**PREINSTALACIÓN DE UN NODO TOR**

1. Instalar el NTP

apt-get install ntp ntp-doc

1. Verificar que esté funcionando

ntpq –p

1. Mantener actualizaciones de forma automatizada

apt-get install unattended-upgrades apt-listchanges

nano /etc/apt/apt.conf.d/50unattended-upgrades

1. Introducir la siguiente configuración

Unattended-Upgrade::Origins-Pattern {

"origin=Debian,codename=${distro\_codename},label=Debian-Security";

"origin=TorProject";

};

Unattended-Upgrade::Package-Blacklist {

};

1. Añadir lo siguiente si queremos que se reinicie solo

Unattended-Upgrade::Automatic-Reboot "true";

1. Crear el siguiente archivo

nano /etc/apt/apt.conf.d/20auto-upgrades

1. Introducir el siguiente código

APT::Periodic::Update-Package-Lists "1";

APT::Periodic::AutocleanInterval "5";

APT::Periodic::Unattended-Upgrade "1";

APT::Periodic::Verbose "1";

1. Ver que las actualizaciones funcionen

unattended-upgrade –d

**PREPARACIÓN DE NODO**

1. Poner los repositorios de Tor

nano /etc/apt/sources.list

1. Incluir estas líneas:

deb https://deb.torproject.org/torproject.org stretch main

deb-src https://deb.torproject.org/torproject.org stretch main

1. Permitir repositorios sobre SSL

apt-get install apt-transport-https

1. Preparar PGP y Tor

apt-get install dirmngr

apt-get install gnupg

1. Importar claves

gpg --keyserver https://keys.gnupg.net --recv A3C4F0F979CAA22CDBA8F512EE8CBC9E886DDD89

gpg --export A3C4F0F979CAA22CDBA8F512EE8CBC9E886DDD89 | apt-key add -

1. Actualizar y preparar la red Tor

apt-get update

apt-get upgrade

apt install tor deb.torproject.org-keyring

1. Configurar el nodo

nano /etc/tor/torrc

1. Incluir este contenido:

#cambiar el nombre "myNiceRelay" al nombre del nodo

Nickname myNiceRelay

ORPort 443

ExitRelay 0

SocksPort 0

ControlSocket 0

# cambiar email por un correo electrónico válido

ContactInfo email

1. Reiniciar el proceso

systemctl restart tor@default

1. Ver que esté el ORPort como reachable

cat /var/log/syslog

**CONFIGURAR FIREWALL**

1. Crear el archivo de iptables

nano iptables.sh

1. Crear regla de bloqueo y abrir el puerto de uso

echo 1 > /proc/sys/net/ipv4/ip\_forward

iptables -F

iptables -X

iptables -Z

iptables -t nat -F

iptables -A -p tcp --sport 443 -j ACCEPT

iptables -A -p tcp --dport 443 -j ACCEPT

iptables -P FORWARD DROP

iptables-save > /etc/iptables.up.rules

1. Dar permisos al firewall

chmod 770 iptables.sh

1. Ejecutarlo

./iptables.sh

**CONVERTIR EL NODO EN NODO DE SALIDA**

1. Intervención con ISP

* Ver si permiten nodos de redes Tor
* Solicitar un DNS inverso (registro PTR) a nuestra IP pública
* Intentar añadir en el Whois que es un nodo Tor de Salida

