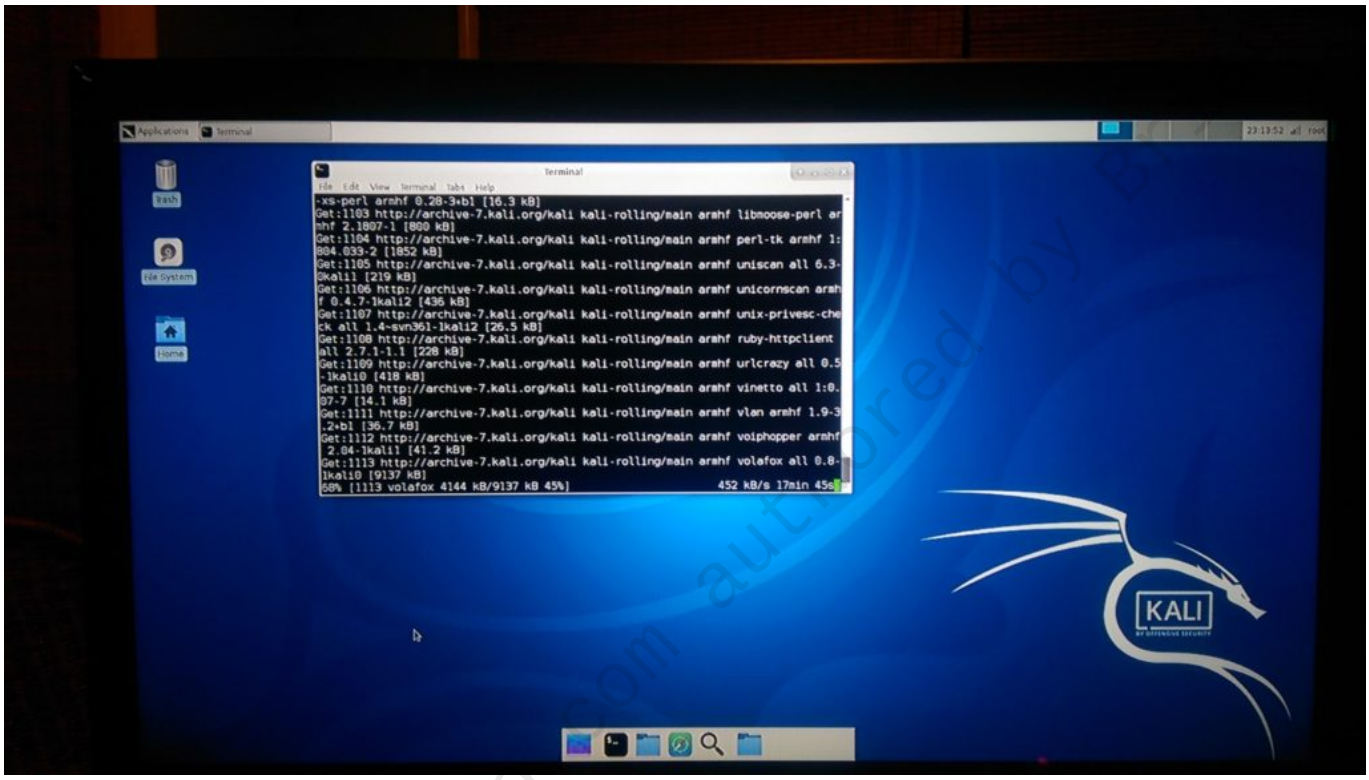
Comparing Security Distributions Of Linux

Hello readers,

In recent years I've had the opportunity to test and use many of the Linux Distributions, centered around information security. To be clear what I'll be doing in this article is evaluating overall impressions of the distribution, and not the specific tool sets. Many of the tools are suited to many IT tasks and might be confusing to use as a basis for comparison, especially considering they can generally be added to other distributions of Linux. Our evaluation will include overall performance, ease of use, adaptability, and scale, as these are the important factors to consider wheen selecting a tool for protecting an infrastructure.

