Penetration Test Report

Pulkit Sanadhya

8th September 2019

Contents

Executive Summary

Background

The primary goal of this exercise is to get hands of experience with DNS reconnaissance, the fierce domain scanner, forward and reverse lookups and CeWL.

Recommendation Summary

The kali linux attack machine will be used to perform the required operation using multiple linux commands in the CLI.

Technical Report

Information Gathering

Active Intelligence

Now , 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 .
```

Here , we used - threads 10 to expedite the scanning process.

which resulted in the following output :

```
172.30.0.128    ns.m3g4c0rp.com
172.30.0.130    mail.m3g4c0rp.com
10.30.0.90      pdc.m3g4c0rp.com
172.30.0.128    pop.m3g4c0rp.com
172.30.0.128    www.m3g4c0rp.com
```

Now, after going through the source code of fierce we found that the wordlist is stored in "hosts.txt" at the path usr/share/fierce and we found that the words ns,mail,pdc,pop were already included in fierce's wordlist.

Now , after using the cewl command on kali linux box as follows :

cewl wordlist.txt m3g4c0rp.com we created a new wordlist .
Now , after running the following command taking wordlist as a parameter :

```
fierce -dns m3g4c0rp.com -wordlist wordlist.txt
```

we were able to find the KEY005 as FhgkymHrtGwaRWKlfsXdlg .

So, finally we can affirm that the required key is:
KEY005:FhgkymHrtGwaRWKlfsXdlg

Conclusion

So , it can be concluded that we were successfully able to find the required key *KEY005:FhgkymHrtGwaRWKlfsXdlg.* as per the problem statement.