Penetration Test Report

Pulkit Sanadhya

12 September 2019

Contents

Executive Summary

Background

The goal of this exercise is to get familiarized with wireshark.

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 traceroute and see the packets going through the terminal using the command :

traceroute -I plunder.pr0b3.com

Now , we can see a large number of ICMP packets traversing through the network as we have used -I to elicit this particular behaviour.
So , after traversing through a number of these packets ,we came to know the required key KEY004:vBqFyfr .

A large number of ICMP packets were found in this process where the Source IP's were found to be 45.79.141.233 , 282.158.115.1 ,172.24.0.1 and the destination IP's were found to be 172.24.0.10 , 172.24.0.1 .

The TTL field was found to be 64 . So , we can infer that the number of hops before which the communication halts is 64 . It was observed that most of the communication took less than 64 hops .Traceroute sends 3 ICMP packets with an increasing TTL starting from 1 till the destination is reached. Here initially the source sends 3 ICMP packets with a TTL 1 , so the packet returns a destination unreachable message along with the 1st hop IP address , then it sends 3 ICMP packets along with the TTL of 2 , so again the error message destination unreachable observed along with the IP address of the second hop address. Finally, the it sends 3 ICMP with a TTL of 3 and finally the host responds with an ECHO REPLY. So , it was able to find the destination host successfully.

Finally , after using traceroute against ns.m3g4c0rp.com the gateway was found to be 172.24.0.1 and the destination was found to be 172.30.0.128 .

Passive Intelligence

Now , after providing the command
traceroute –help 2¿1 — less to the kali CLI , we landed to the manual page and observed that here 2 and 1 represents the file descriptors , as a descriptor is assigned to every open file which defines their location , so here 1 represents the file descriptor for standard output(stdout) and here 2 represents the standard error (stderr) , so here 2¿1 signifies that the contents of standard error is overwritten on the location where standard output is defined .

Conclusion

Finally we were able to get ourselves familiarized with wireshark along with having a basic overview of wireshark and traceroute commands , hence we able able to successfully find KEY004:vBqFyfr