

Forum:[Hack Forums](#)

Thread: [Should I run my programs in a virtual machine?](#)

nitvit610 - April 25, 2015, 10:22 am

So I'm pretty new to everything here, I have 1 question: when I am doing my stuff (for example: binding stuff to things), should I be doing it in a virtual machine? To insure myself if I mess up not all is lost?

??st??B?? ? - April 25, 2015, 11:23 am

(Apr 25, 2015 10:22 AM)nitvit610 Wrote: [\[CITE\]](#) So I'm pretty new to everything here, I have 1 question: when I am doing my stuff (for example: binding stuff to things), should I be doing it in a virtual machine? To insure myself if I mess up not all is lost?

Virtual machines are very useful.

It pretty much shows you what would happen if you put a virus, RAT or anything on another computer.

I wouldn't say that you should use it when binding files, as that is usually safe.

But things such as viruses, RATs, Keyloggers, anything that looks shady can be tested on a VM. ?

nitvit610 - April 25, 2015, 11:35 am

So say I wanted to open a suspicious file (a zip), would it be better to do it in VM. The reason I ask is because someone I know sent me some programs in zips, but I don't 100% trust it. Hence why I ask this question.

Masked - April 25, 2015, 11:38 am

(Apr 25, 2015 11:35 AM)nitvit610 Wrote: [\[CITE\]](#) So say I wanted to open a suspicious file (a zip), would it be better to do it in VM. The reason I ask is because someone I know sent me some programs in zips, but I don't 100% trust it. Hence why I ask this question.

Opening a suspicious file is something you shouldn't do, but it'd be safer to open it in a VM instead of on your actual desktop.

Although there's still plenty of methods that can get you infected even if you're running the executable/suspicious file in a VM. But you lower the risks by running it through a VM or by a SandBox.

??st??B?? ? - April 25, 2015, 11:43 am

(Apr 25, 2015 11:38 AM)Masked Wrote: [\[CITE\]](#) Opening a suspicious file is something you shouldn't do, but it'd be safer to open it in a VM instead of on your actual desktop.

Although there's still plenty of methods that can get you infected even if you're running the executable/suspicious file in a VM. But you lower the risks by running it through a VM or by a SandBox.

^ This.

Make sure you have a working, fully functional AntiVirus on your actual computer.

Even if you're running the file inside a VM, some malware can "break containment"...

If you are too unsure about doing this, you can always scan the files themselves on an online AV scanner such as [VirusTotal](#). ?

nitvit610 - April 25, 2015, 11:51 am

Okay thanks a lot for the help! I've decided I'm going to be setting up a virtual box, but I am unsure. Are there any good tutorials for this on HF?

Masked - April 25, 2015, 11:56 am

(Apr 25, 2015 11:51 AM)nitvit610 Wrote: [\[CITE\]](#) Okay thanks a lot for the help! I've decided I'm going to be setting up a virtual box, but I am unsure. Are there any good tutorials for this on HF?

You need to download a virtual box software, such as VMWare Workstation, Virtual Box VM or something else, then you need to download a disk image of the OS you wish to install (ex. Ubuntu, Windows, etc) then just click "create new VM" on your virtual box, and select the file directory of your disk image, configure settings - and you're set.

You can find lots of disk image files on official sites, if not just use a torrent site.

EDIT: I found a tutorial for you on how to set up a VirtualBox VM;
[hackforums\(dot\)net/showthread.php?tid=203882](http://hackforums(dot)net/showthread.php?tid=203882)

Geno - April 25, 2015, 1:55 pm

Fuck yeah, I can't stress how important virtual machines are any time you're testing something new. A lot of people just try it on their machines and they either get fucked up or they end up causing a mess that takes hours to fix.

