

Forum:[Hack Forums](#)

Thread: [\[BHCPU\] Brotherhood academy lesson 1: Setting up a malware test box](#)

-Hyperion - June 1, 2014, 12:27 pm

Hey guys it's -Hyperion ? I have run my own security company doing pen testing and malware removal the past 3 years. I am also a part of the WHHPIT team.

This is part 1 of a 3 part series on analyzing malware and removing it.

Introduction

Part 1. Setting up a malware test box

Part 2. Analyzing malware

Part 3. Removing malware

RequirementsVirtual Box:[Here](#)

Windows XP with SP3(you can download this from various sites if you do not have a CD)

Malware Analysis/Removal Toolkit: [Here](#)

Setting up the Test Box

I will refer you to this thread [Here](#) for setting up a virtual machine. After you have windows XP installed there are a few things to do first to change first.

Start by launching VM and clicking on setting.

PICTURE

Spoiler [\(Click to View\)](#)

Then navigate to Network.

PICTURE

Spoiler [\(Click to View\)](#)

Finally enable Bridged Networking.

PICTURE

Spoiler [\(Click to View\)](#)

That is the only setting that needs to be changed. Now you can boot up the virtual machine. Once loaded into XP there are 3 things you need to do.

First update windows and turn off AV by going to Security Center.

PICTURE

Spoiler [\(Click to View\)](#)

Second select "Check for the latest updates from Windows Update" and then click on Recommendations and choose I have my AV software.

PICTURE

Spoiler ([Click to View](#))

Go [Here](#) and run the installer.

Last is to download and install the programs in the Toolkit that need installing and placing the others on the Desktop.

Now you can restart the VM then turn it off.

Creating a snapshot of the Test Box

Now I will walk your through taking a snapshot of the VM. You will restore to this snapshot after every file you test. This will take the VM back to its state before you tested anything allowing you a clean environment each time and a back up if something goes wrong.

First click on the snapshot button with the machine powered off.

PICTURE

Spoiler ([Click to View](#))

Then click on Take Snapshot.

PICTURE

Spoiler ([Click to View](#))

Finally type in a name and description then hit okay.

PICTURE

Spoiler ([Click to View](#))

To restore to this snapshot any time you power off the machine just select restore.

PICTURE

Spoiler ([Click to View](#))

Conclusion

That's it you now have a test box set up with all the necessary tools and a way to restore after each test. In lesson 2 we will go over using these tools and analyzing a piece of malware. Stay tuned ?

Jagster™ - June 1, 2014, 1:03 pm

Nice work buddy cant wait to see the other 2 parts of this series!

-zERAI - June 1, 2014, 1:47 pm

Great work, can't wait to see the other parts!

-zERaIt?

T e s s e r a c t - June 1, 2014, 2:05 pm

I like this tutorial, I support Virtual Machine use. HF users should do it more often, however, I support VMware over all other vendors. You just can't beat them.

cyberducky - June 1, 2014, 2:14 pm

(Jun 1, 2014 02:05 PM)MaiTriCks Wrote: [\[CITE\]](#) I like this tutorial, I support Virtual Machine use. HF users should do it more often, however, I support VMware over all other vendors. You just can't beat them.

VirtualBox is good for simple users but VMWare has a boat load of features.

Mittens - June 1, 2014, 2:19 pm

Thanks for this tutorial, I always wondered how members tested files on a virtual machine.

Roger Waters - June 1, 2014, 2:29 pm

Nice tutorial, -Hyperion. Hope to see some more tutorials like this from you.

Aura - June 1, 2014, 4:35 pm

(Jun 1, 2014 02:19 PM)Mittens Wrote: [\[CITE\]](#) Thanks for this tutorial, I always wondered how members tested files on a virtual machine.

All the smart one does. The WHHPIT at least do and the common helpers here too ?

