Ex030

Joshua Main-Smith

2020-09-24

Contents

Executive Summary

Background

We scanned the domain for hosts for a general vulnerability assessment. The scans we performed looked for any sensitive information that is possibly being leaked, crawled through the hosts in search of key words that could aid us, and took note of any vulnerable hosts.

Risk Ranking/Profile

Based on the DREAD model presented below, the overall risk rating is currently **Medium**.

General Findings

We found several domains by doing a generic search, a wordlist search generated from a webiste crawl, and a leaked subdomain that's possibly not meant for the public eye.

Recommendation Summary

It is recommended to configure or deregister any networks that are leaking internal IP address spaces.

Technical Report

Risk Assessment

Damage Rating - Medium

A misconfigured network could be subject to a subdomain takeover and used as a pivot point for other hosts for interested parties in gaining access to sensitive information, if not already present on the initial one.

Reproducibility Rating - High

Over the past week of testing, the steps taken in discovering these hosts have been reliably reproduced.

Exploitability - Low

Being a reconnaissance test, there were no exploits performed. But, the findings produced from our reconnaissance could aid in exploitation and sought out by malware writers.

Affected Users - Low

User information and resources contained under the vulnerable hosts could be affected

Discoverability - Medium

The subdomains **ns, mail, pdc, pop, www** were found with a simple domain scan. Three others, **patronum, herd, KEY005-IHIHIWJRhzMTH4qXCCwOuA**, were found by generating a wordlist. Then three more were found, **innerrouter, devbox, linuxserver**, were found performing a scan of the entire class C network.

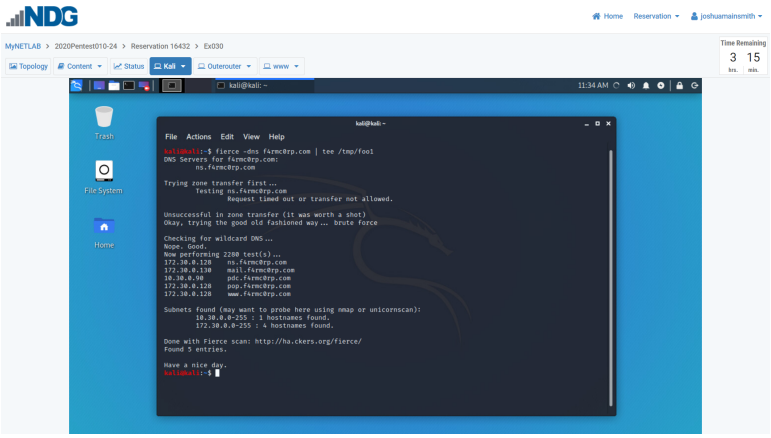
Vulnerability Description

There is a potential misconfigured network that is leaking an internal address space. Particularly, KEY005-IHIHIWJRhzMTH4qXCCwOuA.f4rmc0rp.com. This could be due to forgetting to configure or deregister from a 3rd party server.

Attack Narrative

Host Detection Using Fierce

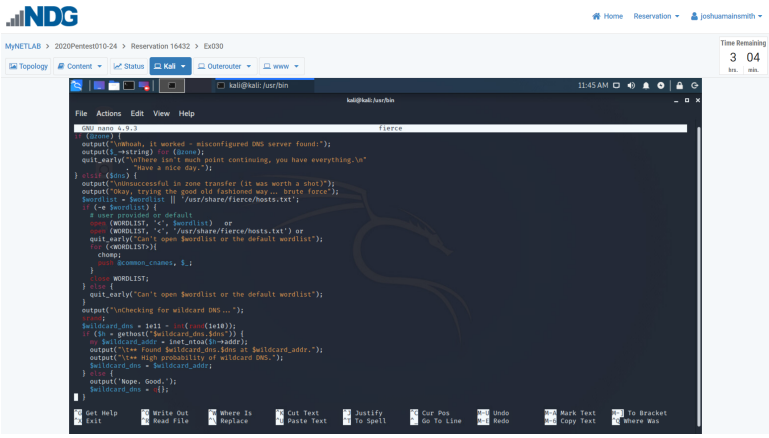
To start, we began scanning the f4rmc0rp.com domain to get an idea of the IP address blocks supported under F4rmc0rp. The command we used was **fierce -dns f4rmc0rp.com | tee /tmp/foo1**.



