Análisis de malware

Análisis dinámico básico

Gustavo Romero López - gustavo@ugr.es

Updated: 3 de marzo de 2025

Departamento de Ingeniería de Computadores, Automática y Robótica

Parte 1: Análisis básico

Capítulo 1: Técnicas estáticas básicas

Capítulo 2: Análisis de malware en máquinas virtuales

Capítulo 3: Análisis dinámico básico

Parte 2: Análisis estático avanzado

Capítulo 4: Curso intensivo de ensamblador x86

Capítulo 5: IDA Pro

Capítulo 6: Reconocimiento de construcciones de C en ensamblador

Capítulo 7: Análisis de programas maliciosos para Windows

Parte 3: Análisis dinámico avanzado

Parte 4: Funcionalidad del malware

Parte 5: Anti-ingeniería inversa

Parte 6: Temas especiales

Lo que ya sabéis hacer...

Análisis estático:

- ◎ Identificar ficheros: MD5, SHA1, SHA256,...
- Antivirus: www.virustotal.com
- Detección de empaquetado: PEid y UPX
- O Cadenas: strings
- Sormato PE:
 - PEview
 - Depends
 - objdump
 - Resource Hacker
- O Desensamblado: IDA Pro

Lo que os falta por aprender...

Análisis Dinámico:

- O Entorno seguro
 - sandbox: Cuckoo, Joe Sandbox, Microsoft Sandbox
 - o máquina virtual: Gnome Boxes, VMware, VirtualBox
- O Process Monitor
- Process Explorer
- Regshot
- O ApateDNS + INetSim
- O Wireshark
- O Depuración:
 - OllyDbg/Immunity Debugger: modo usuario
 - Windbg: modos usuario y núcleo

Motivación

- Stamen de la ejecución del malware.
- Il análisis estático puede acabar en un callejón sin salida...
 - o ofuscado/empaquetado/cifrado
 - conocimientos insuficientes/exceso de dificultad
- Observar el comportamiento del malware puede ser más eficaz y sencillo.
- O Podemos hacerlo de dos formas:
 - En vivo: monitorizar mientras se ejecuta.
 - A posteriori: comparar el sistema antes y después.
- La mejor forma de averiguar que hace el malware.
- ◎ Usar sólo después de un análisis estático básico.

Entorno aislado ("SandBox")

- Definición: mecanismo de seguridad para ejecutar programas en un entorno seguro.
- ◎ Mejor cuanto más se parezca a un sistema real
- Automatizan el proceso de rastreo de actividad y elaboran informes sobre el comportamiento del malware.
- Semplos:
 - Cuckoo:

https://cuckoosandbox.org/https://cuckoo.cert.ee

- Joe Sandbox: https://www.joesecurity.org
- Microsoft Sandbox
- Inconvenientes:
 - pueden ser detectados
 - vulnerabilidades en el anfitrión
 - o sin opciones desde el intérprete de órdenes
 - sin interacción de red
 - diferencias con un sistema real: entorno, registro,...

Entorno aislado ("SandBox")

o Permite observar el la actividad del malware sobre....

- procesos/hebras
- sistema de ficheros
- mutex
- registro
- red
- antivirus
- Inconvenientes:
 - o no utiliza opciones de línea de órdenes
 - no registra todos los eventos por falta de tiempo
 - puede ser detectado por el malware
 - comportamiento anómalo por diferencias con un sistema real
 - no lanzamiento de DLLs
 - falta de conclusiones precisas

Ejecutables (*.exe):

- o doble click desde un interfaz gráfico
- ø ejecución desde el intérprete de órdenes:
 - c:\virus.exe

Bibliotecas de enlace dinámico (*.dll):

- ⊚ c:\>rundll32.exe rip.dll, Install
- Convertir DLL en ejecutable cambiando su cabecera
- ◎ Instalar DLL como un servicio y ejecutarlo

c:\>rundll32.exe iprx32.dll, InstallService ServiceName

c:\>net start ServiceName

Process Monitor

- Monitoriza: registro, sistema de ficheros, red y procesos.
- ◎ Genera tanta información que es vital filtrarla.
- © Ejercicio: ¿Que hace el solitario de Windows?
 - 1. Arranca Process Monitor
 - 2. Detener la captura de eventos
 - 3. Crea el filtro:

"Process Name is not sol.exe then Exclude"

- 4. Reactivar la captura de eventos
- 5. Lanza el solitario

Process Monito	or Filter			
Filters were in effect	the last time yo	u exited Process Monit	ior:	
Process Name	is not	sol.exe	w then Exe	:lude 🔽
Reset			Add	emove
Column	Relation	Value	Action	^
Process	is	Procexp.exe	Exclude	B
Process	is	Autoruns.exe	Exclude	
Process	is	System	Exclude	
Process	is not	sol.exe	Exclude	
🗹 😵 Operation	begins with	IRP_MJ_	Exclude	
Coeration	begins with	FASTIO	Exclude	~
			Cancel	Apply



