James McKenzie's Project 1 Report

James McKenzie

18 November 2019

Foreward

For my Project, I was tasked with learning about Dynamic Malware Analysis. To do this, I researched and tried several different Malware Analysis tools to try and Analyse some Malware of my own.

The Tools I tried out were AnyRun, FlareVM, and Cuckoo.

How Does Dynamic Malware Analysis Work

Dynamic Malware Analysis involved Analysing a VM which is infected with malware and looking at the state of the machine before, during, and after the malware has run. With both FlareVM, and Cuckoo, you store the VM locally on your machine. With FlareVM, you can check the state while the malware is running, FlareVM has included a lot of extra software that allows you to look at things such as process trees, CPU scheduling, Shell Monitoring as well as some more advanced resource monitoring. You can also send the report of the malware to the host machine or as a plain text email to a specified address. The FlareVM project is considered as the most fully featured of the Dynamic Malware Analysis tools. With Cuckoo, which is available for Linux, you get a full rundown of what changes were made to the system, what files were accessed, what network traffic involved, and a whole lot more. Cuckoo is considered to be a module based system, where other Linux Ops utils can help Cuckoo in producing its malware analysis report. Cuckoo is also considered to be the cutting edge approach to malware analysis, and it has a very large community that are constantly writing modules for it and upgrading it to catch even more types of malware. Any Run is the last malware analysis system that I tried. The difference being that unlike cuckoo and flare, the VM's are hosted by AnyRun. Something interesting regarding AnyRun, is that it stores all malware submitted to it, and Hashes it, allowing for quick lookup of submitted files, so that potentially, the files wouldn't even need to be fed into a VM if there was already a result for its hash in the database. There are also a lot of tools that can be used to get more information out of your malware analysis, and to try and get more accurate information out of your malware analysis. There are a lot of

Why Is Dynamic Malware Analysis Important?

Everyone makes mistakes now and again, even people who know what they're doing. Having a piece of Malware breach a company's network could result in Millions of dollars worth in damage, and the potential loss of files and network security. Putting some Dynamic Malware Analysis tools into the on-site email filter can potentially prevent situations like these from happening, by catching the malware and running it in a controlled environment, and potentially quarantining it, before it gets accidentally inside the network. Even though some malware may slip through the cracks, by putting some Malware Analysis in your

line of defence, you are massively reducing your company's risk of being held at ransom by malware such as Wannacry or Ryuk.

The Challenges of Dynamic Malware Analysis

There are many challenges that come across with Dynamic Malware Analysis, from installing the initial tools, to convincing malware to behave normally, every step comes with its own challenges. I ran into a large number of problems when i was trying to install Cuckoo Malware Analysis. Specifically regarding the networking. I still am unsure why I had such an issue with this on the OP network, as it seemed to work fine from my own flat, but that could also be due to the Operating System i was using (Arch/Alpine/NetBSD at my flat, Ubuntu at the Polytechnic). I used different Systems at Polytech to be sure that they were well tested with the Malware Analysis tools, so that the Malware couldn't escape the machine, Which is something that is possible now.

Another Problem with Dynamic Malware Analysis is that Malware designers are writing their software with these tools in mind. It is quite common now for malware to detect when they are running inside a virtualised environment. There are a number of ways for it to detect this, although one of the more common ways is to look at the number of files and the types of files on the system. If there is a lack of Downloads, Music or Documents, the malware can assume that either there isn't anything of value on the machine, and to not do anything to it, or that it is running in a virtualised environment. If it is running in a virtualised environment, The malware's best bet is to shut down, without doing any more activity, so to be considered safe by the malware analyzer. There are 2 ways around this. FlareVM comes with a lot of files and Music installed onto the base VM. The other way that we can detect malware from hiding from us in by installing some kernel modules, that analyze the malware from a Kernel level, this allows it to see exactly what files the malware is looking for. Some more advanced kernel modules can serve the malware dd'd files to trick it into thinking the system is real. Other kernel modules just detect that the malware is looking for files, and flag that as suspicious activity, however, this results in a handful of false positives

My Experience With Cuckoo

My Experience with Cuckoo was a strange one. While i was able to install Cuckoo and get a basic install working on my own machines running both Arch and Alpine, I was unable to get Cuckoo to install at all on the Polytech network using an Ubuntu machine. I didn't want to change to a distribution on the Polytech network that worked on my own machines as there have been reports of malware escaping the virtual machines on those distributions of GNU/Linux.

I tried several installation attempts. Some were more complex than others, but I always failed when it came to the networking, so I am not sure what i did

wrong. I asked for some help on a Pleroma/Security irc, however, no one really knew what to do there either.

Thankfully, Cuckoo had a lot of documentation for me to look through that taught me a lot about both Malware Analysis and general system security in general. So even though I did not manage to install cuckoo correctly, In the future, if i even needed to install a Dynamic Malware Analysis system, cuckoo would be at the top of my list for things to try.

My Experience With AnyRun

Any Run was more or less of an easier piece of Software to learn although, that ended up not being overly helpful to help further my understanding of Dynamic Malware analysis. With AnyRun, there was little documentation, purely because you needed no prior Malware Analysis Experience in order to use it. You just uploaded the executable files to AnyRun, and it ran it and told you if it was malware or not. While this was nice, I couldn't think of a way that i could feasably integrate it into an existing ops system, which was one of the things i was looking for in my malware analysis system

Conclusion

I learnt a fair bit about the usefulness of Malware Analysis Systems, and I now understand the point of using them. This is exceptionally impressive for me as I didn't manage to get a self hosted Malware Analysis System to work. I did not get enough time to give FlareVM a proper trial so I am still unsure what my overall opinion of that is, But i really did enjoy trying to install and use Cuckoo, as there was a lot of information regarding not just how to use it, but on what to expect, and how to use Dynamic Malware Analysis tools in general.