Lab Exam

- The Security of IT Systems -

This Lab Exam consists of 3 subjects, each having a total of maximum 3 earnable points. 1 point is awarded automatically for the physical presence.

1. Linux Permissions:

Create a Shell Script or a List of Commands to be inputed in the console in order to configure file and folder POSIX and ACL permissions to satisfy the requirements:

Scenario – we asume that an organization has:

- 10 users: **user11**, **user12**, **user13**, **user14**, **user15**, **user16**, **user17**, **user18**, **user19** and **user20**.
  Each user has its own home directory in **/home/user<u>X</u>** (“X” represents the number of the user) where the owner is that respective user and the group is **users**, and the permissions are **700** on each of these directories.

- The first 3 users (**user11**, **user12**, **user13**) belong to the **administration** group.

- The next 3 users (**user14**, **user15**, **user16**) belong to the **management** group.

- The next 3 users (**user17**, **user18**, **user19**) belong to the **contact** group.

- The last user (**user20**) belongs to the **it** group.

- 5 common folders: **comm1**, **comm2**, **comm3**, **comm4**, **comm5**. (All folders have owner **root** and group **root**)

Using the above information, type in the necessary commands in order to set the permissions required by the following statements:

(each requirement has 0,5 points)

1). Set the first 2 folders (**comm1**, **comm2**) to be accesible only by the **owner**

2). Allow full control to folder **comm4** and **comm5** for **anybody**.

3). Allow full control to folder **comm3** only for the **owner** and **group**

4). Set the **comm3** folder with supplemental access for group **management** as full access

5). Allow supplemental access only to **user16** and **user17** to only read contents (and not modify anything) in folder **comm2**.

6). Allow supplemental access to **user18** as full control over folder **comm1** and **user19** read-only access to folder **comm1**.

Type in all the required commands in a script file / text document and for results reporting create screenshots or type in “ls” or “getfacl” in the console to show the output. Include the output in the results.

2. OpenSSL & Encryption:

(each requirement has 0,5 points, except points #3 and #4 which value 0,25 points)

Perform the following operations using OpenSSL or 7 Zip, when appropriate:

First, generate a file containing a random text/string and save it. Then:

1. **Encrypt** the file using **OpenSSL**
2. **Decrypt** the file using **OpenSSL**
3. Create a **SHA256 checksum** for all the files in the directory and output it to a file called “**checksums1.txt**”
4. Create an **encrypted ZIP archive**
5. Generate a **Root CA key** and **certificate**
6. Generate a **server key**, **CSR** and **sign** the **Server CSR** with the **RootCA’s key** to obtain a **Server final Certificate**.
7. Generate a **client key**, **CSR** and **sign** the **Client CSR** with the **RootCA’s key** to obtain a **Client final Certificate**.

Type in all the required commands in a script file / text document and create an archive of all the files used and send it via e-mail to the teacher, for evaluation.

3. Linux Firewall:

(each rule has 0,5 points)

Consider an organization which has to implement a Firewall Security Policy by using 6 IPTABLES rules.

The organization has the following network configuration:

LAN1: 172.16.1.0/24	PC1: 172.16.1.3
LAN2: 172.17.2.0/24	PC2: 172.17.2.4
LAN3: 172.18.3.0/24	PC3: 172.18.3.2

Type in all the required iptables rules in order to satisfy the following requirements (we assume that the default policy of the Firewall is DROP)

1. Block all unsecured email receiving by Internet Messaging Access Protocol from the IP of smtp.google.com (determine the IP address!) to LAN1 .

2. Block secured web traffic from LAN3 to LAN2.

3. Allow DNS traffic from PC3 to any destination on TCP.

4. Allow secure email sending from anywhere to all 3 LANs.

5. Deny unsecure console access from PC1 to any LAN.

6. Allow access to Windows Remote Desktop Protocol from anywhere to all LANs.

GOOD LUCK ! :-)