TEMA 1 PRÁCTICA 3: DISPONIBILIDAD

Nmap

Vamos a utilizar la aplicación zenmap, que es el nmap modo gráfico en este caso para Windows.

Vamos a escanear distintos equipos de la red.

Ejecutamos por ejemplo el comando nmap –A 192.168.2.148/24

-> Zenmap			×
Sc <u>a</u> n <u>T</u> ools <u>P</u> rofile <u>H</u> elp			
Target: 192.168.2.148/24	-	Scan	Cancel
Command: nmap -A 192.168.2.148/24			
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans			
OS • Host nmap -A 192.168.2.148/24		•	Details
Starting Nmap 5.51 (http://nmap.org) at 2011-10-19 09:06 Hora de verano romance			

Con este comando podemos ver información, acerca de su sistema operativo, puertos disponibles y aplicaciones ejecutándose.

Seguridad y alta disponibilidad



- Zenmap		x
Sc <u>a</u> n <u>T</u> ools <u>P</u> rofile <u>H</u> e	lp	
Target: 192.168.2.148/24	▼ Profile: ▼ Scan Car	ncel
Command: nmap -A 192.	.168.2.148/24	
Hosts Services	Nmap Output Ports / Hosts Topology Host Details Scans	_
OS • Host •	nmap -A 192.168.2.148/24	tails
	TRACEROUTE HOP RTT ADDRESS 1 9.82 mg 192.168.2.142	^
	Skipping SYN Stealth Scan against 192.168.2.148 because Windows does not support scanning your own machine (localhost) this way. Skipping OS Scan against 192.168.2.148 because it doesn't work against your own machine (localhost) Nmap scan report for 192.168.2.148 Host is up.	
	FORT STATE SERVICE VERSION	
	1/tcp unknown tcpmux	
	3/tcp unknown compressnet	
	4/tcp unknown unknown	
	6/tcp unknown unknown	
	//tcp unknown ecno 9/tcn unknown discard	
	3/top unknown davtime	
	17/tcp unknown gotd	
	19/tcp unknown chargen	
	20/tcp unknown ftp-data	
	21/tcp unknown ftp	
	22/tcp unknown ssh	
	23/tcp unknown telnet	
	24/tcp unknown priv-mail	
	25/tcp unknown smtp	
	26/tcp unknown rsftp	
	30/tcp unknown unknown	
	32/tcp unknown unknown	
	33/tcp unknown dep	
	37/tcp unknown time	
	42/tcp unknown nameserver	
Filter Hosts	43/tcp unknown whois	*

Ejecutamos el comando nmap –sO 192.168.2.148/24

6	2	ມາ∘ບ) ະ	nessus 4 - Microsoft Word				_ @ ×
C		Inicio Insertar	Diseño de página Referencias Correspondencia Revisar Vista				۲
	∞ Ze	nmap	the second second second second second		• ×	A A A	Buscar *
	Scan	<u>T</u> ools <u>P</u> rofile <u>H</u>	p			BbCc. AaBbCcDi Aa	Reemplazar
1	Targe	et: 192.168.2.148/24	▼ Profile:	▼ Scan	Cancel	ibtitulo Enfasis sutil 👻 estilos *	Seleccionar *
	Com	mand: nmap -sO[19	168.2.148/24			6	Edición
-						17 . 1 .	
- 9	н	osts Services	Nmap Output Ports / Hosts Topology Host Details Scans				
-	05 4	Host • •	nmap -sO 192.168.2.148/24	•	Details		
2	1 -1	192.168.2.24	Starting Nmap 5.51 (http://nmap.org) at 2011-10-19 09:11 Hora de verano romance				
	1	192.168.2.30					
1	1	192.168.2.42					
6	3	192.168.2.44					
- 10	1	192.168.2.48					
- 1	P	192.168.2.50					
11	1	192.168.2.54					
	1	192.168.2.60 ==					
1 - 1	1	192.168.2.66					
13.	1	192.168.2.72					
1	1	192.168.2.93					
- 14	1	192.168.2.96					
÷	1	192.168.2.102					
1	1	192.168.2.108					
- 16		192.168.2.120					
1	35	192.168.2.136					
-	35	192.168.2.142					
18		192.168.2.148					-
1	(5) 20	192.100.2.155					1
- 19		192.100.2.100 +					
Pá		Filter Hosts					U 🕀
	9				•	es 🔺 🎼 🗊	9:12 19/10/2011

