

Password

- User **passwords** are **encrypted** and kept in /etc/shadow. The /etc/shadow file is read only and can only be read by root.
- Users can change their **password** with the /usr/bin/passwd command.

```
[root@centos7 ~]# tail -4 /etc/shadow
paul:$6$ikp2Xta5BT.Tml.p$2TZjNnOYNNQKpwLJqoGJbVsZG5/Fti8ovBRd.VzRbiDSl7TEq\
IaSMH.TeBKnTS/SjlMruW8qffC0JNORW.BTW1:16338:0:99999:7:::
tania:$6$8Z/zovxj$9qvoqT8i9KIrmN.k4EQwAF5ryz5yzNwEvYjAa9L5XVXQu.z4DlpvMREH\
eQpQzvRnqFdKkVj17H5ST.c79HDZw0:16356:0:99999:7:::
laura:$6$glDuTY5e$/NYYWLxfHgZFWeoujaXSMcR.Mz.lGOxtcxFocFVJNb98nbTPhWFXfKWG\
SyYh1WCv6763Wq54.w24Yr3uAZBOm/:16356:0:99999:7:::
valentina:$6$jrZa6PVI$1uQgqR6En9mZB6mKJ3LXRB4CnFko6LRhbh.v4iqUk9MVreui1lv7\
GxHOUDSKA0N55ZRNhGHa6T2ouFnVno/0o1:16356:0:99999:7:::
[root@centos7 ~]#
```

Kontrol akses jaringan (Network Access Control)

- **Firewall linux** :
  alat pengontrolan akses antar jaringan yangmembuat linux dapat memilih host yang berhak / tidak berhak mengaksesnya.

- **Fungsi Firewall linux :**
  - **Analisa dan filtering paket**

    Memeriksa paket TCP, lalu diperlakukan dengan kondisi yang sudah ditentukan, contoh paket A lakukan tindakan B.
  - **Blocking content dan protocol**

    Bloking isi paket seperti applet java, activeX, Vbscript, Cookies
  - **Autentikasi koneksi dan enkripsi**

    Menjalankan enkripsi dalam identitas user, integritas satu session dan melapisi data dengan algoritma enkripsi seperti : DES, triple DES, Blowfish, IPSec, SHA, MD5, IDEA, dsb.

Enkripsi

Penerapan Enkripsi di linux :

- Enkripsi password → menggunakan DES (Data Encryption Standard)
- Enkripsi komunikasi data :
  1. **Secure Shell (SSH)** → Program yang melakukan loging terhadap komputer lain dalam jaringan, mengeksekusi perintah lewat mesin secara remote dan memindahkan file dari satu mesin ke mesin lainnya. Enkripsi dalam bentuk Blowfish, IDEA, RSA, Triple DES. Isi SSH Suite :
     - scp (secure shell copy) → mengamankan penggandaan data
     - ssh (secure shell client) → model client ssh seperti telnet terenkripsi.
     - ssh-agent → otentikasi lewat jaringan dengan model RSA.
     - sshd (secure shell server) → di port 22
     - ssh-keygen → pembuat kunci (key generator) untuk ssh

     Konfigurasi dilakukan di :
     - /etc/sshd_config (file konfigurasi server)
     - /etc/ssh_config (file konfigurasi client)
  2. **Secure socket Layer (SSL)** → mengenkripsi data yang dikirimkan lewat port http. Konfigurasi dilakukan di : web server APACHE dengan ditambah PATCH SSL.

Logging

- Prosedur dari Sistem Operasi atau aplikasi merekam setiap kejadian d an menyimpan rekaman tersebut untuk dapat dianalisa.
- Semua file log linux disimpan di directory /var/log, antara lain :

  - **Lastlog** : rekaman user login terakhir kali
  - **last** : rekaman user yang pernah login dengan mencarinya pada file /var/log/wtmp
  - **xferlog** : rekaman informasi login di ftp daemon berupa data wktu akses, durasi transfer file, ip dan dns host yang mengakses, jumlah/nama file, tipe transfer(binary/ASCII), arah transfer(incoming/outgoing), modus akses(anonymous/guest/user resmi), nama/id/layanan user dan metode otentikasi.
  - **Access_log** : rekaman layanan http / webserver.
  - **Error_log** : rekaman pesan kesalahan atas service http / webserver berupa data jam dan waktu, tipe/alasan kesalahan
  - **Messages** : rekaman kejadian pada kernel ditangani oleh dua daemon :
    - Syslog → merekam semua program yang dijalankan, konfigurasi pada syslog.conf
    - Klog → menerima dan merekam semua pesan kernel

KEAMANAN SISTEM OPERASI

WINDOWS

(www.microsoft.com)

Windows Logon Scenarios (1)

Users can perform an interactive logon to a computer in either of two ways:

- ✓ **Locally**, when the user has direct physical access to the computer, or when the computer is part of a network of computers:
  - A local logon grants a user permission to access Windows resources on the local computer. **A local logon requires that the user has a user account in the Security Accounts Manager (SAM) on the local computer**. The SAM protects and manages user and group information in the form of security accounts stored in the local computer registry. The computer can have network access, but it is not required. Local user account and group membership information is used to manage access to local resources.
  - A network logon grants a user permission to access Windows resources on the local computer in addition to any resources on networked computers as defined by the credential's access token. Both a local logon and a network logon require that the user has a user account in the Security Accounts Manager (SAM) on the local computer. Local user account and group membership information is used to manage access to local resources, and the access token for the user defines what resources can be accessed on networked computers.
  - A local logon and a network logon are not sufficient to grant the user and computer permission to access and to use domain resources.
- ✓ **Remotely,** through Terminal Services or Remote Desktop Services (RDS), in which case the logon is further qualified as remote interactive.

