REQUERIMIENTOS DE LABORATORIO

- Windows 10, 90 días de prueba -> <u>https://www.microsoft.com/en-us/evalcenter/evaluate-windows-10-enterprise</u>
- 2) Ubuntu or Kali Linux, recomendamos Kali pero cualquier distro de linux debería funcionar-> Ubuntu http://old-releases.ubuntu.com/releases/18.04.2/

Kali Linux -> https://www.kali.org/downloads/

- 3) Virtual Box -> <u>https://www.virtualbox.org/wiki/Downloads</u>
- 4) Inetsim software -> <u>https://www.inetsim.org/downloads.html.</u>
- 5) Inetsim instrucciones -> <u>https://www.inetsim.org/packages.html</u>.
- 6) Microsoft Visual studio con C# y C++.

Nota: Recomendamos instalar solo la partición C: en tu Windows 10 virtual machine.

GUIA PARA INSTALAR INETSIM

Esta guía es solo un apoyo, tienes todo este material en video en la sección Configurando el Laboratorio.

Instalando Inetsim en Linux virtual machine.- Escribe estas instrucciones una por una en la consola de Linux:

- 1) echo "deb http://www.inetsim.org/debian/ binary/" >
 /etc/apt/sources.list.d/inetsim.list
- 2) echo "deb-src http://www.inetsim.org/debian/ source/" >>
 /etc/apt/sources.list.d/inetsim.list
- 3) wget -O https://www.inetsim.org/inetsim-archive-signingkey.asc | apt-key add -
- 4) apt update
- 5) apt install inetsim
- 6) sudo gedit /etc/network/interfaces
- 7) Ahora que está abierto el editor escribe esto al final del mismo:

auto eth0 -> esto es el nombre de tu interface

iface eth0 inet static

address 10.0.5.4 -> esto es la dirección ip de tu Linux virtual machine

netmask 255.255.255.0

Ahora debería lucir así

This file describes the network interfaces available on your system # and how to activate them. For more information, see interfaces(5).

The loopback network interface
auto lo
iface lo inet loopback

auto eth0 iface eth0 inet static address 10.0.5.4 netmask 255.255.255.0 Nota: Usa el comando "ifconfig" en la consola de Linux para averiguar el nombre de tu interface y tu dirección ip (si no sabes como, mira el video "Configurando Inetsim en Kali Linux virtual machine")

- 8) Ahora escribe esto en la consola de Linux: sudo gedit /etc/inetsim/inetsim.conf
- 9) Busca esta línea en el editor que se ha abierto: #service_bind_address 10.10.10.1
- 10) Debajo de esta línea añade el mismo comando sin el # y tu dirección ip como se muestra en la figura de abajo:

11) Ahora busca esta línea: #dns_default_ip 10.10.10.1. Repetimos el procedimiento de arriba, debe quedar así:

Eso es todo, escribe "inetsim" en la consola de Linux y la simulación empezará a ejecutarse. A continuación se debe configurar Virtual Box:

Configurando Virtual Box.- Debes configurar la opción de Red de Linux virtual machine y de Windows virtual machine. Las opciones pueden variar un poco de acuerdo a la versión pero debes poner: "Adaptador solo anfitrión" o "Host only adapter"

