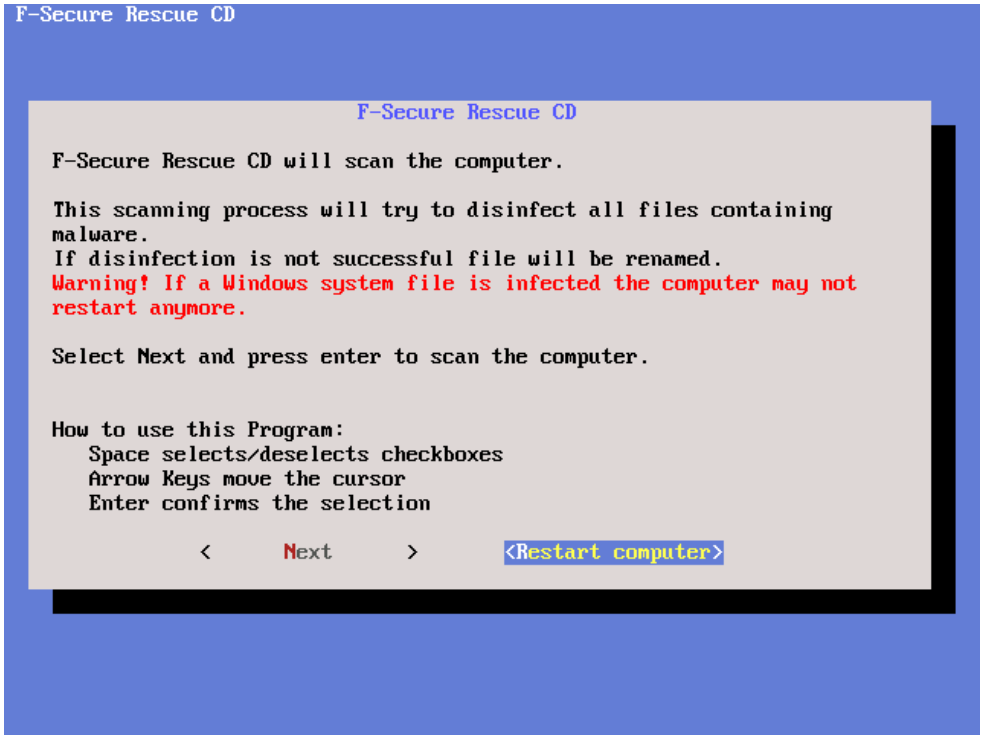
Using Linux to Disinfect Windows

May 19, 2010 By Gene Liverman (in

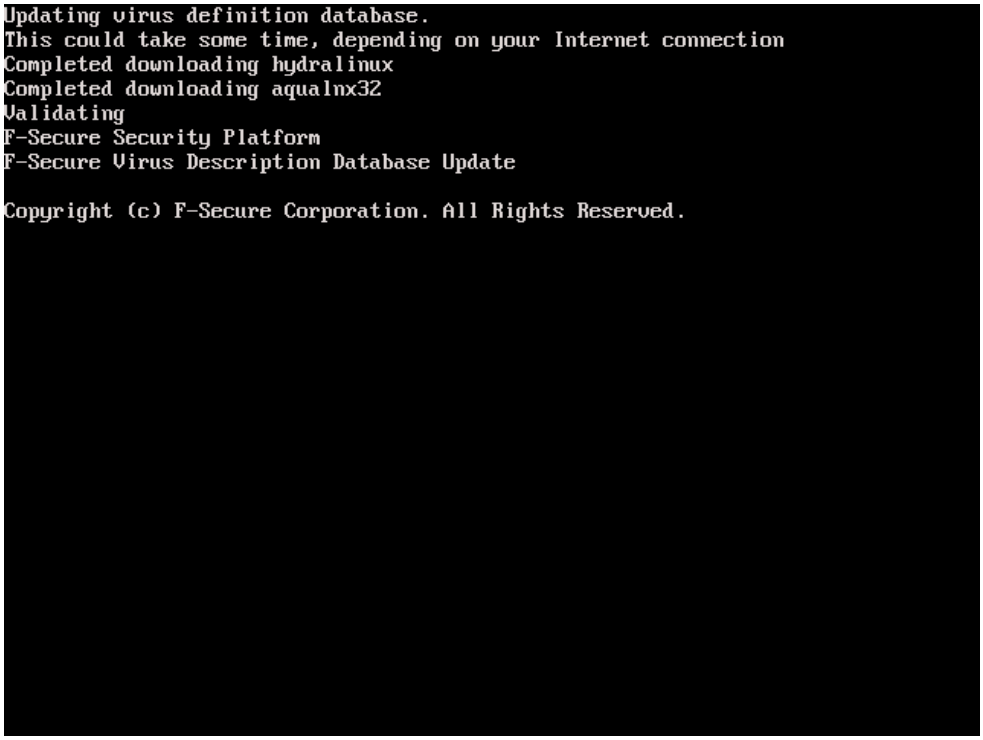
Are you responsible for one or more Windows computers? If yes then the odds are really good that you have had to deal with cleaning viruses and malware. Did you know F-Secure offers a free Rescue CD built on Knoppix (for just this purpose? Let's take a look at how easy the F-Secure Rescue CD is to use.