Seguridad y alta disponibilidad



Ejecutamos el comando –sn 192.168.2.148/24

F	irefox	💴 🗊 Inicio		+						x
4	121	() water tuesd	ticom	/#m=blome&func=index			5-0	🖌 🛃 - Google	م	
M	👁 Zei	nmap	-	states of the same of the same is not if an observed of the same			×		Mar	cadores
	Scan	Tools Profile	He	p						
	Targe	t: 192.168.2.14	8/24	Profile:	-	Scan	Cancel	ir fotos 🕈 👘 🔆 🗸		
	Comr	mand: hmap -s	in 192	168.2.148/24				migos		
	Н	osts Service	s	Nmap Output Ports / Hosts Topology Host Details Scans				en Hotmail, Gmail o		
	os 🕯	Host •		nmap -sn 192.168.2.148/24	-		Details			-
	10 (3)	192.168.2.4 192.168.2.20		Host is up (0.0010s latency). <u>MAC Address:</u> 00:80:53:69:E6:59 (Tulip Computers Internat'l B.V)			^	scar amigos		
	-1	192.168.2.24		Hmap Scan report for 192.168.2.24 Host is up (0.067s latency).						
	-1	192,168,2,30		MAC Address: 00:27:10:9C:4F:3C (Intel Corporate)						
	-	192 168 2 42		Nmap scan report for 192.168.2.30				> estás conectado		
	n	102 168 2 44		<u>MAC Address:</u> 00:14:85:C3:D3:81 (Giga-Byte)			=	Conectar		
	3	102.169.2.49		Nmap scan report for 192.168.2.42						
		192.100.2.40	=	Host is up (0.065s latency). MAC Address: 00:21:63:87:2C:79 (Askey Computer)						
		192.108.2.50		Nmap scan report for 192.168.2.44				cias de amistad		
	1	192.168.2.54		Host is up (0.00s latency).				Hard Comment Hardware		
	1	192.168.2.60		Mac Address: 20:07:30:09:A9:42 (Asuster Computer)				García		
	-1	192.168.2.66		Host is up (0.0010s latency).				Añadir Innorar		
	-1	192.168.2.72		MAC Address: 00:14:85:C3:CC:D2 (Giga-Byte)				Anadir Ignoral		
	-1	192.168.2.93		Nmap scan report for 192.168.2.50				Posa Conzález Cózar		
	-	192168296		MAC Address: 00:01:E6:9C:F3:2D (Hewlett-Packard Company)				Añadie Issaes		
	-	102 168 2 102		Nmap scan report for 192.168.2.54				ignoral ginoral		
		192.100.2.102		Host is up (0.0010s latency).						
		192.108.2.108		Mac address: 00:0F:EA:51:15:00 (Giga-byte Technology Co.)						
	1	192.168.2.120		Host is up (0.0010s latency).						
	33	192.168.2.136		MAC Address: 00:0F:EA:51:1E:3B (Giga-Byte Technology Co.)						
	3	192.168.2.142		Hmap scan report for 192.168.2.66 Host is up (0.0030s latency).						
		192.168.2.148		MAC Address: 00:14:85:C3:D2:94 (Giga-Byte)						
	Ø5	192.168.2.155	-	Nmap scan report for 192.168.2.72						
		Filter Hosts		Host is up (0.0010s latency).			-			-
							_		FC 9-35	
	7								ES 🔺 👔 🗔 🐚 10/10/2	011

NESSUS 4.

Sirver para comprobar los puertos de un equipo determinado.

Procedemos a instalar Nessus, introducimos el código que nos ha llegado al correo y arrancamos el server.

