Wireshark: ICMP/ARP

ESCENARIO

Máquinas virtuais: Rede: 10.0.0.0

Máquina virtual A: RAM ≥ 2048MB CPU ≥ 2 PAE/NX habilitado Rede Interna ISO: Kali Live i386 IP/MS: 10.10.10.10/8 Máquina virtual B: RAM \ge 1024MB CPU \ge 1

Rede Interna Disco virtual: Microsoft Windows 10 IP/MS: 10.10.10.11/8



NOTAS:

(1) SMR_ALUXY -onde XY pode tomar os valores 01, 02, ..., 30 e corresponde ao número de PC que tes asignado.

(2) Debes facer entrega desta exercicio mediante **un arquivo en formato PDF**, noutro formato non será corrixido. O arquivo debe conter respostas/imaxes coa solución dos apartados. O arquivo a entregar na aula virtual terá o nome: **Solucion-RL-Exercicio3_ALUXY.pdf**

Exercicio 3 - Wireshark: ICMP/ARP

Máquina virtual A: Kali i386

1. Configuración da rede:

kali@kali:~\$ setxkbmap es #Cambiar o mapa de teclado ao idioma español.

kali@kali:~\$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)

root@kali:~# /etc/init.d/avahi-daemon stop #Parar o demo avahi-daemon(control resolución de nomes) para poder configurar de forma manual a configuración de rede e non ter conflicto con este demo.

root@kali:~# /etc/init.d/network-manager stop || pkill NetworkManager #Parar o demo network-manager(xestor de rede) ou o script NetworkManager (executado sen ser demo) para poder configurar doutro xeito (co comando ip(ifconfig) de forma manual ou mediante networking (ficheiros /etc/init.d/networking, /etc/init.d/networking.d) a configuración de rede e non ter conflicto con este xestor.

root@kali:~# ip addr show #Amosar a configuración de todas as tarxetas de rede. Nesta caso, na máquina A, as tarxetas de redes: loopback(lo), NAT(enps03) e interna(enps08).

root@kali:~# ip addr add 10.10.10.10/8 dev eth0 #Configurar a tarxeta de rede interna eth0, coa IP: 10.10.10.10 e máscara de subrede: 255.0.0.0.

root@kali:~# ifconfig eth0 10.10.10.10/8 #Comando equivalente ao anteriro, é dicir, configurar a tarxeta de rede interna eth0, coa IP: 10.10.10.10 e máscara de subrede: 255.0.0.

root@kali:~# ip addr show #Amosar a configuración de todas as tarxetas de rede. Nesta caso, na máquina A, as tarxetas de rede: loopback(lo) e interna(eth0).

2. Táboa arp:

root@kali:~# arp #Revisar a táboa arp, é dicir, visualizar a caché arp do sistema: asignación IP coa súa correspondente dirección física (MAC Address).

root@kali:~# exit #Saír da consola do usuario root, para voltar á consola do usuario kali sen permisos de root kali@kali:~\$

3. Arrancar Wireshark:

kali@kali:~\$ sudo wireshark & #Lanzar o programa wireshark (sniffer) para poder visualizar o que acontece na rede (protocolos, paquetes). O comando sudo permite executar o programa wireshark con permisos de root(administrador) e o caracter & serve para executar en segundo plano o programa e así devolver o prompt da consola para poder seguir traballando nela.

4. Agora minimizamos a máquina virtual A (Kali i386) xa que imos traballar coa máquina virtual B (Microsoft Windows 10).

Máquina virtual B: Microsoft Windows 10

- 5. Configuración da rede:
 - a. Arrancar a consola de comandos con permisos de administrador(clic botón dereito icono cmd \rightarrow clic botón dereito Símbolo del sistema \rightarrow Ejecutar como administrador):



b. Permitir cambios no dispositivo: Sí



c. ipconfig #Amosar a configuración de todas as tarxetas de rede..



