Phishing

This threat act of trying to steal sensitive information such as usernames, passwords, credit card numbers, and bank account details. Attackers fool victims by masquerading as trustworthy sources with attractive requests like fishermen using bait to catch fish. During my internship, I explored and used a tool called "**Zphisher"** to simulate real-world phishing scenarios. This hands-on experience allowed me to understand how phishing works, from creating convincing fake login pages to observing how attackers capture victims' credentials.

Zphisher Tool

It is an open-source powerful phishing tool. It's very popular now and used to phish Target. There are phishing templates available for 33 popular websites including Facebook, Instagram, Google, Snapchat, GitHub, Yahoo, Netflix, LinkedIn, WordPress, Microsoft, and others. They are making it a versatile tool for cyber attackers. The tool allows users to create and deploy phishing attempts with little technical knowledge.

Here's what appears on the screen when we start Zphisher, as shown in Figure 1. The interface shows a list of phishing attack options, each corresponding to a popular website or service like Facebook, Instagram, Google, and many others. The tool is designed to be user-friendly, allowing us to select your target simply by entering the number associated with the desired service. It also offers additional options like viewing information about the tool or exiting. In this scenario, we choose Instagram which is option “02”.

Figure 1 - Zphisher Interface

The next step shown in Figure 2, is to select the type of phishing page we want to create. There are several options, like a Traditional Login Page, Auto Followers Login Page, 1000 Followers Login Page, and Blue Badge Verify Login Page. In this example, option 01, the "Traditional Login Page," was selected, this means that the tool will create a phishing page that mimics the Instagram login page.

Figure 2 - Page Options

After that, the link "**http://172.0.0.1:8080**" is shown in Figure 3, if we click it, it will direct us to the target fake Instagram Page.

Figure 3 - Fake Link

In this final step, the phishing tool captures the login information entered by the victim. In screenshot 4 shown below, it can be seen that the tool has been able to locate the login details, including the username "MaryamOkaidi" and the password "1230@Maryam". This information is then saved in the file auth/usernames.dat for later retrieval. The tool remains active, waiting to capture more login information until the user manually stops it by pressing it.

Figure 4 - Captured Information

This lab demonstrated the effectiveness of phishing tools like Zphisher in simulating real-world attack scenarios. The practical implementation of creating fake login pages and capturing credentials, it highlighted the simplicity and potential danger of phishing attacks. Such exercises are crucial for developing an understanding of cybercriminal tactics and fostering a proactive approach to cybersecurity. By equipping individuals and organizations with the knowledge to recognize and counter these threats, we can significantly reduce the risk of falling victim to phishing attempts. This lab underscores the importance of continuous education and the adoption of robust security practices in an increasingly interconnected digital landscape.