Abdilo - June 10, 2014, 3:52 am

I did this a few weeks ago when i accidentally infected my self, I found the guys ip address and I geolocated his ip and spammed the keylog file till the keylog file was 30mb then i waited for him to connect and download the 30mb keylog file... then i removed the virus from my virtual machine :P

T e s s e r a c t - June 10, 2014, 9:33 am

(Jun 10, 2014 03:52 AM)Grey Hat Mafias Bitch Wrote: [\[CITE\]](#) I did this a few weeks ago when i accidentally infected my self, I found the guys ip address and I geolocated his ip and spammed the keylog file till the keylog file was 30mb then i waited for him to connect and download the 30mb keylog file... then i removed the virus from my virtual machine :P

That is so rude to the poor phisher. Why would you do that? ?

Jk. ? That was pretty cool. You should have made the file 1GB and let it go spam overnight next time.

Darc - June 10, 2014, 3:11 pm

I really like this tutorial. I really like Virtual Machines and this is a really good tutorial. My favorite VM is VMware but there are other great ones out there.

kingpin69 - June 10, 2014, 5:38 pm

anyone got a link for just a straight up .iso of xp sp3?

all i can seem to find is zip files with setup.exe inside ?

ihearyou - June 11, 2014, 1:24 am

Just be care if you bridge your connection, You can still infect the host which is VM's are running on. I use VMware Workstation and i Vlan the box off so there is no communication to any other PC's on my network.

-Hyperion - June 11, 2014, 6:06 am

(Jun 11, 2014 01:24 AM)ihearyou Wrote: [\[CITE\]](#) Just be care if you bridge your connection, You can still infect the host which is VM's are running on. I use Vmware Workstation and i Vlan the box off so there is no communication to any other PC's on my network.

This is a test box I specifically set it up as a bridged connection for monitoring purposes.

Abdilo - June 11, 2014, 10:30 pm

(Jun 11, 2014 06:06 AM)-Hyperion Wrote: [\[CITE\]](#) This is a test box I specifically set it up as a bridged connection for monitoring purposes.You could setup fakenet on your host computer then bridge the connections through that.

Or what I do is lock it to a dmz and use fiddler to mess with the traffic :P

??????M1kep?????? - June 15, 2014, 10:51 pm

Awesome tutorial! I always love these types of tutorials! So, can you explain how we would set up a safe bridge connection and what the dmz thing is, and fiddler... O.o

??????M1kep?????? - June 17, 2014, 12:25 am

So I guess not? Ok :/

Also when can we expect part two?

Aura - June 17, 2014, 3:21 am

(Jun 17, 2014 12:25 AM)??????M1kep?????? Wrote: [\[CITE\]](#) So I guess not? Ok :/

Also when can we expect part two?

-Hyperion is a bit busy right now, Part II was supposed to be a week ago but his job (he owns his company) keeps him really busy. I'll link it that thread so he doesn't forget it alright ? ?

-Hyperion - June 17, 2014, 6:10 am

Also moving this week so I have a shit ton of boxes to move.

Alex© - June 17, 2014, 11:26 am

Really nice guide, looking forward to other parts.

tusharthehottie - December 2, 2014, 10:04 am

I followed Aura's tutorial on installing a VM. There he had posted screenshots about installation of a windows 7 OS. What changes should I make in the settings if I want to do the testing on a windows 7 OS? Or should I use XP only?

Aura - December 2, 2014, 2:15 pm

(Dec 2, 2014 11:04 AM)tusharthehottie Wrote: [\[CITE\]](#) I followed Aura's tutorial on installing a VM. There he had posted screenshots about installation of a windows 7 OS. What changes should I make in the settings if I want to do the testing on a windows 7 OS? Or should I use XP only?

As long as all your sharing options between the host system and the VM are disabled, and you use a NAT adapter in the VM, you should be good.

-Hyperion - December 2, 2014, 4:26 pm

(Dec 2, 2014 11:04 AM)tusharthehottie Wrote: [\[CITE\]](#) I followed Aura's tutorial on installing a VM. There he had posted screenshots about installation of a windows 7 OS. What changes should I make in the settings if I want to do the testing on a windows 7 OS? Or should I use XP only?

there are no setting changes they exactly the same basically

Algo-rhythm - December 3, 2014, 9:34 am

What is the idea behind enabling bridged networking? Is it to allow a direct connection to the router without passing through the host OS connection?