- d. Configurar a tarxeta de rede interna coa IP: 10.10.10.11 e máscara de subrede: 255.0.0.0
 - i. No cmd(consola de comandos): control \rightarrow red \rightarrow Ver conexiones de red



ii. Ethernet \rightarrow clic botón dereito rato \rightarrow Propiedades



iii. Protocolo de internet versión 4 (TCP/IPv4) → dobre clic botón esquerdo rato → Usar la siguiente dirección IP:
 Dirección IP: 10.10.10.11

Propiedades de Ethernet		×		
Funciones de red		Propiedades: Protocolo de Internet ver	sión 4 (TCP/IPv4)	×
Conectar con:		General		
Intel(R) PRO/1000 MT Desktop Adapt	ter	Puede hacer que la configuración IP se	asigne automáticamente si la	
Esta conexión usa los siguientes elementos:	Configurar	red es compatible con esta funcionalidar consultar con el administrador de red cu apropiada.	d. De lo contrario, deberá iál es la configuración IP	
 E Cliente para redes Microsoft Uso compartido de archivos e impre 	, esoras para redes M	 Obtener una dirección IP automáti Usar la siguiente dirección IP: 	camente	
Programador de paquetes QoS	D /ID. A)	Dirección IP:	10 . 10 . 10 . 11	
Protocolo de multiplexor de adaptad	Jor de red de Micros	Máscara de subred:	255.0.0.0	
Controlador de protocolo LLDP de N Image: A controlador de Internet versión 6 (TCP	∕licrosoft P/IPv6)	Puerta de enlace predeterminada:		
	>	Obtener la dirección del servidor D	NC automáticamente	
<			No automaticamente	
< Instalar Desinstalar	Propiedades	Usar las siguientes direcciones de s	servidor DNS:	
Instalar Descripción	Propiedades	 Usar las siguientes direcciones de s Servidor DNS preferido: 	servidor DNS:	
Instalar Desinstalar Descripción Protocolo TCP/IP. El protocolo de red de. predeterminado que permite la comunicaci redes concetadas entre sí	Propiedades área extensa ión entre varias	Usar las siguientes direcciones de s Servidor DNS preferido: Servidor DNS alternativo:	servidor DNS:	
Instalar Desinstalar Descripción Protocolo TCP/IP. El protocolo de red de predeteminado que permite la comunicaci redes conectadas entre sí.	Propiedades área extensa ión entre varias	Usar las siguientes direcciones de : Servidor DNS preferido: Servidor DNS alternativo: Ualidar configuración al salir	Opciones avanzadas.	



iv. ipconfig #Amosar a configuración de todas as tarxetas de rede..

🔤 Administrador: Símbolo del sistema	
C:\Windows\system32>ipconfig	
Configuración IP de Windows	
Adaptador de Ethernet Ethernet:	
Sufijo DNS específico para la conexión : Vínculo: dirección IPv6 local : fe80::c02d:8855:6edb:b313%15 Dirección IPv4 : 10.10.10.11 Máscara de subred : 255.0.0.0 Puerta de enlace predeterminada :	
C:\Windows\svstem32>_	

- 6. Táboa arp:
 - a. arp -a #Revisar a táboa arp, é dicir, visualizar a caché arp do sistema: asignación IP coa súa correspondente dirección física (MAC Address).

Inter	faz: 10.10.10.11	0xf		
Dire	ección de Interne	et Dirección	física	Tipo
10.2	255.255.255	ff-ff-ff-ff-ff-ff	estático	
224.	.0.0.22	01-00-5e-00-00-16	estático	
224.	.0.0.252	01-00-5e-00-00-fc	estático	
239.	.255.255.250	01-00-5e-7f-ff-fa	estático	
255	.255.255.255	ff-ff-ff-ff-ff-ff	estático	

 Agora minimizamos a máquina virtual B (Microsoft Windows 10) xa que imos traballar coa máquina virtual A (Kali i386).

