Security

Gregory Mounie

2012-10-16 mar.

Outline

Security of network

The main problem

Internet connection are bi-directional.

- Any computer of the world may be connected to any other one
- Intruders will appear.
- If Somebody want access, he will get it with:
  - time and money
  - if collected/modified data are valuable for him

Goal of security

Delay the intrusion as long as possible

Security

The security is not a product

A secure computer is not connected to a network, is locked in a strongbox, and is turn off.

The security is an activity

You have to collect data and to manage and change your network

The security will annoy your user

You have to keep the balance between security and usability

Collect of data

- security institution http://www.cert.org
- hacking website
- mailing-list (eg. ter)
- website of system provider (microsoft)

Security by obscurity do not work, but it helps to gain some time.

3 kinds of network attack

1. DoS (Denial of Services). Easy to do: just send a lot of requests.
2. Intrusion: More difficult
   - need a connection to a host (web server, ftp server)
   - sometimes required password sniffing
   - sometimes required spoofing
3. Intrusion and root access
   - required system exploit
   - full access to data, troyan horse installation, relay

Security breaks

1. the users
2. external connections
3. physical access

Standard recommendation

ANSSI

The national agency of the security of information systems, created in 2008, (http://www.ssi.gouv.fr) define the security rules for the information systems of French national institutions. It investigates attacks. It also edits the rules that are presented in the following slides.

On-line exercise among the lecture

For every general recommendation in the following slides
Could you find

1. how to do it easily;
2. what are the requirement to do it;
3. why you or the users will not apply it.

Know the information system and its user

Build and maintain a map of hardware and software

- Keep the map on par with the reality.
- The map include network architecture (external connection, servers)
- The map of the network should not be stored in the network

List of all administrator accounts

- Keep the list on par with the reality
- not only root
- including users with their own hosts (root on their systems)

Know the information system and its user II

Write the procedure of arrival and departure of users

- how to create/destroy account
- physical access management
- mobile access management

Control and manage the network

Limit Internet access

No connection of personal hardware to the information system

Upgrade the software

Know how to upgrade your software

Check new published vulnerability and software update

Define the upgrade policy and apply it strictly

Authentication and password

Identify every user
No generic account

Define rules and length of password
http://xkcd.com/936

Check and enforce password rules

Authentication and password II

Do not keep passwords on the system

Suppress default passwords and certificates

Use physical device authentication
access card with PIN code

Secure the hosts

Homogeneous security policy

- No useless services
- as low as possible access right

No mobile storage
or at least no autorun (and no exec)

Central management tool of the security and upgrade

Secure the hosts II

Same security policy for mobile hosts

Crypt the data on mobile host and mobile storage

Split the network and control user dictionary

Audit frequently your central directory

Active Directory, LDAP, etc.

- Especially data access right

Split the network

Hosts with sensitive data should be on a sub-network with a specific gateway

Protect you network from the Internet

No internet access on admin hosts

Limit the number of gateway to the Internet

No admin interface should be accessible from the Internet

Avoid Wifi or any radio network

At least, use wifi on an isolated subnetwork. use WPA (EAP-TPS, WPA2 CCMP) with certificate when a large number of external clients will use the wifi (no share password).

Monitor your system

Define monitoring goal

Check the logs

Protect administrator station

Specific sub-network for admin hosts
Physical or Logical (IPSec tunnel)

Never give admin right to the users
Especially not to the manager !

Remote access only with strong authentication and cryptography

Control physical access

Control mechanism should define profile
employee, internship, external, ...

Keep secure the keys and alarm code

No physical access to the internal network in a public room

Printing rule
eg. destroy forgotten documents

Organize the reactions to incidents

Prepare reaction before the incident

Check for propagation, not only the treatment of the infected host

Plan the standard activities in case of incident

Every user should know the guy to contact in case of problem

Educate

Educate your user to minimal rules

- data are important
- data security is dependent of rule respect

Check your security

Check your security
at least once a year.

Next lecture

Disabing an account

lock :: passwd -l username unlock :: passwd -u username

sudo

sharing administrator right username ALL=(ALL) ALL

quota

activate it in /etc/fstab: usrquota, grpquota soft and hard limits on blocks and on inodes