University
Carlos III of Madrid

Distributed Systems Security

Lab Assignments

IT Security Group

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

Remembering module 1…

- Firewall configuration
  - All users should have granted access to Fakebook
  - The machine should have granted access to security updates
  - Any other access should've not be granted
  - Remote access and PING should be logged
  - Remote connections only from a specific IP address
- SSH
  - Remote administration (SSH)
- File-system Permissions
  - New web administrator user

What are we going to do today?

- Last session…
  - Several improvements were presented to secure the server
- Today's session…
  - A set of **tools** which will help you to perform a formal analysis…
  - …this analysis will allow you to **detect vulnerabilities and identify threats**
- At the end of the aforementioned analysis…
  - You will have to be able to identify security problems presented during last session
  - You will have to be able to search and apply other tools different than the ones presented today by yourself

Threats and vulnerabilities

- Disaster and catastrophe
  - A catastrophe is any tragic event (fact) with great loss
  - A disaster happens when a catastrophe implies terrible consequences for a system
    - A disaster is due a vulnerability on the system
- Example:
  - A hurricane is a natural catastrophe
  - When a hurricane destroys a forest is not considered a disaster but a catastrophe
  - When a hurricane destroys a population it is considered a disaster

Security management: Risks

- Security management
  - Information systems are subject to a number of **risks**
  - An inappropriate management of the risk can lead to a hazard exposing the organization to a **disaster**
- Risk
  - Can be estimated analyzing
    - **Threats** affecting the **assets** of the organization
    - **Vulnerabilities** to which they can be exposed, and the
    - **Impact** of possible vulnerability exploits over any of the assets

Consequences and countermeasures

- Consequences of an inappropriate management of the risk
  - Hazard/catastrophe exposing the organization to a disaster
- Consequences of a disaster
  - Loss of operational capability of an organization
- **Business Continuity Planning** (BCP)
  - To ensure the continuity of a business in case of a disaster
  - Lifecycle:
    - **Analysis** of the impact, threats and scenarios
    - Design of necessary solutions, implementation, test and maintenance

BCP: Risk analysis

- Specific disasters:
  - Theft
    - Insider
    - Outsider
  - Earthquake
  - Floods
  - Sabotage
  - Terrorism
  - …
  - Cyber attack

Cyber attack

- Some classic threats
  - Buffer overflow and code injection
  - SQL Injection
  - XSS
  - DoS
- Two tools for detecting vulnerabilities and identifying threats
  - Nmap
  - Nikto
- Task: Look for other similar tools

Nmap

- Port scanner
- Lets you find out:
  - Open ports, filters, etc… of a machine
  - Operating System
- Some uses
  - Analysis of TCP
    - SYN, ACK, FIN
  - UDP port scans
  - Null and Xmas Analysis
  - System configuration discovery

Nmap

- Installation… as always:
  - sudo apt-get install nmap
- Documentation
  - man nmap
- Execution
  - sudo nmap [type of scan] [options] target specifications
- How to detect a firewall?
  - Sending TCP ACK!
- How to detect the configuration of the system?
  - With –O option!

Nikto

- Web server vulnerability analyzer
- Allows
  - Detect web server configurations, plugins and versions
  - Detecting vulnerable configurations
  - Updates
- Some tests
  - URL encoding
  - Self-reference directories
  - Premature request ending
  - Long URLs
  - ...

Nikto

- Installation… as always:
  - sudo apt-get install nikto
- Documentation
  - man nikto
- Execution
  - sudo nikto –update (updates vulnerability data base)
  - sudo nikto –V (shows versions of plugins)
  - sudo nikto (shows execution options)
  - sudo nikto –host localhost

Next session

- Denial of Service Attack
  - We will see how to detect a DoS…
- Snort
  - … by means of Snort
  - An Intrusion Detection System (IDS)

University
Carlos III of Madrid

Distributed Systems Security

Lets work!

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