Process Monitor

Process Monitor - Sysinternals: www.sysinternals.com

_ 7 🗙

File Edit Event Filter Tools Options Help

😂 🖬 🛠 🕸 🖾 🗢 📥 🏵 🗉 🛤 📕 🎎 🔩 🜌 🖪

Time of Day	Process Name	PID	Operation	Path	Result	Detail	^
1:23:20,3108884	🖬 sol.exe	2180	27 Process Start		SUCCESS	Parent PID: 1628, Command In	
1:23:20,3108912	sol.exe	2180	Seate Thread Create		SUCCESS	Thread ID: 2152	
1:23:20,3183103	🖥 sol.exe	2180	🗟 QueryNameInformationFile	C:\WINDOWS\system32\sol.exe	SUCCESS	Name: \WINDOWS\system32\	
1:23:20,3184368	🖥 sol.exe	2180	ar Load Image	C:\WINDOWS\system32\sol.exe	SUCCESS	Image Base: 0x1000000, Image	
1:23:20,3185268	🖥 sol.exe	2180	ar Load Image	C:\WINDOWS\system32\ntdl.dll	SUCCESS	Image Base: 0x7c900000, Imag	
1:23:20,3185363	🖥 sol.exe	2180	QueryNameInformationFile	C:\WINDOWS\system32\sol.exe	SUCCESS	Name: \WINDOWS\system32\	
1:23:20,3186380	🖬 sol.exe	2180	CreateFile	C:\WINDOWS\Prefetch\SOL.EXE-1C0C14EB.pf	NAME NOT FOUND	Desired Access: Generic Read,	
1:23:20,3187807	👔 sol.exe	2180	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Exec	NAME NOT FOUND) Desired Access: Read	
1:23:20,3188033	📄 sol.exe	2180	式 RegOpen Key	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Read	
1:23:20,3188282	📄 sol.exe	2180	RegQuery∀alue	HKLM\System\CurrentControlSet\Control\Session Manager\CWDIllegalIn	NAME NOT FOUND) Length: 1.024	
1:23:20,3196635	📄 sol.exe	2180	🕰 RegCloseKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS		
1:23:20,3197856	📄 sol.exe	2180	🛃 CreateFile	C:\WINDOWS\system32	SUCCESS	Desired Access: Execute/Trave	
1:23:20,3199119	📄 sol.exe	2180	💐 Load Image	C:\WINDOWS\system32\kernel32.dl	SUCCESS	Image Base: 0x7c800000, Imag	
1:23:20,3200786	📄 sol.exe	2180	🕵 RegOpenKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	Desired Access: Read	
1:23:20,3200993	📄 sol.exe	2180	🕵 RegQueryValue	HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat	SUCCESS	Type: REG_DWORD, Length: 4	
1:23:20,3201217	👔 sol.exe	2180	🕵 RegCloseKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS		
1:23:20,3201314	👔 sol.exe	2180	🕵 RegOpen Key	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Exec	NAME NOT FOUND) Desired Access: Read	
1:23:20,3211346	👔 sol.exe	2180	🚑 Load Image	C:\WINDOWS\system32\msvcrt.dl	SUCCESS	Image Base: 0x77c10000, Imag	
1:23:20,3213520	📄 sol.exe	2180	Sead Image	C:\WINDOWS\system32\advapi32.dll	SUCCESS	Image Base: 0x77dd0000, Imag	
1:23:20,3219764	📄 sol.exe	2180	Sea Load Image	C:\WINDOWS\system32\rpcrt4.dll	SUCCESS	Image Base: 0x77e70000, Imag	
1:23:20,3221174	📄 sol.exe	2180	Service Coad Image	C:\WINDOWS\system32\secur32.dll	SUCCESS	Image Base: 0x77fe0000, Image	
1:23:20,3222851	📄 sol.exe	2180	Ser Load Image	C:\WINDOWS\system32\gdi32.dl	SUCCESS	Image Base: 0x77f10000, Image	
1:23.20,3228388	📄 sol.exe	2180	🚑 Load Image	C:\WINDOWS\system32\user32.dl	SUCCESS	Image Base: 0x7e410000, Imag	
1:23:20,3230039	📄 sol.exe	2180	FileSystemControl	C:\WINDOWS\system32	SUCCESS	Control: FSCTL_IS_VOLUME	
1:23:20,3230838	📄 sol.exe	2180	🛃 QueryOpen	C:\WINDOWS\system32\cards.dl	SUCCESS	CreationTime: 14/04/2008 14:0	
1:23:20,3231628	💽 sol.exe	2180	🛃 CreateFile	C:\WINDOWS\system32\cards.dl	SUCCESS	Desired Access: Execute/Trave	
1:23:20,3235087	💽 sol.exe	2180	🛃 CreateFileMapping	C:\WINDOWS\system32\cards.dl	SUCCESS	SyncType: SyncTypeCreateSec	
1:23:20,3235372	💽 sol.exe	2180	🛃 CreateFileMapping	C:\WINDOWS\system32\cards.dl	SUCCESS	SyncType: SyncTypeOther	
1:23:20,3235531	💽 sol.exe	2180	a RegOpenKey	HKLM\System\CurrentControlSet\Control\SafeBoot\Option	NAME NOT FOUND	/ Desired Access: Query Value, S	
1:23:20,3235724	💽 sol.exe	2180	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	SUCCESS	Desired Access: Query Value	
1:23:20,3236120	💽 sol.exe	2180	≝KegQuenyValue	HKLM\SDFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers\T.	SUCCESS	Type: REG_DWORD, Length: 4	
1:23:20,3236338	💽 sol.exe	2180	a RegCloseKey	HKLM\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers	SUCCESS		
1:23:20,3236486	💽 sol.exe	2180	at RegOpenKey	HKCU\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	NAME NOT FOUND) Desired Access: Query Value	
1:23.20,3237258	💽 sol.exe	2180	K CloseFile	C:\WINDOWS\system32\cards.dl	SUCCESS		
1:23:20,3240786	💽 sol.exe	2180	ar Load Image	C:\WINDOWS\system32\cards.dl	SUCCESS	Image Base: 0x6fc10000, Image	
1:23:20,3241962	💽 sol.exe	2180	ar Load Image	C:\WINDOWS\system32\shell32.dll	SUCCESS	Image Base: 0x7c9c0000, Imag	
1:23:20,3247815	sol.exe	2180	Toad Image	C:\WINDUWS\system32\shiwapi.dl	SULUESS	Image Base: Ux/7f60000, Image.	
1:23:20,3249259	Sol.exe	2180	RegUpenKey	HKLM\Software\Microsoft\Windows\CurrentVersion\SideBySide\AssembL	NAME NOT FOUND	/ Desired Access: Enumerate Sub	
1:23:20,3249997	isol.exe	2180	NueryUpen	L:\WINDUWS\system32\sol.exe.Local	NAME NOT FOUND)	
1:23:20,3250726	isol.exe	2180	NueryUpen	L:\WINDUWS\WinSx5\x86_Microsoft Windows.Common-Controls_6595	SULLESS	Ureation Line: 11/04/2020 15:2	
1:23:20,3251338	Sol.exe	2180	CreateFile	L:\WINDUWS\Win5x5\x86_Microsoft Windows.Common-Controls_6595	SULLESS	Desired Access: Execute/Trave	• ٧
Showing 667 of 39.3	39 events (1.%)	Dr.	ocorrettonitor d by virtual mem	OFX			

Process Explorer

- Gestor de tareas que permite analizar en detalle el uso que los procesos hacen del sistema.
- Identificación mediante colores:
 - servicios: rosa
 - procesos: azul
 - procesos nuevos: verde (temporal)
 - procesos finalizados: rojo (temporal)
- Opciones más interesantes:
 - Verificar: compara la imagen de un proceso en memoria con su original en disco (binarios firmados).
 - Comparar cadenas: diferencias sustanciales indicarían un reemplazo de proceso.
 - Utilizar Dependency Walker: localizar uso de DLLs.
 - Analizar documentos maliciosos: uso de recursos.

Process Explorer

◎ Ejercicio: ¿Cuántas hebras lanza Firefox?