Aura - December 3, 2014, 9:42 am

(Dec 3, 2014 10:34 AM) Algo-rhythm Wrote: [\[CITE\]](#) What is the idea behind enabling bridged networking? Is it to allow a direct connection to the router without passing through the host OS connection?

There's no idea behind enabling it, you don't want to enable it and stay on a NAT network.

Algo-rhythm - December 3, 2014, 10:00 am

(Dec 3, 2014 10:42 AM) Aur? Wrote: [\[CITE\]](#) There's no idea behind enabling it, you don't want to enable it and stay on a NAT network.

I think you do enable it when portforwarding. But here we are not portforwarding. So, why has it been mentioned in the tutorial?

Aura - December 3, 2014, 10:05 am

(Dec 3, 2014 11:00 AM) Algo-rhythm Wrote: [\[CITE\]](#) I think you do enable it when portforwarding. But here we are not portforwarding. So, why has it been mentioned in the tutorial?

Probably -Hyperion's inattention as he thought of it as a normal VM setup and not one you used for malware testing. Keep the NAT setting.

-Hyperion - December 3, 2014, 4:08 pm

(Dec 3, 2014 11:05 AM) Aur? Wrote: [\[CITE\]](#) Probably -Hyperion's inattention as he thought of it as a normal VM setup and not one you used for malware testing. Keep the NAT setting.

I mentioned it in the tutorial because when this was written it allowed easier monitoring with Wireshark and it fooled some malware into thinking it was on a network. I now have a new program being tested that will allow this while still allowing a NAT setting.

SureAintMe - December 13, 2014, 1:22 pm

(Jun 1, 2014 02:05 PM) MaiTriCks Wrote: [\[CITE\]](#) I like this tutorial, I support Virtual Machine use. HF users should do it more often, however, I support VMware over all other vendors. You just can't beat them.

Man, thank the computer gods for virtualization! I don't know how I lived without it! I setup a couple ESXi servers and use both the vSphere client and VMware Workstation (on a local PC) for my lab environment. It's unbelievably handy and time-saving to be able to revert back to snapshots every step of the way and have multiple VMs with different OS's up and running to practice and learn penTesting. Plus, it's easier to contain an accidental or unwanted infection and adds another layer of security to the network.

VirtualBox is good enough for most basic users-- the price is certainly right! But since I get access to VMware Workstation from my work, I prefer it much over VBox.

Aura - December 13, 2014, 4:27 pm

(Dec 13, 2014 02:22 PM) SureAintMe Wrote: [\[CITE\]](#) Man, thank the computer gods for virtualization! I don't know how I lived without it! I setup a couple ESXi servers and use both the vSphere client and VMware Workstation (on a local PC) for my lab environment. It's unbelievably handy and time-saving to be able to revert back to snapshots every step of the way and have multiple VMs with different OS's up and running to practice and learn penTesting. Plus, it's easier to contain an accidental or unwanted infection and adds another layer of security to the network.

VirtualBox is good enough for most basic users-- the price is certainly right! But since I get access to VMware Workstation from my work, I prefer it much over VBox.

VirtualBox is good for anyone, it's just easier to use VMWare Workstation when you have 10+ VMs.

I currently use VirtualBox with 6-7 VMs and I have no issues with it.

oxon - May 24, 2015, 1:41 am

well, good tutorial sir, learn something new.. thnks for sharing

HiddenMalware - May 24, 2015, 3:53 am

I'll be sure to try this out! I've wanted to get into malware removal and analasys for a while now ;)

Binary Ghoul - October 12, 2015, 8:09 am

Disregard this i was wrong

I would recommend doing another snapshot with guest additions installed

-Hyperion - October 12, 2015, 11:02 am

(Oct 12, 2015 08:09 AM)Binary Ghoul Wrote: [\[CITE\]](#) I would recommend doing another snapshot with guest additions installed

you do not want guest additions installed on a malware test box

Binary Ghoul - October 12, 2015, 12:23 pm

(Oct 12, 2015 11:02 AM)-Hyperion Wrote: [\[CITE\]](#) you do not want guest additions installed on a malware test box

Any particular reason?