🚾 Nessus Server Manager	x
NESSUS-	Nessus
Start the Nessus server when Win	dows boots
started by Windows every time the syste	m boots up.
Nessus Server Configuration	
Downloading the Nessus Plugin	s. Please wait
Activation code:	
F888-C62F-B92A-A5D2-414C	Register
The Nessus server is not running.	
Stop Nessus Server	Start Nessus Server

Introducimos un usuario y contraseña para cuando accedamos al modo cliente.

🖉 Nessus Server Manager 🛛 🗶
NESSUS -
Start the Nessus server when Windows boots
When enabled, the Nessus server will be automatically started by Windows every time the system boots up.
Your scanner is registered and can download new plugins from Tenable.
Add/Edit a user
Add/Edit a user
User name : Miguel
Password :
Password (again) :
Administrator
Cancel Save

Ejecutamos el navegador, y nos vamos al localhost, en la ventana de login ponemos los datos anteriores.



Para poder realizar una prueba, tenemos que configurar unos determinados parámetros, creamos una nueva política, la llamamos **Clase.** Marcamos la 2 y 3 opcion de los checkbox.

Jessus				miguel Help About Lo
icies	Reports Scans Policies	Users		
Edit Policy	Basic		Network Congestion	
	Name Clase		Reduce Parallel Connections on Congest	
General	Visibility Private		Use Kernel Congestion Detection (Linux Or	
	Description		Port Scanners	
Credentials			TCP Scan SNMP Scan	Ping Host 😨
Plugins			UDP Scan Netstat SSH Sc	n 🖸
Preferences	Scan			
	Save Knowledge Base		Port Scan Options	
	Sile chedis		Por Scarraige Deada	
	Silent Dependencies		Performance	
	Log Scan Details to Server		Max Unicks Per Hus	0
	Stop Host Scan on Disconnect		Max Hosts Per Scan	100
	Avoid Sequential Scars		Network Hoberve Timeout (seconds)	9
			Max simulaneous TCP sessions Per Host	Unimiteo
	Designate Hosts by their DNS Name		Max Simultaneous TCP Sessions Per Scan	unlimited

Una vez tengamos creado la política, vamos a realizar un escaneado de diferentes equipos, haciendo referencia las políticas que hemos configurado.



Comienza el escaneo.

Firefox 💌 🙍 Nessus	+		2 2		
+ localhost https://localhost:8834				☆ - C 🚼 - Google	۶ 🏫
M Gmail: correo electróni 🎢 Cursos de Inforact	tiva 🧯 A.J León, Valdepeñas () 🕻 INTE	:CO - Seguridad, I 🕥 Miguel Ángel García F	🎿 Bienvenidos a la portada 🔀 Seci	urityFocus	Marcadores
💩 Nessus		Scan was successfully launched	Close		miguel Help About Log out
Scans Reports	Scans Policies Users				
		Add	🖉 Edit 🍈 Browse	📀 Launch 🕕 Pause	💿 Stop 😑 Delete
Name	▼ Owner	Status		Start Time	
Ejemplomiguel	miguel		0 IPs / 3 IPs	Oct 14, 2011 13:34	

Una vez terminado, nos vamos al resultado, y comprobamos el número de puertos que ha podido escanear.

Firefo	🗴 🚬 🧟 Nessus	+						
()	localhost https://localhost:8834				合 - (🖻 🚼 = Google	۹ (م	
M Gma	il: correo electróni 饰 Cursos de Inforac	tiva 🤰 A.J León, Valdepeñas (🕽 🌔 INTECO - Segurida	d, I 💿 Miguel Ángel Gar	cía F 🎿 Bienvenidos a la	a portada 🖄 SecurityFocus		Marcadores	
o 🔊	essus						miguel Help About Log out	
Repo	eports Reports Scans Policies Users							
	Report Info	Ejemplomiguel					3 results	
	Name: Ejemplomiguel	Host	Total	High	Medium	Low	Open Port	
1	Last Update: Oct 14, 2011 13:34	192.168.2.4	48	2	6	30	10	
	Status: Completed	192.168.2.142	29	0	0	24	5	
		192.168.2.220	27	0	0	23	4	
	Show Filters							
	Reset Filters							
	Active Filters							

De cada una de las IP seleccionadas, nos mostrará los puertos que se estén usando, nombre, tipo de protocolo y otros términos.

