Tracking Every Keystroke

Group A

Alex Beuther, Omar Nayfeh, Logan Howard

Introduction:

Throughout this course, we have noticed that there are many resources available on the internet for individuals to learn how to hack, however, there are equally many resources that aid users on how to secure their systems from these attacks. Knowing that technology is becoming more prevalent in this day and age, a recent statistic showed that "61% of hackers begin hacking before the age of 15"(1). When deciding on the topic of this project, we remembered that script kiddies, attackers who lack knowledge necessary to perform the attack on their own, can create attacks that require little to no skill. Therefore, we wanted to replicate an attack that script kiddies could easily achieve and document how easy creating and deploying the attack was. After some research, we discovered that "keyloggers are one of the script kiddies' favorite tools"(2). We became very interested in how keylogging is used and why script kiddies actively deploy it. This is an important topic everyone should be aware of because we need to make sure our systems are secure such that hackers like script kiddies with limited knowledge will not be able to uncover our sensitive information.

Problem Statement:

The problem that we worked on is how to develop and deploy a keylogger that we created through tutorials and manual pages online in order to replicate a keylogger created by a script kiddie. Then, we plan to document how several of our systems would react to a basic keylogger compared to our virtual machines that have little to no protection. The results will show if this piece of software can be detected on our systems as is without any additional protection, such that we can find the vulnerabilities that are present within them. The purpose of this project is to demonstrate that a simple tool script kiddies can use can leave devastating effects that can result in identity theft and financial losses. Therefore, it is a necessity to properly secure our system to fend off these attacks and keep our information safe.

Methodology:

The idea behind this project was to create something that relates to cybersecurity and we felt the most approachable topic for the average person as well as a relatable project would be a keylogger, something most people know but have probably never seen before. The original scope was pretty simple and was just to get a working keylogger. This proved to be quite a challenge as tracking the strokes of a computer can be quite hard when the machine itself is aware you're doing it. Upon studying the pynput and logging manpages we realized that, while complex, the keylogger can be created in a very short amount of condensed code. This meant the scope would justifiably increase in size. The scope then became what can we do with this information that we grab from the keyboard. The keystrokes being gathered were one thing but another would be where we can take them. We decided a good target would be to try to export them to another file. If we can type on our keyboards and generate a file that has all of the keylogged information in it it would be a miraculous feat considering this is what most people would start to consider an effective keylogger that might be used for attack. With the logging import and manpages it is somewhat simple to choose the format we want the keys to be in, this can be anything from a simple message that says '(key) has been pressed" or starting a new line every time they press space. In order to infiltrate one's computer with this keylogger, it can be manually downloaded through a flash drive, or sent through phishing emails and links to download it.

Findings:

- For Alex's computer, overcoming the computer's antivirus was a challenge. The windows machine that was being used was very adamant on removing the code that was trying to be created. It was persistent that we were creating malware and would constantly quarantine and delete the file that was being worked on. This grew to be quite a pain as we cannot even run the code until we create an intentional hole in the computer's firewall to allow for the malware to run on the local machine. Any time a change was made to the file we had to re-edit the firewall to constantly allow the program to run and convince the machine not to quarantine and delete all the work we had been doing. This goes to show that while cybersecurity can often be scary and frightening it also is not as easy for people to be attacked as they think. It took lots of intense labor and searching to even get around our own machines' protection let alone that of someone else's machine.
- For our Linux VM, the keylogger deployed perfectly without any issues. It started to record every keystroke, which means that sensitive information could easily be breached. This was attributed to the fact that the VM does not have any sort of protection such as a firewall or antivirus. Therefore, it is typically unsafe to use a VM for anything that requires sensitive information, and that we must make sure our systems are secure by routinely checking if the antivirus and firewall are actively deployed.

Prevention:

After deploying and discovering the vulnerabilities present within our systems, we have found out that there are multiple ways to secure them. Since we purposefully made a hole within Alex's Windows computer by disabling the firewall and antivirus software, it is a necessity for all Windows users to have both active. It would be good practice to routinely check that they are deployed. As for the Linux VM, there are commands that can be used within the terminal to install and enable firewalls, which would help prevent these attacks from happening. However, the most effective way of deterring such attacks is through education. Everyone should know how to properly secure themselves and understand that phishing emails and suspicious links could cause irreversible damage. There are plenty of resources online to educate oneself such that these attacks can be prevented.

Demo:

https://drive.google.com/file/d/1WlDJeXjNiEVn-c7yCnYRcf0hjlzau6X5/view

Group Work:

- Alex primarily worked on creating the keylogger, deploying it on his system, reporting his findings, and creating a working demonstration for the report.
- Omar worked on writing an introduction and problem statement, deploying the keylogger, and reporting the findings.
- Logan worked on writing about the group work and challenges, deploying the keylogger, and reporting his findings.

Challenges:

- The primary challenge for our group was coordination. We all have different schedules and thus found problems such as being unable to meet for several weeks. Furthermore, with other coursework, we struggled with losing even more free time working on other projects and homework.
- For the project itself, overcoming the computer's antivirus was a challenge. The longest time sink that was invested on the project was getting it to actually run on the computer it is being tested on. The windows machine that was being used was very adamant on removing the code that was trying to be created.
- Another challenge involved finding the information required to create it as with something very broad it was difficult to find the version we wanted to use within our own vision and something our machines could handle.

References:

1. Newman, Simon. “The Rise of Script Kiddies: Where Inexperience Meets Opportunity.” Security Boulevard, 6 Feb. 2023,

https://securityboulevard.com/2023/02/the-rise-of-script-kiddies-where-inexperience-meets-opportunity/.

2. “Ethical Hacking - Keyloggers.” GeeksforGeeks, GeeksforGeeks, 6 Sept. 2022, https://www.geeksforgeeks.org/ethical-hacking-keyloggers/.
3. “Logging Howto.” Python Documentation, https://docs.python.org/3/howto/logging.html.
4. “Pynput Package Documentation¶.” Pynput Package Documentation - Pynput 1.7.6 Documentation, https://pynput.readthedocs.io/en/latest/.