						firefox.e	ke:1224	Proper	ties					
🛛 📵 Página de inicio de Mozila Fire 🗄	×\+				1	Image	Perfor	nance	Pe	rforman	ce Graph	Disk	and Netw	ork.
	_				16	Threads	TC	P/IP	Sec	urity	Enviro	nment	Strin	ngs
Firefox Término de búsqueda	o direcció	in		(Count: 4	в							
						T. +	CPU	CSwitch	h	Start A	Address			^
						204	< 0.01		3	ucrtbas	e.dll+0x3d5	ь0		
💐 Process Explorer - Sysinterna		w.sysinternal	s.com [UGR-B	31EF6CCDB53\gustavo] (Adn		216				xul di+0)x62c09c			
File Options View Process Find I	Users H	lelp			11	236	< 0.01		10	ucrtbas	e.dl+0x3d5	60		
Property	CDU	Drivers Dores	Astrophics Cas	PID Description	11	240				ucribas	e.dl+0x300	DU		
Surtem Idle Process	99.00	Private bytes	Working Set	0 Descapson	11	404				ucribas	e.dli+0x3d5 e.dll40x3d5	60 60		
System rate i rocess	35.00	01	212 K	4		560				kemel3	2 dl+0x107	29		
lotem pts	20.01	0K	0 K	n/a Hardware Interrupts and DP		568				ucrtbas	e.dll+0x3d5	ь0		
	1 3.01	196 K	440 K	364 Windows NT Session Mana		992				ucrtbas	e.dll+0x3d5	ь0		
CSISS.exe		1.736 K	4.208 K	588 Client Server Runtime Proce		1028				firefox.e	xe+0x5eed			
🗏 🚺 winkaan exe		6.312 K	4.676 K	612 Windows NT Logon Applica		1096	< 0.01		12	ucrtbas	e.dll+0x3d5	ь0		
services exe		1.664 K	3.452 K	656 Services and Controller ann		1124				ucrtbas	e.dll+0x3d5	ь0		
VBoxService.exe		3.260 K	4.236 K	836 VirtualBox Guest Additions S		1308				ucrtbas	e.dll+0x3d5	60		-
sychost.exe		3.036 K	4.940 K	884 Generic Host Process for W		1324				ucitbas	8.08+0x305	DU		
svchost.exe		1.916 K	4.432 K	964 Generic Host Process for W		1,000				sucurre under	0.02C03C	ь0		
🖃 🧮 svchost.exe		23.976 K	35.860 K	1060 Generic Host Process for W		1476				ole32 d	8.0ii+0x303	00		
wscntfy.exe		548 K	2.404 K	1584 Windows Security Center No		1600				sul di+f	b62cll9c			
sychost.exe		1.280 K	3.560 K	1104 Generic Host Process for W		1624	< 0.01		11	ucrtbas	e.dll+0x3d5	ьо		
svchost.exe		1.456 K	3.868 K	1172 Generic Host Process for W		1704				ucrtbas	e.dll+0x3d5	ь0		
spoolsv.exe		3.100 K	4.812 K	1456 Spooler SubSystem App		1772				ucrtbas	e.dll+0x3d5	ь0		
svchost.exe		1.252 K	3.744 K	1976 Generic Host Process for W		1868				ucrtbas	e.dll+0x3d5	ь0		
alg.exe		1.116 K	3.552 K	1416 Application Layer Gateway S		1884	< 0.01		12	ucrtbas	e.dll+0x3d5	60		
isass.exe		3.844 K	6.412 K	668 LSA Shell (Export Version)		1920				xul di+0	bd52c09c	~~		
🗉 😼 esplorer. exe		25.008 K	10.116 K	1628 Windows Explorer		1940				Kernela	2.01+0x107	29		~
🧐 VBoxTray.exe		2.060 K	4.184 K	1748 VirtualBox Guest Additions T		2002				Lonnas	e (1141 K 1/0)			_
otimon.exe		892 K	3.272 K	1764 CTF Loader		Thread ID:		1028			Sta	dk 🛛	Module	ŧ
C procexp.exe	1.00	46.936 K	51.672 K	1944 Sysinternals Process Explore		Start Time:		2:03:59	13/04	1/2020				
🕘 hrefox.exe		135.132 K	138.420 K	1224 Firefox		State:		Wait:Use	rReau	est	Base Priori	ty:	8	
						Kernel Time		0.00.00	640		Dynamic P	iority:	10	
						Lines Times		0.00.00	000		0 / · · a · · · ·			
						user time:		0:00:02.	093					
						Context Sv	acches:	9.565						
					11									
PU Usage: 1.00% Commit Charge: 2	3.69%				I.				Perm	issions	К		Suspen	ď
					L				_					_
Descargas	Marcad	iores Hist	conai Com	piementos Sync							0	ĸ	Can	cel
							_	_	_	_	_			
🗧 start 👘 🤰 Process Explore		😻 Página i	de inicio de M									2	° 🔿	2:0

Comparando instantáneas del registro: Regshot

- Permite tomar y comparar instantáneas del registro.
- O Uso:
 - 1º foto
 - ejecutar malware
 - 2^ª foto
 - comparar

💼 Regshot 1.8.3-beta1V5	_ 🗆 🔀
Compare logs save as: Plain TXT HTML document	1st shot 2nd shot
Scan dir1[;dir2;dir3;;dir nn]: C:\WINDOWS	Compare Clear
Output path: C:\DOCUME~1\gustavo\LC	Quit About
Add comment into the log:	English 🔽

Comparando instantáneas del registro: Regshot

◎ Ejercicio: ¿Afecta el solitario al registro de Windows?

Compare logs pundades conce O Texto D Documento HTML 2da Foto	
Residea Escener drijdrijdr mi Conserver	
Resta de salde: C(100CME-r)[gadred]C Sore	÷ .
	* ÷
Fie Edit Format Vew Help	الما كارك
Regshot 1.8.3-betalv5 Comentarios: Perha y how a:2020/A/13 00:12:22 , 2020/4/13 00:12:32 Computador:US-BIEF6CCB53 , UGR-BIEF6CCD63 USuarioigustavo , gustavo ,	<u>^</u>
Valores modificados:6	
LINUXOFTWARE (MICrosoft VCryptigraphy) HMC/Seed: DI E3 40 27 75 55 73 bi 1 90 07 F5 CE 08 83 47 79 77 F1 85 55 MICVS-1-1-21 5727746-199396796-198426398-1003 Software MICrosoft Window VCurrent version NED plorent VserAssis MICVS-1-21 5727740-199396796-198426398-1003 Software MICrosoft Window VCurrent version NED plorent VserAssis MICVS-1-21 5727740-199396796-198426398-1003 Software MICrosoft Window VCUrrent version NED plorent VserAssis MICVS-1-21 5727740-199396796-198426398-1003 Software MICrosoft Window VCUrrent version NED plorent VserAssis MICVS-1-21 5727740-199396796-198426398-1003 Software MICrosoft Window VCUrrent version NED plorent VserAssis MICVS-1-21 5727740-199396796-198426398-1003 Software MICrosoft Window VCUrrent version NED plorent VserAssis MICVS-1-21 5727740-199396796-198426398-1003 Software MICrosoft Window VCUrrent version NED plorent VserAssis MICVS-1-21 5727740-199396778-198426398-1003 Software MICrosoft Window VCUrrent version NED plorent VserAssis MICVS-1-21 5727740-199396778-198426398-1003 Software MICrosoft Window VcUrrent version NED plorent VserAssis MICVS-1-21 5727740-199396778-198426398-1003 Software MICrosoft Window VcUrrent version NED plorent VserAssis MICVS-1-21 5727740-199396778-198426398-1003 Software MICrosoft Window VcUrrent version NED plorent VserAssis MICVS-1-21 5727740-199396778-198426398-1003 Software MICrosoft Window VcUrrent version NED plorent VserAssis MICVS-1-21 5727740-199396778-198426398-1003 Software MICrosoft Window VcUrrent version NED plorent VserAssis MICVS-1-21 5727740-199396778-198426398-1003 Software MICrosoft Window VcUrrent version NED plorent VserAssis MICVS-1-21 5727740-199396778-198426398-1003 Software MICrosoft Window VcUrrent version NED plorent VserAssis MICVS-1-21 5727740-199396778-198426398-1003 Software MICrosoft Window VcUrrent version NED plorent VserAssis MICVS-1-21 5727740-199396778-198426398-1003 Software MICrosoft Window VcUrrent Version NED plorent VserAssis MICVS-1-21 5727740-199396778-198426398-1003 Software MICrosoft	4C 3D DB CO 98 A6 BB 48 F0 10 t 75048700-EF: t 75048700-EF: t 75048700-EF: t 75048700-EF: t 75048700-EF: t 75048700-EF: t 75048700-EF: t 75048700-EF: t 75048700-EF:
Total de cambios:6	
Cick here to begin	2 213

- I malware suele comunicarse con servidores de control.
- O Crear una red falsa permite obtener pistas:
 - DNSs
 - IPs
 - paquetes que utilizar como identificadores
- ApateDNS: servidor DNS bajo nuestro control.
- ◎ Netcat: la navaja suiza del TCP/IP.
 - stdin -> red
 - red -> stdout

Trasteando en la red

◎ Ejercicio: Haga que la página web de la UGR le salude.

