Project Report

Course: Comp 421-A-Spring_2022

Group Members:

Mahad Rashid Khurshid (22-11108)

Sundas Javaid (19-10685)

Sumera Shafi (231452028)

Penetration testing is important. When you create an exploit or payload and sends it to the target system with different means such as email or social engineering, the antivirus in the target system ends up detecting that payload/exploit and hence the attack is a failure. Hence it is especially important to understand how antivirus software's work and how to evade them. We cannot make 100 % evasion. That is impossible. Here in our project, we will be using signature-based antivirus software. Signature-based detection is a process where a unique identifier is established about a known threat so that the threat can be identified in the future. In the case of a virus scanner, it may be a unique pattern of code that attaches to a file, or it may be as simple as the hash of a known bad file.

So, there are many different types of tools for evading firstly, we tried The Fat Rat but it couldn't be used because its has not been updated for a while. The errors we faced during installation is that the tool was not able to work with the updated Kali Linux libraries then we switched to Lucky Strike and was able to build a payload that can get access to the target machine's directory till the root level but the problem was it could not evade the antivirus.

Lastly, we used Veil Evasion, we have windows 10 running on our target system. our host machine is kali Linux from which we are going to attack. we installed veil evasion apt on kali Linux first. After that, we restarted our system so that there would be less chance of errors. after restarting the system, we opened veil evasion through the command terminal of kali Linux. it showed two options for tools:

- Evasion
- Ordnance

out of these two options, we select evasion tool to further go ahead with our evasion process. it shows the menu of veil evasion. we checked the available payloads by writing list command which displays all the available payloads. we evade windows defender through the payload, but it will fail when it comes to evade other antivirus softwares. we select reverse tcp python. we get our Ip address by writing " ipconfig" in the terminal. we copy our Ip address and write the command for LHOST as: set LHOST Ip-address". then

we press enter. we write another command of generate. the system asks for a name which give of our choice.it then asks for how to create payload executable. we select pyinstaller. it displayed the output folder in the end. we copy that output (executable folder) and paste it to the windows i.e., the system on which attack is to be made. we create reverse tcp file of python for which we use Metasploit. by writing some commands, we select the payload and then we set the lhost and the Ip address we use is the host's Ip address. we run the setup and it started the reverse tcp handler. in the end, just open that output folder that was copied from the kali Linux to the window and one can see that the veil evasion is successfully done without being detected by windows defender.

Link: https://drive.google.com/file/d/1T4w6OEWw6V26Dd_AvHZXZM5DXikrGq7T/view?usp=sharing