INSTITUTO TECNOLÓGICO SUPERIOR DE JUAN RODRIGUEZ CLARA

**Administración y Seguridad de Redes**

Carrera: Ing. TIC´s

Docente: Jamil de Jesús Deseano

Alumna: María Guadalupe Rodríguez Ramos

Grupo: 802

No. De control: 159T0037

Fecha: 11 – mayo – 2019

Contenido

[**CONFIGURACIÓN DE** 2](#_Toc9066196)

[ **BIND9** 2](#_Toc9066197)

[**Archivo *named.conf.local*** 2](#_Toc9066198)

[***Archivo db.lupita.com*** 3](#_Toc9066199)

[**Archivo *db.192.168.1*** 3](#_Toc9066200)

[**Archivo *db.facebook.com*** 4](#_Toc9066201)

[**Archivo */etc/resolv.conf*** 4](#_Toc9066202)

[**Directivas** 4](#_Toc9066203)

[**Registro de recursos** 4](#_Toc9066204)

[**Comando *host lupita.com*** 5](#_Toc9066205)

[ **SHOREWALL** 6](#_Toc9066206)

[**Archivo *shorewall.conf*** 6](#_Toc9066207)

[**Archivo *policy*** 6](#_Toc9066208)

[**Archivo *rules*** 7](#_Toc9066209)

[**Archivo *zones*** 8](#_Toc9066210)

[**Archivo *interfaces*** 8](#_Toc9066211)

[ **ISC-DHCP** 9](#_Toc9066212)

[**Archivo */etc/dhcp/dhcpd.conf*** 9](#_Toc9066213)

# **CONFIGURACIÓN DE**

## **BIND9**

Servidor DNS.

* DNS es una gran base de datos distribuida y en principio el objetivo es resolver a partir de un nombre de host perteneciente a un dominio una dirección IP; pero no es el único objetivo de DNS, también lo es realizar la operación inversa, es decir a partir de una dirección IP resolver un nombre de host. Para esto se crea otro espacio de nombres DNS, formados por dominios, pero en donde cada etiqueta del árbol es una parte de la dirección IP.
* BIND (*Berkeley Internet Name Daemon*) es la implementación de referencia del protocolo DNS (*Domain Name System*).

### **Archivo *named.conf.local***

La sentencia acl (o sentencia de control de acceso) define grupos de hosts a los que se les puede permitir o negar el acceso al servidor de nombres.

acl “lupita”{

127.0.0.1/8;

192.168.1.0/24;

};

La declaración zone define las características de una zona tal como la ubicación de su archivo de configuración y opciones específicas de la zona

zone “lupita.com”{

#TYPE: define el tipo de zona.

#MASTER: designa que el servidor de nombres actual como el que tiene la autoridad para esa zona.

type master;

#FILE: especifica el nombre del archivo en el directorio de trabajo named que contiene los datos de configuración de zona

file “/etc/bind/db.lupita.com”;

};

zone “1.168.192.in-addr.arpa”{

type master;

file “/etc/bind/db.192.168.1”;

};

zone “facebook.com”{

type master;

file “/etc/bind/db.facebook.com”;

};

### ***Archivo db.lupita.com***

;

;BIND data file for lupita.com

;

$TIL 604800

@ IN SOA lupita.com. root.lupita.com. (

13 ; Serial

604800 ; Refresh

86400 ; Retry

2419200 ; Expire

604800 ) ; Negative Cache TTL

;

@ IN NS lupita.com.

@ IN A 192.168.1.67

### **Archivo *db.192.168.1***

;

;BIND data file for lupita.com

;

$TIL 604800

@ IN SOA lupita.com. root.lupita.com. (

13 ; Serial

604800 ; Refresh

86400 ; Retry

2419200 ; Expire

604800 ) ; Negative Cache TTL

;

@ IN NS lupita.com.

### **Archivo *db.facebook.com***

;

;BIND data file for local loopback interface

;

$TIL 604800

@ IN SOA facebook.com. root.facebook.com. (

13 ; Serial

604800 ; Refresh

86400 ; Retry

2419200 ; Expire

604800 ) ; Negative Cache TTL

;

@ IN NS localhost.

