Penetration Test Report

Pulkit Sanadhya

19th September 2019

Contents

Executive Summary **2**

Background 2

Recommendation Summary 2

Technical Report **2**

Information Gathering 2

Active intelligence 2

Conclusion **3**

Executive Summary

Background

The goal of this exercise is to use metasploit to gain shell access to a machine and get experience with meterpreter .

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 used the command nmap -A 172.24.0.42 , and found the different services runnning on the host. Now , we can see all the services running on the given host . The services were found to be DNS(53),http(80) which had a version nginx,SSL(443) version was found to be nginx.

We have to use the command openVAS-start to open the openVAS terminal and set the target as 172.24.0.42 directed towards the port 8180 running the tomcat application.

We were able to see multiple vulnerabilities on the target machine and one of them was found to be Apache tomcat server administration unauthorized access vulnerability.

Fire up the metasploit console by using the command msfconsole .

Now search the module related this particular vulnerability by using the command .

grep exploit search tomcat

Now, we can see a number of modules pertaining to tomcat , we need the module that would provide the remote access to our host . So, we used the module tomcat mgr deploy for this specific purpose and the following commands were used to set the host and target port.

set rhost 172.24.0.42
set port 8180

Now, after setting the suitable payload , giving the command exploit to exploit the vulnerability and giving the user as tomcat and password as tomcat , we were able to remotely log into the machine . And after logging into the machine we can easily download the files we are interested using the meterpreter prompt.

This vulnerability allows an attacker to upload and execute arbitary code which in turn compromises the whole machine. The mitigation step would be to apply the latest patches and updating the software from trustful sources .

Conclusion

Finally we were able to get ourselves familiarized with metasploit and get experience with meterpreter