Penetration Test Report Title

Gary Jones

Contents

Executive Summary

Summary of Findings

KEY005-TrvlNmWThZ4Aj2EDyYQx1A

Recommendation Summary

Technical Report

Vulnerability Description

There appears to be two IP addresses that may be intended to remain private currently publicly available which were identified using a wide traversal of IP addresses with fierce. These domain addresses are: ceo.artstailor.com and devbox.artstailor.com.

Attack Narrative

Task 1

Utilizing the fierce –domain artstailor.com command I was able to identify 6 hosts associated with the artstailor.com domain (see figure 1):

1. ns.artstailor.com
2. mail.artstailor.com
3. innerouter.artstailor.com
4. pdc.artstailor.com
5. pop.artstailor.com
6. books.artstailor.com

Task 2

Utilizing the same command as in Task 1 I was able to identify a similar amount of IP address blocks (see figure 1):

1. ns.artstailor.com: 217.70.184.38
2. mail.artstailor.com: 217.70.184.3
3. innerouter.artstailor.com: 217.70.184.3
4. pdc.artstailor.com: 10.70.184.90
5. pop.artstailor.com: 217.70.184
6. books.artstailor.com: 10.70.184.91

Task 3

Utilizing Github the wordlist was identified as default.txt and is located in the directory: fierce/fierce/lists/default.txt

Using the same command as in Task 1 and 2 and comparing the output with the default.txt I was able to determine that the following domains were found because of the words identified in the default.txt:

1. ns.artstailor.com
2. mail.artstailor.com
3. innerouter.artstailor.com
4. pdc.artstailor.com
5. pop.artstailor.com

Task 4

Utlizing the cewl command in linux and creating a separate wordlist I ran the command 'fierce –domain artstailor.com –subdomain-file word.txt' and identified the following additional hosts (see figure 2):

1. costumes.artstailor.com
2. linuxserver.artstailor.com
3. KEY005-TrvlNmWThZ4Aj2EDyYQx1A.artstailor.com

Task 5

See below for an explanation of how fierce identified each host name:

1. ns.artstailor.com: this was identified by the default wordlist
2. mail.artstailor.com: this was identified by the default wordlist
3. innerouter.artstailor.com: this was identified by the IP address being close to the mail.artstailor.com host
4. pdc.artstailor.com: this was identified by the default wordlist
5. pop.artstailor.com: this was identified by the default wordlist
6. costumes.artstailor.com: this was identified by the custom wordlist
7. linuxserver.artstailor.com: this was identified by the IP address being close to the costumes.artstailor.com host
8. KEY005-TrvlNmWThZ4Aj2EDyYQx1A.artstailor.com: this was identified by the IP address being close to the costumes.artstailor.com host
9. ceo.artstailor.com: a wide traversal of IP addresses
10. devbox.artstailor.com: a wide traversal of IP addresses

While each of these hosts were identified through either the default wordlist or by having their IP address be in close proximity to one of those hosts another way to find those address is to search for a wider range of ip addresses through the command 'fierce –domain artstailor.com –traverse 255' (see figure 3).

Task 6

By using the dnsmap commands with the default wordlist and custom wordlist the following hosts were identified (see figures 4 and 5):

