Penetration Test Report

Pulkit Sanadhya

15th September 2019

Contents

Executive Summary

Background

The goal of this exercise is to use nmap to explore the services available on the domain www.m3g4corp.com.

Recommendation Summary

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

Technical Report

Information Gathering

Active intelligence

Now , as per out requirement we are supposed to find the active ethernet ports that we will be listening to so as to capture the traffic going through that port using wireshark. So after giving the following command in kali CLI : ip a , we were able see that we can use the active ethernet port eth0 for listening to the network traffic.

We can open a parallel terminal window and fire up the wireshark window to analyze the packets going through eth0 port.

Now , we can use nmap to scan the give domain using the command in TCP mode :

nmap -T4 -O -V -sT www.m3g4c0rp.com

Now , we can easily se multiple services running on the host such as ssh(22) , dns(53) , http(80) , http-proxy(8080) along with their service versions and it was found that it was running the OS : Linux4.4 .

It was observed that ssh was running on version openSSH 7.9 p1 which was found to be vulnerable according to CVE-2018-15919.And no exploit was found on internet for this vulnerability. It was found that port 80 was running on the service version Apache httpd 2.4.38 and the vulnerabilities for this version were found to be CVE-2018-17199 ,CVE-2018-17189 and no exploits were found for these vulnerabilities . It was found that the port 8080 was running on service version Nginx 1.3.9 which was found to be vulnerable according to CVE-2017-7529 and no exploit was found for this vulnerability. Wireshark is used to analyse the behavious of network .

Now nmap scan was used in UDP withe help of following command: .

nmap -sU -p1-256 www.m3g4c0rp.com
We found that UDP port 40 and 53 were open . However an open UDP port 40 looks like an oddity .
It was observed that nmap when scanned in UDP mode took much more time than in TCP mode. However ,nmap TCP scanned more ports than nmap UDP mode.

Conclusion

Finally we were able to get ourselves familiarized with nmap along with getting familiarity with the services running on the target domains and the vulnerabilities associated with the service version.