Like with most everything, the first step is knowing where to download what you need... in this case that is from www.f-secure.com/en_EMEA/security/tools/rescue-cd (. Once you download the ZIP and then burn the ISO it contains, stick your new disk in the infected computer and reboot. Upon rebooting you should be greeted with a screen like this:

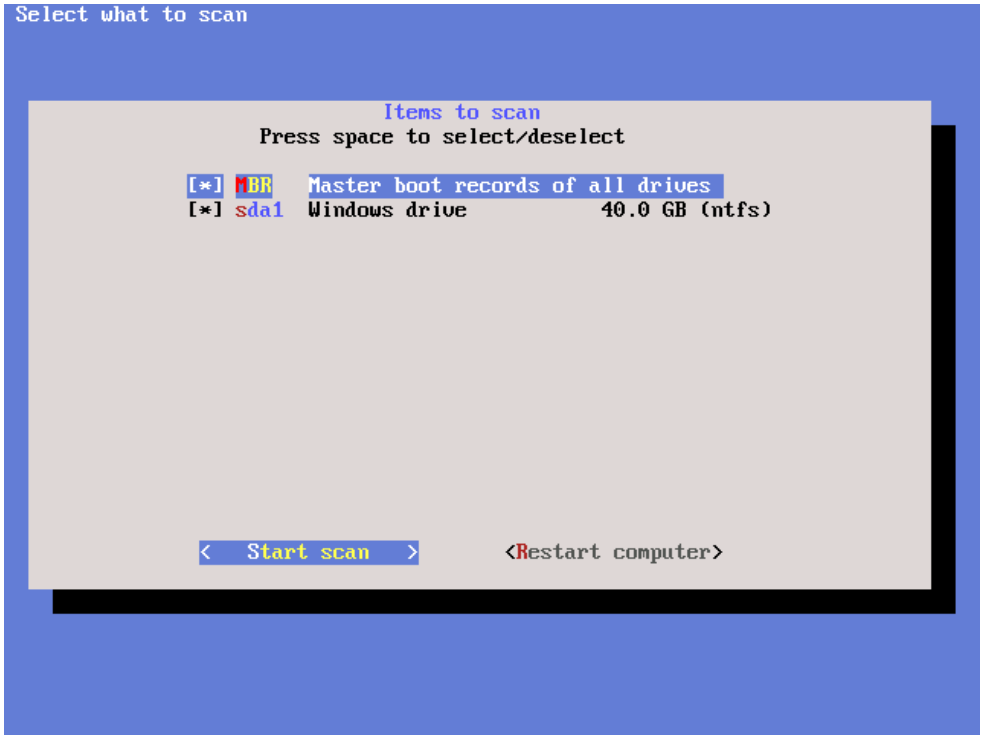
After hitting enter you will see your basic malware removal warning...



