

Ex030 - DNS Reconnaissance

Simon Tobon

2021-07-08

Contents

Executive Summary	2
Attack Narrative	2

Executive Summary

The goal for this exercise was to experience DNS reconnaissance by deploying the fierce domain scanner. The f4rmc0rp.com domain was scanned first using the fierce built in wordlist. We then generated a new wordlist using CeWL. This word list was piped into Fierce and the domain was then scanned again. We found several hostnames using these processes. Finally, the amass domain scanner was deployed and the results were compared to the results we found earlier using Fierce.

Attack Narrative

To begin, the fierce domain scanner was deployed to scan the f4rmc0rp.com domain. This was done by running the `fierce -dns f4rmc0rp.com` command. The following IP address blocks appeared as a result:

```
172.30.0.128 ns.f4rmc0rp.com
172.30.0.130 mail.f4rmc0rp.com
10.30.0.90 pdc.f4rmc0rp.com
172.30.128 pop.f4rmc0rp.com
172.30.0.128 www.f4rmc0rp.com
```

We then located the fierce wordlist. This was found in `/usr/share/fierce/hosts.txt`. All 5 of the domain names listed above can be found in the fierce wordlist. I confirmed this by using the `grep` command several times, as documented below:

```
grep -w ns /usr/share/fierce/hosts.txt
grep -w mail /usr/share/fierce/hosts.txt
grep -w pdc /usr/share/fierce/hosts.txt
grep -w pop /usr/share/fierce/hosts.txt
grep -w www /usr/share/fierce/hosts.txt
```

There were results for each `grep` which confirmed that the keyword/hostname was in fact in the wordlist generated by fierce. This means that fierce found these hostnames by traversing the wordlist.

The next step taken was to use CeWL to generate an alternate wordlist to be used with fierce to see if anymore hosts could be found, as opposed to using the default wordlist. This was achieved by running the following commands:

```
cewl http://www.f4rmc0rp.com -d 3 -o -w ex-wordlist
```

This generated the wordlist to be used in fierce. We then pipe this wordlist through fierce by running:

```
fierce -dns f4rmc0rp.com -wordlist ex-wordlist This outputs:
```

```
10.30.0.97 patronum.f4rmc0rp.com
10.30.0.98 herd.f4rmc0rp.com
10.30.0.102 KEY005-IHIHIWJRhzMTH4qXCCw0uA.f4rmc0rp.com
```

Fierce found the patronum hostname by using the wordlist generated by CeWL. It then searched +- 5 in the last octet and found herd and KEY005. It is

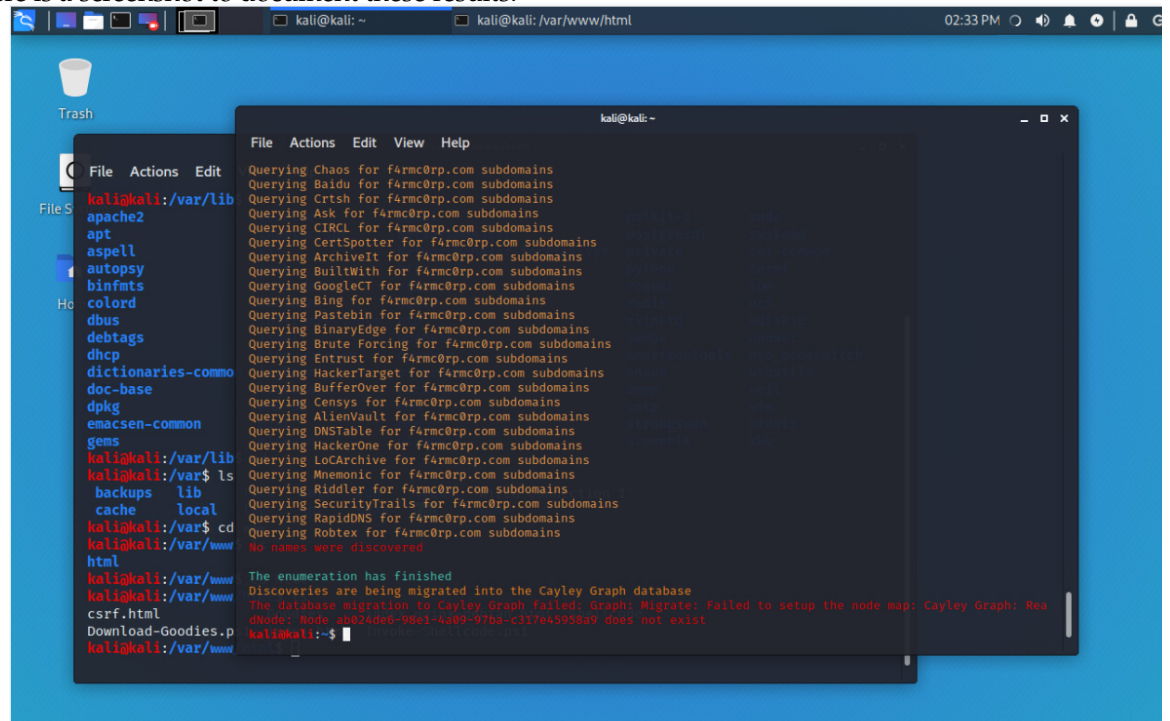
important to note that we could've found these with the default wordlist if we simply added `-traverse` to specify `fierce` to search a wider IP range.