Máquina virtual A: Kali i386

- 8. Agora maximizamos a máquina virtual A (Kali i386).
- 9. Play (icono azul aleta tiburón) en wireshark, é dicir, arrancamos o wireshark.

						(Captu	uring from	n eth0							-	n x
Arch	ivo	<u>E</u> dición	<u>V</u> isua	lización	n <u>I</u> r	<u>C</u> aptura	Ar	nalizar	<u>E</u> stadís	ticas	Telefon <u>í</u> a	Wireles	ss <u>I</u>	<u>H</u> errar	nienta	is <u>A</u> yud	a
		2		#101 0110 0111	X	6	9) 🖄	•	₹		Ð	Q			
A	oliqu	e un filtro	o de vis	sualizac	ión	<ctrl-></ctrl->											- +
No.		Time		Source	e			Destina	tion		Protoco	l Lengt	h Info	D			
4																	Þ
0 7	7	eth0: <liv< th=""><th>ve capt</th><th>ure in p</th><th>orogre</th><th>ss></th><th></th><th></th><th></th><th>No</th><th>o hay paqu</th><th>etes</th><th></th><th></th><th>Per</th><th>fil: Defau</th><th>lt .</th></liv<>	ve capt	ure in p	orogre	ss>				No	o hay paqu	etes			Per	fil: Defau	lt .

10. Facer ping á máquina virtual B(Microsoft Windows 10): root@kali:~# ping -c4 10.10.10.11 #Envíar 4 paquetes ICMP dende a máquina Kali a Máquina Windows 10

			rc	oot@kali	:~		
Archivo	Acciones	Editar	Vista	Ayuda			
rootākal PING 10. 64 bytes 64 bytes 64 bytes 64 bytes 64 bytes 10.1 4 packet rtt min/ rootākal	<pre>i:~# ping 10.10.11 f from 10. from 10. from 10. from 10. 0.10.11 p s transmin avg/max/moti:~#</pre>	-c4 10.1 (10.10.10 10.10.11: 10.10.11: 10.10.11: 10.10.11: 10.10.11: tted, 4 r dev = 0.5	0.10.1).11) 5 icmp_ icmp_ icmp_ icmp_ stics receive 54/1.4	1 6(84) seq=1 seq=2 seq=3 seq=4 ed, 0% 94/2.1	bytes of ttl=128 ttl=128 ttl=128 ttl=128 packet 1 18/0.605	f data. time=2.12 time=1.39 time=1.92 time=0.55 loss, time 5 ms	ms ms Ms 4 ms 3005ms

11. Stop (icono vermello cadrado) en wireshark, é dicir, paramos o wireshark.

Archivo	<u>E</u> dición <u>V</u> isua	lización <u>I</u> r <u>C</u> aptura <u>4</u>	nalizar <u>E</u> stadísticas	Telefon <u>í</u> a <u>W</u>	ireless <u>H</u> erramient	as <u>A</u> yuda	i i i i i i i i i i i i i i i i i i i	
		= 🗋 🖹 🎑 ۹	🕈 😫 🍬 🔷	₹.		1 6		
Apliq	📕 Aplique un filtro de visualización <ctrl-></ctrl->							
No.	Time	Source	Destination	Protocol L	ength Info			
	1 0.000000000	PcsCompu_06:2b:58	Broadcast	ARP	42 Who has 10.:	10.10.11?	Tell 10.10.10.10	
1	2 0.001276349	PcsCompu_28:b1:da	PcsCompu_06:2b:58	ARP	60 10.10.10.11	is at 08	:00:27:28:b1:da	
	3 0.001291184	10.10.10.10	10.10.10.11	ICMP	98 Echo (ping)	request	id=0x2ec6, seq=1	/256, ttl=64 (reply in 4)
	4 0.002067068	10.10.10.11	10.10.10.10	ICMP	98 Echo (ping)	reply	id=0x2ec6, seq=1	/256, ttl=128 (request in 3)
	5 1.001847096	10.10.10.10	10.10.10.11	ICMP	98 Echo (ping)	request	id=0x2ec6, seg=2	2/512, ttl=64 (reply in 6)
	6 1.003164191	10.10.10.11	10.10.10.10	ICMP	98 Echo (ping)	reply	id=0x2ec6, seg=2	2/512, ttl=128 (request in 5)
	7 2.003880571	10.10.10.10	10.10.10.11	ICMP	98 Echo (ping)	request	id=0x2ec6, seg=3	8/768, ttl=64 (reply in 8)
	8 2.005734595	10.10.10.11	10.10.10.10	ICMP	98 Echo (ping)	reply	id=0x2ec6, sea=3	2/768, ttl=128 (request in 7)
	9 3.005179302	10.10.10.10	10.10.10.11	ICMP	98 Echo (ping)	request	id=0x2ec6, seg=4	/1024, ttl=64 (reply in 10)
1	0 3.005702583	10.10.10.11	10.10.10.10	ICMP	98 Echo (ping)	reply	id=0x2ec6, seq=4	/1024, ttl=128 (request in 9)