🛃 ApateDh	15				Archivo Editar Ver H	listorial Marcadores 📑 🗖 🔀
Capture Wine	dow DNS Hex View				Children (Income and	
Time	Domain Requested		DNS Retur	^	Inc. (///////.ogi.es/	~ (
02:03:56	www.ugr.es		FOUND		()	c » =
02:03:56	www.ugr.es		FOUND			
02:03:56	www.ugr.es		FOUND			
02:03:56	www.ugr.es		FOUND		hola :)	
02:03:56	www.ugr.es		FOUND			
02:03:57	www.ugr.es		FOUND			
02:03:57	www.ugr.es		FOUND			
02:03:57	www.ugr.es		FOUND	_		
02:03:57	www.ugr.es		FOUND			
02:03:57	www.ugr.es		FOUND			
02:03:57	www.ugr.es		FOUND			
02:03:57	www.ugr.es		FOUND	_		
02:03:57	www.ugr.es		FOUND			
DNS Re # of NM	ply IP (Default: Current Gatway/DNS): 10.0.2.2 DOMAIN's: 0		Start Se	Tevre		
🗬 gusta	vo@localhost:~					
🛃 logi	n as: gustavo			^		
3 count	avoid 0 2 2's password:					
Leet lo	gin: Tue Ang 14 14:06:45 2020					
Laugt au	oficesheet -15 sude ng -1 -n 80					
CET / H	TTD/1 1					
0E1 / 1						
HOSC: 0	www.ugz.es					
oser-rd	enc: mozilia/5.0 (Windows NT 5.1; r	(V152.0) GECR6/20100101 F	merox/52.0			
accept:	text/ntmi,appiication/xhtml+xml,ap	prication/xml;q=0.9,*/*;c	1=0.8			
accept-	Language: es-rs,es;q=0.8,en-US;q=0.	5,en;q=0.3				
Accept-	Encoding: gzip, deflate					
Connect	ion: keep-alive					
Upgrade	-Insecure-Requests: 1					
^C				~		.4
🐴 start	📢 IDA - C:\Do 💊 2 Firefox 🔹 🤇	PEview - C: 📴 apateDNS	Comman	d P	🛃 gustavo@lo 🛛 🔽 Ap	akeDNS 🛛 😨 😤 🏹 2:05

Capturando tráfico de red con Wireshark

- ◎ Intercepta y almacena tráfico de red.
- Facilita la visualización y el análisis tanto de paquetes individuales como de intercambios secuenciados.

