Seguridad en Sistemas de Información: Tarea 2

Jorge E. Chávez Saab

CINVESTAV-IPN

12 de Junio 2020

En esta práctica arrancamos la imagen de un sistema mínimo con sistema de archivos ya funcional y verificamos que la máquina virtual este propiamente conectada al internet.

1. Configuración de la Máquina Virtual

Primero descargamos la imagen del sistema que se provee y la seleccionamos como entrada de disco para la máquina virtual que habíamos creado en el trabajo anterior.



Antes de iniciar la máquina, verificamos en la configuración de red que el tipo de adaptador sea el de virtio-net.



Habiendo completado esto arrancamos la máquina y verificamos que esta vez sí inicia correctamente, permitiéndonos el acceso con root/holahola.



			MiLinux	c Miniatura [F	Running] - Oracle VM \	/irtualBox	_ 🗆 ×
File	Machine	View	Input	Devices	Help		
Youh (15 (15 kt miss miss ady cost cassw cogin	1.850037 avethe Auto (1.852821 1.8554751 91983400) 1.8597031 1.8686131 1.8721101 1.8744941 1.8744941 1.8822351 1.8943241 1.8943241 stema min 1.9019371 ing - tai 1.9126271) login: ord: [102]: rc	sapture ko sapture ko precision (Free) Freei Freei Freei State Freei State Freei State Freei State Freei State St	type eyboard o rmor f cmos rt ing unu e prote ing unu nm: Che nm: Che nm: Che che init a stá ini io: mod kernel io-pci 2.93546 gin on	fscruption turned toption turned top	registered dog This will cause t shal policy setting syste nel image (in he kernel rea nel image (te: nel image (ro X mappings: p. ser space pag X mappings: p. process do ification fai :03.0: virtio : ADDRCONF(NE	the Virtual Machine to automati hashing enabled em clock to 2020-06- itmem) memory: 1672K d-only data: 16384k xt/rodata gap) memor data/data gap) memor data/data gap) memor assed, no W+X pages e tables assed, no W+X pages led: signature and/o _pci: leaving for le TDEU_CHANGE): eth0:	cally I I I I I I I I I I I I I I I I I I
				- · · ·			🖉 🔮 Right Ctrl
				Graphi Remot Record	<u>cs Controll</u> er: e Desktop Server: lina:	VMSVGA Disabled Disabled	
						Disabica	

2. Modificar Archivos de Configuración

Dentro de la máquina virtual, usamos el comando vi /etc/resolv.conf para ver la configuración de DNS, y observamos que el DNS está registrado con la dirección ip que se usó como ejemplo en clase.

			Mi Linux	Miniatura [F	lunning] - Oracle VM V	irtualBox	_ - ×
File	Machine	View	Input	Devices	Help		
# nam	eserver 1	10.0.2	.3				
~ names	erver 140	5.247.	102.1				X E
~							
~							
~							
~							
~							
~							
~							
~							
~							
~							
~							
~							
~							
~							
~							
~							
- /et	c∕resolv	.conf	1/2 50%				
						o 🐚 🗗 🌶 📖 🖬 🖉 🖉	🛂 Right Ctrl
				Graphi	cs Controller:	VMSVGA	
				Remot	e Desktop Server:	Disabled	
				Record	ing:	Disabled	
				S			

En el sistema anfitrión, usamos el comando

cat /etc/resolv.conf para ver el contenido del mismo archivo, y copiamos la dirección del DNS para nuestra red, que en este caso es 192.168.1.254. Pegamos esta dirección al archivo de la máquina virtual y guardamos los cambios.



Para evitar repetir este paso en el futuro, hemos vuelto a generar un archivo .iso basado en este pero con este archivo ya modificado, siguiendo los pasos del Trabajo 1.

3. Pruebas de Conexión

Al ejecutar los comandos ifconfig y route en la máquina virtual, podemos ver que la dirección IP de la máquina es 10.0.2.15 y el default Gateway es 10.0.2.2.