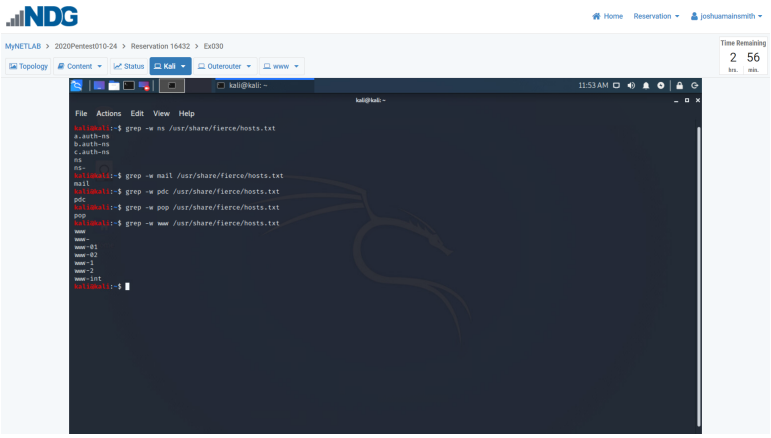
As can be seen in the image above, the IP blocks for the f4rmc0rp.com domain are:

Subdomain	IP Address
ns	172.30.0.128
mail	172.30.0.130
pdc	10.30.0.90
pop	172.30.0.128
www	172.30.0.128

To determine which of these hosts were found using fierce's builtin wordlist, we had to look into the source code. As can be seen in the image below of the source code, $wordlist indicates that it's located under **/usr/share/fierce/hosts.txt**.

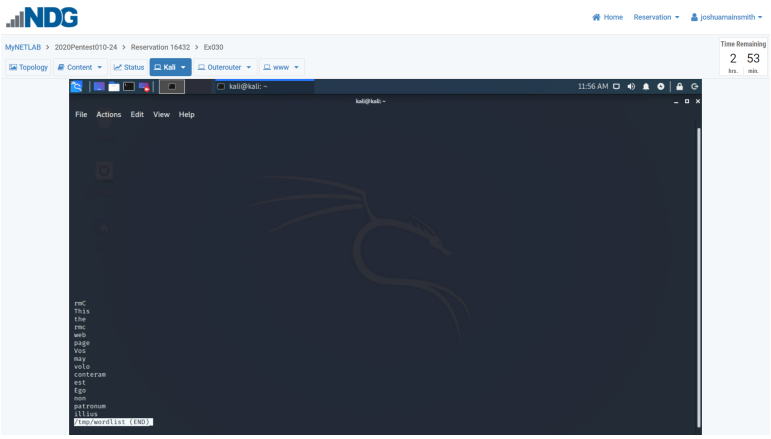


In determining which hosts were found by using fierce's wordlist, it was a simple manner of grepping each subdomain name to the terminal if it's located in the *hosts.txt* file, using the command **grep -w** ***subdomain*** **/usr/share/fierce/hosts.txt**, where the **-w** flag searches for the exact string. The results of this can be seen in the image below, which shows that all of the hosts found were contained in the wordlist. Meaning, the method to which fierce found all of the hosts here was from the wordlist.



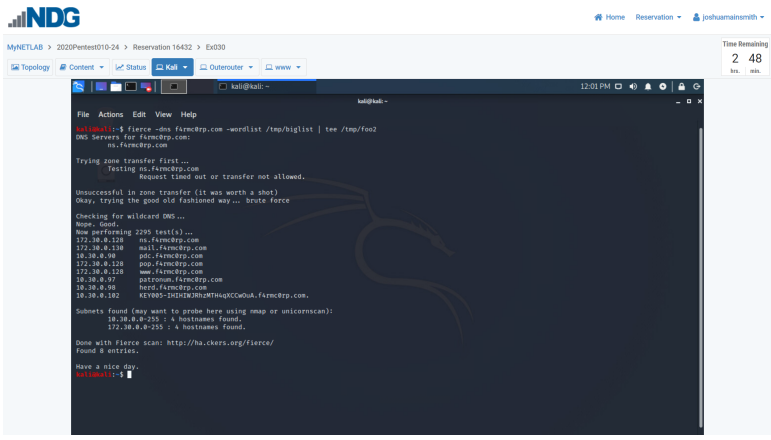
Utilizing Cewl

Adding commonly used words found on the domain may be a good way to find other hosts that weren't initially found by fierce. Using cewl crawls through a given domain and does exactly this. The command we used to do this is **cewl https://www.f4rmc0rp.com -d 3 -w /tmp/wordlist**. The **-d 3** flag tells cewl to scan three levels deep with the given domain and is saving the results to a file called **wordlist**. A list of words that cewl saved is shown in the image below.

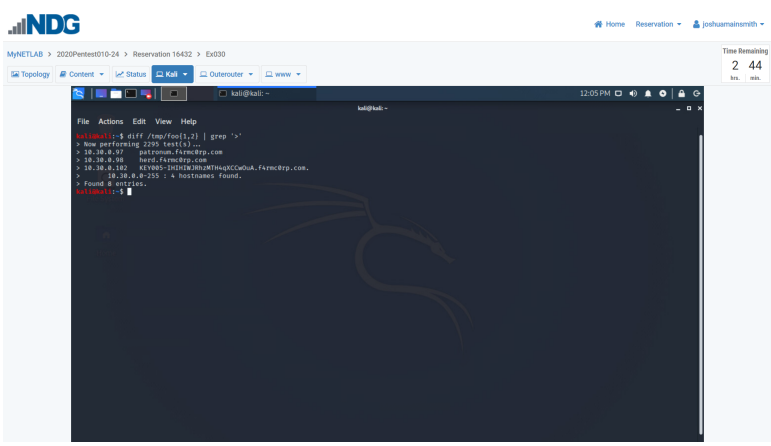


We the concatenated the two wordlists (fierce's and the one generated by cewl) into a larger wordlist to do a new fierce scan utilizing this larger wordlist. Specifically, the command we used was **cat /usr/share//fierce/hosts.txt /tmp/wordlist ¿biglist**. We then ran fierce again with the new wordlist by using **fierce -dns f4rmc0rp.com -wordlist /tmp/biglist | tee /tmp/foo2**. The result of which can

be seen in the image below.