Kali Linux

Originally BackTrack Linux: It became the most widely known security distribution and for years has been the defacto standard. It comes in a wide variety of desktop configurations, and it's tool selection is generally considered the best for pen testing instruction. Where it impresses us the most currently is it's inclusion of arm architecture, which promises to encompass a much wider array of devices than ever before. A chopped down version can run on Raspberry Pi3 or compatible sbcs and soon quite possibly other similar devices. The overall feel depends greatly on the desktop, and while Gnome isn't the fastest horse in the race, the alternative desktops feel peppy enough to warrant trying out as a daily OS. Overall we rate it a 4.5 as it's expanding tool base often requires considerably more space, due to a much wider assortment of tools out of the box, impacting performance somewhat. This performance score doesn't include the Kali Cloud, however that seems reliable and improves the scale to a 5.



Kali running on SBC

Performance 4, Ease of Use 4, Adaptability 5, Scale 5

Overall 4.5

Parrot OS

Definitely an often overlooked contender with performance and scale that rivals Kali, the default Mate desktop seems a bit sluggish on some hardware but up and running it has a wonderful base system, and a unique style that appeals to early Linux adopters. Parrot has a cloud system as well, and works marvelously well in spite of being a much smaller project. If we look closely at the backend we find the cosmetic differences between Parrot OS and Kali are just the beginning. Similar tools, and a somewhat increased focus on privacy seem to round out the options nicely for Information security specialists who have brought more of their own scripting into the environment. We certainly wouldn't say Parrot isn't wonderfully adaptable, but some minor things keep it from being a logical teaching tool, so we'll take away a point to say it's just about the same as Kali overall.

Performance 5, Ease of Use 4, Adaptability 4, Scale 5

Overall 4.5

Backbox Linux

A fascinating Xfce Ubuntu Distro with security tools including tor by default, and a ram wiping on exit option. I honestly believe this tool would be better if it was designed on a KDE dektop, or even Cinnamon, just to give it a cosmetic edge. Outside of that I think it has a wonderful tool

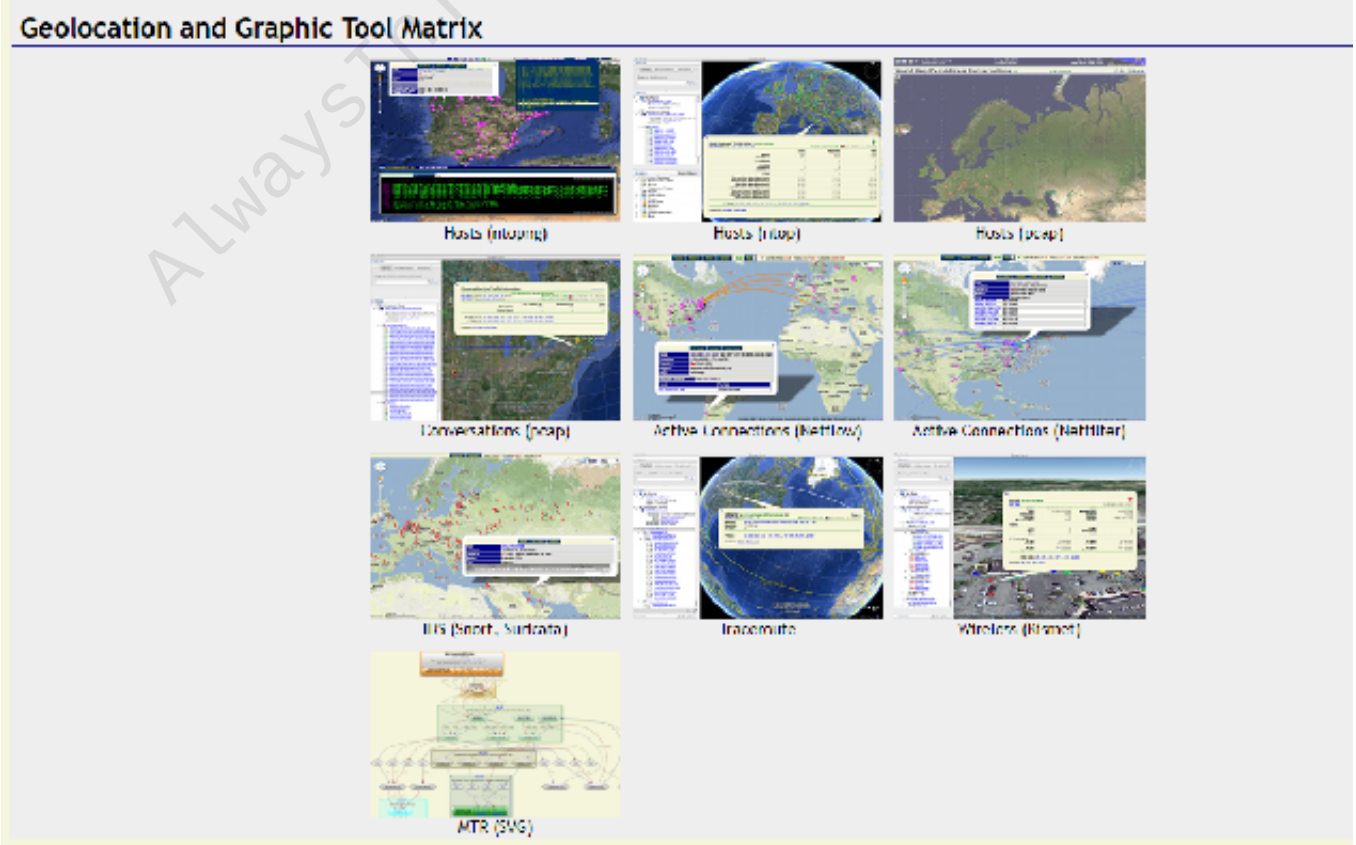
set, is snappy and reliable enough unless you are someone who mistakenly removes panel items in Xfce - don't act like you haven't... It's customization friendly to a fault though. The truth is Xfce has some theme options that can ruin browsing, and while it may be possible on other desktops, it seems almost inevitable on Xfce. I hate to say it but that actually makes it harder to recommend this tool to professionals with limited experience fixing their OS. That said it does fine in virtual settings, and can be tailored to many uses all around a great distro.

