

Forum:[Hack Forums](#)

Thread: [Most Secure Noob Friendly OS?](#)

Haters Ganna Hate - June 21, 2013, 11:56 am

Okay,

So Im going to be deploying an OS using VirtualBox using an old formatted computer I have lying around. The purpose of these is to collect information about specific people I want to infect. These people are not computer noobs and have a good sense of how malware works, though not deep.

I have my own malware ready to go. The only thing is that I need a system to collect this information.

As for being traced back, thats not a problem because I have that part fully covered. I just dont want anything happening to the actual OS.

Im using an old computer that has been cleaned and the OS virtual machine is on a USB stick. Now, it comes to the decision of what OS to use.

I know FreeBSD is very strong when it comes to security but im so used to Windows that using only a command-line with no GUI is just a very big pain!

The next option is Ubuntu which seems great because its almost like Windows except based on Linux and almost everything. I also heard that theres something called a "jail" which is like a limited user and you can set exactly what runs and goes in/out so if anyone were to exploit into the system, they cannot change the OS settings (but I only heard about that on FreeBSD, not on Ubuntu)

Ofcourse, if theres another OS, please recommend it to me!

Thanks! :D

Loki123 - June 21, 2013, 12:17 pm

Could take a look at PC-BSD. It comes with a GUI..

Plernatious - June 21, 2013, 12:25 pm

Use TAILS. It's made by the same people who made TOR, and it comes packaged with all the internet security tools you will need. It's designed to be run as a LiveCD/USB, too.

GlitnirSwan - June 21, 2013, 1:43 pm

I recommend TAILS as well. If you run it as LiveCD nothing can be permanently installed on it and everything gets wiped out once you power off, leaving no trace.

Haters Ganna Hate - June 21, 2013, 4:57 pm

(Jun 21, 2013 12:25 PM)Plernatious Wrote: [\[CITE\]](#) Use TAILS. It's made by the same people who made TOR, and it comes packaged with all the internet security tools you will need. It's designed to be run as a LiveCD/USB, too.

(Jun 21, 2013 01:43 PM)GlitnirSwan Wrote: [\[CITE\]](#) I recommend TAILS as well. If you run it as LiveCD nothing can be permanently installed on it and everything gets wiped out once you power off, leaving no trace.

Tried it and personally don't like it. It's used to use the computer but hide your activity, not run a webserver.

I'm already using TOR to hide all my traffic (hence the reason why I said I got that covered)

The Fail Collective - June 21, 2013, 6:20 pm

You're going to relay captured information to a computer you own physically?
this is pretty a bad idea, if you want to know why then ask, if not.. meh

Any linux OS on an encrypted HDD(multiple layer encryption) with the bootloader on a memory-stick, will be secure from physical access.

Just keep up to date and don't install anything you don't need/trust and don't use it for personal use i.e web browsing etc.

Loki123 - June 21, 2013, 6:36 pm

Adding to what The Fail Collective said. You are not 100% covered when using TOR. As stated on their site, TOR is not perfect.

As you are using this just to collect that info you can use any distro you like.
It is more likely that this will be traced back to you even if using TOR rather than something happening to the system.

Rent a server, anonymously to collect the data, then always connect to it using some kind of Proxy like TOR. You are still not 100% safe but better than have it on your physical machine.

P.S always delete LOG files and end of each session you connect to the servers with the shred command.