Cie Edit V												
Ele Ede M	ap										- 0	×
the cur v	iew Go Captur	e Analyze Statistics	Telephony 1	Wireless Tools He	lp							
4 ■ <i>6</i> ⊗	0 📕 🖻 🗙 🖏	30027	4 🗮 🔳 6	a a a 🗉								
arely a risel	wfiter s(tri-i>									-	* Extres	ion i 4
No. Teo			Destination	Bestocol	Lacoth Jafe							=
48.6	25749 175	16 8 122	288 121 1 13	TCP	54 [TC	P Mindow Unda	atel FTCP AC	(ed unceen s	egment1 88 .	10554 L	ICK1 Sec	
5 8.6	376967 280	.121.1.131	172,16,0,122	ТСР	1454 FTC	P Previous s	eggent not c	actured1 [TC	P Sourious I	Retransmi	ssion] 1	
			200.121.1.13			P Dup ACK 2#	11 FTCP ACKe	d unseen see	ment1 80 - :	10554 FAC	<1 Seg=1	
						P Spurious R		1] 18554 → 8	B [ACK] Seq	5681 Ack	-1 Win=6	5
												- =
												s.,
												_
									0 [ACK] Seq			s.,
												-
									0 [ACK] Seq			5
14 0.1			200.121.1.13				5] 80 → 1055	\$ [ACK] Seq=	1 Ack=11201			
15 0.2	207145 200	.121.1.131	172.16.0.122	TCP	1454 105	54 + 80 [ACK]] Seq=11201 (Ack=1 Win=65	535 Len=1409	B [TCP set	gment of	
16 0.2	172 1756 172	.16.0.122	200.121.1.13	1 TCP	54 88	→ 10554 [ACK]] Seq=1 Ack=:	12601 Win=63	000 Len=0			
12.0.1	(32621 289	.121.1.131	172.16.0.122	t TCP	1454 105	54 + 80 [ACK]] Seq=12601 (Ack=1 Win=65	535 Len=1408	ETCP set	gment of	-
17 0.0												
18 0.2	32629 172	.16.0.122	200.121.1.13	11 TCP	54 88	→ 10554 [ACK]] Seq=1 Ack=:	14001 Win=63	000 Len=0			
18 8.2	232629 172 58365 200	.16.0.122	200.121.1.13 172.16.0.122	1 TCP 1 TCP	54 80 1454 105	→ 10554 [ACK 54 → 80 [ACK]] Seq=1 Ack=:] Seq=14001 (14001 Win=63 Ack=1 Win=65	000 Len=0 535 Len=140	ETCP se	gment of	-
17 6.2 18 8.2 19 8.2 28 8.2	232629 171 158365 200 158373 172	.16.0.122 .121.1.131 .16.0.122	200.121.1.13 172.16.0.122 200.121.1.13	11 TCP 1 TCP 11 TCP	54 80 1454 105 54 80	→ 10554 [ACK 54 → 80 [ACK → 10554 [ACK] Seq=1 Ack=:] Seq=14001 /] Seq=1 Ack=:	14001 Win=63 Ack=1 Win=65 15401 Win=63	000 Len=0 535 Len=1400 000 Len=0	e [TCP se	gment of	-
17 0.2 18 0.2 19 0.2 28 0.2 2 Frame 15:	232629 17: 258365 288 58373 172 1454 bytes on	1.16.0.122 1.121.1.131 .16.0.122 wire (11632 bits)	200.121.1.13 172.16.0.122 200.121.1.13	11 TCP 1 TCP 11 TCP captured (11632	54 88 1454 185 54 88 bits)	+ 10554 [ACK 54 + 80 [ACK + 10554 [ACK] Seq=1 Ack=] Seq=14001 (] Seq=1 Ack=:	14001 Win=63 Ack=1 Win=65 15401 Win=63	300 Len=8 535 Len=148 300 Len=8	9 [TCP se	gment of	-
17 8.2 18 8.2 19 8.2 28 8.2 > Frame 15: > Ethernet	232629 173 258365 200 158373 172 1454 bytes on II. Src: Vmar	.16.0.122 .121.1.131 .16.0.122 wire (11632 bits) e c0:00:01 (00:50	200.121.1.13 172.16.0.122 200.121.1.13), 1454 bytes :56:c0:00:01)	11 TCP 1 TCP 11 TCP captured (11632 . Dst: Vmware 42	54 80 1454 105 54 80 bits) :12:13 (00	→ 10554 [ACK] 54 → 80 [ACK] → 10554 [ACK] :0c:29:42:12:] Seq=1 Ack=] Seq=14001 ;] Seq=1 Ack=:	14001 Win=63 Ack=1 Win=65 15401 Win=63	000 Len=0 535 Len=1400 000 Len=0	a [TCP se	gment of	-
<pre>17 0 18 0.2 19 0.2 20 0.2 > Frame 15: > Ethernet > Internet</pre>	232629 173 258365 286 258373 172 1454 bytes on II, Src: Vmwar Protocol Versi	.16.8.122 .121.1.131 .16.8.122 wire (11632 bits) e_C0:00:01 (00:50 on 4, Src: 200.12	200.121.1.13 172.16.0.122 200.121.1.13), 1454 bytes :56:c0:00:01) 1.1.131, Dst:	11 TCP 11 TCP 11 TCP captured (11632 , Dst: Vmare_42 172.16.0.122	54 80 1454 105 54 80 bits) :12:13 (00	+ 10554 [ACK] 54 + 80 [ACK] + 10554 [ACK] :0c:29:42:12:] Seq=1 Ack=:] Seq=14001] Seq=1 Ack=: :13)	14001 Win=63 Ack=1 Win=65 15401 Win=63	300 Len=8 535 Len=1486 300 Len=8	a [TCP se	gment of	<u> </u>
17 6 18 6.2 19 6.2 20 7.2 20 7.2	232629 17; 258365 284 258373 172 1454 bytes on II, Src: Vmwar Protocol Versi ion Control Pr	1.16.0.122 1.121.1.131 1.16.0.122 wire (11632 bits) e_c0:00:01 (00:50 on 4, Src: 200.12; atocol, Src Port:	200.121.1.13 172.16.0.122 200.121.1.13), 1454 bytes :56:c0:00:01) 1.1.131, Dst: 10554, Dst P	11 TCP 1 TCP 11 TCP captured (11632 , Dst: Vmware_42 172.16.0.122 ort: 80, Seq: 11	54 80 1454 105 54 80 bits) :12:13 (00 201, Ack: :	+ 10554 [ACK] 54 + 80 [ACK] + 10554 [ACK] :0c:29:42:12: 1, Len: 1400] Seq=1 Ack=:] Seq=14001 -] Seq=1 Ack=: :13)	14001 Win=63 Ack=1 Win=65 15401 Win=63	300 Len=0 535 Len=1480 300 Len=0	a [TCP se	gment of	-
17 6 18 6.2 19 6.2 20 7.2 20 7.2	232629 17/ 258365 284 258373 172 1454 bytes on II, Src: Vmwar Protocol Versi ion Control Pr Port: 18554	1.16.0.122 1.21.1.131 1.16.0.122 wire (11632 bits) e_c0:00:01 (00:50 on 4, Src: 200.12: otocol, Src Port:	200.121.1.13 172.16.0.122 200.121.1.13), 1454 bytes :56:c0:00:01) 1.1.131, Dst: 10554, Dst P	11 TCP TCP 11 TCP 12 TCP 13 TCP 14 TCP 172.16.0.122 172.16.0.122 172.16.0.5eq: 11	54 80 1454 105 54 80 bits) :12:13 (00 201, Ack: :	+ 10554 [ACK] 54 + 80 [ACK] + 10554 [ACK] :0c:29:42:12: 1, Len: 1400] Seq=1 Ack=:] Seq=14001 .] Seq=1 Ack=: :13)	14001 Win=63 Ack=1 Win=65 15401 Win=63	000 Len=0 535 Len=1400 000 Len=0	9 [TCP se	gment of	-
<pre>> Frame 15: > Ethernet > Internet > Transmiss Source Destin</pre>	232629 17; 258365 200 258373 172 1454 bytes on II, Src: Vmwar Protocol Versi; ion Control Pr Port: 10554 ation Port: 80	1.16.0.122 1.121.1.131 1.16.0.122 wire (11632 bits) e_c0:00:01 (00:50 on 4, Src: 200.12) otocol, Src Port:	200.121.1.13 172.16.0.122 200.121.1.13), 1454 bytes :56:c0:00:01) 1.1.131, Dst: 10554, Dst P	11 TCP 1 TCP 11 TCP 12 TCP 131 TCP 132 top 132 top 132 top 132 top 132 top 132 top 132 top 133	54 80 1454 105 54 80 bits) :12:13 (00 201, Ack: :	+ 10554 [ACK] 54 + 80 [ACK] + 10554 [ACK] :0c:29:42:12: 1, Len: 1400] Seq=1 Ack=:] Seq=14001 .] Seq=1 Ack=: :13)	14001 Win=63 Ack=1 Win=65 15401 Win=63	000 Len=0 535 Len=1400 000 Len=0	a [TCP se	gment of	-
17 8.2 18 8.2 19 8.2 20 8.2 > Frame 15: > Ethernet > Internet > Transmiss Source Destin [Strea	232629 17; 258365 200 258373 17; 1454 bytes on II, Src: Vmwar Protocol Versi ion Control Pr Port: 10554 ation Port: 80 m index: 0]	1.16.0.122 1.21.1.131 1.16.0.122 wire (11632 bits; e_c0:00:01 (00:50 on 4, Src: 200.12; otocol, Src Port;	200.121.1.13 172.16.0.122 200.121.1.13), 1454 bytes :56:c0:00:01) 1.1.131, Dst: 10554, Dst P	11 TCP 11 TCP 11 TCP 11 TCP 11 TCP 11 TCP 111 TCP 1120 1110 110	54 80 1454 105 54 80 bits) :12:13 (00 201, Ack: :	 → 10554 [ACK] 54 → 80 [ACK] → 10554 [ACK] → 10554 [ACK] → 00554 [ACK] → 00554] Seq=1 Ack=:] Seq=14001 .] Seq=1 Ack=: :13)	14001 Win=63 Ack=1 Win=65 15401 Win=63	000 Len=0 535 Len=1400 000 Len=0	a [TCP se	gment of	-