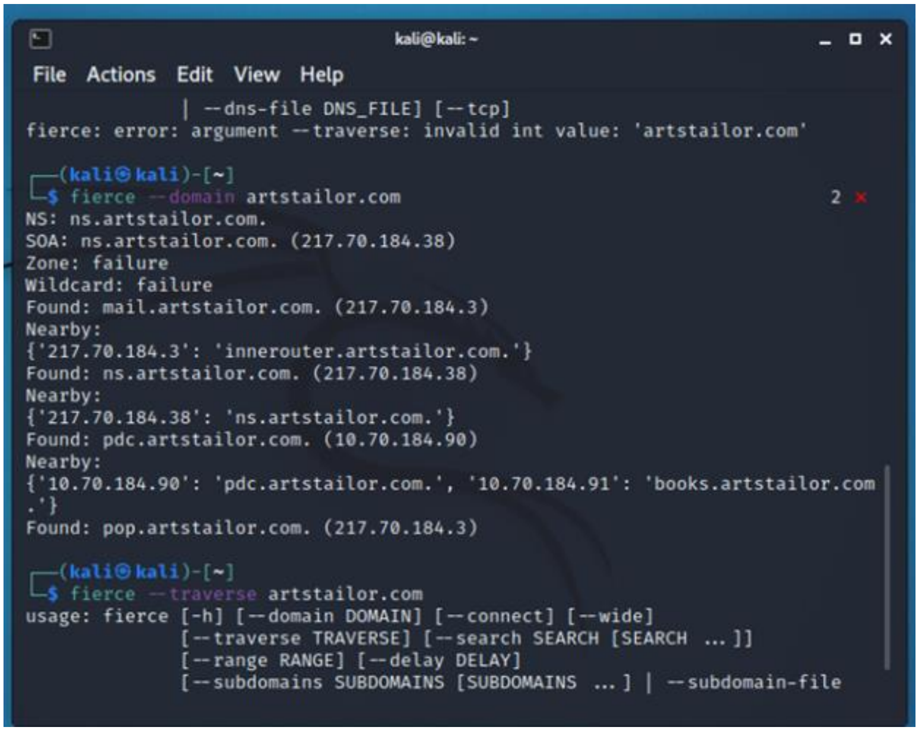
1. mail.artstailor.com
2. ns.artstailor.com

3. pop.artstailor.com
4. www.artstailor.com
5. costumes.artstailor.com

the only unique find is www.artstailor.com. Overall the results were less than what was found with fierce save one new finding.

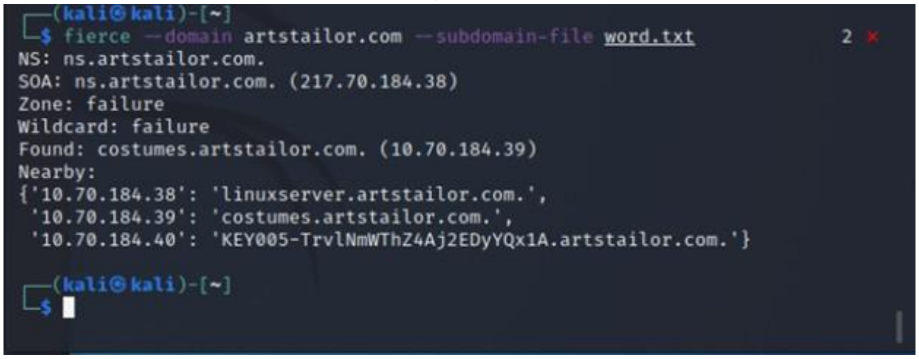
Task 8

Upon initial review there appears to be two IP addresses that may be intended to remain private currently publicly available which were identified using a wide traversal of IP addresses with fierce. These domain addresses are: ceo.artstailor.com and devbox.artstailor.com.



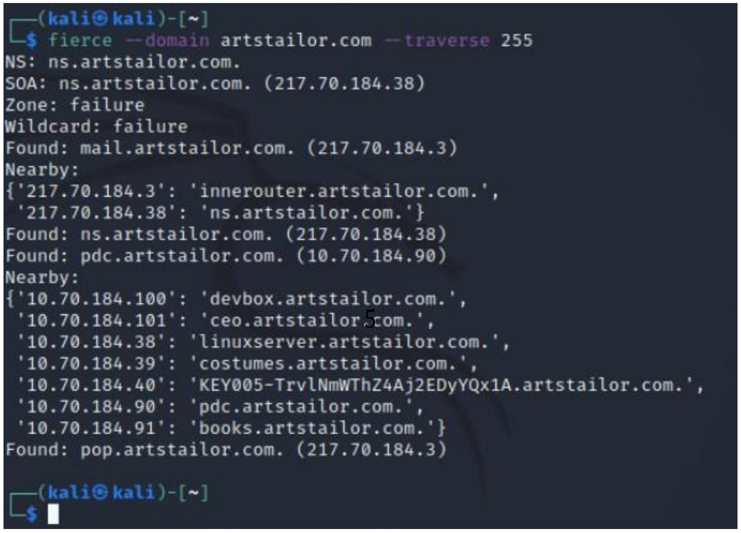
```
             | --dns-file DNS_FILE] [--tcp]
fierce: error: argument --traverse: invalid int value: 'artstailor.com'

┌──(kali㉿kali)-[~]
└─$ fierce --domain artstailor.com                                    2 ×
NS: ns.artstailor.com.
SOA: ns.artstailor.com. (217.70.184.38)
Zone: failure
Wildcard: failure
Found: mail.artstailor.com. (217.70.184.3)
Nearby:
{'217.70.184.3': 'innerouter.artstailor.com.'}
Found: ns.artstailor.com. (217.70.184.38)
Nearby:
{'217.70.184.38': 'ns.artstailor.com.'}
Found: pdc.artstailor.com. (10.70.184.90)
Nearby:
{'10.70.184.90': 'pdc.artstailor.com.', '10.70.184.91': 'books.artstailor.com
.'}
Found: pop.artstailor.com. (217.70.184.3)

┌──(kali㉿kali)-[~]
└─$ fierce --traverse artstailor.com
usage: fierce [-h] [--domain DOMAIN] [--connect] [--wide]
              [--traverse TRAVERSE] [--search SEARCH [SEARCH ...]]
              [--range RANGE] [--delay DELAY]
              [--subdomains SUBDOMAINS [SUBDOMAINS ...] | --subdomain-file
```