1. Crear una Web informativa de ser nodo de salida Tor

apt-get install apache2

cd /etc/apache2/mod-available

a2enmod ssl

mkdir /var/www/html/tor

nano /var/www/html/tor/index.html

EJEMPLO WEB:

https://gitweb.torproject.org/tor.git/plain/contrib/operator-tools/tor-exit-notice.html

cp /etc/apache2/sites-availables/000-default.conf tor.conf

nano /etc/apache2/sites-availables/tor.conf

ServerName: TorPedo.com

DirectoryIndex index.html

Poner la IP del servidor en el VirtualHost con el puerto

1. Asociar la web

nano /etc/tor/torrc

1. Pegar el siguiente código

DirPort 80

DirPort IP:80

**DNS DE SALIDA (DNSSEC)**

1. Instalar servicio DNSSEC

apt install unbound

1. Agregar servidores DNS fiables

nano /etc/resolve.conf

nameserver 80.58.61.250

**nameserver 8.8.8.8 --> NO**

nameserver 127.0.0.1

**POLÍTICA DE SALIDA**

1. Cambiar el nodo a nodo de salida

nano /etc/tor/torrc

Cambiar ExitRelay de 0 a 1

1. Agregar puertos funcionales en torrc

ExitPolicy accept \*:20-21 # FTP

ExitPolicy accept \*:43 # WHOIS

ExitPolicy accept \*:53 # DNS

ExitPolicy accept \*:80 # HTTP

ExitPolicy accept \*:110 # POP3

ExitPolicy accept \*:143 # IMAP

ExitPolicy accept \*:220 # IMAP3

ExitPolicy accept \*:443 # HTTPS

ExitPolicy accept \*:873 # rsync

ExitPolicy accept \*:989-990 # FTPS

ExitPolicy accept \*:991 # NAS Usenet

ExitPolicy accept \*:992 # TELNETS

ExitPolicy accept \*:993 # IMAPS

ExitPolicy accept \*:995 # POP3S

ExitPolicy accept \*:1194 # OpenVPN

ExitPolicy accept \*:1293 # IPSec

ExitPolicy accept \*:3690 # SVN Subversion

ExitPolicy accept \*:4321 # RWHOIS

ExitPolicy accept \*:5222-5223 # XMPP, XMPP SSL

ExitPolicy accept \*:5228 # Android Market

ExitPolicy accept \*:9418 # git

ExitPolicy accept \*:11371 # OpenPGP hkp

ExitPolicy accept \*:64738 # Mumble

**ExitPolicy reject \*:\*** (Deniega todo, salvo tráfico permitido arriba)

1. Recomendaciones

Añadir al archivo anterior las siguientes líneas:

ExitPolicy reject \*:25 (quitamos SMTP para evitar Spam)

RunAsDaemon 1 (ejecutarlo como proceso)

DataDirectory /var/lib/tor (Directorio de Cache, Huella de clave, etc)

RelayBandwidthRate 20 MB (ancho de banda para el nodo, 100MB o más para Flag Fast Exit)

RelayBandwidthBurst 20 MB (limitar las ráfagas)

ORPort 443 (puerto de entrada recomendado)

Address IP\_Pública\_Nodo

OutboundBindAddress IP\_Pública\_Nodo

Nickname Torpedo (nickname)

ContactInfo [javier.blanco@comunixgroup.com](mailto:javier.blanco@comunixgroup.com) (email contacto valido, anónimo o no)

DirPort 80 (puerto de la web, puede ser 443 si se configura SSL)

DirPortFrontPage /var/www/html/index.html (Directorio Web aviso Nodo Salida Tor)

**HACER UN BRIDGE**

1. Editar el torrc:

SocksPort 0

ORPort 443

BridgeRelay 1

ExitPolicy reject \*:\*

**SERVICIOS OCULTOS**

1. Un servicio oculto es cualquier servicio (FTP, servidor Web, servidor de archivos, email, etc.) que sólo es accesible desde la red Tor
2. Añadir estas líneas por servicio oculto en el archivo torrc, con el puerto usado por cada aplicación:

HiddenServiceDir /home/debían/hidden\_service (directorio donde se almacena la clave pública)

HiddenServicePort 21 127.0.0.1:21 (debe ser la IP local, nunca pública)

1. En el directorio indicado, Tor crea un archivo llamado hostname con la URL .onion y un private\_key con la clave que nadie más debe tener.