17 0.2 18 0.2 19 0.2 20 0.2 > Frame 15: > Ethernet > Internet * Transmiss Source Destin [Strea [TCP S	232629 17: 588365 200 588373 17: 1454 bytes on II, Src: Vmwar Protocol Versi ion Control Pr Port: 10554 ation Port: 80 m index: 0] egment Len: 144	1.16.0.122 1.12.1.131 1.16.0.122 wire (11632 bits; e_c0:00:01 (00:50 on 4, Src: 200.12; otocol, Src Port; 30]	200.121.1.13 172.16.0.122 200.121.1.13), 1454 bytes :56:c0:00:01) 1.1.131, Dst: 10554, Dst P	11 TCP 11 TCP 11 TCP captured (11632 , Dst: Wmare_42 172.16.0.122 ort: 80, Seq: 11	54 80 1454 105 54 80 bits) :12:13 (00 201, Ack: :	 → 10554 [ACK] 54 → 80 [ACK] → 10554 [ACK] → 10554] Seq=1 Ack=:] Seq=14001 (] Seq=1 Ack=: :13)	14001 Win=63 Ack=1 Win=65 15401 Win=63	000 Len=0 535 Len=1404 000 Len=0	a [TCP se	gment of	-
17 0.2 18 0.2 19 0.2 20 0.2 > Frame 15: > Ethernet > Internet > Transmiss Source Destin [Strea [TCP S Sequen	132629 17: 158365 204 158373 17: 1454 bytes on 14,54 bytes on 11, Src: Vmwar Protocol Versi ion ion Control Pr Port: Port: 10554 ation Port: 80 # index: 0] egment Len: 14:	1.16.0.122 1.12.1.131 1.16.0.122 wire (11632 bits) e_cd:00:01 (00:50 on 4, Src: 200.12: atocol, Src Port: 10] 10] 11] (relative se	200.121.1.13 172.16.0.122 200.121.1.13), 1454 bytes :56:c0:00:001 1.1.131, Dst: 10554, Dst P	11 TCP 1 TCP 13 TCP 14 TCP 15 Captured (11632 172.16.0.122 172.16.0.122 172.16.0.122 175.10 11 11 11 11 11 11 11 11 11	54 80 1454 105 54 80 bits) :12:13 (00 201, Ack: :	 → 10554 [ACK] 54 → 80 [ACK] → 10554 [ACK] → 10554 [ACK] :0c:29:42:12: :0c:29:42:12: Len: 1400] Seq=1 Ack=:] Seq=14001 (] Seq=1 Ack=: :13)	14001 Win=63 Ack=1 Win=65 15401 Win=63	000 Len=0 535 Len=1401 300 Len=0	a [TCP se	gment of	-
17 0.2 18 0.2 19 0.2 20 0.2 > Frame 15: > Ethernet > Internet > Transmiss Source Destin [Strea [TCP S Sequen [Next	232629 17: 258365 264 158373 17: 1454 bytes on 11, Src: Vewar Protocol Versi 100, Control Pr Port: 1854 # index: 0] egment Len: 144 ce number: 1124 sequence number: 1124	1.16.0.122 0.121.1.131 1.16.0.122 wire (11632 bits) e_cd:00:01 (00:50 on 4, Src: 200.12: atocol, Src Port: 30] 31 (relative so 1 12601 (relative so	200.121.1.13 172.16.0.122 200.121.1.13 0), 1454 bytes 56:c0:00:001 1.1.131, Dst: 10554, Dst P	11 TCP 1 TCP 11 TCP 11 TCP 11 CP 172.16.0.122 172.16.0.122 ort: 80, Seq: 11 number)]	54 80 1454 105 54 80 bits) :12:13 (00 201, Ack: :	+ 10554 [ACK 54 + 80 [ACK + 10554 [ACK] :0c:29:42:12: 1, Len: 1400] Seq=1 Ack=:] Seq=14001 (] Seq=1 Ack=: :13)	14001 Win=63 Ack=1 Win=65 15401 Win=63	000 Len=0 535 Len=1400 000 Len=0	e [TCP se	gment of	-
17 8.2 18 8.2 19 8.2 20 8.2 > Frame 15: > Ethernet > Internet * Transmiss Source Destin [Strea [TCP S Sequen [Next Acknow	232629 17. 258365 204 258375 17. 1454 bytes on 11, Src: Vinwar Protocol Versil Protocol Versil 10554 ation Port: 10554 ation Port: 80 # index: 0] sequence number: 112 sequence number: 112 sequence number: 112	1.16.0.122 1.121.1.131 1.16.0.122 wire (11632 bits) e_c6:00:01 (00:50 on 4, Src: 200.12 otocol, Src Port: 1001 11 (relative sc 12001 (relative 11 (relative)	200.121.1.13 172.16.0.122 200.121.1.13), 1454 bytes 56::0:00:00:11 1.1.131, Dst: 10554, Dst P	<pre>11 TCP 1 TCP 11 TCP 12 TCP 13 TCP captured (11632 , Dst: Vmsare_42 172.16.0.122 ort: 80, Seq: 11 r) number)]</pre>	54 80 1454 105 54 80 bits) :12:13 (00 201, Ack: :	+ 10554 [ACK] 54 + 80 [ACK] + 10554 [ACK] :0c:29:42:12: 1, Len: 1400] Seq=1 Ack=:] Seq=14081 (] Seq=1 Ack=: :13)	14001 Win=63 Ack=1 Win=65 15401 Win=63	000 Len=0 535 Len=1400 200 Len=0) [TCP se	gment of	-
17 0.2 18 0.2 19 0.2 20 0.2	232629 17. 258365 204 258365 204 258373 17. 1454 bytes on 11, Src: Vinwar Protocol Vorisi Protocol Vorisi Port: 10554 ation Port: 10554 ation Port: 88 # index: 0] gement Len: 144 ce number: 1122 sequence number Ledgment number	<pre>.16.6.122 b.121.1.131 b.121.1.131 b.16.8.122 wire (11632 bits; e_c6:00:01 (00:50 on 4, Src: 200.12; dtocol, Src Port: dtocol, Src Port: 10[1] 11 (relative so :: 12601 (relative :: 12601 (relative so :: 12601 (relati</pre>	200.121.1.13 172.16.0.122 200.121.1.13), 1454 bytes 56:c0:00:01 1.1.131, Dst: 10554, Dst P squence number sck number) 5)	11 TCP 11 TCP 11 TCP 12 captured (11632 , Dst: Vmaare_42 172.16.0.122 ort: 80, Seq: 11 number)]	54 88 1454 105 54 88 bits) :12:13 (00 201, Ack: :	+ 10554 [ACK 54 + 80 [ACK + 10554 [ACK :0c:29:42:12: 1, Len: 1400] Seq=1 Ack=:] Seq=14601 /] Seq=1 Ack=: :13)	14001 Win=63 Ack=1 Win=65 I5401 Win=63	000 Len=0 535 Len=1400 200 Len=0) (TCP se	gment of	-
17 0.2 18 0.2 19 0.2 20 0.2	232629 17; 258355 2040 258373 17; 258373 17; 25737 17; 2	<pre>:16.6.122 .121.1.131 :16.0.122 wire (11632 bits; </pre>	200.121.1.3 172.16.0.122 200.121.1.3), 1454 bytes :55:c0:00:01) 1.1.131, Dst: 10554, Dst P cquence number tive sequence ack number) 5)	<pre>11 TCP 11 TCP 12 TCP 13 TCP 14 TCP 14 TCP 14 TCP 15 Unsare 42 172.16.0.12 0rt: 80, Seq: 11 r) number)]</pre>	54 80 1454 105 54 80 bits) :12:13 (G0 201, Ack: :	+ 10554 [ACK 54 + 80 [ACK + 10554 [ACK] :0c:29:42:12: 1, Len: 1400] Seq=1 Ack=] Seq=14601 (] Seq=1 Ack= :13)	14001 Win=63 Ack=1 Win=65 I5401 Win=63	000 Len=0 535 Len=1404 000 Len=0) (TCP se	gment of	
10 0.2 10 0.2 10 0.2 20 0.2	232629 17: 258365 2040 258373 17: 1454 bytes on II, Src: Vewar 17: Protocol Versi ion Control Pr Port: 1854 ation Port: 88 ation Port: 88 index: 0) egment Len: 141 sequence number: Ledgment number: 120 20 38 de 56 a7 20 38 de 56 a7	<pre>ii6.0.122 ii6.0.122 ii6.0.122 wire (1602) bits' e.ec:000101 (00:50 on 4, Src: 200.12; atocol, Src Port: 30] 31 (relative ss i: 12601 (relative ingth: 20 bytes (5 5c: 30 68 2c 22, 53 55 4f: 78 42 56 35 5 </pre>	200.121.1.3 172.16.0.122 200.121.1.3), 1454 bytes :56:c0:00:01) 1.1.131, Dst: 10554, Dst P equence number tive sequence ack number) 5) me bf 50 10 & 45 52 52	<pre>11 TCP 11 TCP 12 TCP 13 TCP 14 TCP 14 TCP 17 16-122 172.16-0.122 0rt: 80, Seq: 11 17 10 17 10 17 10 17 10 17 10 17 10 17 10 17 10 17 10 17 10 17 10 17 10 17 10 17 10 17 1 1 1 1</pre>	54 88 1454 105 54 88 bits) :12:13 (00 281, Ack: :	+ 10554 [ACK 54 + 80 [ACK + 10554 [ACK :0c:29:42:12: 1, Len: 1400] Seq=1 Ack=:] Seq=14001 (] Seq=1 Ack=: :13)	14001 Win=63 Ack=1 Win=65 I5401 Win=63	000 Len=0 535 Len=140 000 Len=0	9 [TCP se	gment of	-
