Project Catalyst

FUNINTEC
FUNDACIÓN IBEROAMERICANA PARA LA INNOVACIÓN Y LA TECNOLOGÍA

**Project:**

# STUDY CONTROL SYSTEM FOR UNIVERSITIES
# DIPLOM~~A~~D~~A~~#1100266
# MILESTONE 2 COMPLIANCE REPORT
# Penetration testing to identify and mitigate security risks

**1. GENERAL INFORMATION:**

- **Project Name:DIPLOM~~A~~D~~A~~**
- **Test Date: Wednesday, May 15, 2024**
- **Objective of the Tests: Check the defenses and resistance of the system against possible attacks and intrusion attempts from external networks to the LAN network**

**2. SCOPE OF THE TESTS:**

- **Areas Included in the Tests:**

**Two (2) HP Proliant physical servers**

**PROXMOX Virualization Environments**

- **Linux Containers (LxC) with Debian 12 Servers for Development, Quality, Production virtual machines and the backup server.**

- **Areas Excluded from Testing:**

**Switch for LAN network**
**Router for access to the WAN network and Internal WIFI**

**3. TESTING METHODOLOGY:**

- **Testing Approach:**

**The testing approach is used at the layer level of the OSI model.**
**It involves applying intrusions at each layer of the model: IP addresses for layer 3, logical ports for layer 4, and so on.**

- **Used tools:**

**IP Scanner**
**Port Scanner**
**SynFlood**
**ICMP Flood**
**Winnuke**

- **Techniques Used:**

**Verification of ports and IP addresses of the PROXMOX environment of the servers and virtual machines to verify access to permitted applications and services and blocking those that represent dangers and vulnerabilities for the system.**

**4. FINDINGS OF THE EVIDENCE:**

- **Identified Vulnerabilities:**

**- Description of the vulnerabilities found: None**
**- Severity of Vulnerabilities: None**

**- Exploitation of Vulnerabilities:**
**- Examples of how identified vulnerabilities could be exploited**

**If present, the vulnerabilities could allow the following threats:**

**An intruder can access virtual machines at the command line level, even with root privileges:**

**The website presented to the public can be modified/deleted or its content modified.**
**Creation of smart contracts by falsifying the identity of the author.**
**Change of the business logic of a new smart contract.**

## 5. RECOMMENDATIONS AND MITIGATIONS:

**- Recommendations to Mitigate Vulnerabilities: (see image below)**

**- Suggested actions to correct identified vulnerabilities:**

**Existence of an external Firewall that filters incoming traffic based on IP addresses and destination ports.**

**Establish, update, and query a blacklist of source IP addresses to identify potential attackers.**

**- Prioritization of Actions:**

**Review of the origin of incoming traffic and application of white / black lists.**
**Review of destination IP addresses and service ports.**
**Block traffic directed to FTP, SSH, Telnet, RDP, and any type of remote access services.**
**Protect, with the appropriate permissions (read, write and execute) the directories (folders) and files of the applications.**
**Protect root keys for servers, operating systems and applications.**

## 6. VALIDATION TESTS:

**- Confirmation of Vulnerability Correction:**

**- Verification that the identified vulnerabilities have been corrected: None.**

**- Posterior Penetration Testing: Periodic review of protection policies is recommended, as well as the incorporation of new rules as other communication protocols appear.**

## 7. CONCLUSIONS:

**- Summary of the results obtained in the penetration tests:**

**In the penetration tests it was confirmed that the allowed traffic corresponds to ports 80, 443. The remote access ports were blocked.**

