Penetration Test Report

Pulkit Sanadhya

14th October 2019

Contents

Executive Summary

Background

The goal of this exercise is to exploit a linux machine using a recent linux vulnerability.

Recommendation Summary

The kali attack box will be used for this purpose .

Technical Report

Exploitation

Here , the IP of devbox.m3g4c0rp.com was found to be 10.30.0.32 . So , here we connected to the machine 10.30.0.98 by using the rdesktop command and created a meterepreter session on this machine .

Now , here as as we need to do ssh to the machine devbox.m3g4c0rp.com , we created a port forward in meterpreter session by using the following command.

portfwd add -l 22 -p 22 -r 10.30.0.32

Now , executing the following command on our kali machine:

ssh m.mason@127.0.0.1

and using the password Lambchop928 that we found in the mykeys file in previous exercise , we were able to gain acccess to the machine.

Now, using the following command on the machine

nmap -sV localhost we got to know the services running on the this linux machine which were 22, 53, 80, 631 .

Now, we used the command uname -a to see the linux version which was found to be debian 4.19.37 .

Now, after going through the system files we saw dirtycow and snapd folders we execute the dirty_sock.py file by using the following command :

python dirty_sock.py but we were not able to exploit this vulnerablity in the linux host as it was throwing the error as 401 unauthorized.

Then we observed that the user was allowed to run command ps as a root user , so according to the recent linux vulnerability , we copied the file /bin/bash to /bin/ps by using the following command :

cp /bin/bash /bin/ps

Now, we tried using the command sudo ps and we were able to get root access into the host.
The vulnerability was found to be CVE-2019-14287 which is exploited by bypassing security policies in sudo.

Conclusion

We were able to successfully access the system devbox.m3g4c0rp.com and get the root access.