sudo dnf install google-authenticator -y

sudo dnf install qrencode -y

google-authenticator

. Configurar PAM para usar Google Authenticator

sudo nano /etc/pam.d/sshd

auth required pam_google_authenticator.so

4. Configurar SSH para solicitar 2FA

sudo nano /etc/ssh/sshd_config

ChallengeResponseAuthentication yes

UsePAM yes

PasswordAuthentication yes

sudo systemctl restart sshd

udo dnf install httpd vsftpd -y

Habilitar y arrancar servicios

sudo systemctl enable httpd --now

sudo systemctl enable vsftpd --now

sudo systemctl enable sshd --now

sudo systemctl status httpd

sudo systemctl status vsftpd

sudo systemctl status sshd

curl http://10.0.0.101

ftp 10.0.0.101

ssh r20241244@10.0.0.101

Bloquear puertos con IPtables

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

exit

sudo service iptables save 2>/dev/null || sudo iptables-save | sudo tee /etc/iptables.rules

sudo iptables -L -n -v

Bloquear puertos usando firewall

sudo firewall-cmd --permanent --add-rich-rule='rule family="ipv4" port protocol="tcp" port="80" reject'

sudo firewall-cmd --permanent --add-rich-rule='rule family="ipv4" port protocol="tcp" port="21" reject'

sudo firewall-cmd --permanent --add-rich-rule='rule family="ipv4" port protocol="tcp" port="22" reject'

sudo firewall-cmd --reload

Habilitar nuevamente:

sudo firewall-cmd --permanent --remove-rich-rule='rule family="ipv4" port protocol="tcp" port="80" reject'

sudo firewall-cmd --permanent --remove-rich-rule='rule family="ipv4" port protocol="tcp" port="21" reject'

sudo firewall-cmd --permanent --remove-rich-rule='rule family="ipv4" port protocol="tcp" port="22" reject'

sudo firewall-cmd --reload

Ver reglas del firewall:

sudo firewall-cmd --list-all

Instalar gpg2

sudo dnf install gnupg2 -y

Crear directorio de práctica y moverse a él

mkdir ~/practica1

cd ~/practica1

Crear un archivo de ejemplo

echo "Este es un mensaje secreto del clon" > mensaje.txt

Cifrar el archivo con contraseña

gpg2 -c mensaje.txt

Ver que el archivo cifrado existe

ls -l mensaje.txt.gpg

Intentar abrir el archivo cifrado

cat mensaje.txt.gpg

Enviar el archivo cifrado al clon usando SSH/SCP

scp mensaje.txt.gpg r20241244@10.0.0.131:~/

Descifrar el archivo localmente

gpg2 -d mensaje.txt.gpg

Guardar el archivo descifrado en otro archivo

gpg2 -d mensaje.txt.gpg > mensaje_descifrado.txt

Ver el contenido del archivo descifrado

cat mensaje_descifrado.txt

sudo dnf install google-authenticator -y

sudo dnf install qrencode -y

google-authenticator

. Configurar PAM para usar Google Authenticator

sudo nano /etc/pam.d/sshd

auth required pam_google_authenticator.so

4. Configurar SSH para solicitar 2FA

sudo nano /etc/ssh/sshd_config

ChallengeResponseAuthentication yes

UsePAM yes

PasswordAuthentication yes

sudo systemctl restart sshd