@ IN A 127.0.0.1

### **Archivo */etc/resolv.conf***

Aquí se debe configurar correctamente este archivo para poder resolver los nombres de los servidores en Internet.

# Generated by NetworkManager

# dirección IP del servidor de nombres a usar.

nameserver 127.0.0.1

### **Directivas**

Las directivas inician con el símbolo de dollar (***$***) seguida del nombre de la directiva.

En los archivos aparece el directivo:

**$TTL*:*** Ajusta el valor Time to Live (TTL) predeterminado para la zona. Este es el tiempo, en segundos, que un registro de recurso de zona es válido. Cada recurso puede contener su propio valor TTL, el cual ignora esta directiva.

### **Registro de recursos**

El componente principal de un archivo de zona es su registro de recursos.

Hay muchos tipos de registros de recursos de archivos de zona. A continuación, están los que utilizamos en la práctica:

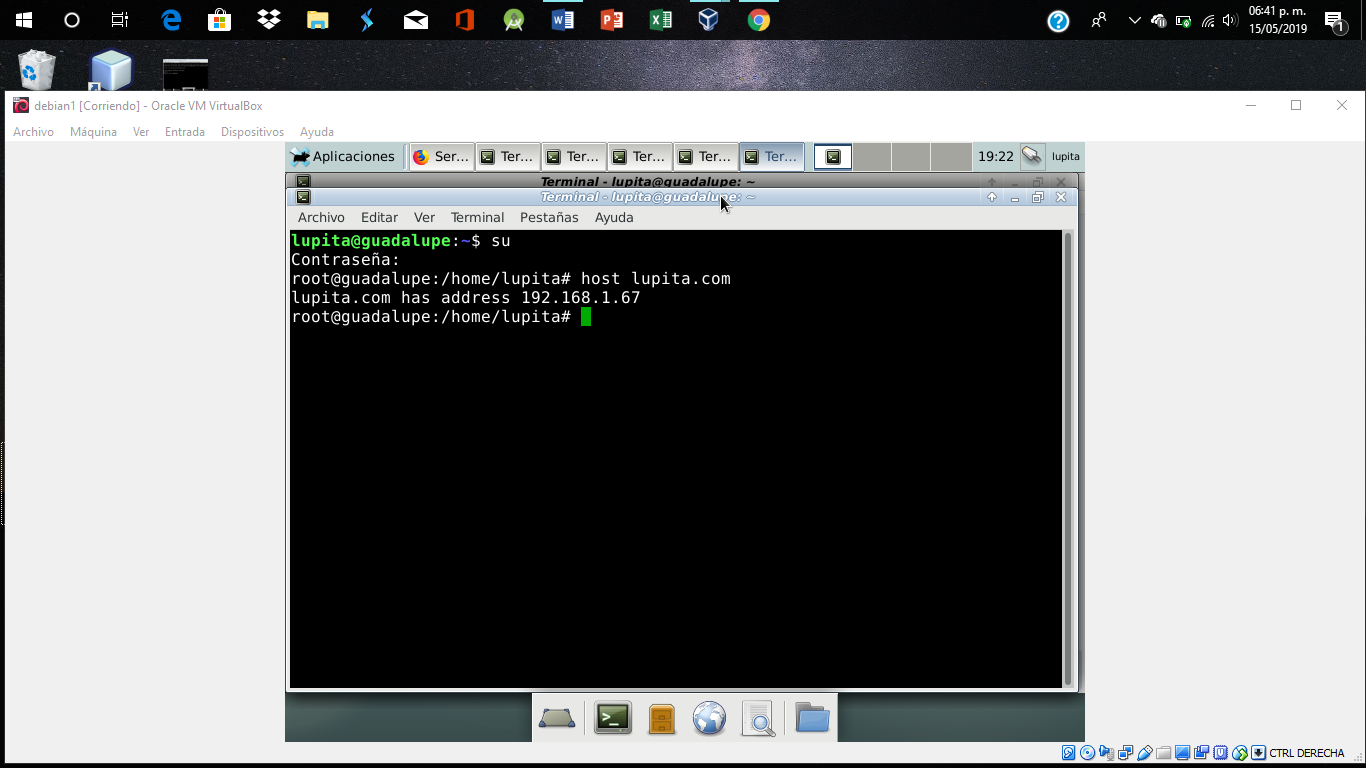
* **A:** Registros de dirección que especifica una dirección IP que se debe asignar a un nombre
* **NS:** Registro NameServer, el cual anuncia los nombres de servidores con autoridad paa una zona particular.
* **SOA:** Registro de recursos Start Of Authority, que declara información importante de autoridad relacionada con espacios de nombres al servidor.
* **Serial:** es un valor numérico que es incrementado cada vez que se cambia el archivo de zona para así indicar a named que debería recargar esta zona.
* **Refresh**: es el valor numérico que los servidores esclavos utilizan para determinar cuánto tiempo debe esperar antes de preguntar al servidor de nombres maestro si se han realizado cambios a la zona. El valor serial es usado por los servidores esclavos para determinar si está usando datos de la zona desactualizados y si debería refrescarlos.
* **Retry:** es un valor numérico usado por los servidores esclavo para determinar el intervalo de tiempo que tiene que esperar antes de emitir una petición de actualización de datos en caso de que el servidor de nombres maestro no responda.
* **Expire:** Si el servidor maestro no ha respondido a una petición de actualización de datos antes que se acabe el intervalo de tiempo expire, los servidores esclavo paran de responder como una autoridad por peticiones relacionadas a ese espacio de nombres.
* **Negative cache TTL:** es el número de segundos que los registros se mantienen activos en los servidores NS caché antes de volver a preguntar su valor real.

