Penetration Test Report

Pulkit Sanadhya

17th September 2019

Contents

Executive Summary

Background

The goal of this exercise is to use openVAS utility to run scan agains the intended target.

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 Start OpenVAS and then create and run a new scan to check 172.24.0.42 for vulnerabilities

Now , we can use the command openVAS to open the openVAS terminal and set the target as 172.24.0.42.

openvas-start

Now , we can easily see multiple vulnerabilities that exist on the target system.On having a closer look we found that the host had vsftpd compromised source packages vulnerability .

Now, we can run the metasploit console by using the command msfconsole.

We found that metasploit has VSFTPD 2.3.3 module for this specific vulnerability. Now using this exploit in metasploit and using a specific payload and setting the options , finally running the exploit.

Now, wireshark was opened in a parallel window and the traffic behaviour was observed.

Now, using follow TCP stream on a FTP packet , we observed that the username was found to be R9Au:) and the passwordd was found to be DRFEJK.
Now , here by using openVAS scanner we were able to find the vulnerability vsftpd in the destination host . In this vulnerability the backdoor payload is initiated in response to a :) character combination in the username which we observed in out packet capture process which also represents a smiley face. By exploiting this vulnerability the user can gain access to the destination

machine remotely. The effective mitigation to this vulnerability will upgrading the software to latest version.

Conclusion

Finally we were able to get ourselves familiarized with openVAS and metasploit .