Performance 5, Ease of Use 5, Adaptability 3, Scale 4

Overall 4

NST Linux

Definitely the coolest concept for visualizing IT data, put everything possible on maps like a 90's movie. Sleek appearance and sexy interfaces, make this militaristic OS a must see for purists. Unfortunately it runs on Fedora, which isn't anyone's first choice if they have used other distributions primarily. It has resource requirements that bar it completely from older machines, limited adaptability, terrible ease of use as it requires a lengthy setup... Make no mistake it's totally worth it to dedicate a machine to NST but beyond the wow factor, it's not as useful beyond the reporting aspect without highly specialized training or lots of practice.



Performance 3, Ease of Use 2, Adaptability 3, Scale 4

Overall 3

Deft

Italy makes good security distributions, cars, and food... arguably wine as well. Before I get carried away with loving Italy, let's look at what makes Deft a worthwhile OS. It's fast, it's sleek, it's useful enough to warrant inclusion, but it's not particularly scaled or easy to use. Deft for one job, yes. Deft for 3 Jobs... well... Not so much. Almost like Cain this is a tool that can be run without being installed so it's not trying to outdo Kali under most use cases. It's great in a pinch, but less of a daily OS than even NST, which is saying a lot.

Performance 4, Ease of Use 2, Adaptability 2, Scale 3

Overall 2.75

Caine

You have to try it to appreciate the conundrum. Excellent bones make you want it on some older hardware, but it won't get as much use as Backbox. It's a powerful tool, it has great potential in the right hands, but I don't know a single IT pro who would run it on the newest hardware except in a virtual environment, or as intended, from a USB stick.

Performance 5, Ease of Use, 4, Adaptability 2, Scale 1.

Overall 3

Tails

I will say, anyone running it in a virtual machine has no idea how the internet works and should just go take a nap. Tails can work, if the right conditions are met. Cable modem? Hmmm... Virtual? Nope. Dialup? lol... It's possible that a DSL user somewhere is enjoying that anonymity that so many users imagine is possible but realistically no one OS is going to truly grant that privacy. As an OS it's chopped down to useful minimums, and it works as well as anything. Let's not evaluate the hype though, as even the best tools are no guarantee of privacy.

Performance 4, Ease of Use, 4, Adaptability 2, Scale 1

Overall 2.75

Conclusion

Yes there are other Linux Security Distributions, arguably they deserve recognition, and even homespun distros can get the job done. I miss the original Crunchbang loaded for bear via scripts that made you wonder if you would get in trouble just for having the tools. Fortunately you can not. To learn how to make use of such tools visit Cybrary.com or your local online hacking resource of choice, and let us know what you think of our assessment.