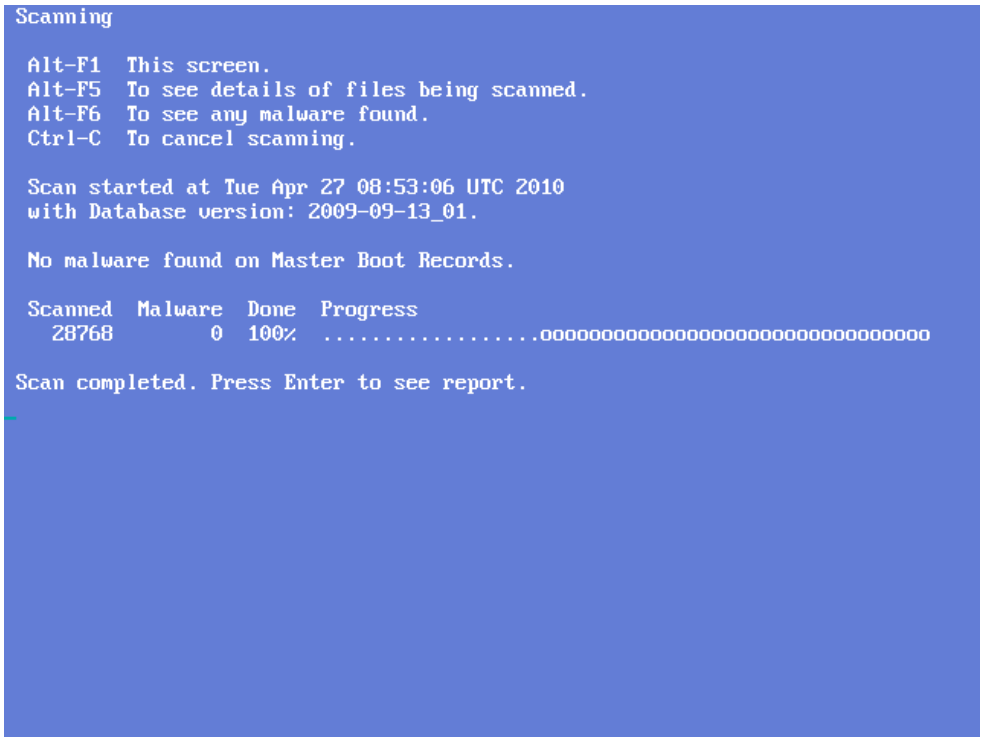
Next it will try and update itself from either a USB drive or the internet.



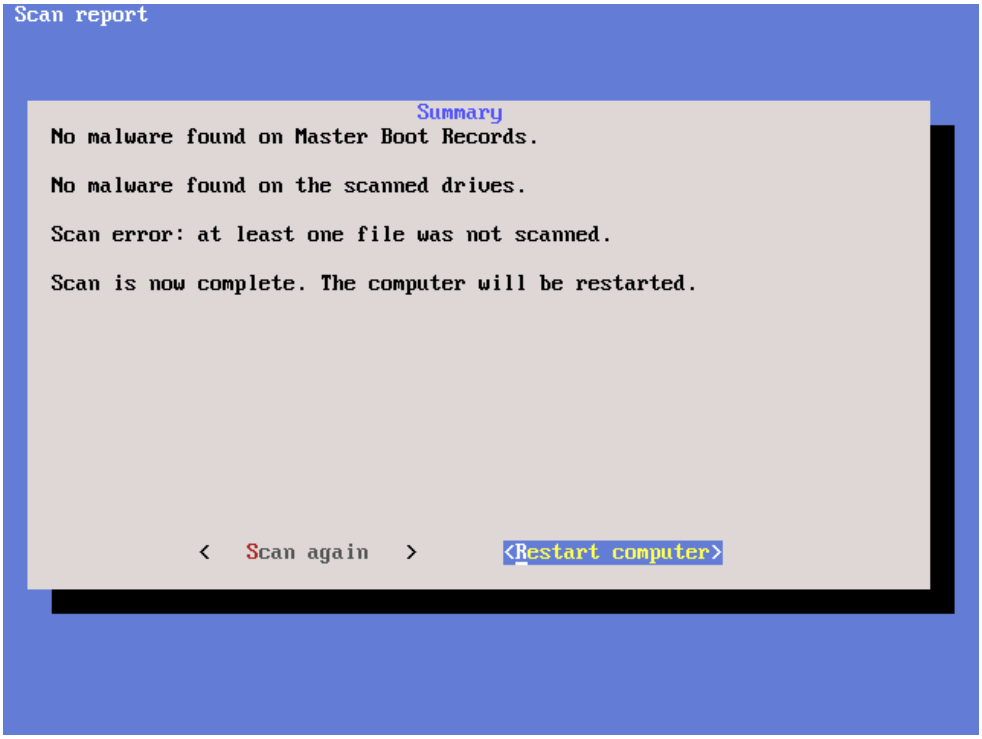
Once it has the newest version of everything it will present you with a list of all the partitions it sees and let you choose which ones to scan.



