

Definición de zonas desmilitarizadas con Shorewall

Tabla de contenidos

- Instalación del entorno de prácticas
- Habilitar el Firewall
- Escaneando la Red
 - FUERA
 - DENTRO
 - DMZ
 - FIREWALL3
- Configuración de Shorewall
- Reglas y cadenas IPTABLES
- Escaneando la Red
 - FUERA
 - DENTRO
 - DMZ
 - FIREWALL3
- Opinión personal
- Bibliografía

Instalación del entorno de prácticas

Iniciamos el autoinstalador para Linux

```
curl -o- \
  http://ccia.esei.uvigo.es/docencia/CDA/1819/practicas//ejercicio-dmz-openvpn.sh \
  | bash -
```

Seguir cualquier indicación mostrada en [esta página](#) en caso de duda o error.

Habilitar el Firewall

Lo primero será habilitar la redirección del tráfico en la máquina **FIREWALL3** con el comando `echo 1 > /proc/sys/net/ipv4/ip_forward | cat /proc/sys/net/ipv4/ip_forward`

Escaneando la Red

Procederemos a escanear la red desde diferentes perspectivas:

FUERA

Escaneamos la red desde fuera de la DMZ:

```
nmap -T4 193.147.87.47 # FIREWALL3
nmap -T4 10.10.10.11   # DENTRO
nmap -T4 10.20.20.22   # DMZ
```

En mi caso usaré el comando `nmap -T4 193.147.87.47 10.10.10.11 10.20.20.22` para escanear las tres a la vez. El resultado será el siguiente:

```
Starting Nmap 7.40 ( https://nmap.org ) at 2018-11-15 11:27 CET
Nmap scan report for firewall3.cda.net (193.147.87.47)
Host is up (0.00013s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
79/tcp    open  finger
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
3260/tcp  open  iscsi
3306/tcp  open  mysql
MAC Address: 08:00:27:66:66:66 (Oracle VirtualBox virtual NIC)
Nmap done: 3 IP addresses (1 host up) scanned in 5.25 seconds
```

Como podemos observar, sólomente están visibles los servicios del FIREWALL3. El resto de las máquinas aparecen como desconectadas.

DENTRO

Realizamos el mismo proceso desde dentro con el comando `nmap -T4 193.147.87.33`

10.10.10.1 10.20.20.22 (ahora hemos cambiado la primera IP por la de la máquina FUERA y ahora el FIREWALL3 actúa como gateway)

Resultado:

```
Starting Nmap 7.40 ( https://nmap.org ) at 2018-11-15 11:40 CET
Nmap scan report for dmz.cda.net (10.20.20.22)
Host is up (0.00072s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
79/tcp    open  finger
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
3260/tcp  open  iscsi
3306/tcp  open  mysql
Nmap scan report for firewall3.cda.net (10.10.10.1)
Host is up (0.00047s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
79/tcp    open  finger
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
3260/tcp  open  iscsi
3306/tcp  open  mysql
MAC Address: 08:00:27:44:44:44 (Oracle VirtualBox virtual NIC)
Nmap done: 3 IP addresses (2 hosts up) scanned in 7.32 seconds
```

Podemos observar que ahora están visibles los servicios del FIREWALL3 y de la DMZ.

DMZ

Seguimos realizando el mismo proceso, esta vez desde la DMZ con el comando `nmap -T4 193.147.87.33 10.10.10.11 10.20.20.1` (Recordar que el FIREWALL3 ahora es el gateway de la DMZ)

```
Starting Nmap 7.40 ( https://nmap.org ) at 2018-11-15 11:42 CET
Nmap scan report for dentro.cda.net (10.10.10.11)
Host is up (0.00080s latency).
Not shown: 990 closed ports
```

```
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
79/tcp    open  finger
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
3260/tcp  open  iscsi
3306/tcp  open  mysql
Nmap scan report for firewall3.cda.net (10.20.20.1)
Host is up (0.00033s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
79/tcp    open  finger
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
3260/tcp  open  iscsi
3306/tcp  open  mysql
MAC Address: 08:00:27:55:55:55 (Oracle VirtualBox virtual NIC)
Nmap done: 3 IP addresses (2 hosts up) scanned in 7.36 seconds
```

El resultado es similar al del escaneo interno. Podemos ver todos los servicios menos los de la máquina externa.