Mi Linux Miniatura [Running] - Oracle VM VirtualBox										-	•	×
File Mach	hine Vie	ew Input	Devices	Help								
~ # ifconf Feth⊖	ig Link en inet ad inet6 a UP BROM RX pack TX pack collisi RX byte	ncap:Ether idr:10.0.2 addr: fe80 ADCAST RUN kets:11 er kets:23 er ions:0 txd es:966 (96	enet HW 2.15 Bo 0::a00:2 INING MU erors:0 erors:0 ueueler 66.0 B)	Aaddr 08: cast:10.0 ?ff:fe1e ULTICAST dropped: dropped: 1:1000 TX byte	00:27:1 .2.255 :3607/6 MTU:15 0 over 0 over s:1930	LE:36:0 Mask 54 Scop 500 Ma Suns:0 Suns:0 (1.8	07 :255.25! pe:Link etric:1 frame:(carrie) KiB)	5.255.0 9 r:0)			
10	 Link encap:Local Loopback inet addr:127.0.0.1 Mask:255.0.0.0 inet6 addr: ::1/128 Scope:Host UP LOOPBACK RUNNING MTU:65536 Metric:1 RX packets:0 errors:0 dropped:0 overruns:0 frame:0 TX packets:0 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:1000 RY hutes:0 (0 0 R) TX hutes:0 (0 0 R) 											
~ # route Kernel IP Destinatio default 10.0.2.0 ~ #	routing on (y table Gateway 10.0.2.2	6 6 2	Genmask).0.0.0 255.255.2	55.0	Flags UG U	Metric 0 0	Ref 0 0	Use 0 0	lfa eth eth	се 0 0	
						0	8 🌶 🗐 🛛		9 💁 Ri	ight (Itrl	
		necoraniy.		01300	icu:							

Esto es consistente con la documentación de Virtual Box, la cual indica que la máquina virtual existe en una subred propia con el manejador de Virtual Box actuando como router. Especificamente, se señala en <u>https://www.virtualbox.org/manual/ch09.html#changenat</u> que:

"In NAT mode, the guest network interface is assigned to the IPv4 range 10.0.x.0/24 by default where x corresponds to the instance of the NAT interface +2. So x is 2 when there is only one NAT instance active. In that case the guest is assigned to the address 10.0.2.15, the gateway is set to 10.0.2.2 and the name server can be found at 10.0.2.3."

Lo cual coincide con nuestros datos (excepto que ya hemos cambiado la dirección del DNS para que sea el que provee nuestro ISP).

Para verificar que el DNS es alcanzable, podemos hacer un ping a la dirección que introducimos usando ping 192.168.1.1, y verificamos que el DNS responde:

		Mi Linux Miniatura [Running] - Oracle VM VirtualBox _ C								• ×
	File	e Machine	View	Input	Devices	Help				
ir	~									
	~									
	2									
	~									
	~									
	~									
	~ #	ping 192.1	168.1.1	-c 10	4 4 1 -	< 1-4-	14			
	64 h	172.100.1 Mutes from	192.16	38.1.1:	c.(1). c sen=1	o aata ttl=63	time=1.376	ms		
	64 b	ytes from	192.16	8.1.1:	seq=2	ttl=63	time=1.334	ms		
	64 b	ytes from	192.16	68.1.1:	seq=3	ttl=63	time=1.395	ms		- 1
	64 b	ytes from	192.16	68.1.1:	seq=4	ttl=63	time=1.317	MS		
	64 b	ytes from	192.16	68.1.1:	seq=5	ttl=63	time=1.306	MS		
	64 b	ytes from	192.16	8.1.1	seq=6	tt1=63	time=1.104	MS		
	64 D	bytes from	192.10	08.1.1	seq=7	ttl=63	time=1.247	MS		
	64 b	ytes from	192.10	8 1 1	564-0 264-0	ttl=63	time=1 305	ms ms		
	01 1	gees from	176.10	.1.1.	seq-s	ιι <u>ι</u> -03	¢100-1.303	iiis		
		192.168.1	1 ping	stati:	stics -					
	10 packets transmitted, 9 packets received, 10% packet loss									
	rour	nd-trip min	1/avg/n	nax = 1	.104/1.	325/1.5	544 ms			
	~ #									
							•	• 💵 🗗 🥟 💼 🖻 🚰 🐼 🥝	🕙 Right C	:trl
			Ne	coruny.			abteu			

Y finalmente verificamos que el DNS resuelve los nombres de dominio correctamente usando

nslookup google.com



Todo indica que la máquina se ha conectado correctamente a la red.