Windows Logon Scenarios (2)

- **Network logon**
  - A network logon can only be used after user, service, or computer authentication has taken place. During network logon, the process does not use the credentials entry dialog boxes to collect data. Instead, previously established credentials or another method to collect credentials is used.
  - This process confirms the user's identity to any network service that the user is attempting to access. This process is typically invisible to the user unless alternate credentials have to be provided.

Windows Logon Scenarios (3)

- To provide this type of authentication, the security system includes these authentication mechanisms:
  - Kerberos version 5 protocol
  - Public key certificates
  - Secure Sockets Layer/Transport Layer Security (SSL/TLS)
  - Digest
  - NTLM, for compatibility with Microsoft Windows NT 4.0-based systems

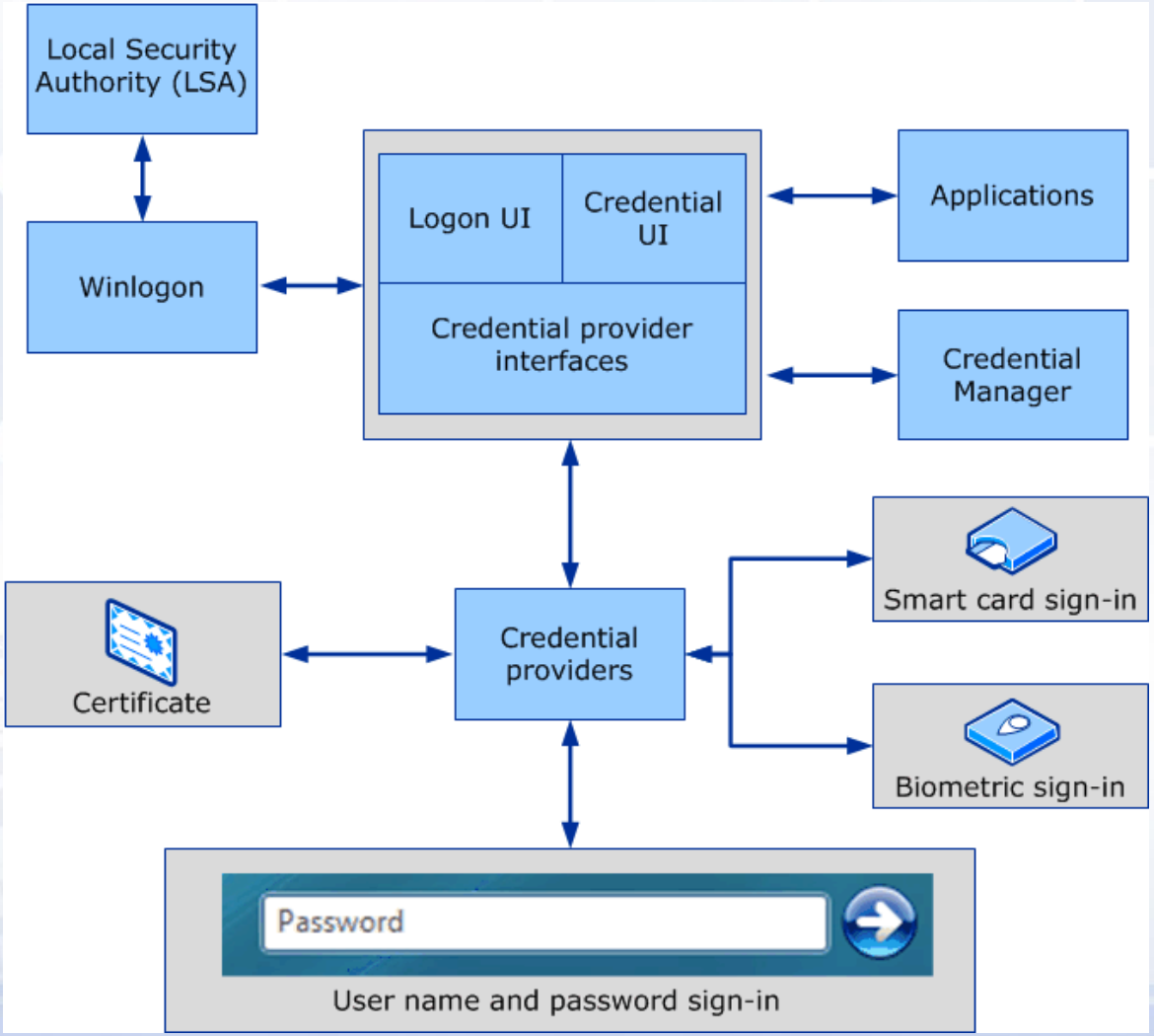
Smart card logon (1)

- Smart cards can be used to log on only to domain accounts, not local accounts. Smart card authentication requires the use of the Kerberos authentication protocol. Introduced in Windows 2000 Server, in Windows-based operating systems a public key extension to the Kerberos protocol's initial authentication request is implemented.
- In contrast to shared secret key cryptography, public key cryptography is asymmetric, that is, two different keys are needed: one to encrypt, another to decrypt. Together, the keys that are required to perform both operations make up a private/public key pair.

