

# Security and Protection

René Serral-Gracià<sup>1</sup>

<sup>1</sup>Universitat Politècnica de Catalunya (UPC)

March 8, 2022

# Lectures

- 1 System administration introduction
- 2 Operating System installation
- 3 User management
- 4 Application management
- 5 System monitoring
- 6 Filesystem Maintenance
- 7 Local services
- 8 Network services
- 9 **Security and Protection**
- 10 Virtualization

# Outline

- 1 Introduction
  - Goals
- 2 About security
- 3 Security components

# Goals

## Knowledge

- Main aspects of system's security
  - Local security
  - Network security
- Network services security

## Abilities

- Installation, execution and analysis about the results of security auditing tools

# Outline

- 1 Introduction
- 2 About security
- 3 Security components

- Confidentiality
  - Protection against undesired data access
- Integrity
  - Protection against unwanted destruction modification, or data loss
- Availability
  - System must be up and running for legitimate users
- Consistency
  - Avoid unwanted changes to system behavior
- Isolation
  - Avoid unauthorized access to external people (hackers)

# Perfect security?

- There is not such a thing
  - Even if the machine is down
  - With enough resources (time, money, . . . ) everything is hackable
  - Natural disasters

**Goal:** get a “*secure enough*” system

- Secure against automatic attacks (*script kiddies*)
- Easy to be back up and running

# Security and usability

## Normally two sides of the same coin

- Highest security, lowest usability
  - Limited access to services and apps
  - Constant identifications
    - Burdensome to the users
    - Slow and tiring
- More usability means less security

## Too much security can have the opposed effect

- Users write all their passwords in a post-it
- Use tools to automate resource access



# Goals in attacking a computer

- Get information
- Get/destroy data
- Denial of Service
- Obtain resources
- Use machines as proxy to other attacks (DDoS)

# Some attacks

- Obtain passwords
- Filesystem abuse
- Unexpected parameters
- Buffer overflows
- Race conditions
- Resource abuse
- Trojan, Viruses, ...
- Port scanning
- Spoofing: IP, DNS, ARP, ...
- Man-in-the-middle
- Sniffers
- Worms, ...
- Social Engineering
- ...

# Outline

- 1 Introduction
- 2 About security
- 3 **Security components**
  - Physical Security (I)
  - Local Security
  - Network Security

# Physical Security

- Physical access to the console
  - Reboot with a system disk
  - Data stealing (hard drive, backups)
  - System alteration
  - Computer stealing
- Physical access to network cables
  - Network Monitoring
  - Denial of Service
- Physical access to the office
  - Look for passwords below the keyboard!
- Access to destroyed documents

# Physical Security (II)

- Sometimes it doesn't take a malicious attack to destroy data
  - Accidents: power shortages, fire, ...
  - Ambient conditions: temperature, humidity, ...
  - Natural catastrophes: hurricanes, earthquakes, ...
  - Other: bugs, food, beverages, ...
- Sensors, special materials, raised floor, ...

# Local Security

**Goal:** protect against attacks from the users of the system

- Attacker has a non privileged user account
- Even a privileged one
- Users willing to escalate privileges
- Protect the system locally before connecting it to the network

# Passwords

- Enforce a strong password policy
  - Long passwords (+8 characters)
  - Mix of numbers, letters, and special characters
  - Hard to guess
  - Easy to remember
  - NOT a dictionary word – or variation
- Password expiration policy
  - Be careful it can become quite annoying
- Check password strength on each change/periodically
- Protect encrypted passwords (/etc/shadow)

# Permission and protection

## Minimum access policy

- An user should not access a file he/she doesn't need
- Grant the minimum privileges and ...
  - assign more under demand
  - Grant only group level permissions
- Assign a sensible file creation mask

```
umask 027 (rwx r-x ---), 022 (rwx r-x r-x)
```

- Be aware of potentially dangerous files
  - with SetUID bit
  - Holding system configuration



# Resource abuse

- Excessive use of resources by a single user
  - CPU/processes
  - Memory
  - Disk
- Set up limits and quotas
  - `/etc/security/limits.conf`
  - `ulimit`
  - disk quotas

# Filesystem integrity

- Often attackers modify the filesystem to hide the attack
  - Modification of log files
  - Rootkits
- Tools to detect changes in the filesystem
  - Through digital signature of files
- Partition/Devices in read-only

# System Logs

- May contain information about the attacks
  - Permit to know if a system has been compromised
  - Post-mortem analysis
- Unsecure to store them on the same server
  - Better in a remote server
  - Print them?

# Local security – Example

## ● tiger: security auditing tool

```
$ sudo tiger
Configuring...
Will try to check using config for x86_64 running Linux 3.6.8...
--CONFIG-- [con005c] Using configuration files for Linux 3.6.8. Using
configuration files for generic Linux 3.
Tiger security scripts *** 3.2.3, 2008.09.10.09.30 ***
11:21> Beginning security report for asuso.lomillor.org.
11:21> Starting file systems scans in background...
11:21> Checking password files...
11:21> Checking group files...
11:21> Checking user accounts...
11:29> Checking .rhosts files...
11:29> Checking .netrc files...
11:29> Checking ttytab, securetty, and login configuration files...
11:29> Checking PATH settings...
11:30> Checking anonymous ftp setup...
11:30> Checking mail aliases...
11:30> Checking cron entries...
11:30> Checking services configuration...
11:30> Checking NFS export entries...
11:30> Checking permissions and ownership of system files...
11:30> Checking for indications of break-in...
11:30> Performing rootkit checks...
11:37> Performing system specific checks...
12:12> Performing root directory checks...
12:12> Checking for secure backup devices...
12:12> Checking for the presence of log files...
12:12> Checking for the setting of user s umask...
12:12> Checking for listening processes...
12:12> Checking SSHD s configuration...
12:12> Checking the printers control file...
12:12> Checking ftpusers configuration...
12:12> Checking NTP configuration...
12:12> Waiting for filesystems scans to complete...
12:12> Filesystems scans completed...
12:12> Performing check of embedded pathnames...
12:14> Security report completed for asuso.lomillor.org.
Security report is in /var/log/tiger/security.report.hostname.121204-11:21
```

