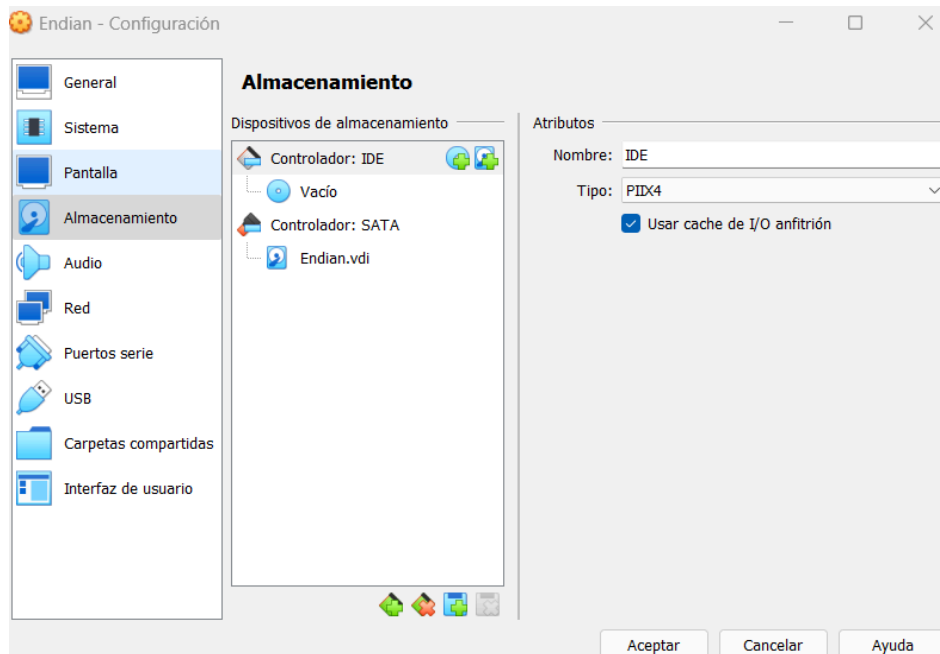
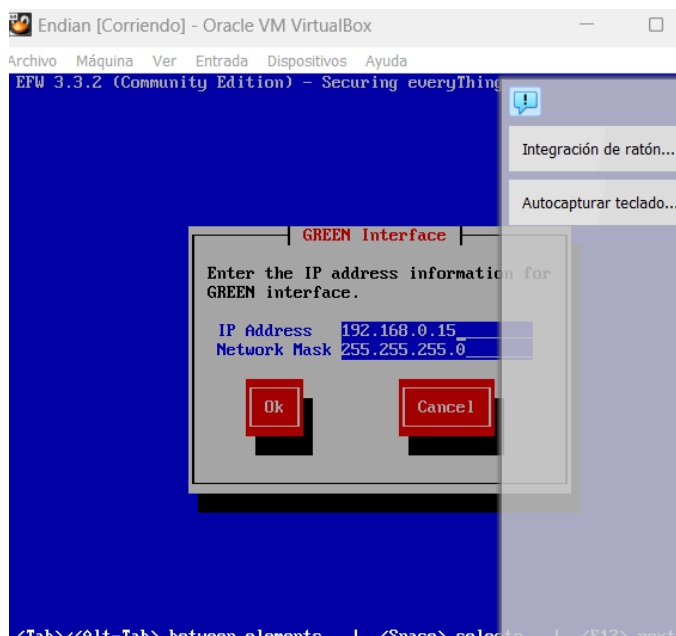


## TAREA #982: INSTALACIÓN DE UN UTM Y CONFIGURACIÓN DEL FIREWALL CREANDO UNA REGLA POR CADA SERVICIO EN EL MS2

Realizo la instalación de Endian y lo configuro:



Me genera la ip por default para levantar el servicio:



Cerrar sesión
Ayuda

SistemaEstadoRedServiciosFirewallProxyVPNRegistros e informes

Control principal
Configuración de red
Notificaciones de eventos
Updates
Usuarios
Consola web
Acceso SSH
Configuración del interfaz
Backup
Apagar

