Penetration Test Report

Pulkit Sanadhya

7th September 2019

Contents

Executive Summary

Background

The goal of the exercise is to exploit infrastructure configurations.

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 .
rdesktop 172.30.0.3

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, the firm M3g4c0rp should not keep the default credentials on its innerrouter so as to avoid the exposure and a credential change policy should be implemented so as to change passwords in every 90 days.

Conclusion

We were able to successfully exploit the windows misconfigurations.