Figure 1:

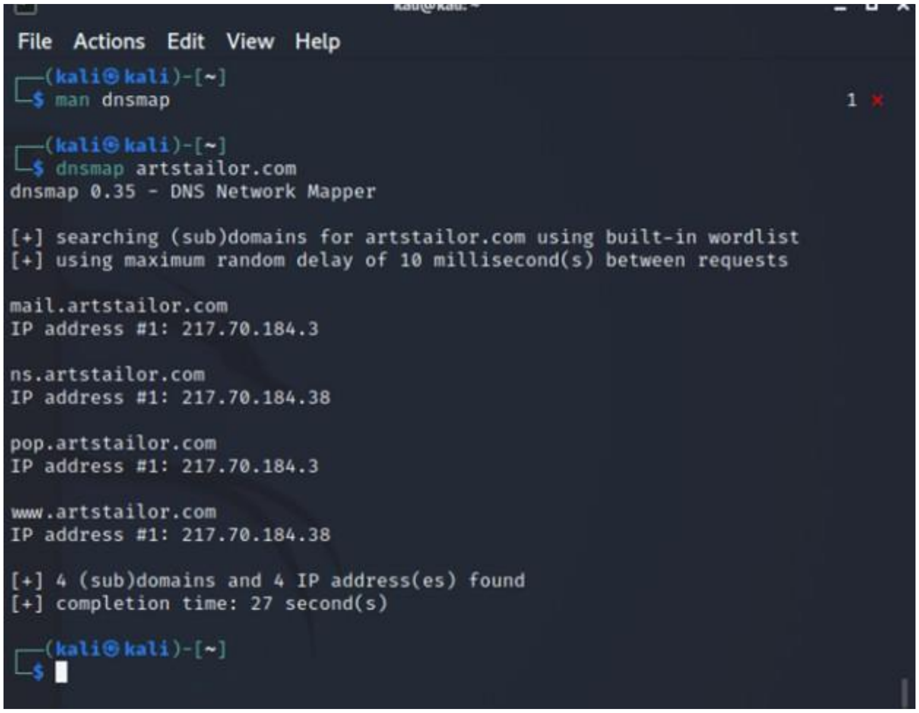


```
┌──(kali㉿kali)-[~]
└─$ fierce --domain artstailor.com --subdomain-file word.txt          2 ×
NS: ns.artstailor.com.
SOA: ns.artstailor.com. (217.70.184.38)
Zone: failure
Wildcard: failure
Found: costumes.artstailor.com. (10.70.184.39)
Nearby:
{'10.70.184.38': 'linuxserver.artstailor.com.',
 '10.70.184.39': 'costumes.artstailor.com.',
 '10.70.184.40': 'KEY005-TrvlNmWThZ4Aj2EDyYQx1A.artstailor.com.'}

┌──(kali㉿kali)-[~]
└─$ 
```

Figure 2:

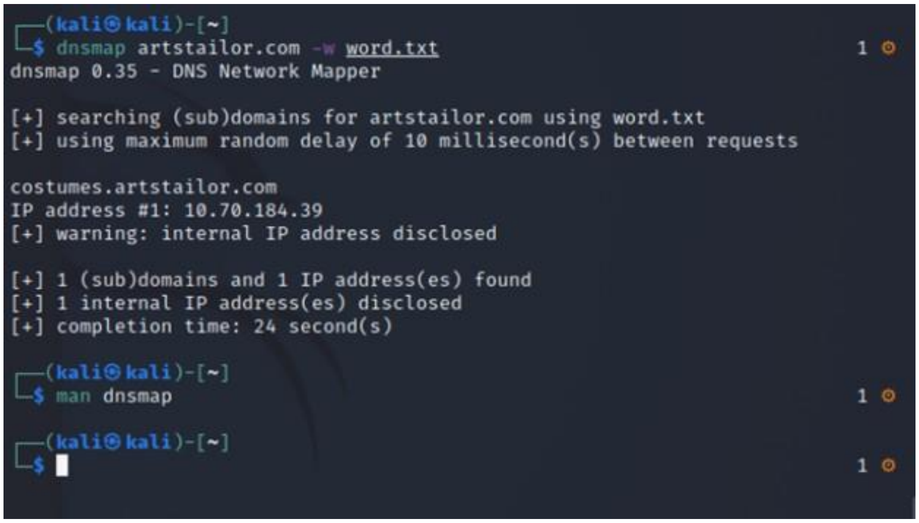


```
┌──(kali㉿kali)-[~]
└─$ fierce --domain artstailor.com --traverse 255
NS: ns.artstailor.com.
SOA: ns.artstailor.com. (217.70.184.38)
Zone: failure
Wildcard: failure
Found: mail.artstailor.com. (217.70.184.3)
Nearby:
{'217.70.184.3': 'innerouter.artstailor.com.',
 '217.70.184.38': 'ns.artstailor.com.'}
Found: ns.artstailor.com. (217.70.184.38)
Found: pdc.artstailor.com. (10.70.184.90)
Nearby:
{'10.70.184.100': 'devbox.artstailor.com.',
 '10.70.184.101': 'ceo.artstailor.com.',
 '10.70.184.38': 'linuxserver.artstailor.com.',
 '10.70.184.39': 'costumes.artstailor.com.',
 '10.70.184.40': 'KEY005-TrvlNmWThZ4Aj2EDyYQx1A.artstailor.com.',
 '10.70.184.90': 'pdc.artstailor.com.',
 '10.70.184.91': 'books.artstailor.com.'}
Found: pop.artstailor.com. (217.70.184.3)

┌──(kali㉿kali)-[~]
└─$ 
```



```
┌──(kali㉿kali)-[~]
└─$ man dnsmap                                                          1 ×

┌──(kali㉿kali)-[~]
└─$ dnsmap artstailor.com
dnsmap 0.35 - DNS Network Mapper

[+] searching (sub)domains for artstailor.com using built-in wordlist
[+] using maximum random delay of 10 millisecond(s) between requests

mail.artstailor.com
IP address #1: 217.70.184.3

ns.artstailor.com
IP address #1: 217.70.184.38

pop.artstailor.com
IP address #1: 217.70.184.3

www.artstailor.com
IP address #1: 217.70.184.38

[+] 4 (sub)domains and 4 IP address(es) found
[+] completion time: 27 second(s)

┌──(kali㉿kali)-[~]
└─$ █
```

Figure 4:



```
┌──(kali㉿kali)-[~]
└─$ dnsmap artstailor.com -w word.txt                                    1 ⚙
dnsmap 0.35 - DNS Network Mapper

[+] searching (sub)domains for artstailor.com using word.txt
[+] using maximum random delay of 10 millisecond(s) between requests

costumes.artstailor.com
IP address #1: 10.70.184.39
[+] warning: internal IP address disclosed

[+] 1 (sub)domains and 1 IP address(es) found
[+] 1 internal IP address(es) disclosed
[+] completion time: 24 second(s)

┌──(kali㉿kali)-[~]
└─$ man dnsmap                                                           1 ⚙

┌──(kali㉿kali)-[~]
└─$ █                                                                    1 ⚙
```

Figure 5: