Penetration Test Report

Pulkit Sanadhya

14th October 2019

Contents

Executive Summary

Background

The goal of this exercise is to exploit a variety of misconfigurations to contact a host using remote desktop through a pivot,elevate to NT AUTHORITY/SYSTEM, and exfiltrate sensitive data.

Recommendation Summary

The kali attack box will be used for this purpose .

Technical Report

Exploitation

Here , we have to initially log into the machine 172.30.0.3 by using the default credentials .

Now, after changing the NAT setting to port forward on IP 10.30.0.97 , we tried connecting to it using rdesktop from our kali box but we were unable to do it .

So, we can try a different approach and we used msfvenom to create a payload which can be executed on herd.m3g4c0rp.com , the payload is created in /usr/bin/msfvenom .

Now , share that payload to herd using rdesktop .

We used the command mstsc from herd to patronum and hence verified that rdp is working on patronum.
Now, create a payload for reverse tcp handler in the host kali machine using meterpreter multi handler.

Now , execute the payload in herd and create a meterpreter session.

Now, use the portfwd command to forward the port 3389 to patronum from herd by using the following command.

```
portfwd add -l 3389 -p 3389 -r 10.30.0.97
```

Now ,using the command rdesktop 127.0.0.1 on the kali host we were able to connect to the patronum.m3g4c0rp.com

Now continuously pressing shift we were able to access the shell of the machine.

By using the command net user , we were able to see that we are logged into the Local Admin account.

Now, if we have NT AUTHORITY/SYSTEM privilege then by using the PowerUp module we can do privilege escalation and create a new user having LocalAdmin privileges.
We were able to see all the files by using the command dir , after going through different directories we saw file mykeys.txt that we were unable to access , so we used the following commands to do the privilege escalation and take ownership of the file.

TAKEDOWN /F mykeys.txt to take the ownership of the file , however then we used the command ICACLS mykey.txt /grant %username%:F

And, we were able to open the file and see the username and passwords and were able to get the Key 13 :

KEY13:aj/NlP3XbIWdHSrwpM0q7Q==

Conclusion

We were able to achieve the goal successfully and were able to get the key13