### **Comando *host lupita.com***

Host es un comando que se debe ejecutar desde la terminal o línea de comandos existe en tu dispositivo con sistema operativo Linux. Esta función te permitirá ver la dirección IP asociada a un dominio, o a la inversa, dependiendo de lo que incluyas a la hora de ejecutar el comando.

Para ejecutar este proceso, se hace lo siguiente:

host lupita.com



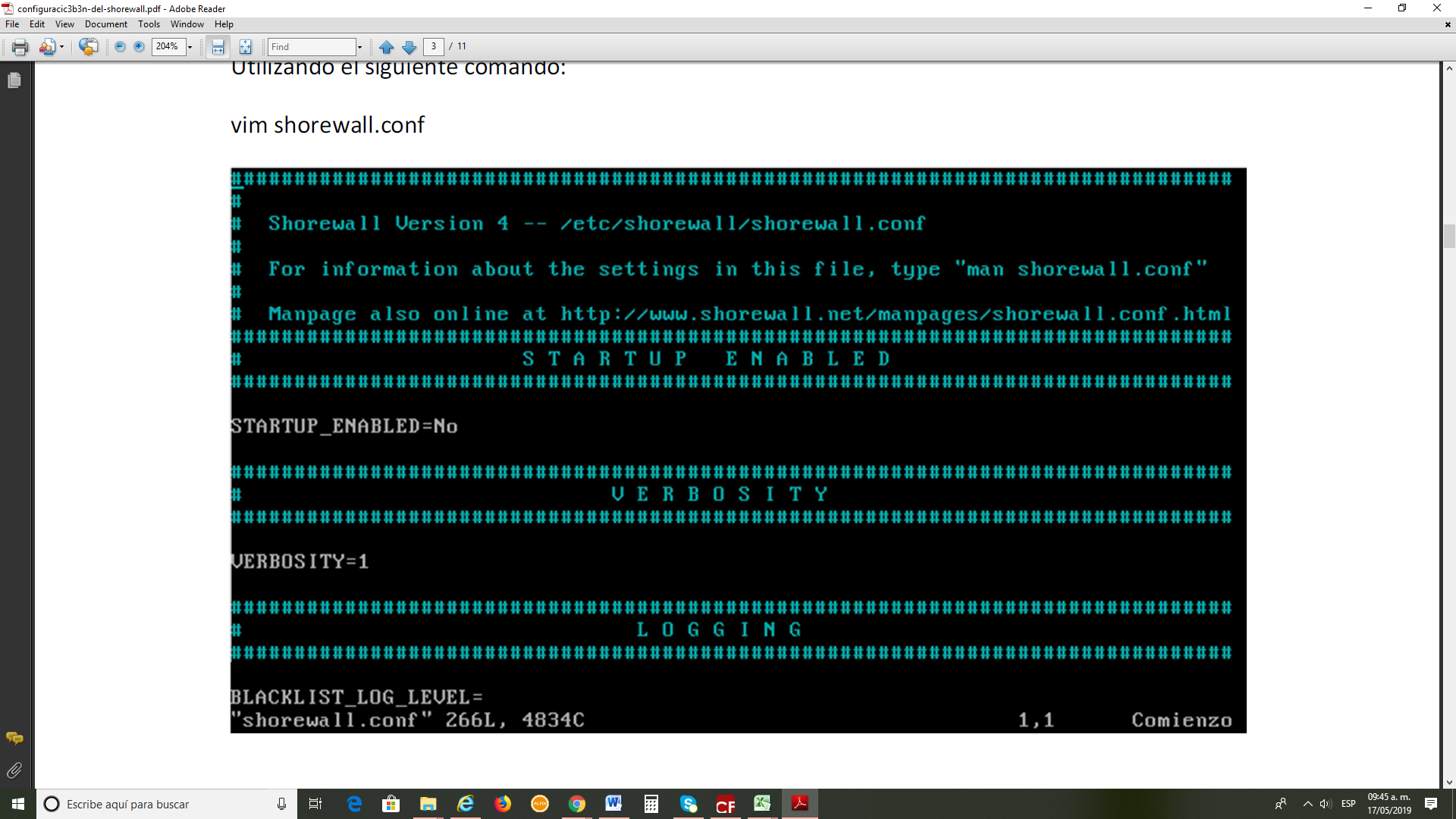
## **SHOREWALL**

Shorewall es un firewall, un cortafuego, es decir un software que nos ayudará a mantener segura nuestra red, controlando el tráfico entrante como saliente. Se necesita establecer una serie de zonas, las cuales nos permitirán controlar el flujo de información, indicando que tipo de información podrá ingresar.

Lo primero que hay que modificar es:

### **Archivo *shorewall.conf***

Este archivo contiene las configuraciones generales del firewall. Con el comando nano /etc/shorewall.conf entramos y modificamos.



#STARTUP ENABLED

# Se utiliza para activar Shorewall. De modo predefinido está desactivado, solo se necesita cambiar No por Yes.

STARTUP\_ENABLED=Yes

### **Archivo *policy***

Se establece como se accederá desde una zona hacia otra y hacia la zona de internet.

#SOURCE DEST POLICY LOG LEVEL LIMIT: BURST

fw net ACCEPT

net fw ACCEPT

net all ACCEPT

#THE FOLLOWING POLICY MUST BE LAST

all all REJECT info

Lineas

1. el cortafuego mismo puede acceder hacia la zona de internet

2. Lo que venga del internet debe pasar por el cortafuego

3. Se permiten conexiones desde internet hacia el resto de las zonas.

4. Se establece una política de rechazar conexiones para todo lo que se haya omitido

Con esto ya tendremos nuestro pequeña red bien segura, pero no podremos hacer nada, ya que solamente tenemos acceso a la red desde el firewall, todo está bloqueado, por eso necesitaremos editar el archivo ***rules (reglas)***.

### **Archivo *rules***

Todos los puertos están cerrados de modo predefinido yla modificación de este archivo nos permitirá establecer las reglas de restricciones por parte del firewall. Entramos y modificamos con el comando nano rules.

Agregaremos debajo de la línea SECTION NEW las reglas que queramos, por ejemplo, las siguiente permitirá la conexión al puerto 22 (SSH), 80 y 443 de apache, y 3306 de MySQL desde ***Internet (net)*** a nuestro firewall.