If we would like to see which hosts were found by cewl that weren't found by fierce, we could look at the difference between the two generated files **foo1** and **foo2** by using the shell command **diff /tmp/foo**{**1,2**} | **grep '>'**. This greps only the differences present for the right file (i.e. foo2). The hosts found due to cewl's crawling can be seen in the image below.



Something interesting about this list is that one of the hosts, KEY005, wasn't included in the wordlist of terms cewl found earlier. This is because, along with fierce's wordlist it also scans non-contiguous address spaces that match the pattern of whatever domain it's scanning for. It attempts to locate likely targets that are suspected to be part of the corporate network. While scanning, sometimes fierce will find misconfigured networks that leak internal address

spaces. Here are the IP adresses of the new subdomains found by fierce utilizing cewl's wordlist:

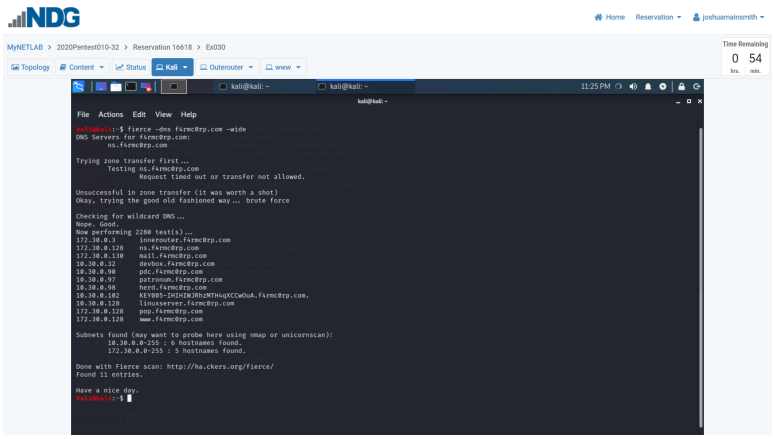
Subdomain	IP Address
patronum	10.30.0.97
herd	10.30.0.98
KEY005-IHIHIWJRhzMTH4qXCCwOuA	10.30.0.102

Something to note here is that each of these IP address spaces are close to each other, so fierce probably followed the pattern from patronum to herd and continued searching up address spaces until it found KEY005. More information on this topic can be seen here.

Additionally, since this is the KEY005 that we were meant to look for, it follows that the value of the key (after some syntactical reconfiguration) is: *KEY005:IHIHIWJRhzMTH4qXCCwOuA==*.

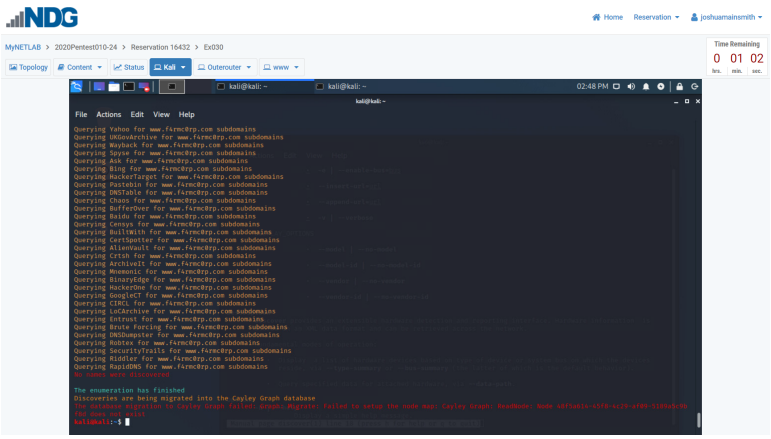
Alternative to Cewl

Although the wordlist generated from cewl is useful, an alternative to use is the **-wide** flag with fierce. This is a noisier method in scanning, but was useful in uncovering more hosts. It works by scanning the entire class C network and returning any hosts it finds. The entire command is **fierce -dns f4rmc0rp.com -wide**. As can be seen in the image below, all the hosts found from cewl's wordlist have been found again along with a few more (innerrouter, devbox, linuxserver).



Comparing Amass

We also used amass to search for hosts and compared these with the fierce and cewl combination. To get amass started, we used the linux command **amass enum -d f4rmc0rp.com | tee /tmp/foo3**. This took longer than expected, but when it finally finished we found that there were no names found either in the terminal or in the foo3 file generated. This can be seen below.



The enumeration flag performs network mapping and DNS enumeration of systems connected to the internet. Perhaps the network we were testing on was an internal network, having no connection to an external network.

Zoom Link

September 22, 2020