After you select what you want to scan it will show you the progress and allow you to see what is being scanned and what malware has been found.



The report that follows will show you any errors that were encountered and will also show you a summary page with the scan's results.



That's it. Linux has once again made life simpler. The system should now at least be clean enough that you can use traditional tools that run inside of Windows to finish up.

Gene Liverman is a Help Desk Support Service Specialist at a university.

Comments

Comment viewing options

Select your preferred way to display the comments and click "Save settings" to activate your changes.

Great (
Submitted by Issac (not verified) on Jun 19, 2010.

Great Post
http://techrosyncvibe.blogspot.com/ (

Not always OK in an office environment (
Submitted by benbong (on May 26, 2010.

Hi All,
I'm the IT manager of a small company (we have around 10 servers (9 windows and 1 linux) and 50 desktops (all windows)).
I tried Avira, and some other linux AV distros. (

The main problem with most of them is that even if DHCP is working, only a few can be easily setup to use a proxy to update the virus database.

If you can show me one that you can configure in one or 2 cliks, I'll be happy to use it, even buy it !!
For Avira you can do it but have to manually configure every time you use it can be painful, as often the infection spreads quite easily and I already had to disinfect all the PCs ... Even with an enterprise grade antivirus on each machine.

Benbong

Tried this for the experience (
Submitted by Menlotechnical ((not verified) on May 22, 2010.

I have tried these for the experience - live CD's.

As an IT Consultant, I would say I am only interested in grabbing all their important data: docs, pics, music, bookmarks, iTunes itl files, intuit stuff, outlook hidden stuff... possibly the software keys to the MS stuff.
A list of all the programs to help you rebuild..
Do this in Knoppix or Puppy.
Run a disk utility like spinrite v6 from grc.com
Then wipe, reinstall up to date of the Windows OS, then lock it down with Chrome browser, FireFox, OpenDNS, and a limited account being the main account.
Use driveSnapshot or clonzilla to clone the machine for future rebuilds at this point...
Set up off site backups and antivirus (nod32 works)

This will be the fastest and most reliable way, with the least about of time.
I tried KasperskyLiveCD, AntiVir LiveCD and ran MalwareBytes inside of XP. Only sparse things were removed - but at least they allowed you bring the machine back from the dead.
After running this series of liveCD's I ran SpyBot and it picked up another 120 problems - beyond just cookies.
It is clear that each utility helps cleam it, but it is way way faster to just backup everything and blow the drive away. Drives are cheap and it may make more sense to install on a new drive.

This is my experience with Windows.
There is also an advantage to installing things on OS X, Linux and Windows with a partition for /, and another for data, but most Windows consumers are simply not interested in learning to change drive letter C to D :-)

Hope this helps everyone. Again, this is just from the 'how little time can I spend on getting this back up and running and not wasting time.'
I can't get my clients to buy into Linux for the desktop, but a good bridge to this is Apple refurbished MacMini or better.

Didn't work for me :(

Submitted by Anonymous (not verified) on May 20, 2010.

Hi,
I have a Windows 2000 on a virtual machine, so I thought I'd give the rescue CD a try, I copied one virus of the collection I keep for this experiments and started the VM from the iso image. It took a while to scan the full computer and didn't find anything. I thought maybe that particular virus was not detected by f-secure so I copied a bunch more on different locations in the virtual machine. Started again with the rescue CD and to my astonishment nothing happened... again! Of course it could be I'm doing something wrong, but I reallu don't see what, particularly when clam detects all of them without problems.

Only use eicar for testing AV software

Submitted by Anonymous (not verified) on May 22, 2010.

I read you have a list of virusses to check your AV software. You had better use just one specially constructed speudo virus: EICAR-STANDARD-ANTIVIRUS-TEST-FILE . All anti virus software knows this file and acts though it was a real virus. But all the file does when executing, is printing the text EICAR-STANDARD-ANTIVIRUS-TEST-FILE. Please copy it from http://www.eicar.org/anti_virus_test_file.htm or just google about it before trying.

Johan

Concerning EICAR

Submitted by Anonymous (not verified) on May 24, 2010.

Hi Johan,

using EICAR would have been an option, but a misleading one in my opinion. As you point out, most of the AV programs detect EICAR, so let's assume I had used it: f-secure would have detected it and I would be under the false assumption that this rescue CD could be a reasonable tool in case of disaster.

As it turned out, using a (possibly too small) sample of the kind of virus active in my environment I know now that it would be wise to try something else first in case a windows machine gets infected in my neighbourhood.

I see I didn't mention before that I don't really "collect" virus, they're the ones I get through email, or I find in internet links or in my colleagues' media. Instead of destroying them I just put them away to test AVs.

Greetings

Jaime

Very nice

Submitted by Anonymous (not verified) on May 20, 2010.

I used F-Secure for MS-DOS back in the day and loved it. I don't use any anti-virus products and have been looking for something like this to run every so often. People assume that because they have a real-time AV product installed, they can't get infected. Only an impenetrable medium such as a secondary OS sitting on a read-only, bootable CD is guaranteed free of infection. Or at least as

close to a guarantee as you can possibly get.

Obviously, no AV product catches EVERYTHING but F-Secure has proven itself many times over to me that they actually know a few things about viruses, worms, etc.

Added to my arsenal of power tools. Thanks!

Bootable AV
Submitted by dexterneedsabrain (not verified) on May 20, 2010.

Bitdefender and Kaspersky also have rescue CD.
i have had better results with kaspersky, as i can go to linux shell and do disaster recovery.
http://devbuilds.kaspersky-labs.com/devbuilds/RescueDisk/
and then there is INSERT

http://sourceforge.net/projects/insert/files/

dexter

OK, so I actually got to use
Submitted by Chase Crum on May 20, 2010.

OK, so I actually got to use this in a real world environment shortly after your post went out. I'll agree with the others in saying that there are plenty of distros out there with similar function. I'll stringently agree with metalx2000's install solution. What I can say about this particular distro is this:

I find it to be the most "to the point" of these solutions. Most of the others I saw were distros that had this feature. In this case, the feature was the distro and not an after thought.

second, it did exactly what it was meant to do, perfectly. Using it was very plain and straight forward. It found my problems and resolved them as well, without exception.

All in all, excellent write up !!!

-Chase

Chase Crum is the IT Infrastructure Manager for Voicenation and a self-proclaimed Linux FANATIC.

Thanks
Submitted by Gene Liverman on May 20, 2010.

Thanks for the feedback Chase!

Gene Liverman is a Help Desk Support Service Specialist at a university.