#ACTION SOURCE DEST PROTO DEST

# PORT

?SECTION ALL

?SECTION ESTABLISHED

?SECTION RELATED

?SECTION INVALID

?SECTION UNTRACKED

#SECTION NEW

#

ACCEPT net $FW tcp 22

ACCEPT net $FW tcp 80

ACCEPT net $FW tcp 443

ACCEPT net $FW tcp 3306

### **Archivo *zones***

Se utiliza para definir las zonas que utilizará el muro cortafuegos. Entramos a modificar con el comando nano zones

#ZONE TYPE OPTIONS IN OUT

# OPTIONS OPTIONS

fw firewall

net ipv4

* **Ipv4:** Corresponde a la zona estándar manejada por shorewall
* **Firewall:** Determina el firewall

### **Archivo *interfaces***

Se utiliza para definir cuáles dispositivos de red corresponden a una zona del muro cortafuegos en particular y las opciones que se requieran para cada una de éstas. Entramos a modificar con el comando nano interfaces

#ZONE INTERFACE OPTIONS

net enp0s3 dhcp,tcpflags,nosmurfs,routefilter,

logmartians,sourceroute=0

## **ISC-DHCP**

Servidor para direcciones IP. DHCP (sigla en inglés de **D**ynamic **H**ost **C**onfiguration **P**rotocol) es un protocolo de red que permite a los nodos de una red IP obtener sus parámetros de configuración automáticamente.

Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme estas van estando libres, sabiendo en todo momento quien ha estado en posesión de esa IP, cuanto tiempo la ha tenido, a quien se la ha asignado después.

Provee los parámetros de configuración a las computadoras conectadas a la red informática que lo requieran (Mascara de red, puerta de enlace y otros) y también incluyen mecanismo de asignación de direcciones de IP.

### **Archivo */etc/dhcp/dhcpd.conf***

#Identifica la maquina donde se va a alojar el servidor de DHCP. Su uso se aplica cuando la maquina en cuestión tiene varias direcciones asignadas en una misma interfaz de red.

server-identifier lupita.com;

#DDNS-UPDATE-STYLE: Parámetro que especifica si el servidor DHCP hará actualizaciones DNS del nombre del cliente junto con la asignación de la IP.

#INTERIM: es el estilo de sincronización recomendado.

ddns-update-style interim;

#Mediante el uso de este parámetro, se añadirá <nombre> al final del nombre de la maquina cliente, para formar un nombre de dominio totalmente cualificado (FQDN)

ddns-domainname “lupita.com”;

#Se usa el valor “in-addr.arp” sin importar de que segmento de red se trate

ddns-rev-domain “in-addr.arp”;

#Permite la actualización de las asignaciones de un cliente a requerimiento de este, o bien las asignaciones se actualizan cuando el servidor así lo requiera.

ignore client-update;

#Podrá enviar mensajes DHCPNACK (respuesta del servidor para indicarle al cliente que su concesión ha vencido o si el cliente anuncia una configuración de red errónea) a aquellos clientes que envían un DHCPREQUEST (solicitudes varias del cliente, por ejemplo, para extender su concesión) con una petición de IP no válida.

#Poner el parámetro al comienzo del archivo supone que el servidor DHCP reasignara direcciones mal configuradas por el motivo que sea, incluso una la configuración nueva del servidor.

authoritative;

#Bloquea el reenvia de paquetes del DNS

option ip-forwarding off;

#SUBNET: segmento de subred sobre el cual actuara el dhcp

#NETMASK: mascara de red de la subred

subnet 192.168.1.0 netmask 255.255.255.0{

#Rango sobre el cual DHCP asignara direcciones IP

range 192.168.1.10 192.168.1.15;

#Parámetro que especifica mediante IP la ubicación del DNS

option domain-name-servers 192.168.1.1;

#Parámetro que describe el nombre de nuestro dominio

option domain-name “lupita.com”;

#Parámetro que especifica mediante IP la ubicación de router

option routers 192.168.1.1;

#Parámetro que especifica la IP de broadcast

option broadcast-address 192.168.1.255;

#Parámetro que indica el tiempo entre cada nueva asignación de IP a los equipos

default-lease-time 900;

#Parámetro que indica el tiempo de vigencia de la dirección IP para cada equipo

max-lease-time 7200;

}

#Parámetro que describe el nombre del equipo

host guadalupe{

#Parámetro que describe la dirección MAC asociada a la tarjeta ethernet del equipo

hardware ethernet 08:00:27:24:39:12;

#Parámetro que describe la dirección IP destinada a un equipo

fixed-address 192.168.1.50;

}