Smart card logon (2)

- To initiate a typical logon session, a user must prove his or her identity by providing information known only to the user and the underlying Kerberos protocol infrastructure. The secret information is a cryptographic shared key derived from the user's password. A shared secret key is symmetric, which means that the same key is used for both encryption and decryption.

Smart card logon (3)



How passwords work in Windows

- In Windows and many other operating systems, the most common method for authenticating a user's identity is to use a secret passphrase or password.
  - Securing your network environment requires that strong passwords be used by all users. This helps avoid the threat of a malicious user guessing a weak password, whether through manual methods or by using tools, to acquire the credentials of a compromised user account. This is especially true for administrative accounts. When you change a complex password regularly, it reduces the likelihood of a successful password attack.
- Password policy settings control the complexity and lifetime of passwords. Password policies affect Windows passwords, not necessarily feature passwords.
- Users' ability to modify their passwords is governed by the password policies and the available interfaces. For example, through the Secure Desktop, users can change their password at any time based upon the password policies administered by the system administrator or domain administrator. Features such as Windows Vault, BitLocker, and Encrypting File System allow users to modify passwords specific to that feature.
- In Windows, password is stored One-way function/HASH.

Local Security Authority

- The Local Security Authority (LSA) is a protected subsystem that authenticates and signs in users to the local computer. In addition, LSA maintains information about all aspects of local security on a computer (these aspects are collectively known as the local security policy). It also provides various services for translation between names and security identifiers (SIDs).
- The security subsystem keeps track of the security policies and the accounts that are on a computer system. In the case of a domain controller, these policies and accounts are those that are in effect for the domain in which the domain controller is located. These policies and accounts are stored in Active Directory. The LSA subsystem provides services for validating access to objects, checking user rights, and generating audit messages.

Security Support Provider Interface

- The Security Support Provider Interface (SSPI) is the API that obtains integrated security services for authentication, message integrity, message privacy, and security quality-of-service for any distributed application protocol.
- SSPI is the implementation of the Generic Security Service API (GSSAPI). SSPI provides a mechanism by which a distributed application can call one of several security providers to obtain an authenticated connection without knowledge of the details of the security protocol.

Network Security

- Windows Firewall is an important security application that's built into Windows. One of its roles is to block unauthorized access to your computer. The second role is to permit authorized data communications to and from your computer.
- Windows Firewall does these things with the help of rules and exceptions that are applied both to inbound and outbound traffic. They are applied depending on the type of network you are connected to and the location you have set for it in Windows, when connecting to the network. Based on your choice, the Windows Firewall automatically adjusts the rules and exceptions applied to that network.
- Windows Firewall is an important security application that's built into Windows. One of its roles is to block unauthorized access to your computer.
- Windows Firewall does these things with the help of rules and exceptions that are applied both to inbound and outbound traffic. They are applied depending on the type of network you are connected to and the location you have set for it in Windows, when connecting to the network. Based on your choice, the Windows Firewall automatically adjusts the rules and exceptions applied to that network.

Windows file security

- In Windows, files are securable objects. Access is managed by the same access control model that manages all other securable Windows objects.
- Windows compares the permissions and information requested by the thread access token with the information in the security descriptor of the file or directory. If there is a match, a handle is returned to the thread and authorization is granted.

File permissions in Windows (1)

- There are basically six types of permissions in Windows: Full Control, Modify, Read & Execute, **List Folder Contents**, Read, and Write. **List Folder Contents** is the only permission that is exclusive to folders.
- Every file and every folder in Windows has its own set of permissions. Permissions can be broken down into **Access Control Lists** with users and their corresponding rights

File permissions in Windows (2)

Permission	Meaning for Folders	Meaning for Files
Read	Permits viewing and listing of files and subfolders	Permits viewing or accessing of the file's contents
Write	Permits adding of files and subfolders	Permits writing to a file
Read & Execute	Permits viewing and listing of files and subfolders as well as executing of files; inherited by files and folders	Permits viewing and accessing of the file's contents as well as executing of the file
List Folder Contents	Permits viewing and listing of files and subfolders as well as executing of files; inherited by folders only	N/A
Modify	Permits reading and writing of files and subfolders; allows deletion of the folder	Permits reading and writing of the file; allows deletion of the file
Full Control	Permits reading, writing, changing, and deleting of files and subfolders	Permits reading, writing, changing and deleting of the file

end