Something Awesome Poster – Rootkits

Coming into this project I had no idea what a kernel was let alone a rootkit. Now the two terms have become so familiar to me it’s so weird to think there was a time I did not know what either meant. I always knew that it was something that I've wanted to do for a long time, but never had the technical adeptness for. But after 3 years of Computer Science study, I felt I was ready to dive into the world of kernels and rootkits. I decided that the best way to go about researching a rootkit, was to also develop one, though not a completely functioning one. I felt that this was okay as long as I understood the concepts behind the functionality of the rootkit. This is exactly what the book provided me with. After studying and understanding every concept, I applied it, by coding programs in the FreeBSD OS. Every single concept was new to me, however my previous study of COMP2121 (Assembly Code) and COMP3331 (Socket Programming) did help a lot in understanding the concepts of x86 call statements and hiding an open TCP-based port.

There were many times where I spent hours trying to understand the examples given and when I finally did, I put them to practice on my own (evidence on open learning page). For example, when learning about system calls and character device modules, I made my own ones. Specifically, I made a character device module that could read and write data to buffers, all in the kernel. Then, when learning about hooking, I found a way to hook the functions of the character device module to do anything I wanted, such as log keystrokes, delete list elements or simply just print a message to the console.

After reading the book, and understanding all the concepts presented, I went into researching a real-world example of where a rootkit was used. I decided on Stuxnet, as it was previously mentioned in the lectures and got my attention straight away as it involved the Israeli and U.S. governments: very exciting stuff. Along the way, I also engaged in activities outside the scope of my proposal. This included tasks such as setting up Samba (the FreeBSD file sharing service), researching on OS theory and many other kernel manipulation tasks

One of the more interesting aspects of my journey was learning how to hide processes. When I learnt that the process list, like the one displayed when using Task Manager, could be appended, I was shocked. It made me think about how easy it would be to fool those who are not extremely adept in computers into being oblivious to a malicious process running on their system. Sure, there were other ways to find a process, for example by its process id, but even this could be hidden (by using removing the processes’ entry in a hash table that is stored in the kernel).

From here on the concepts just got more and more interesting. I learnt that it was possible to hide an open TCP port. This meant that your computer could be sending data on the internet, without you even confirming it, let alone knowing its even happening. It got me thinking on the countless possibilities there are when attempting to attack someone’s PC.

Then I learnt about hooking not only functions, but objects themselves. Something such as a character device itself could be hooked directly, meaning we do not need to go and change its functions. We just need to point the devices’ functions to our hooked functions! So simple yet so awesome.

Undertaking this project gave me a lot of insight into the world of rootkits, the kernel and security in general. There are so many ways to detect a rootkit, but at the same time those ways become public, hackers find a counter-measure. So, it’s just a never-ending race between those in the security industry and hackers. From the knowledge I have gained so far, my next step will be to produce a working rootkit, not on FreeBSD, but on a more commercial OS, such as Windows or Mac. The concepts that I learned are translatable, though obviously not easily, between the FreeBSD OS and other OS's. Overall, this project felt like the beginning for me in my career in security.