Finally, we ran `amass` to see if there would be greater results. However, after about an hour of running 2 `amass` commands neither yielded results. Both of the following commands were run:

```
amass enum -d f4rmc0rp.com
```

```
amass enum -d f4rmc0rp.com -brute
```

Here is a screenshot to document these results:



```
kali@kali: ~  
File Actions Edit  
Querying Chaos for f4rmc0rp.com subdomains  
Querying Baidu for f4rmc0rp.com subdomains  
Querying Crtsh for f4rmc0rp.com subdomains  
Querying Ask for f4rmc0rp.com subdomains  
Querying CIRCL for f4rmc0rp.com subdomains  
Querying CertSpotter for f4rmc0rp.com subdomains  
Querying ArchiveIt for f4rmc0rp.com subdomains  
Querying BuiltWith for f4rmc0rp.com subdomains  
Querying GoogleCT for f4rmc0rp.com subdomains  
Querying Bing for f4rmc0rp.com subdomains  
Querying Pastebin for f4rmc0rp.com subdomains  
Querying BinaryEdge for f4rmc0rp.com subdomains  
Querying Brute Forcing for f4rmc0rp.com subdomains  
Querying Entrust for f4rmc0rp.com subdomains  
Querying HackerTarget for f4rmc0rp.com subdomains  
Querying BufferOver for f4rmc0rp.com subdomains  
Querying Censys for f4rmc0rp.com subdomains  
Querying AlienVault for f4rmc0rp.com subdomains  
Querying DNSTable for f4rmc0rp.com subdomains  
Querying HackerOne for f4rmc0rp.com subdomains  
Querying LoCArchive for f4rmc0rp.com subdomains  
Querying Mnemonic for f4rmc0rp.com subdomains  
Querying Riddler for f4rmc0rp.com subdomains  
Querying SecurityTrails for f4rmc0rp.com subdomains  
Querying RapidDNS for f4rmc0rp.com subdomains  
Querying Robtex for f4rmc0rp.com subdomains  
No names were discovered  
The enumeration has finished  
Discoveries are being migrated into the Cayley Graph database  
The database migration to Cayley Graph failed: Graph: Migrate: Failed to setup the node map: Cayley Graph: Rea  
dnode: node-9b024de0-98e1-4d89-97ba-c317e45958a9 does not exist  
kali@kali:~$
```

After some syntactic repairs we find the KEY for the exercise: **KEY005:IIHIWJRhzMTH4qXCCw0uA==**.

Having access to many subdomain names within a hostname can lead to serious security issues. These can be traced back to the origin and can be compromised, kidnapped, and even shutdown.