PLEASE do use a virtual machine, they are highly recommended.
[Take this from someone who has gone down that road many times]

The Drama Llama - April 26, 2015, 2:48 am

Does it matter what VM you use?
What one would you suggest for beginners?

htuts - April 26, 2015, 3:50 am

Doesn't matter much, I like VMware player free

ProfessionalTEMP2 - April 26, 2015, 3:52 am

(Apr 26, 2015 02:48 AM)Slup Wrote: [\[CITE\]](#) Does it matter what VM you use?
What one would you suggest for beginners?
It shouldn't matter. Look up some tutorials on Youtube.

But make sure you download a legit version of a VM from their official website.

??s†??B?? ? - April 26, 2015, 5:52 am

(Apr 26, 2015 02:48 AM)Slup Wrote: [\[CITE\]](#) Does it matter what VM you use?
What one would you suggest for beginners?
People say that Sandboxie is better with security, however I see nothing wrong with VirtualBox. ?

#Skyline - April 26, 2015, 7:07 am

Either that or a RDP.
Your choice.

nitvit610 - April 26, 2015, 12:04 pm

I ended going with Oracle's VirtualBox along with Kali Linux for OS.

Ghost420 - April 26, 2015, 12:30 pm

There are no ways for viruses to escape from VM. I launched 9999+ viruses/worms/trojans and even ransomware on VM. And none of them are on actual computer. I dont know why ppl think malware can escape VM. Thats IMPOSSIBLE.

nitvit610 - April 26, 2015, 2:03 pm

(Apr 26, 2015 12:30 PM)Ghost420 Wrote: [\[CITE\]](#) There are no ways for viruses to escape from VM. I launched 9999+ viruses/worms/trojans and even ransomware on VM. And none of them are on actual computer. I dont know why ppl think malware can escape VM. Thats IMPOSSIBLE.

I suppose the only way you would get infected then if one were to use VM is when they download something (gets infected without knowing) and then opening it in VM.

Eternal. - April 26, 2015, 2:56 pm

You can also use Sandboxie for testing programs.

Kasthorn - April 26, 2015, 3:17 pm

use vmworkstation 11, go google pirate city vmware workstation 11 license keys, forget downloading the crack or whatever program, right above the download in the page is like 5-7 license keys, volume license keys unlimited use no real purchase needed, easy to do and use without spending.

also, use the clone option, linked clone. its not an entire vm linked to your host but more of a link to the vm you cloned to make it. so its even harder to get infected if its breaking containment since its not a full link from it. much smaller in disk space size to do too.

but for the most part, for testing my programs i use shared folder settings from host to a non editable folder in the virtual machine being provided the folder or files to it. it cuts it off from returning to host computer. so it IS a contained thing especially if run on an external hard drive too.

nitvit610 - April 26, 2015, 3:42 pm

(Apr 26, 2015 03:17 PM)Kasthorn Wrote: [\[CITE\]](#) use vmworkstation 11, go google pirate city vmware workstation 11 license keys, forget downloading the crack or whatever program, right above the download in the page is like 5-7 license keys, volume license keys unlimited use no real purchase needed, easy to do and use without spending.

also, use the clone option, linked clone. its not an entire vm linked to your host but more of a link to the vm you cloned to make it. so its even harder to get infected if its breaking containment since its not a full link from it. much smaller in disk space size to do too.

but for the most part, for testing my programs i use shared folder settings from host to a non editable folder in the virtual machine being provided the folder or files to it. it cuts it off from returning to host computer. so it IS a contained thing especially if run on an external hard drive too.

Thanks for the tips! I'll be sure to try these out, especially the last one.

??s†??ß?? ? - April 27, 2015, 8:40 am

(Apr 26, 2015 12:30 PM)Ghost420 Wrote: [\[CITE\]](#) There are no ways for viruses to escape from VM. I launched 9999+ viruses/worms/trojans and even ransomware on VM. And none of them are on actual computer. I dont know why ppl think malware can escape VM. Thats IMPOSSIBLE.

I'm pretty sure it's not impossible, some forms of malware can "escape".

This is usually bad luck or a glitch with the VM that passes certain connections over to the host OS.

Again, it is very rare but can happen. ?