FIREWALL3

Por último realizamos los escaneos desde el FIREWALL3 con el comando `nmap -T4 193.147.87.33 10.10.10.11 10.20.20.22`

```
Nmap scan report for fuera (193.147.87.33)
Host is up (0.00033s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
79/tcp    open  finger
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
3260/tcp  open  iscsi
3306/tcp  open  mysql
MAC Address: 08:00:27:33:33:33 (Oracle VirtualBox virtual NIC)
```

```
Nmap scan report for dentro.cda.net (10.10.10.11)
Host is up (0.00037s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
79/tcp    open  finger
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
3260/tcp  open  iscsi
3306/tcp  open  mysql
MAC Address: 08:00:27:11:11:11 (Oracle VirtualBox virtual NIC)
Nmap scan report for dmz.cda.net (10.20.20.22)
Host is up (0.00028s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
79/tcp    open  finger
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
3260/tcp  open  iscsi
3306/tcp  open  mysql
MAC Address: 08:00:27:22:22:22 (Oracle VirtualBox virtual NIC)
Nmap done: 3 IP addresses (3 hosts up) scanned in 9.29 seconds
```

En este caso es posible observar cómo todas las máquinas aparecen levantadas junto a sus servicios abiertos.

Configuración de Shorewall

Para configurar Shorewall seguimos los siguientes pasos:

Copiamos y descomprimos la plantilla disponible en

`/usr/share/doc/shorewall/examples/three-interfaces/` dentro de `/etc/shorewall` usando la secuencia de comandos:

```
cp /usr/share/doc/shorewall/examples/three-interfaces/* /etc/shorewall/
cd /etc/shorewall
gunzip -f *.gz
```

Con `nano interfaces` dentro de `/etc/shorewall` actualizaremos los nombres de las

interfaces para que queden de la siguiente manera:

```
?FORMAT 2
net      enp0s9      tcpflags,routefilter,norfc1918,nosmurfs,logmartians
loc      enp0s3      tcpflags,detectnets,nosmurfs
dmz      enp0s8      tcpflags,detectnets,nosmurfs
```

Posteriormente, con `nano policy` definimos las políticas de conexión (importante dejar `all` como la última política):

```
loc      all      DROP      info
net      all      DROP      info
dmz      all      DROP      info
all      all      REJECT    info
```

Definimos el enmascaramiento con `nano masq` para la red interna y la DMZ. De esta forma el trafico saliente de las redes internas se reescribirá usando la IP del FIREWALL3:

```
enp0s9      10.10.10.0/24 # Dentro
enp0s9      10.20.20.0/24 # DMZ
```

Añadiremos reglas de conexión con Shorewall modificando el archivo `rules` . Debemos comentar la línea `DNS(ACCEPT) $FW net` dado que no nos interesa y añadir lo siguiente al final del archivo:

```
# Redireccion puertos http, https, smtp, pop3 de la red externa a la DMZ
DNAT net dmz:10.20.20.22 tcp 80,443
DNAT net dmz:10.20.20.22 tcp 25,110
# Acceso web y ssh desde la red interna hacia la externa
ACCEPT loc net tcp 80,443
ACCEPT loc net tcp 22
# Acceso mail desde el server de la DMZ hacia la red externa
ACCEPT dmz:10.20.20.22 net tcp 25
# Acceso desde la DMZ al servidor MySQL interno
ACCEPT dmz:10.20.20.22 loc:10.10.10.11 tcp 3306
# Acceso DNS desde la red interna y la DMZ a la red externa
DNS(ACCEPT) loc net
DNS(ACCEPT) dmz net
```

Por último cambiamos `STARTUP_ENABLED=No` a `STARTUP_ENABLED=Yes` dentro del archivo `shorewall.conf` y borramos cualquier regla residual con `rm /etc/shorewall/stoppedrules` .

¡Ya estamos listos para ejecutar el comando `shorewall start` !

Reglas y cadenas IPTABLES

Con el comando `iptables -L [nombre de la cadena]` podemos ver las reglas definidas por Shorewall:

```
target      prot opt source                destination
# iptables -L net-dmz
# Regla de acceso hacia la DMZ desde el exterior
ACCEPT      tcp  --  anywhere              dmz.cda.net
            multiport dports http,https,smtp,pop3
# iptables -L dmz-loc
# Regla de acceso hacia el servidor MySQL desde la DMZ
ACCEPT      tcp  --  dmz.cda.net           dentro.cda.net        tcp dpt:mysql
```

Escaneando la Red

Procederemos a escanear de nuevo la red desde diferentes perspectivas:

FUERA

Resultado `nmap -T4 193.147.87.47 10.10.10.11 10.20.20.22` :

```
Nmap scan report for firewall3.cda.net (193.147.87.47)
Host is up (0.0014s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE
25/tcp    open  smtp
80/tcp    open  http
110/tcp   open  pop3
443/tcp   closed https
MAC Address: 08:00:27:66:66:66 (Oracle VirtualBox virtual NIC)
Nmap done: 3 IP addresses (1 host up) scanned in 15.32 seconds
```

Podemos observar que ahora los puertos sólo los servicios expuestos hacia el exterior de la DMZ están disponibles (el puerto https aparece como cerrado dado que la DMZ no tiene configurado ningún servicio https).