🕄 Oracl	e VM VirtualBox Administrad	lor	uda									- 0 ×
100	Herramientas	Se Kali-Linux-2019.1-vbox-amd64 - Configuración ? X										
000			General	Red								
6	Kali-Linux-2019.1-vbox-an	1	Sistema	Adaptador	1 Adap	tador 2 Adaptador 3 Ada	aptador 4					Tomada 09/01/2020 1:55 (hace 23 horas
64	windows7pruebas (Instantá		Pantalla	🖂 Habilita	ar adaptador	de red						
	(U) Apagada	9	Almacenamiento	Co	nectado a:	Adaptador sólo-anfitrión •		conty: A priv	ate networ	κs	nar	ed with the host
64	windows7pruebas2 (Instant		Audio		Nombre:	VirtualBox Host-Only Ethernet A	lapter				•	
			Red	Avanzadas	wanzadas							
4	(b) Apagada		Puertos serie									
64	WindowsXp1	Ø	USB									
WP	V Apagaua		Carpetas compartidas									
E4 XP	WindowsXp2 (b) Apagada		Interfaz de usuario									
	pentesterlab1 (b) Apagada											
2	Ubuntu (Instantánea 1)								Aceptar	Can	celar	i
windows10Enterprise3 (Instantánea 9)												
windows10Enterprise4_clonadode3												
												Tomar Restaurar

Desactivar características de seguridad de Windows 10 virtual machine

Es importante desactivarlas porque de lo contrario podrían detectar nuestras muestras de malware e incluso eliminarlas.

1) Busca seguridad de Windows

0						
Recycle	All Apps Documents Settings F	Photos	More 🔻	Feedback		
	Best match					
earptatal (VBC)XS)	Windows Security Trusted Microsoft Store app	\rightarrow		*		
G IDA Pro	Apps Local Security Policy Windows Defender Firewall with	>	Winc Trusted	Jows Security Microsoft Store app		
S.	Advanced Security Settings Security processor	>	□ Open -⇔ Pin to Start			
DA Free	 Security processor troubleshooting Windows Security 	>	 App settings 			
arib	Windows Security settings Check for updates Windows Update settings	> > >				
June	\bigcirc Advanced Windows Update options	>			e	Windows 10 Enterprise Evaluation Windows License valid for 26 days Juild 18362.19h1_release.190318-1202
-	𝒫 security		H 😂 🥽 🏦	Â		Same de la construction de la construcción de l

2) Busca protección contra virus y amenazas.

	Windows Se	ecurity			- 0	×
- -)	← ≡ ŵ Hom	ie & threat protection	% Virus & threat protection settings Real-time protection is off, leaving your device vulnerable. Turn on	Change your privacy sett View and change privacy for your Windows 10 dev Privacy settings Privacy dashboard	ings r settings rice.	
	오 Acco (미) Firew 디 App - 고 Devic	unt protection vall & network protection & browser control ce security	Manage settings Virus & threat protection updates Security intelligence is up to date. Last update: 1/8/2020 6:45 PM	Privacy statement.		
	☞ Devic	ce performance & health ly options	Ransomware protection Set up OneDrive for file recovery options in case of a ransomware attack. Set up OneDrive			
	⊗ Settir	ngs Type here to search	Manage ransomware protection	^ ≒ ⊕ ∢	4:06 PM 1/9/2020	F 3

- 3) Desactiva toda la protección de virus y amenazas.
- 4) **Aquí un truco**. Aunque desactives la protección en tiempo real, Windows volverá a activarla cuando menos lo esperes, haz esto: Busca exclusiones y añade el drive C: esto ayudará a que Windows Defender ignore este directorio.

Wine	dows Security		- 0 ×
+ ≡	Home	Exclusions Add or remove items that you want to exclude from Windows Defender Antivirus scans.	Have a question? Get help
0 8	Virus & threat protection Account protection	+ Add an exclusion	Help improve Windows Security Give us feedback
(iji)	Firewall & network protection App & browser control	C'\ Folder	Change your privacy settings
⊒ ⊗	Device security Device performance & health		for your Windows 10 device. Privacy settings Privacy dashboard
Ø\$	Family options		Privacy Statement
\$\$	Settings		△ mm (中) 小 4:14 PM ■
	P Type here to search	Ħ C 📮 🏦 🕿 🕂	^ ≒ ⊕ ₫× 1/9/2020

5) Desactiva todas las protecciones de firewall.



Eso es todo, recuerda que tienes todo esto en video en la sección Configurando el Laboratorio.