Penetration Test Report

Pulkit Sanadhya
Exercise 8

22th September 2019

Contents

Executive Summary

Background

The goal of the exercise is to Exploit a buffer vulnerable program. and use fuzz testing and make logical inferences

Recommendation Summary

The kali linux box will be used to achieve the above goal.

Technical Report

Information Gathering

Active intelligence

Now , here as per our requirement , we are supposed to perform nmap scan on the IP www.m3g4c0rp.com so as to check the services running on the target machine .

nmap -sV www.m3g4c0rp.com

Now , we can see all the services running on the given host . The services were found to be DNS,http,SSH . However we observed one more service on port 1337(waste).

Vulnerability assessment

Technical Vulnerability

As per the problem only the username is required to log into the target machine on the port 1337 , which can be assumed as a critical vulnerability and we will move forward towards exploiting that vulnerability as a part of our assessment.

Exploitation

Target selected for exploitation

In the reconnaissance phase we observed that port 1337 was hosting a service WASTE.Now , using the netcat command so as to connect to the host on the port 1337,

netcat www.m3g4c0rp.com 1337

As per the problem statement only the username was required to login into the server .So , after using a large number of passwords , we used brian as a username and we were able to get shell access to the system .

Post Exploitation

It was observed that we were able to get access into the system but it was observed that the incorrect username that we used before providing the correct username has overwritten the commands that we can execute after getting the shell access.

Conclusion

Finally,we were able to exploit the buffer program on the port 1337.