Grupo Viernes - 7PM-10PM - Laboratorios del módulo VI

Practica 1:

sudo apt install gnupg2 -y

mkdir ~/intento

cd

ls

cd ~/intento

sudo nano vegeta.txt

cat vegeta.txt

sudo gpg2 --symmetric ~/intento/vegeta.txt cat vegeta.txt

ls

cat vegeta.txt.gpg

sudo rm vegeta.txt

ls

sudo gpg2 --output ~/intento/vegeta.txt.gpg --decrypt ~/intento/vegeta.txt.gpg

ls

cat vegeta.txt.gpg

Practica 2

sudo apt update

sudo apt install -y apache2 vsftpd openssh-server

sudo systemctl enable --now apache2 vsftpd ssh

sudo systemctl status apache2 vsftpd ssh

sudo iptables -A INPUT -p tcp --dport 80 -j DROP

sudo iptables -A INPUT -p tcp --dport 21 -j DROP

sudo iptables -A INPUT -p tcp --dport 22 -j DROP

sudo iptables -L --line-numbers

sudo iptables -D INPUT -p tcp --dport 80 -j DROP

sudo iptables -D INPUT -p tcp --dport 21 -j DROP

sudo iptables -D INPUT -p tcp --dport 22 -j DROP

sudo iptables -L --line-numbers

sudo apt install ufw -y

sudo ufw enable

sudo ufw status

sudo ufw deny 80

sudo ufw deny 21

sudo ufw deny 22

sudo ufw enable

sudo ufw status

sudo ufw allow 80

sudo ufw allow 21

sudo ufw allow 22

sudo ufw status

Practica 3:

sudo su

sudo apt-get install snort

dpkg-reconfigure snort

cd /etc/init.d/snort restart

sudo nano /etc/snort/rules/local.rules

alert icmp any any -> $HOME_NET any (msg:"Trafico ICMP detectado"; sid: 100001; rev:1;)

alert tcp any any -> $HOME_NET 21 (msg:"Trafico FTP detectado"; sid: 100002; rev:1;)

alert tcp any any -> $HOME_NET 22 (msg:"Trafico SSH detectado"; sid: 100003; rev:1;)

alert tcp any any -> $HOME_NET 80 (msg:"Trafico HTTP detectado"; sid: 100004; rev:1;)

```
sudo nano /etc/snort/snort.conf

cd /etc/snort/

snort -A console -c snort.conf -i ens33
```