University
Carlos III of Madrid

Distributed Systems Security

Lab Assignments

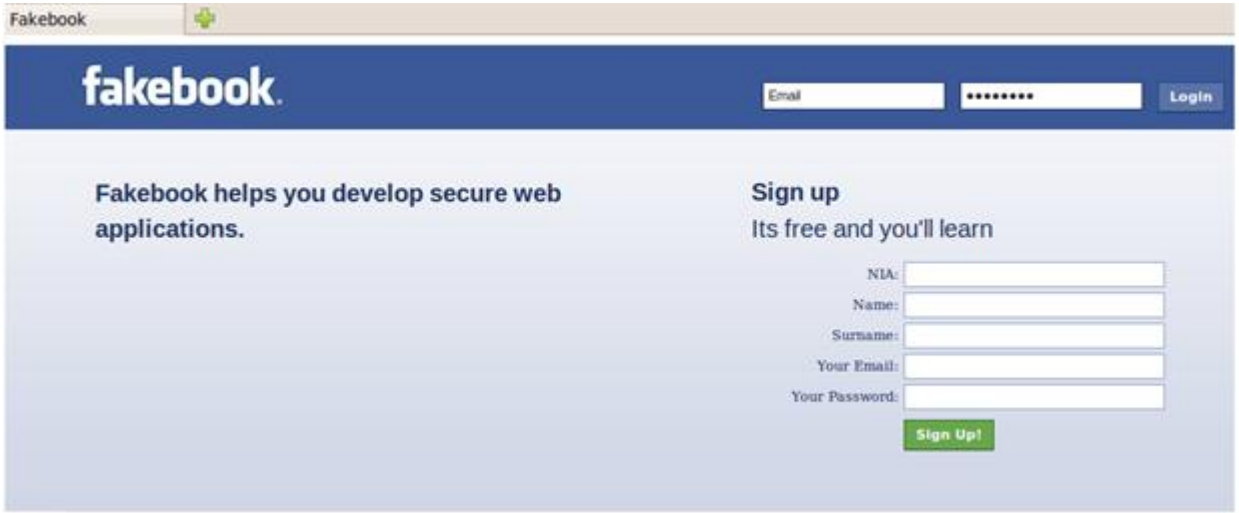
Module I

IT Security Group (SeTI)

Guillermo Suarez de Tangil
(guillermo.suarez.tangil@uc3m.es)

Remembering...

- Server should offer:
  - Web application (*Fakebook*)



  - Remote administration (SSH)
  - Always having **security** in mind!

Goals

- Secure a Web Server (2 modules)
  - **Operating system**
  - **Service providing applications and Web application**
- By the end, you should be able to:
  - Identify threats
  - Identify the consequences of the threats
  - Implement the mechanisms needed to mitigate each threat
  - Check the correct implementation of the aforementioned mechanisms
  - Identify the organization's exposure to internal and external threats as part of the BCP

Module 1: Operative System

- Only one user should administrate the Web
  - Local and remote access
  - Administration actions should be limited to the context of the Web
- All users should have granted access to *Fakebook*
- The machine should have granted access to security updates
- Any other access should not be granted
- Remote access and PING should be logged

Practical Assessment

- Deliveries:
  - Written report, scripts and configuration files
  - Deadline: November the 4th, 2011
  - Outline
    - Security analysis
    - Security vulnerabilities
    - Vulnerability risk: **Information Assurance** vs. **Information Availability**
    - Vulnerability exploitation
    - Countermeasures (*justifying decisions taken*)

Tips and Useful Advises

- Divide and conquer
  - Break the module down (smallest work scopes)
- Before implementing, **abstraction**!
  - Textual description of the changes to tackle
- Backup copies
- Criticize your own decisions
- Discuss in with other pairs
  - **Do not plagiarize! (Knowledge assessment)**

Administration and Remote Access

- What actions can the administrator do on the server? What can a user do when establishing a remote connection through SSH?
  - **File-System Permissions**
- Should I grant remote access to all the users?
  - **SSH configuration file**
- From which IP address?
  - **Firewall**

File-System Permissions

- Is administrator's password strong enough?
  - John the ripper
- Does it make sense to create an specific user to administrate the Web?
  - Think how can you mitigate an identity theft (rootkits, etc.)!
  - What about insiders?
- What kind of permissions should I grant to the Web admin?
  - Think which kind of services he is going to administrate!
  - And to which folders needs access!

Firewall

- Definition
  - “A part of a computer system or network that is designed to **block unauthorized access** while permitting outward communication”
- Analyze what kind of traffic you need for the services required
- What traffic (tip: **ports**) do you have to allow/restrict?
- What is the default **policy**?
- System updates
  - How do they work?
    - Tip: Use wireshark

IPTABLES

- Linux firewall
- Network packets filter-based firewall based on host
- Command */sbin/iptables*
  - **Add/Delete/Edit** rules
- Type of fables:
  - **Filter**
  - NAT (*Network address translation*)
  - MANGLE (quality of service and fault tolerance)

IPTABLES: Filter table

- Check the content of the packets…
- …**Accept/Reject/Drops** according to established rules.
- Rule chains:
  - **INPUT chain**
    - Inspects packets which are sent to the firewall
  - **OUTPUT chain**
    - Inspects packets which are sent from the firewall
  - **FORWARD chain**
    - Inspects packets which are resent from one network interface to other

IPTABLES: Criterions

- Every rule of the firewall specifies an specific **criterion** for each packet:
  - **ACCEPT**: Accepts the packet
  - **DROP**: Drops the packet
- Sequentially:
  - Incorporation and verification of rules…
  - … until one match a packet
- Default policy:
  - In case no rule matched

IPTABLES: Main options

- Add, insert, delete, replace, and list rules:
  - -A add
  - -D delete
  - -R replace
  - -I inserts
  - -L list
  - -F flush
- … **Man IPTABLES**

IPTABLES: Main parameters

- Specifies conditions of a rule:
  - -p: protocol of the packet
  - -s: source of the packet
  - --sport: source port
  - -d: destination of the packet
  - --dport: destination port
- Again … **Man IPTABLES**

IPTABLES: Example

- **iptables –A OUTPUT –i eth0 –p tcp --source-port 21 –j ACCEPT**
- iptables
  - –A OUTPUT
  - –i eth0
  - –p tcp
  - --source-port 21
  - –j ACCEPT

References

- Assignment description
  - Man iptables
  - Don’t forget Google
- Man SSH
  - Also in Google
- Linux filesystem permissions
  - And of course, always in Google

Let's Work!