Stop wasting CD-Rs
Submitted by Gal Frishman (not verified) on May 20, 2010.

I made a post about how to use all those bootable cd's in one multiboot-able usb pen (disk-on-key). Check it out:

http://frishit.wordpress.com/2010/05/13/usb-multibooting/

--
Visit my blog: http://frishit.wordpress.com

All well and good...if...
Submitted by David Lane on May 21, 2010.

One of the advantages CD-Rs have is in environments where USB are verboten (such as the federal sector). You can walk into a data centre with a stack of CDs, but if you have even one USB based device, back to the car you go. Sure, it is dumb and makes no sense, but that is what the security guards are trained for. Logic plays no role.

USB was not the main subject
Submitted by Gal Frishman (not verified) on May 21, 2010.

The main subject was multibooting. The method can be adapted to CD-Rs as well with mkisofs command... but yeah, what you said is right.

--
Visit my blog: http://frishit.wordpress.com

AVG has one too.....

Submitted by linux fan (not verified) on May 19, 2010.

AVG has a great boot CD also. http://www.avg.com/us-en/avg-rescue-cd (

Dr. Web (
Submitted by Anonymous (not verified) on May 19, 2010.

You can also try Dr. Web Live CD. freedrweb.com

Avira is another good choice (
Submitted by Dixie Normess (not verified) on May 19, 2010.

I will have to give the F-Secure CD a chance the next time I need a very good a/v program. Avira has been good, although it seems too easy to lock/halt the system with this software.

Linux Installer. (
Submitted by metalx2000 (on May 19, 2010.

I find that most Distros of Linux have a Windows Disinfector. It's called the installer. On an Ubuntu LiveCD it's on the Desktop. At the "Prepare Disk Space" screen you choose "Use Entire Disk". Like magic, you will never have any problems with Windows again.

http://filmsbykris.com/ (
Everything you ever need to know about Open-Source Software.

Avira also had a rescue cd based on linux (
Submitted by vicm3 ((not verified) on May 19, 2010.

Avira Download site (it's called Avira AntiVir Rescue System, I think it's updated daily,I just downloaded and run on qemu, and also offers update via network (but not USB) also the info/readme box says based on Linux kernel 2.6, busybox and ntfs-3g it's a 66MB iso or exe download, ah it runs by default on German, but can be changed to English selecting a very visible icon.

Handy when you had a MS machine that don't even boot.

Avira (
Submitted by Bill Bowes (not verified) on May 23, 2010.

I have used Avira many times.

What I really like is the fact that I can use it from the command line. It gives you full control over the Windows drive, and permits you to delete files.

However, like anything else, it gets rid of 90% of the problems. When the Windows box comes back up, you will have to run virus and malware scans several times to be sure they are all gone.

yaa (yet another alternative) (
Submitted by Angel Osuna (not verified) on May 19, 2010.

you can do the same with clamav or any other antivirus available for linux, just mounting the infected partition(s)

Timely advice (
Submitted by Chase Crum (on May 19, 2010.

As it stands now, I have three Linux boxes on my desk, and a Windows laptop that's massively infected with a sticky-note that reads "fix-me". Thanks for the post ! It's a tremendous help.
-Chase

Chase Crum is the IT Infrastructure Manager for Voicenation and a self-proclaimed Linux FANATIC.

Linux make your windows be secure (
Submitted by nu1 ((not verified) on May 19, 2010.

I like this, but i think if you want to got a really secure you must using Linux. Because Linux say I dont care about virus.

Post new comment

Please note that comments may not appear immediately, so there is no need to repost your comment.

Your name:

Anonymous

E-mail:

The content of this field is kept private and will not be shown publicly.

Homepage:

Subject:

Comment: *

Allowed HTML tags: <a>   <cite> <code> <pre><tt>   <dl> <dt> <dd> <i> <b><blockquote>
Lines and paragraphs break automatically.
Web page addresses and e-mail addresses turn into links automatically.

Notify me when new comments are posted

All comments Replies to my comment