Security Vulnerabilities for Discord

Krista Zargarian
Department of Computer Science, Cal Poly Pomona
Faculty Advisor: Dr. Mohammad Husain, Cal Poly Pomona
Cyber Security Research 2023

Problem

Discord is a popular web and mobile application that uses voice, video, and text chat to communicate with anyone ages 13 and up. However, like most online platforms, Discord is not immune to security vulnerabilities. There are hackers and malicious actors that may attempt to exploit vulnerabilities in Discord's security protocols to gain unauthorized access to user accounts or obtain sensitive information.

Approach

One way to track these potential security vulnerabilities on Discord is to monitor IP addresses that are associated with suspicious activity. To do this, I used Wireshark to capture packets on two virtual machines. Wireshark is a powerful packet sniffing tool that can capture and analyze network traffic, such as IP addresses. I created a "testing" Discord account to send my personal Discord account a text message and track the IP addresses of the activity. By tracking IP addresses, security professionals can identify the geographic location of a user and potentially detect unusual or malicious activity that may indicate a security breach. Wireshark also releases the different protocols that were found in the capture; therefore, I can identify and narrow down what exactly I am looking for. For example, to find the geographic location, I used the filter option in Wireshark and typed in "ip.addr == [IP Address]" syntax. After that, I can right-click on one of the packets and copy as printable text. Then, I opened a web browsers and went to a geolocation service website. I used "https.www.iplocation.net/". This allows for me to receive an approximate geolocation on a map and provide me with details about the location.

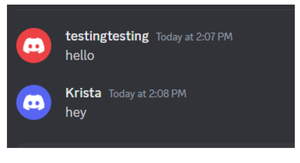

Figure 1: Screenshot of messages between my personal Discord account and "testing" account

Figure 2: Screenshot of geolocation for IP address saying CPP- This is my public IP address.

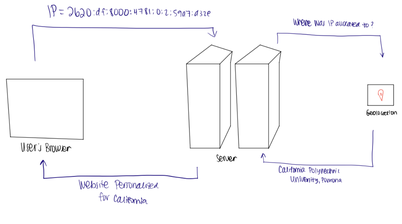

Figure 3: Diagram I drew that represents IP addresses, server, and geolocation

Challenges

One of the challenges that I faced while working on this project was obtaining the right amount of traffic on Discord. Without clearing all search history and data, I saw too many captures and IPs. My goal was to identify the traffic for the text messages in Discord and Discord only.

Another challenge that I faced was finding the geolocations for the IP addresses related to Discord. This was a crucial step for my project, as finding geolocations helped narrow down the suspicious activity within the captures. As we can see in figure 4 below, I took a screenshot of entering in an IP address that I found in the Wireshark capture. We see that it says the location is in San Francisco, CA, and that the ISP is CloudFare Inc., which is an IT company. Also, in figure 5, we see that the IP address I searched the geolocation of says the ISP is Amazon Data Services NoVa in Virginia, which is also suspicious behavior. Figure 6 shows the location in California, and the ISP as Microsoft Corporation.

Figure 4: Screenshot of finding geolocation that was not CPP

Figure 5: Screenshot of finding geolocation that was not CPP

Figure 6: Screenshot of finding geolocation that was not CPP

Conclusion

In conclusion, while Discord is a convenient and popular platform for online communication amongst gamers, streamers, and college students, Discord is not immune to security vulnerabilities. Malicious actors will always be looking for ways to hack and exploit security weaknesses in Discord's protocols to gain that unauthorized access to user accounts or secure sensitive information. However, individuals can take precaution and identify potential security breaches, such as monitoring IP addresses and their geo locations to see if they are associated with suspicious activity. Wireshark is a great tool to be able to do this, along with track network traffic to detect potential security threats.