18 0.2 19 0.2	232629 17: 258365 204 258373 17: 1454 bytes on 11, Src: Vmwar Protocol Versi 10, Control Pr Port: 10554 # index: 0] ggment Len: 144 sequence number ledgment number 20 20 20 20 20 20 20 20 20 20	16.6.122 122.1.131 1.16.6.122 wire (11632 bits; e.cd:00:01 (00:50 on 4, 5nc: 200.12; atocol, 5nc Part; 20] 11 (relative s; ': 12601 (relative ': 12601 (relative ': 12601 (relative ': 1260 ato bytes (') 5: 30 08 e2 e2 c4 4f 78 42 56 35	200.121.1.3 172.16.0.122 200.121.1.13), 1454 bytes 55.c6:00:031 1.1.131, Det 10554, Dat P equence number squence number ack number) 3) me bf 50 10 64 45 52 52 1 34 78 35	11 TCP 11 TCP 11 TCP 12 TCP 13 TCP 14 TCP 14 TCP 172.16.0.122 17	54 88 1454 105 54 88 bits) :12:13 (00 281, Ack: :	+ 10554 [ACK 54 → 80 [ACK + 10554 [ACK :0c:29:42:12: 1, Len: 1400] Seq=1 Ack=:] Seq=14601] Seq=1 Ack=: 13)	14001 Wine53	000 Len=0 535 Len=1400 000 Len=0	a (TCP se	gment of	-
10 0.2 10 0.2	232629 17 258365 284 258373 177 1454 bytes on 11, Src: Vinwar Protocol Versi Protocol Versi 100 ation Port: 88 index: 01 gement Len: 144 cc number: 112 sequence number: 112 b56 06 00 2 66 53 37 34 64 30 37 35	16.6.122 121.1.131 16.6.122 wire (1662 bits_c, c, c	200.121.1.3 172.16.0.122 200.121.1.3 200.121.1.3), 1454 bytes 156.cdr.00.01 1.1.131, Det 10554, Dst P 10554, Dst P 105554, Dst P 105554, Dst P 1055	<pre>11 TCP 11 TCP 12 captured (11632 172.16.0.122 0rt: 80, Seq: 11 172.16.0.122 0rt: 80, Seq: 11 173.16.0.122 0rt: 80, Seq: 11 173.16.0.122 0rt: 80, Seq: 11 173.174 174.17</pre>	54 80 1454 105 54 80 bits) :12:13 (00 281, Ack: : 8 8 8	+ 10554 [ACK 54 + 80 [ACK + 10554 [ACK :0c:29:42:12: 1, Len: 1400] Seq:1 Acks: Seq:14001 n Seq:1 Acks: 13)	14001 Win≂63 Kk=1 Win≂63 I5401 Win≈63	000 (en:0 555 (en:1400 000 (en:0	a (TCP se	gment of	-
10 0.2 10 0.2 10 0.2 20 0.2 > Frame 15 > Ethernet > Internet > Transmiss Source Destin [Strea 1CP 5 Sequen [Next Acknow 0101. - 0028 00 72 5 Sequen 0030 ff ff 0040 71 55 0056 61 22 0056 61 22 0056 61 22 0056 61 23 0056 61 23 0057 71 55 0057 75 0057 75 005	122220 17; 1258365 200 1258375 177 1454 bytes on 177 1454 bytes on 177 1454 bytes on 177 1454 bytes on 177 160 control Protocol Versi 100 160 control Protr 1854 ation Port: 1854 ation Port: 18 sequence number 112 126 sequence number 120 127 sequence 139 34 128 sequence 139 34 129 sequence 139 34 121 sequence 139 34 121 sequence 139 34 121 sequence 3	16.6.122 122.1.131 116.6.122 vire (1632 bits; e.c3c0610 (00:56 on 4, Snc: 200.12; atocol, Snc Part; P0] 81 (relative s; 12.1.2 bytes (1); 13.2 creative s; 14.1 (relative s; 15.2 creative s; 15.2 creative s; 15.2 creative s; 15.2 creative s; 16.2 creative s; 17.4 dr 42 bytes (1); 42.4 dr 42 creative s; 43.4 dr 42 creative s; 44.4 dr 42 creative s; 45.2 creative s; 47.7 dr 42 creative s;	200.121.1.3 172.16.0.22 200.121.1.13), 1454 bytes 55:c0:00:01 10554, Dat P equence number live sequence ack number) 5) ne bf 50 10 64 55 25 13 37 78 35 5:44 97 4c 78 35 5:44 97 4c 78 35 5:44 97 4c 78 35 5:44 97 4c	<pre>11 TCP 11 TCP 12 TCP 13 TCP 14 TCP 15 Det: Unsare_42 172.16.0.122 cort: 80, Seq: 11 cort: 80, Seq</pre>	54 80 1454 105 54 80 bits) :12:13 (00 201, Ack: : 8 5 5 6 0 0	 10554 [ACK, 4 80 [ACK, 4 10554 [ACK, 10554 [ACK, 10529:42:12: 10529:42:12: 11, Len: 1400] Seq:1 Ackel Seq:1405 Seq:1405 Seq:1 Ackel 13)	14001 Wine53	000 Len:0 535 Len:1400 000 Len:0	a (TCP see	gment of	-
10 0.2 10 0.2 10 0.2 20 0.2	122620 17: 1268865 200 158875 200 1858865 200 1858865 200 1858865 200 1858865 200 113.5 200 Protocol Verol Pr Port: 10554 ation Port: 80 100 gewent Len: 144 100 100 gewent Len: 140 100 20 at 06 50 at 100 20 at 06 35 56 at 100	16.6.122 121.1.131 1121.1.131 116.6.122 wire (11632 bits; ec:080:61 (08:56 on 4, 5rc: 208.12) 90] 91] 11 12.1.131 13.1 14.1 15.1 16.6.2 90] 91] 11 12.1 13.1 14.1 14.1 15.2 15.2 16.2 17.4 17.4 17.4 17.4 17.4 17.4 18.2 18.3 19.4 10.4 10.4 11.1 11.1 11.1 11.1 12.2 12.3 12.4 12.4 12.5 12.5 12.5 12.5 12.5 12.5	200.121.1.13 172.16.0.122 200.121.1.13 17.2.16.122 200.121.1.13 1.1.131, Dst: 10554, Dst P squence number tive sequence ack number) 5) b mb f 50 10 64 45 52 52 51 34 78 35 54 44 74 56 32 44 56 48 64 30 56 46 43 56 46 46 30	<pre>11 TCP 11 T</pre>	54 80 1454 105 54 80 bits) :12:13 (00 201, Ack: : 8 5 5 20 0 A	 10554 [ACK. 10554 [ACK. 10554 [ACK. 10554 [ACK. 105:20:42:12: 1, Len: 1400] Seq:1 Acket Seq:1401] Seq:1 Acket 13)	14001 Wine58	000 Len:0	9 (TCP se	gment of	-
10 0.2 10 0.2 10 0.2 20 0.2	233629 17; 258365 204 25837 17; 1545 197 1545 197 1545 197 1545 197 1545 197 1545 197 1545 197 1545 197 1547 197 1547 197 1547 197 1547 197 1547 197 1548 197 155 193 154 193 155 133 154 193 155 133 154 193 154 193 155 133 154 193 155 133 154 193 155 133 155 134 154 193 155 134 154 193	<pre>hi6.6.122 hi6.6.122 hi721.hi8.6.123 wire (13622 bits; a.dc:00:010 (00:55 a.dc:00:010 a.dc:00:010 a.dc:00:010 a.dc:00:010 a.dc:00:010 a.dc:00:010 a.dc:00:010 a.dc:00 a.dc:00:010 a.dc:00 a.dc:00:010 a</pre>	200.121.1.13 172.16.0.122 200.121.1.13 172.16.0.122 200.121.1.13 1.1.131, Dxtr 10554, Dxt P squence number 10554, Dxt P squence number 105554, Dxt P squence number 1055554, Dxt P squence number 1055555, Dxt P squence number 1055555, Dxt P squence number 10555555, Dxt P squence number 1055555, Dxt P squence number 105555555, Dxt P squence number 1055555, Dxt P squence number 105555555, Dxt P squence number 10555555555555555555555555555555555555	<pre>11 TCP 11 T</pre>	54 80 1454 105 54 80 bits) :12:13 (00 281, Ack: : 8 5 5 1 2 0 0 A 2 2	+ 10554 [ACK + 10554 [ACK + 00554 [ACK] = 000000000000000000000000000000000000] Seq:1 Ackets Seq:1401] Seq:1 Acket] Seq:1 Acket :13)	14001 Wine58	000 Len:0 355 Len:100 000 Len:0	9 (TCP se	gment of	