### Control principal

Configuración del control principal

[Mostrar configuración](#)

jazmin.jazmin

Dispositivo	Community
Versión	3.3.2
Tiempo en línea	20m
Community Account	<a href="#">Registrarse</a>

Actualizaciones de firmas

No se encontraron actualizaciones de firmas recientes

Información del hardware

CPU 1	1%
CPU 2	2%
Memoria	7% 3941 MB
Swap	0% 3939 MB
Partición principal	40% 1.8G
Partición de datos	7% 6.7G
Disco de configuración	8% 120M
Disco de registro	5% 4.4G

Interfaces de red

Dispositivo	Tipo	Link	Entrantes	Salientes
<input checked="" type="checkbox"/> eth1	ethernet	Sin conexión	0.0 KB/s	0.0 KB/s
<input checked="" type="checkbox"/> br0	ethernet	Activo	0.5 KB/s	0.6 KB/s
<input type="checkbox"/> eth0	ethernet	Activo	0.6 KB/s	0.6 KB/s

Tráfico entrante en KB/s (máx. de interfaces 6)

Tráfico saliente en KB/s (máx. de interfaces 6)

Enlaces

En MS2 inserto ipconfig para obtener la ip de mi MS2 y ejecuto el comando nmap -T4 -sV -F ip\_de\_ms2, la cual es 192.168.0.29, en la consola de MS2 para hacer la conexión entre MS2 y Endian:

To access official Ubuntu documentation, please visit:  
<http://help.ubuntu.com/>  
No mail.

```

msfadmin@metasploitable:~$ ipconfig
-bash: ipconfig: command not found
msfadmin@metasploitable:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:93:b2:08 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.29/24 brd 192.168.0.255 scope global eth0
    inet6 2806:250:c06:c20d:a00:27ff:fe93:b208/64 scope global dynamic
        valid_lft 32149sec preferred_lft 32149sec
    inet6 fe80::a00:27ff:fe93:b208/64 scope link
        valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$ nmap -T4 -sV -F 192.168.0.29

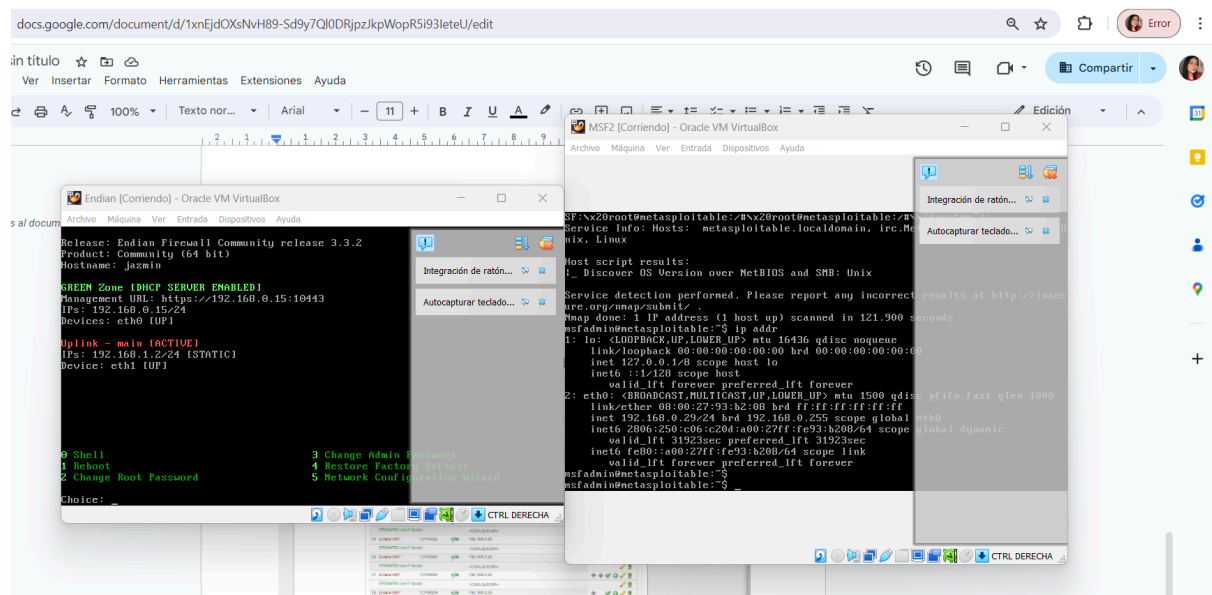
Starting Nmap 4.53 ( http://insecure.org ) at 2024-05-13 18:20 EDT

