Penetration Test Report

Pulkit Sanadhya

26th September 2019

Contents

Executive Summary

Background

The goal of the exercise is to get acquainted with netcat pivots by connecting to plunder.pr0b3.com

Recommendation Summary

The kali attack box will be used for this purpose along with the netcat utility.

Technical Report

Post-Exploitation

Now , using the kali linux , we can connect to the guest account of plunder.pr0b3.com by using the following command.

ssh guest@plunder.pr0b3.com

Now , using the password as guest , we are able to gain access to the machine.

The command ip show link was used to display all the active ethernet links which were found to be lo, ens160, ens33.

The interface ens160 was found to be having an IP address of 192.168.200.13/24 by using the command ip addr show.

Now , running the nmap utility for the network 192.168.200.0/24 , we were able to find another live host in the same network whose IP address was found to be 192.168.200.67.

Using nmap -sV -p80 192.168.200.67 we were able to see that the port 80 was found to be open on the host, hence verifying that port 80 is open on target machine.

Now , using netcat to connect to the machine on port 80 we had to create a pipe on plunder.pr0b3.com using the following command. .

mknod mypipe p

nc -l -p 2019 mypipe || $nc \quad 192.168.200.67 \quad 80\ mypipe$

Now, after opening firefox on our kali host and by typing the following URL 45.79.141.1:2019 we were able to connect to the web application of the host 192.168.200.67.

Conclusion

We were able to successfully use the netcat pivots.