# Exercise

Which issues might present if an attacker modifies the environment variables? (i.e., PATH)

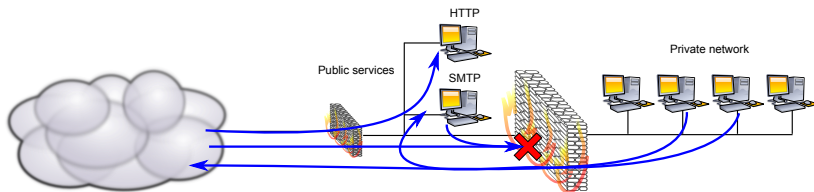
# Network Security

**Goal:** Protect against attacks coming from the outside

- Aimed at:
  - The services we are offering
  - The network itself
  - The information our servers is keeping

# Network Security

- Mandatory to use firewalls
- Two level security: Protected vs DMZ



# Offered services

## Security level depends on the offered services

- System and user information
  - `finger`, `rdate`, `rusers`, ...
- Remote login and connection
  - `telnet`, `rlogin`, `rsh`, ...
- File and data sharing
  - **`NFS`, `Samba`, `LDAP`, `FTP`, `HTTP`, ...**
- E-mail



# Network security

## Minimum access policy

- Disable all the services
  - Or even uninstall them
- Enable only the required services
  - and limit the access only to current users

## Validate the configuration of the installed services

- Even if disabled

# Network security

## Monitor the activity of the installed services

- nmap: list running services

```
$ nmap 10.1.1.1

Starting Nmap 6.00 ( http://nmap.org ) at 2012-12-04 12:03 CET
Nmap scan report for 10.1.1.1 (10.1.1.1)
Host is up (0.00031s latency).
Not shown: 989 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
631/tcp   open  ipp
2049/tcp  open  nfs
3306/tcp  open  mysql
5900/tcp  open  vnc
8080/tcp  open  http-proxy
9090/tcp  open  zeus-admin
```

# Limit access to the services

- Who has acces to what services?
- How to validate user identity
  - Through IP addresses? → IP Spoofing
- Reverse DNS → DNS Spoofing
- User level – authentication, digital certificates, ...
  - Service forwarding

```
ssh -R 12443:10.1.1.10:443 rserral@gw.ac.upc.edu  
ssh -L 443:gw.ac.upc.edu:12443 rserral@10.1.1.10
```

- Kerberos

# Kerberos

## Protocol used for network authentication

- Based on Secret key cryptography (password)
- Kerberos server is used as identity proof
  - Client contacts Key Distribution Center for a ticket
    - KDC encrypts a ticket using client's passwd
    - Client gets the ticket
  - The ticket enables access to specific services
- Transparent for the user

# Intrusion Detection Systems (IDS)

- Network based
  - Traffic analysis to search for attacks
- Host based
  - System activity to search for attacks
    - logs, filesystem, ...

# Security through obscurity

- Not a very good security policy
  - Offers a false sense of security
- Added security on an already secured environment
- Examples
  - Change web server version
  - Change default ports for applications

# Contingency plan

## Actuation protocol in case of system failure

- What to do?
- Who to notify? Using which information?
- It must be defined for each failure
  - Service failure
  - Hardware failure
  - Data center collapsing
- Do simulations to prove its usefulness
- Accordingly to company policies

# Security tools

- Local system configuration
  - titan
  - tiger
- Network system configuration
  - nmap
  - nessus
- IDS
  - tripwire
  - snort
  - logcheck

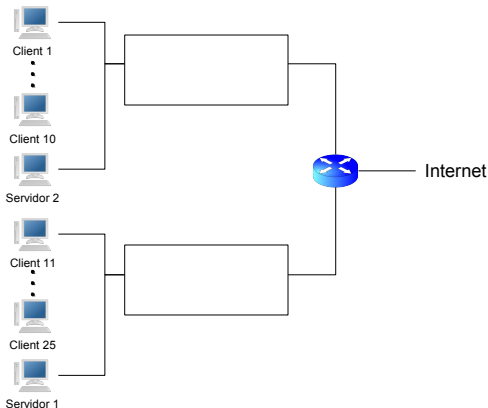


# Some advice

- Never be overconfident
  - There is always someone smarter
- Be somewhat paranoid
- Be prepared for the worst
  - Backups
  - Virtualization
- Run attacks to your systems
  - Better yet from the outside
- Be up to date
  - Security evolves constantly
  - Security forums, newsletters, ...

# Activitat

- De la xarxa vista al final del tema de Xarxa indica:
  - On posaries el (o els) firewall
  - Quines consideracions tindries a l'hora de configurar-los



# Activitat

## Preguntes

- Indica si compraries algun equip mÃ©s a part dels equips de xarxa anteriors
- Distribueix els serveis entre tots els servidors
- Indica on instal·laries el (o els) firewall i quins criteris seguiries per configurar-los