Penetration Test Report

Pulkit Sanadhya

10th December 2019

Contents

Executive Summary

Background

Here , the below penetration report concises all the findings on various penetration testing activities done on the m3g4c0rp network , which are included and segregated in the technical report section accordingly .

Recommendation Summary

Here we have used multiple tools such as kali linux , fierce , cewl , arpspoof, whois , metasploit , meterpreter , BeEF , laudanum , john the ripper , amass etc to achieve our intended goal.

Technical Report

Information gathering

Active Intelligence

Initially in the exercise 1, as the problem statement asserts that KEY003 can be found as a part of the filename in the file system which gives us a clue for proceeding further.So , all we needed was to run the command find for KEY003.
So, finally we were able to find the required key by using that and the required key was :
KEY003:3UXthL6E+G4Y1S5qfKjdFw

According to the problem statement we can easily deduce that we need to find a process and search that process for the key so we have to use the command ps aux to list all the processes and we have to use grep command also along with it to find all the processes having the string key as a part of their name. So , after giving the following command: ps aux (piping operator) grep key. We observed the output where the process name and hence the required key was found to be :
KEY002:/LL10yxHS/CxSf93wVHelg

Now , as per exercise 2 initially we need to log into our kali attack machine with the help of provided credentials , and as per the problem statement we have to run fierce dns scanner against the domain m3g4c0rp.com which can be done by using the following command : fierce -dns m3g4c0rp.com -threads 10 .Now,we used cewl to create a new wordlist and then we used fierce and were able to find the key005 as FhgkymHrtGwaRWKlfsXdlg ;

Now , as per out requirement in exercise 3 we found the active ethernet ports that we will be listening to so as to capture the traffic going through that port using wireshark , so we were able to capture the key 004 by using this as:

KEY004 : vBqFyfr

Now as per the requirement of exercise 5 we used nmap against www.m3g4c0rp.com to took for vulnerabilities .

Now, as per the requirement of exercise 6 used OpenVAS and then created and ran a new scan to check 172.24.0.42 for vulnerabilities.

Here as per exercise 8 we performed nmap scan on the IP www.m3g4c0rp.com so as to check the services running on the target machine and services were found to be DNS,http,SSH . However we observed one more service on port 1337(waste).

Vulnerability assessment

Technical Vulnerabilities

After doing nmap on m3g4c0rp.com as dictated by exercise 5 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.

As per the exercise 6 We were able to find the vulnerability vsftpd in 172.24.0.42 . 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.

As per exercise 7 we used the command openVAS-start to open the openVAS 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.

As per exercise 8 only the username is required to log into the target machine www.m3g4c0rp.com on the port 1337 , which can be assumed as a critical vulnerability.

As per exercise 12 , we used the firefox on our kali host and directly connect to 172.30.0.3 using the username as admin and password as pfesense , which is a critical misconfiguration and a major vulnerability that can be exploited.

Exploitation/Vulnerability Confirmation

Timeline

The exploitation was done during the in class exercises of the Penetration Testing course between 26th August to 10th December

Exploitation Targets

As per exercise 7 we used metasploit to target the tomcat server administration unauthorized access vulnerability to gain access to the server 172.24.0.42 .

As per exercise 8 we used netcat command so as to connect to the host on the port 1337 of www.m3g4c0rp.com . Now 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 .

As per exercise 10 we connected to the guest account of plunder.pr0b3.com .Now , using the password as guest , we were able to gain access to the machine.

As per exercise 12 , we used the firefox on our kali host and directly connect to 172.30.0.3 using the username as admin and password as pfesense.

Now following up on exercise 12, after going to the command line of the account in herd.m3g4c0rp.com we exported the PowerUp module to herd and created a user with username john and password Password123! and were able to find the key KEY011:!y x06 x0b8 := x19 x1a x07 x1c=4 1c*?500

As per exercise 15 we used msfvenom and meterpreter portforward to forward the port 3389 to patronum and after pressing the shift key for 5 times we were able to get access to the machine , so the machine is prone to sticky key vulnerability.

As per exercise 16 , we observed the linux sudo vulnerability CVE-2019-14287 in devbox sudo version which allows the non-privileged user to gain the root access .

As per exercise 18 we observed a http landing page for the https requests on ns.m3g4c0rp.com which allows the hacker to steal the credentials.

As per the exercise 19 we exploited the php vulnerability in www.m3g4c0rp.com/brian which allowed only jpg and png images to be uploaded by we uploaded the shell.php by obfuscating it as a jpg and gained shell access to the system and were able to get the confidential details as
KEY019:vBA+ Y/x7fG/x1cug/x7fP/x1cI/x0f//x06y@./x0a

As per the exercise 20 we tested the effectiveness of the wireless routers placed in m3g4c0rp.com and found out that the network was susceptible to MITM , so we started the fake access point and were able to find the
KEY20:uPPltoxqT1Uuj3jXmPeAuw==

Post Exploitation

As per exercise 7 , we were able to copy the shadow file from the 172.24.0.42 host to our kali host .

As per exercise 9 Now , we used john the ripper to crack passwords found in the shadow file which were found to be batman,123456789, postgres, user,service etc . However even after using rockyou password file passwords were still pending to be cracked.

Now following up on exercise 13 , we used veil to create a meterpreter session between kali host and herd.m3g4corp.com and used it do tcp port scan on patronum.m3g4c0rp.com.

As per exercise 15 , after gaining access to patronum we located the file mykeys.txt and opened it to find the passwords and
KEY13:aj/NlP3XbIWdHSrwpM0q7Q==.

As per exercise 16 , we created a meterpreter session between kali and devbox and used portforwarding to connect to devbox via rdp using the password that we found in the mykeys.txt file in exercise 15 and using the linux vulnerability CVE-2019-14287 we gained root access to the system.

As per exercise 17 we used BeEF to capture browser information of the target host 172.30.0.128 and were able to get the key as
KEY015:wwmUyrUpOB8Q7km0zCtnSQ==

As per exercise 18 we used ssl strip along with arpspoof where the client was identified as 172.30.0.128 while the server was found to be 172.30.0.128 to gather vital information using tcp dump and found
KEY 17:WaGco/h+g7lEQAk0Ey1Clg==
KEY16:v6lF0fAFjWbqkW0GrzdjuQ==

Conclusion

Hence , we were able to test the m3g4c0rp network against a wide variety of parameters. We found out that many devices are susceptible to a number of severe vulnerabilities which we demonstrated by exploited them. These systems are required to be patched as soon as possible in order to prevent any potential loss of information.