

Taller de Seguridad y Hardening en Servidores Linux

Pre-requisitos

- Equipo de cómputo con capacidad de virtualización habilitada desde la BIOS/UEFI
 - **Nota**: Depende del fabricante:

Ejemplo 1:

▶ Hard Disk Boot Priority	[Press Enter]	Item Help
First Boot Device Second Boot Device Third Boot Device Password Check HDD S.M.A.R.T. Capability Limit CPUID Max. to 3 No-Execute Memory Protect CPU Enhanced Halt (C1E) CPU Thermal Monitor 2(TM2 CPU EIST Function	Hard Disk] [Hard Disk] [Hard Disk] [Setup] [Enabled] [Enabled] [Enabled] [Enabled] [Enabled]	Menu Level When enabled, a UMM can utilize the additional hardware capabilities provided by Virtualization Technology
Virtualization Technology Full Screen LOGO Show Init Display First	[Enabled] [Disabled] [PC1]	Sysprobs.com

Ejemplo 2:

1	Securitu	HEP Rower Ac	LETT-PACKARD CO	MPUTER	SETUP
	Setup P Power-O	assword n Password	avanceu		
	Device USB Se Slot S Networ System	Data Execu Virtualiza Intel(R) V	System Secu Ition Prevention Ition Technology /T-d LT) Support	rity — (VTx)	Enabled ▶Enabled Disabled Disabled
	Master System	Security	F10=	Accept,	ESC=Cancel

• Memoria RAM: 8 Gb (mínimo)



- Sistema Operativo: Linux (preferencia) x86_64
- Espacio en disco: 50 Gb (mínimo)

Software de virtualización

El taller se desarrollará utilizando una máquina virtual (VM) preparada para dicha actividad. Se proporcionará en formato **qcow2**, por lo que se recomienda la virtualización basada en KVM.

Se puede utilizar alguna otra tecnología diferente, pero los trabajos de conversión y adecuación de la imagen, tanto para el software de virtualización, como del Sistema Operativo, no están contemplados en este taller.

Máquina Virtual

1. Descargar la imagen de:

http://hakke.rootzilopochtli.com/vmlab01.qcow2

- 2. Importar la VM
 - \$ sudo virt-install --name vmlab01 --memory 1024 --vcpus 1 \
 - --disk /var/lib/libvirt/images/vmlab01.qcow2 --import \
 - --os-variant centos7.0 --noautoconsole
- 3. Verificamos la creación y el acceso a la VM:

\$ sudo virsh console vmlab01

Nota: La contraseña de root de la imagen es: redhat



4. Obtenemos la IP de la VM:

vmlab01 login: root

Password: *****

[root@vmlab01 ~]# ip a

•••

2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000

link/ether 52:54:00:06:29:7f brd ff:ff:ff:ff:ff

inet **192.168.122.74**/24 brd 192.168.122.255 scope global dynamic eth0

inet6 fe80::5054:ff:fe06:297f/64 scope link

[root@vmlab01 ~]# exit

5. Validamos el acceso por ssh a la VM:

\$ ssh root@192.168.122.74 hostname

root@192.168.122.74's password: ******

vmlab01.iti.iii.lab

Referencias

• Fedora

• <u>https://docs.fedoraproject.org/en-US/quick-docs/getting-started-with-virtualization/</u>

- CentOS
 - <u>https://wiki.centos.org/es/HowTos/Virtualization/Introduction</u>
 - Debian
 - <u>https://wiki.debian.org/es/KVM</u>
- Ubuntu
 - <u>https://help.ubuntu.com/community/KVM/Installation</u>
- Arch
 - <u>https://wiki.archlinux.org/index.php/KVM</u>