Podemos observar que como na táboa arp de Kali non estaba recoñecida a dirección física (MAC Address) de Windows 10, averiguase mediante o protocolo ARP. Así, envíase dende Kali unha mensaxe de broadcast(difusión) a todos os nodos da rede preguntando que host ten a dirección física correspondente á IP 10.10.10.10.11; e o host que posee esa IP, o de Windows 10, resposta indicando mediante un paquete ARP a súa dirección física. Deste xeito, agora xa se poden transmitir os paquetes ICMP, porque Kali sabe a que dirección física dirixilos para que poidan ser recibidos. Como podemos observar na imaxe, por cada paquete ICMP de Kali envíase unha pregunta (echo request), o cal ten a súa resposta correspondente da máquina Windows 10 con outro paquete ICMP (echo reply).

12. Comprobar a táboa arp:

root@kali:~# arp #Revisar a táboa arp, é dicir, visualizar a caché arp do sistema: asignación IP coa súa correspondente dirección física (MAC Address). Agora podemos observar como si existe unha entrada para o Windows 10, onde se asigna a IP 10.10.10.11 a súa dirección física (MAC Address ou HWaddress).

Ì	root@kali:~# arp				
ł	Address	HWtype	HWaddress	Flags Mask	Iface
Ì	10.10.10.11	ether	08:00:27:28:b1:da	C	eth0
Ì	root@kali:~#				

Máquina virtual B: Microsoft Windows 10

13. Comprobar a táboa arp:

a. arp -a #Revisar a táboa arp, é dicir, visualizar a caché arp do sistema: asignación IP coa súa correspondente dirección física (MAC Address). Agora podemos observar como si existe unha entrada para Kali, onde se asigna a IP 10.10.10.10 a súa dirección física.

T-+ [40 40 40 44	0.5		
Interfaz: 10.10.10.11 -	- 0XT		
Dirección de Internet	Dirección	física	Tipo
10.10.10.10	08-00-27-06-2b-58	dinámico	
10.255.255.255	ff-ff-ff-ff-ff	estático	
224.0.0.22	01-00-5e-00-00-16	estático	
239.255.255.250	01-00-5e-7f-ff-fa	estático	

Contesta e razoa brevemente:

.....

- 1. Que acontece se voltas a realizar de novo a práctica unha vez existen as entradas arp correspondentes, é dicir, se en Kali xa existe a entrada arp de Windows 10 e viceversa?
- 2. Captura imaxes demostrando o que respostaches na cuestión 1.
- Executa na máquina Kali o comando: arp -d 10.10.10.11 Executa na máquina Windows o comando: arp -d * Captura imaxes coa execución e saída dos comandos anteriores. Que acontece se voltas a realizar de novo a práctica?
- 4. Captura imaxes demostrando o que respostaches na cuestión 3.

Ricardo Fe	eijoo Costa	
00	-	
BY SA		

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License