Wireshark: diálogo Firefox <-> HTTPD

Archivo Editar Ver Historial Marcadores Herramiențas Test Page for the HTTP Server on × +	Ayuda				- X
() 192. 168. 122. 1	C Q, Buscar	☆自	÷	俞	≡
	Fedora Webserver Test Page				^

This page is used to test the proper operation of the Fedora HTTP server after it has been installed. If you can read this page, it means that the web server installed at this site is working properly, but has not yet been configured.

If you are a member of the general public:

The fact that you are seeing this page indicates that the website you just visited is either experiencing problems or undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.

For example, if you experienced problems while visiting www.example.com, you should send e-mail to "webmaster@example.com".

Fedora is a distribution of Linux, a popular computer operating system. It is commonly used by hosting companies because it is free, and includes free web server software. Many times, they do not set up their web server correctly, and it displays this "test page" instead of the expected website.

Accordingly, please keep these facts in mind:

- Neither the Fedora Project or Red Hat has any affiliation with any website or content hosted from this server (unless otherwise explicitly stated).
- Neither the Fedora Project or Red Hat has "hacked" this webserver, this test page is an included component of the

Click here to begin Fedora webserver software.

If you are the website administrator:

You may now add content to the webroot directory. Note that until you do so, people visiting your website will see this page, and not your content.

For systems using <u>Apache Webserver</u>. You may now add content to the directory /vaz/ww/hcml/. Note that until you do so, people visiting your website will see this page, and not your content. To prevent this page from ever being used, follow the instructions in the file /ecc/htspd/conf./welcome.conf.

For systems using Nginx: You should now put your content in a location of your choice and edit the root configuration directive in the nginx configuration file /etc/nginx/nginx.conf.



Wireshark: diálogo Firefox <-> HTTPD

4	Loca	l Area Connecti	ion [Wireshark 1.10).14 (v1.10.14-0-g8	25f971 from	n master-1.10)]	- 7
File	Edi	⊻lew <u>G</u> o <u>C</u> ap	pture <u>A</u> nalyze <u>S</u> tatistic	s Telephony <u>T</u> ools 1	nternals <u>H</u> elp		
0	۲	🛋 🗰 🙇	🖹 🚨 🗶 🎜 I 🤅	🕻 🏟 🏟 🖥 🛓] Q, Q, Q, 🗹 👪 🖄 🥵 % 🖼	
Filte	r:				Express	ssion Clear Apply Save	
No.		Time 9	Source	Destination	Protocol	Length Info	
		0.00000000	10.0.2.15	192.168.122.1		62 cognex-insight > http [SYN] Seq=0 win=64240	Len=0 MSS=1460 SA
	2	0.00052600:	192.168.122.1	10.0.2.15	TCP	60 http > cognex-insight [SYN, ACK] Seq=0 Ack=1	Win=65535 Len=0
	3	0.00053700:	10.0.2.15	192.168.122.1	TCP	54 cognex-insight > http [ACK] Seq=1 Ack=1 Win=	64240 Len=0
	4	0.00072500:	10.0.2.15	192.168.122.1	TCP	54 [TCP Dup ACK 3#1] cognex-insight > http [ACK] Seq=1 Ack=1 Win
	5	0.00090900:	10.0.2.15	192.168.122.1	HTTP	385 GET / HTTP/1.1	
	6	0.00104400:	192.168.122.1	10.0.2.15	TCP	60 http > cognex-insight [ACK] Seq=1 Ack=332 Wi	n=65535 Len=0
	7	0.00154200:	192.168.122.1	10.0.2.15	TCP	1474 [TCP segment of a reassembled PDU]	
	8	0.00154800:	192.168.122.1	10.0.2.15	TCP	1474 [TCP segment of a reassembled PDU]	
	9	0.00155700:	10.0.2.15	192.168.122.1	TCP	54 cognex-insight > http [ACK] Seq=332 Ack=2841	Win=65535 Len=0
	10	0.00168200:	192.168.122.1	10.0.2.15	TCP	1474 [TCP segment of a reassembled PDU]	
	11	0.00168600:	192.168.122.1	10.0.2.15	TCP	1474 [TCP segment of a reassembled PDU]	
	12	0.00169000:	192.168.122.1	10.0.2.15	HTTP	247 HTTP/1.1 403 Forbidden (text/html)	
	13	0.00169600:	10.0.2.15	192.168.122.1	TCP	54 cognex-insight > http [ACK] Seg=332 Ack=5874	Win=65535 Len=0

 Frame 1: 62 bytes on wire (496 Ethernet II, src: CadmusCo_87: Internet Protocol Version 4, St 	bits), 62 bytes captured (496 bits) on interface 0 98:34 (08:00:27:87:98:34), Dst: Realteku_12:35:02 (52:54:00: -c: 10.0.2.15 (10.0.2.15), Dst: 192.168.122.1 (192.168.122.1	L2:35:02)
Transmission Control Protocol,	Src Port: cognex-insight (1069), Dst Port: http (80), Seq: (), Len: 0
0000 52 54 00 12 35 02 08 00 2 0010 00 30 08 43 40 00 80 06 at 0020 7a 01 04 2d 00 50 a4 7e b4	7 87 98 34 08 00 45 00 RT.5'4E. 0 cc 0a 00 02 0f c0 a8 .0.C0	
0030 fa f0 e3 a6 00 00 02 04 0	5 b4 01 01 04 02	- 4 - 4 -
Start Vigustavo\LOCALS~1\Ten	pt Packets: 13 * Displayed: 13 (100.0%) * Dropped: 0 (0.0%) C *Local Area Connecti	Prohie: Default

Wireshark: diálogo Firefox <-> HTTPD

Follow TCP Stream

🛃 start

Test Page for the HT...

*Local Area Connecti...



Follow TCP Stream

😰 🖞 🔇 😰 4:54

- Simulador de los servicios más comunes de Internet.
- Servicios emulados: DNS, FTP, HTTP, HTTPS, IRC, POP, POP₃, SMTP,...
- Simular el comportamiento de los servidores reales para intentar mantener al malware funcionando.
- Registra todas conexiones y peticiones entrantes.

- 1. Process Monitor
- 2. Process Explorer
- 3. Regshot
- 4. ApateDNS + nc/FakeNet/INetSim
- 5. Wireshark

... o todo a la vez desde una caja de arena...

Prácticas

- 1. Labo3-01.exe:
 - 1.1 ¿Qué funciones importa? ¿Qué cadenas contiene?
 - 1.2 ¿Deja señales en el anfitrión (host-based indicators)?
 - 1.3 ¿Hay firmas de red? ¿Cuáles?
- 2. Labo3-02.dll:
 - 2.1 ¿Puede conseguir que se instale?
 - 2.2 ¿Cómo hacer que se ejecute?
 - 2.3 ¿Cómo encontrar el proceso bajo el que se ejecuta?
 - 2.4 ¿Qué filtros usaría en procmon para extraer información?
 - 2.5 ¿Qué rastros deja en el anfitrión?
 - 2.6 ¿Hay firmas de red?