correo erectroni 'III Cursos de	inforactiva 🤹 AJ Leon, Valdep	enas () (INTECO - Segu	indad, i 🕦 Miguei Angel (arcia F Bienve	enidos a la portada 🖉	securityFocus		
sus								miguel Help About
ts Re	ports Scans Polic	ies Users		_			_	
Report Info	Ejemplomiguel	192.168.2.142						13 n
Hosts	Port	▲ Protocol	SVC Name	Total	High	Medium	Low	Open Port
192.168.2.4	0	tcp	general	6	0	0	6	0
192.168.2.142	0	udp	general	1	0	0	1	0
192.168.2.220	135	tcp	epmap	2	0	0	1	1
	137	udp	netbios-ns	2	0	0	2	0
	139	tcp	smb	2	0	0	1	1
	445	tcp	cifs	6	0	0	5	1
	912	tcp	vmware_auth	3	0	0	2	1
	1025	tcp	dce-rpc	1	0	0	1	0
	1026	tcp	dce-rpc	1	0	0	1	0
	1028	tcp	dce-rpc	1	0	0	1	0
	1029	tcp	dce-rpc	1	0	0	1	0
Show Filters	1031	tcp	dce-rpc	1	0	0	1	0
	3306	top	mysql	2	0	0	1	1
Active Filters								

Seguridad y alta disponibilidad

Firefox	🛀 👱 Nessus	+							D <mark>_ X</mark>	
(Docalhost https://localhost:8834						🚖 - C 🚼-	Google	۹ م	
M Gmail: c	correo electróni 🌇 Cursos de Inforact	iiva 🧯 A.J León, Valdepeñas (.) (INTECO - Segurida	d, I 🕔 Miguel Ángel G	arcía F 🎿 Bienven	idos a la portada 😸 !	SecurityFocus		Marcador	
on 💩	Nessus' Miguel Help About Log out									
Report	sports Reports Scans Policies Users									
									10ite	
	Report Into	Ejemplomiguel	192.168.2.220						12 results	
	Hosts	Port 🔺	Protocol	SVC Name	Total	High	Medium	Low	Open Port	
	192.168.2.4	0	tcp	general	6	0	0	6	0	
·	192.168.2.142	0	udp	general	1	0	0	1	0	
	192.168.2.220	135	tcp	epmap	2	0	0	1	1	
		137	udp	netbios-ns	2	0	0	2	0	
4		139	tcp	smb	2	0	0	1	1	
		445	tcp	cifs	6	0	0	5	1	
		912	tcp	vmware_auth	3	0	0	2	1	
		1025	tcp	dce-rpc	1	0	0	1	0	
		1026	tcp	dce-rpc	1	0	0	1	0	
	Download Report	1027	tcp	dce-rpc	1	0	0	1	0	
		1031	tcp	dce-rpc	1	0	0	1	0	
	Show Filters	1032	tcp	dce-rpc	1	0	0	1	0	
	Reset Filters									
	Adua Ciliana									
	Adive Fillers									

Firefo	🗴 🚺 🙋 Nessus	+								
<)>	📃 🧟 localhost https://loc	alhost:8834					☆ - C 🚼 -	Google	۹ (
🗹 Gmai	il: correo electróni 饰 Curs	os de Inforactiva 🧯 A.J León, Valdepeñas	() (INTECO - Seg	uridad, I 🕔 Miguel Ángel	García F 🎿 Bienv	enidos a la portada 😂	SecurityFocus		🖪 Marcado	
💩 ne	essus								miguel Help About Log o	
Repo	ports Reports Scans Policies Users									
	Report Info	Ejemplomiguel	192.168.2.4						13 results	
	Hosts	Port	Protocol	SVC Name	Total	High	Medium	Low	Open Port	
Incline: Incline: <th< td=""><td>0</td><td>0</td><td>2</td><td>0</td></th<>	0	0	2	0						
ł.	192.168.2.142	0	tcp	general	5	0	0	5	0	
	192.168.2.220	0	udp	general	1	0	0	1	0	
		53	udp	dns	2	0	0	1	1	
¢		80	tcp	www	3	0	0	2	1	
		161	udp	snmp	8	2	0	5	1	
		443	tcp	www	13	0	5	7	1	
		520	udp	rip	3	0	1	1	1	
		1024	udp	unknown	1	0	0	0	1	
		1723	tcp	pptp	2	0	0	1	1	
	Show Filtere	1900	udp	ssdp?	1	0	0	0	1	
	GIIOW FIILGIS	2555	tcp	WWW	4	0	0	3	1	
	Reset Filters	8080	tcp	WWW	3	0	0	2	1	
	Active Filters									