```

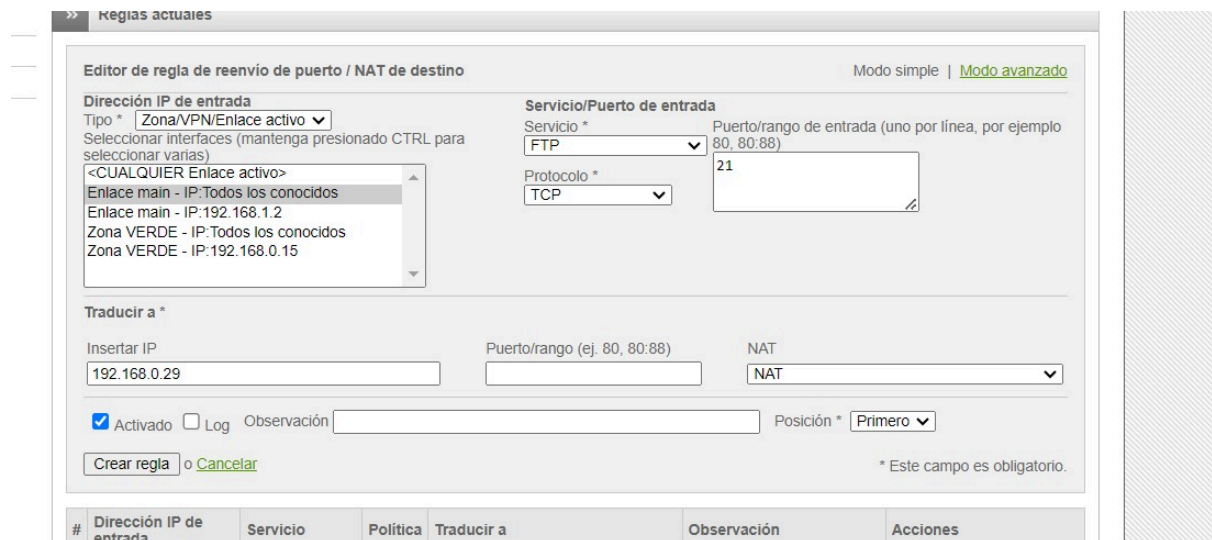
Integración de ratón...
Autocapturar teclado...

CTRL DERECHA

Se empieza a generar los servicios:



**Empiezo a crear reglas por cada servicio que obtuve de MS2**



**Reglas de todos los servicios:**

No seguro

https://192.168.0.15:10443/cgi-bin/dnat.cgi#createrule

Error

endian firewall

community

Cerrar sesión

Ayuda

Sistema

Estado

Red

Servicios

Firewall

Proxy

VPN

Registros e informes

Redirección de puertos / NAT

Tráfico de salida

Tráfico entre zonas

Tráfico VPN

Acceso al sistema

Diagramas de firewall

Redirección de puertos / NAT de destino

Redirección de puertos / NAT de destino

NAT fuente: Tráfico entrado de entrada

!

Port forwarding / Destination NAT rules have been changed and need to be applied in order to make the changes active

Aplicar

Reglas actuales

Agregar nueva regla de reenvío de puerto / NAT de destino

#	Dirección IP de entrada	Servicio	Política	Traducir a	Observación	Acciones
1	Enlace ANY	TCP/21		192.168.0.29		
PERMITIR con IP desde:						<CUALQUIERA>

Leyenda: ☒ Activado (clic para desactivar) ☐ Desactivado (clic para activar) Editar Eliminar

Mostrar reglas del sistema >>

Status: Conectado: main (04 0h 36m 0s) Uptime: 17:32:59 up 45 min, 0 users, load average: 0.02, 0.02, 0.01