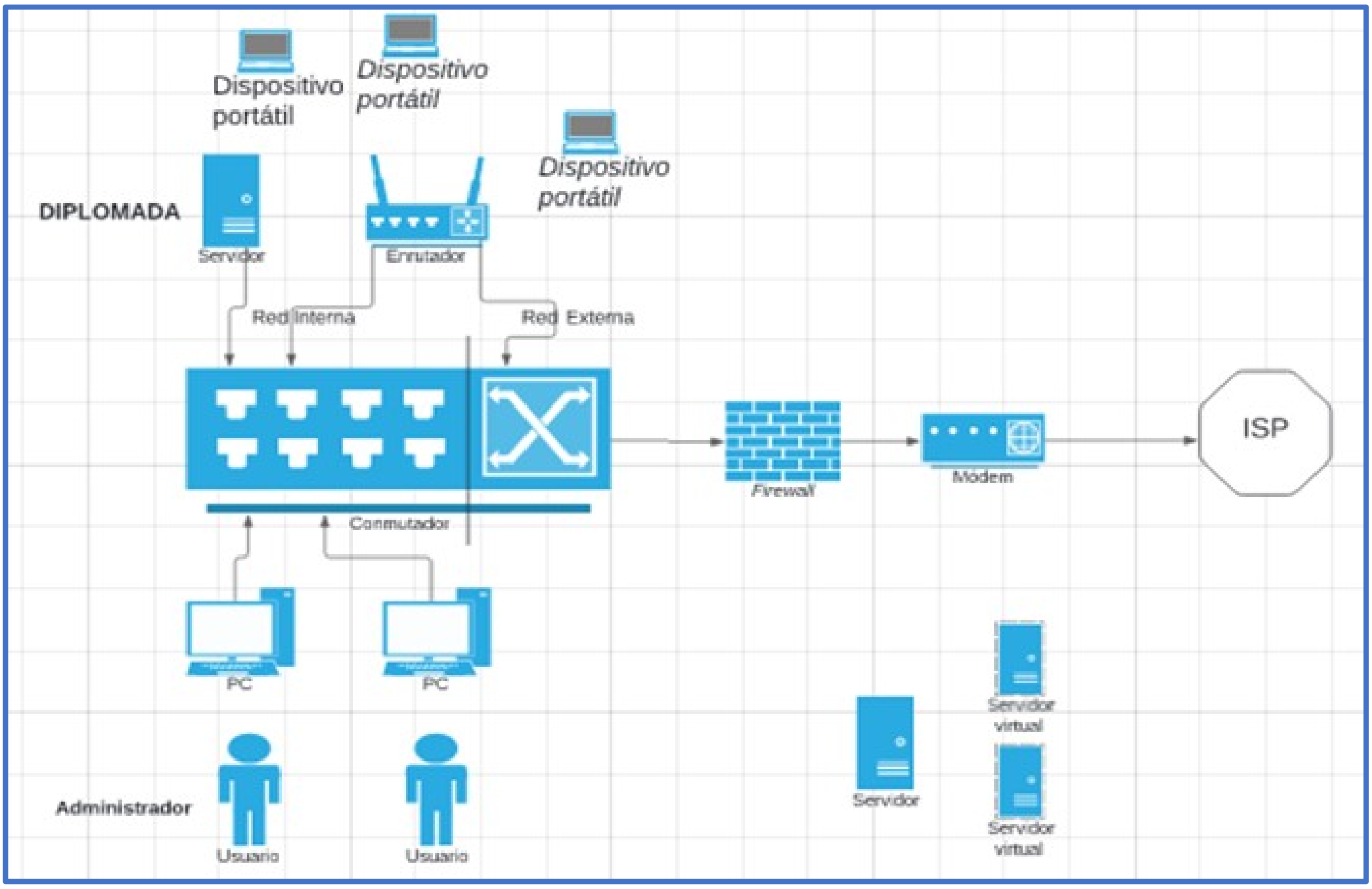
- Importance of addressing and correcting identified vulnerabilities: There was no

- Suggestions to maintain long-term system security - Suggestions for future testing or improvements to system security:

Periodic review of the appearance of new communication protocols and updating of protection rules in the Firewall and internally on the servers.

Physical security is also very important. Adequate access control, uninterrupted power sources, fire extinguishers, grounding system and surveillance camera must be available.

**Logical Network Diagram for the DIPLOMADA Project:**


Dispositivo portátil
Dispositivo portátil
Dispositivo portátil
DIPLOMADA
Servidor
Enrutador
Red Interna
Red Externa
Conmutador
Firewall
Modem
ISP
PC
PC
Servidor virtual
Servidor
Servidor virtual
Administrador
Usuario
Usuario