Baseline Security Analyzer

Es un analizador de vulnerabilidades del sistema de un equipo determinado.

Una vez lo tengamos instalado. Tenemos diferentes opciones, escanear un ordenador, un grupo de ordenadores etc.

Microsoft Baseline Security Analy	zer 21	x
👁 🖲 🌡 Microsoft Baseline	Security Analyzer Microso	oft
Lasks Scan a compater Scan duble compater Were watching by some About Microsoft Dasethe Socially Andreas	Check computers for common security misconfigurations. The Microsoft Baseline Security Analyser can check computers running Microsoft Windows Server 2008 R2, Windows 7, Windows 2, Windows 2, Server 2003, Windows Server 2008, Windows 2000. Scanning computers for security updates utilizes Windows Server 1004 E Services. You must have admissignator privileges for each computer you want to scan. Image: Service 2008 R2: Windows 2000. Scanning computers for security updates utilizes Windows Server 1004 E Services. You must have admissignator privileges for each computer you want to scan. Image: Service 2008 R2: Windows 2000. Scanning computers for security updates utilizes Windows Server 1004 E Services. You must have admissignator privileges for each computer you want to scan. Image: Service 2008 R2: Windows 2000. Scanning computers for security updates using a domain name or a range of P addresses. Image: Service 2008 R2: Windows 2000. Scanning computers for security updates using a domain name or a range of P addresses. Image: Service 2008 R2: Windows 2000. Scanning scale 2008 R2: Windows 2000. Scanning Service 2008 R2: Windows 2000. Scanning 2008 R2: Windows 2000. Scanning 2008 R2: Windows 2008 R2: Wi	
Microsoft Baseline Security Analyzer Help	© 2003-2009 Microsoft Corporation. All rights reserved.	
Mcrosoft Security Web site	A new version of MESA is available: Click here to go to the download page	8

Si hacemos un nuevo escaneo, por ejemplo nuestra IP, 192.168.2.148/24, procederá a realizar una búsqueda de vulnerabilidades.



Una vez finalizado, nos hace un informe con las siguientes vulnerabilidades.

Administra	tive Vulnerabi	ities	
Score	Issue	Result	
٠	Automatic Lodates	Updates are not automatically dominated or installed on this computer.	
٠	Password Expiration	Same user accounts (3 of 4) have non-expiring passwords. What was scanned Result details How to correct this	
0	Incomplete	No incomplete software update installations were found.	
0	Windows Firewall	Windows Frewall is enabled and has exceptions configured. Windows Frewall is enabled on all network connections. Windows scanned Result details How to correct this	
3	Local Account Password Test	Some user accounts (2 of 4) have blank or simple passwords, or could not be analyzed.	
3	File System	All hard drives (2) are using the NTFS file system. What was scanned Result details	
3	Autologon	Autologon is not configured on this computer. What was scanned	
3	Guest Account	The Guest account is disabled on this computer.	
3	Restrict Anonymous	Computer is properly restricting anonymous access. What was scanned	
3	Administrators	No more than 2 Administrators were found on this computer. What was sconned Result details	
Additional	System Inform	ation	
Score	Issue	Result	1
0	Auditing	Neither Logon Success nor Logon Failure auditing are enabled. Enable auditing and turn on auditing for specific events such as logon and logoff. Be sure to monitor your event log to watch for unauthorized access. What was scanned How to correct this	

Podemos hacer un escáner mucho más amplio con varios ordenadores de la red, el proceso es lento y requiere tiempo. Algunos antivirus, pueden denegarnos su acceso.