Endian Firewall Community release 3.3.2 (c) Endian

https://192.168.0.15:10443/cgi-bin/dnat.cgi

Error

Sistema

Estado

Red

Servicios

Firewall

Proxy

VPN

Registros e informes

Redirección de puertos / NAT

Tráfico de salida

Tráfico entre zonas

Tráfico VPN









































































































Acceso al sistema

Diagramas de firewall

Reglas actuales

Agregar nueva regla de reenvío de puerto / NAT de destino

#	Dirección IP de entrada	Servicio	Política	Traducir a	Observación	Acciones
1	Enlace ANY	TCP/21		192.168.0.29		
PERMITIR con IP desde:						<CUALQUIERA>
2	Enlace ANY	TCP/22		192.168.0.29		
PERMITIR con IP desde:						<CUALQUIERA>
3	Enlace ANY	TCP/23		192.168.0.29		
PERMITIR con IP desde:						<CUALQUIERA>
4	Enlace ANY	TCP/25		192.168.0.29		
PERMITIR con IP desde:						<CUALQUIERA>
5	Enlace ANY	TCP/53		192.168.0.29		
PERMITIR con IP desde:						<CUALQUIERA>
6	Enlace ANY	TCP/80		192.168.0.29		
PERMITIR con IP desde:						<CUALQUIERA>
7	Enlace ANY	TCP/111		192.168.0.29		
PERMITIR con IP desde:						<CUALQUIERA>
8	Enlace ANY	TCP/139		192.168.0.29		
PERMITIR con IP desde:						<CUALQUIERA>
9	Enlace ANY	TCP/445		192.168.0.29		
PERMITIR con IP desde:						<CUALQUIERA>
10	Enlace ANY	TCP/513		192.168.0.29		
PERMITIR con IP desde:						<CUALQUIERA>
11	Enlace ANY	TCP/514		192.168.0.29		
PERMITIR con IP desde:						<CUALQUIERA>
12	Enlace ANY	TCP/2049		192.168.0.29		
PERMITIR con IP desde:						<CUALQUIERA>

	Sistema	Estado	Red	Servicios	Firewall	Proxy	VPN	Registros e informes
<div>Redirección de puertos / NAT</div> <div>Tráfico de salida</div> <div>Tráfico entre zonas</div> <div>Tráfico VPN</div> <div>Acceso al sistema</div> <div>Diagramas de firewall</div>				PERMITIR con IP desde:	<CUALQUIERA>			 
	6	Enlace ANY	TCP/80		192.168.0.29			    
				PERMITIR con IP desde:	<CUALQUIERA>			 
	7	Enlace ANY	TCP/111		192.168.0.29			    
				PERMITIR con IP desde:	<CUALQUIERA>			 
	8	Enlace ANY	TCP/139		192.168.0.29			    
				PERMITIR con IP desde:	<CUALQUIERA>			 
	9	Enlace ANY	TCP/445		192.168.0.29			    
				PERMITIR con IP desde:	<CUALQUIERA>			 
	10	Enlace ANY	TCP/513		192.168.0.29			    
				PERMITIR con IP desde:	<CUALQUIERA>			 
	11	Enlace ANY	TCP/514		192.168.0.29			    
				PERMITIR con IP desde:	<CUALQUIERA>			 
	12	Enlace ANY	TCP/2049		192.168.0.29			    
				PERMITIR con IP desde:	<CUALQUIERA>			 
	13	Enlace ANY	TCP/2121		192.168.0.29			    
				PERMITIR con IP desde:	<CUALQUIERA>			 
	14	Enlace ANY	TCP/3306		192.168.0.29			    
				PERMITIR con IP desde:	<CUALQUIERA>			 
	15	Enlace ANY	TCP/5432		192.168.0.29			    
				PERMITIR con IP desde:	<CUALQUIERA>			 
	16	Enlace ANY	TCP/6900		192.168.0.29			    
				PERMITIR con IP desde:	<CUALQUIERA>			 
	17	Enlace ANY	TCP/6000		192.168.0.29			    
				PERMITIR con IP desde:	<CUALQUIERA>			 
	18	Enlace ANY	TCP/8009		192.168.0.29			    
				PERMITIR con IP desde:	<CUALQUIERA>			