El salto a través del FIREWALL3 lo vemos con el comando `tcptraceroute 193.147.87.47 80` :

```
Selected device enp0s3, address 193.147.87.33, port 55889 for outgoing packets
Tracing the path to 193.147.87.47 on TCP port 80 (http), 30 hops max
 1  firewall3.cda.net (193.147.87.47)  0.623 ms  0.585 ms  0.577 ms # FIREWALL3
 2  firewall3.cda.net (193.147.87.47) [open]  1.126 ms  1.556 ms  1.715 ms # DMZ
```

DENTRO

Resultado `nmap -T4 193.147.87.33 10.20.20.22 10.10.10.1 :`

```
Starting Nmap 7.40 ( https://nmap.org ) at 2018-11-15 12:51 CET
Nmap scan report for fuera (193.147.87.33)
Host is up (0.0017s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    closed domain
80/tcp    open  http
443/tcp   closed https
Nmap scan report for dmz.cda.net (10.20.20.22)
Host is up (0.0014s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
Nmap scan report for firewall3.cda.net (10.10.10.1)
Host is up (-0.078s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: 08:00:27:44:44:44 (Oracle VirtualBox virtual NIC)
Nmap done: 3 IP addresses (3 hosts up) scanned in 25.55 seconds
```

En este caso, los servicios dns, ssh y http(s) están permitidos cara la red externa, pero solamente la conexión ssh hacia la DMZ a través del firewall.

Podemos conectarnos a la máquina FUERA con el comando `ssh usuario@193.147.87.33` y la contraseña `usuario` . Si usamos el comando `who` , nos responderá diciendo que estamos conectados con la IP del FIREWALL3 (`usuario pts/1 2018-11-15 13:08 (193.147.87.47)`).

DMZ

Resultado `nmap -T4 193.147.87.33 10.10.10.11 10.20.20.1 :`

```
Starting Nmap 7.40 ( https://nmap.org ) at 2018-11-15 12:58 CET
Nmap scan report for fuera (193.147.87.33)
Host is up (0.0016s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
25/tcp    open  smtp
53/tcp    closed domain
Nmap scan report for dentro.cda.net (10.10.10.11)
Host is up (0.0016s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
3306/tcp  open  mysql
Nmap scan report for firewall3.cda.net (10.20.20.1)
```



```
Host is up (-0.20s latency).
All 1000 scanned ports on firewall3.cda.net (10.20.20.1) are filtered
MAC Address: 08:00:27:55:55:55 (Oracle VirtualBox virtual NIC)
Nmap done: 3 IP addresses (3 hosts up) scanned in 40.93 seconds
```

Desde la DMZ es destacable ver cómo podemos acceder al servidor MySQL de la red interna, además de a los servicios smtp externos.

FIREWALL3

Resultado `nmap -T4 193.147.87.33 10.10.10.11 10.20.20.22 :`

```
Starting Nmap 7.40 ( https://nmap.org ) at 2018-11-15 13:01 CET
Nmap scan report for fuera (193.147.87.33)
Host is up (-0.20s latency).
All 1000 scanned ports on fuera (193.147.87.33) are filtered
MAC Address: 08:00:27:33:33:33 (Oracle VirtualBox virtual NIC)
Nmap scan report for dentro.cda.net (10.10.10.11)
Host is up (-0.20s latency).
All 1000 scanned ports on dentro.cda.net (10.10.10.11) are filtered
MAC Address: 08:00:27:11:11:11 (Oracle VirtualBox virtual NIC)
Nmap scan report for dmz.cda.net (10.20.20.22)
Host is up (-0.20s latency).
All 1000 scanned ports on dmz.cda.net (10.20.20.22) are filtered
MAC Address: 08:00:27:22:22:22 (Oracle VirtualBox virtual NIC)
Nmap done: 3 IP addresses (3 hosts up) scanned in 64.07 seconds
```

Desde el FIREWALL3 es curioso ver cómo las 3 máquinas aparecen como levantadas pero sin ningún servicio accesible.

Opinión personal

En general pienso que las soluciones detalladas dan muy buen resultado con el fin de proteger la red.




Como en todo, siempre existen fallas de seguridad, por ejemplo:

Dado que un usuario interno tiene acceso ssh a servicios externos, puede crear un túnel ssh para brindar un método de conexión directo a la red interna a un atacante externo.

Buenas prácticas en este caso sería la incorporación de herramientas como `Snort` o `Suricata`. También se podrían implementar métodos como el `port-knocking` en el Firewall. Por último, y mi medida de seguridad preferida, sería la implementación de diferentes `honeypots` para monitorizar, controlar y aprender sobre los diferentes ataques a los que está

expuesta tu red.

Bibliografía

-  <https://github.com/Student-Puma/HomeLab>
-  https://en.wikipedia.org/wiki/Port_knocking
-  <http://ccia.esei.uvigo.es/docencia/CDA/1819/practicas/ejercicio-dmz/ejercicio-dmz.html>