Introduction to Linux Security

- for CSC Introduction to Linux and CSC Environment course in May 8, 2014

Urpo Kaila <urpo.kaila@csc.fi>

What is Security?

- Security is a set of appropriate procedures to protect your resources (your data, your account, your services and your reputation) against **risks**

- The main aspects of security are
  - Confidentiality (don't let anybody else know your password or confidential data)
  - Integrity (no malware on your computers, your data is at it should be)
  - Availability (keep your data and services available for those who should use it)

Security Risks and Compliance

- Typical risks for Linux users:
  - Compromised account (#1!)
  - System compromise
  - Denial of Service
  - Surveillance
  - Infrastructure related issues
  - Bad user and system administration
  - Legal issues

- You must comply with legal requirements and agreements
  - Do not endanger other users or the infrastructure
  - Protect personal data and other confidential information
  - As a User, you are responsible to protect your account

Security related obligations in CSC General Terms of Use (1/2)

Do not:

- Share your credentials, leave them for others to see, or neglect any security responsibilities defined in the service description.
- Misuse or abuse any CSC or third party service or property, including intellectual property. Obviously breaking the law is considered misuse.
- Misuse or abuse Users Content, credentials or other confidential information.
- Send or transmit harassing, abusive, libellous, obscene or unsolicited (spam) communications.

Security related obligations in CSC General Terms of Use (2/2)

Do not:

- Tamper with or deliberately disrupt system resources or network traffic to the Services.
- Users agree to notify CSC promptly if their account has been used without permission or if their credentials have been lost or stolen.
- Users are liable, even after the user account has been terminated, for any damage and costs CSC incurs as a result of violating these terms.

How to protect yourself?

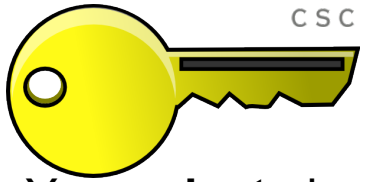
- Compromised account
  - Good passwords, hard to guess, easy to remember
  - 8 chars min., complexity, use password managers (Keepass)
  - Be carefull with public systems and services
  - User keys instead of passwords (but protect your keys too!)
- System compromise
  - Patch your own system regularly, keep firewall (iptables, ufw) on, use only necessary services
- Denial of Service
  - Offer only the necessary services to others
- Surveillance
  - Don’t store any confidential information on cloud services
- Bad user and system administration
  - Beware of test accounts, patch your system

Patch and secure your own computer!

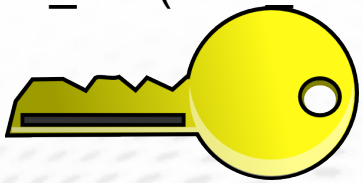
- Install patches regularly:
  - Debian: apt-get update && apt-get uppgrade
  - RHEL/Centos: yum update
  - GUI and scheduled
- Do not run unnecessary services
  - Email, WWW, …
- Anti-virus on windows computers
- Enable local firewall
  - Iptables, yum
    - ufw enable
    - ufw allow ssh, ufw default deny incoming
- Do not keep test accounts with bad passwords
  - Systems are continuously scanned by intruders

Create and use ssh-keys

cscuser@algol ~]$ **ssh-keygen**
Generating public/private rsa key pair.
Enter file in which to save the key (/home/cscuser/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/cscuser/.ssh/id_rsa.
Your public key has been saved in /home/cscuser/.ssh/id_rsa.pub.
The key fingerprint is: 57:2b:b3:c8:f1:3d:46:10:... cscuser@algol.csc.fi
The key's randomart image is:
+--[RSA 2048]----+
| ...oE . . |
...



Your **private** key:
Id_rsa (or id_dsa)



Your **public** key
Id_rsa.pub
On you local **and**
on your remote host

[cscuser@algol ~]$ **scp .ssh/id_rsa.pub user@sisu.csc.fi:.ssh/authorized_keys**
Password:
id_rsa.pub
cscuser$ **ssh sisu.csc.fi**
+-[Welcome]--+
| CSC - Tieteen tietotekniikan keskus - IT Center for Science |
..
Bonus for the laze user: **ssh-agent (if you want to log in many times during thea day)**

CSC is a Reliable Partner

- CSC complies to reqirements and best practices on Information Security
  - National requirements (Raised Information Security Level)
    - Audited several times
  - International Standards
    - ISO 27001:2005 Certification for Datacenter CSC Kajaani
- Peering also on security with national and international partners
- In case of security incidents or other security matters, contact security@csc.fi

IQNet®

THE INTERNATIONAL CERTIFICATION NETWORK

CERTIFICATE

IQNet and
Inspecta Sertifiointi Oy
hereby certify that the organization

CSC – IT CENTER FOR SCIENCE LTD.
ESPOO

for the following field of activities

Datacenter CSC Kajaani.

has implemented and maintains an

Information Security Management System

which fulfils the requirements of the following standard

ISO/IEC 27001:2005

Issued on: 2013-06-18
Expiry date 2016-06-18.

Registration Number: **FI 7031-01**