

**Universiteti i Prishtinës “Hasan Prishtina”**  
**Fakulteti i Inxhinierisë Elektrike dhe Kompjuterike**



Lënda: Siguria në Internet

Tema : Fierce

Mentorë:

Prof. Dr. Blerim Rexha  
Msc. Arbnor Halili

Studentet:

Gresa Salihu	180718100004
Leonita Nika	180714100107
Mihrije Kadriu	180714100014

Prishtinë, 2020

## Permbajtja

1.	Hyrje .....	3
2.	Pjesa testuese e eksperimentit .....	5
2.1	Startimi i vegles Fierce .....	5
2.2	Testimi i komandes: - fierce –dns domain threads .....	7
2.3	Testimi i komandes : - fierce –dns domain -threads –connect path.....	8
2.4	Testimi i komandes: - fierce –dns domain –file .....	10
2.5	Testimi për transferim të zonës .....	11
3.	Konkludimi .....	11
4.	Shtojca e figurava .....	12
5.	Referencat .....	12

## 1. Hyrje

**Fierce** është një vegël e Sistemit Operativ *Kali Linux* e cila është open source (me burim të hapur) që shërben për të numëruar nën domenet e një webfaqe të targetuar. Është shkruar nga Robert Hansen i njohur si RSnake. Ajo është një skripte e shkruajtur me gjuhën programuese PERL dhe është e instaluar paraprakisht në sistemin operativ Kali Linux.<sup>[1]</sup>

Fierce është menduar posaçërisht për të gjetur objektivat e mundshme si brenda ashtu edhe jashtë një rrjeti të korporatave ajo nuk është krijuar për të skanuar të gjithë internetin ose për të kryer ndonjë sulm pa shënjestër. Pra kjo vegël është shumë më tepër sesa një skanues i thjeshtë IP ose një mjet DDoS, çfarë e bënë më të veçantë atë është aftësia të skanoj domenet brenda pak minutash, kjo e bënë atë të jetë një ndër mjetet më të preferuara për kryerjen e kontrolleve të cënueshmërisë në rrjetet e mëdha.

Një tipar interesant tek kjo vegël është se kur gjen një host / IP valid, Fierce do të performojë reverse lookups për një rang specifik. Kjo mund të ndihmojë në zbulimin e hostave shtesë që metoda e forcës brutale nuk mund t'i ketë gjetur.

Disa nga funksionet që kryen Fierce përfshijnë:

- aftësinë e performimit të reverse lookups për një interval të specifikuar
- skanimin e intervalit të brendshëm dhe të jashtëm të IP
- aftësinë e skenimit të plotë të klasës C
- numërimin e rekordeve të DNS mbi targets (shënjestrat)
- kapacitetin e shkëlqyer për realizimin e brute force
- zbulimin e emrit të serverëve dhe sulmit të transferimit të zones

Fierce siq e kemi cekur më lartë e ka aftësinë e performimit të skanimit, këtë proces ajo e fillon me sulme të forcës brutale nëse nuk është e mundur që të kryejë me lehtësi transferimin e zonës së domenit të synuar. Fierce përdor një listë fjalësh të paracaktuar që përmban nënfushat e mundshme që mund të zbulojë. <sup>[3]</sup> Nëse një nën-domen nuk është në listë, nuk do të zbulohet.

Disa nga komandat e këtij skaneri janë:

-help	Paraqet mesazhin ndihmës
-connect	Bën lidhjen HTTP në web-serverët publik si dhe kthen headerët
-delay	Numri i sekondave që duhet pritur midis kërkimeve
-dns	Domeni që dëshironi të skanohet
-dnsfile	Ofron një listë të DNS serverë-ve për reverse lookups
-dnsserver	Përdor një DNS server secifik për reverse lookups
-file	Ruan rezultatin në një file të dëshirueshëm
-fulloutput	Shfaq cdo gjë që webserveri kthen, jo vetëm HTTP headerin, përdoret së bashku me –connect
-nopattern	Shfaq të gjitha domenet në intervalin e zbuluar IP
-range	Skanon një rang të IP, përdoret së bashku me -dnsserver
-search	Lejon kërkimin në hoste shtesë duke u bazuar në emrat specifik që kompania mund të përdor
-traverse	Specifikon numrin e IP-ve para dhe pas zbulimit të hosteve
-wide	Skanon të gjithë klasën C të network-ut
-wordlist	Specifikon një listë fjalësh të personalizuar

## 2. Pjesa testuese e eksperimentit

Për realizimin e këtyre testimeve duhet që ta kemi te instaluar Kali Linux në të cilin vegla Fierce është e instaluar paraprakisht.

### 2.1 Startimi i vegles Fierce

**Metoda 1:** Së pari qasemi në sistemin operativ Kali Linux, te Applications klikojm Information Gathering dhe më pas klikojm DNS Analysis në të cilin zgjedhim veglën Fierce.

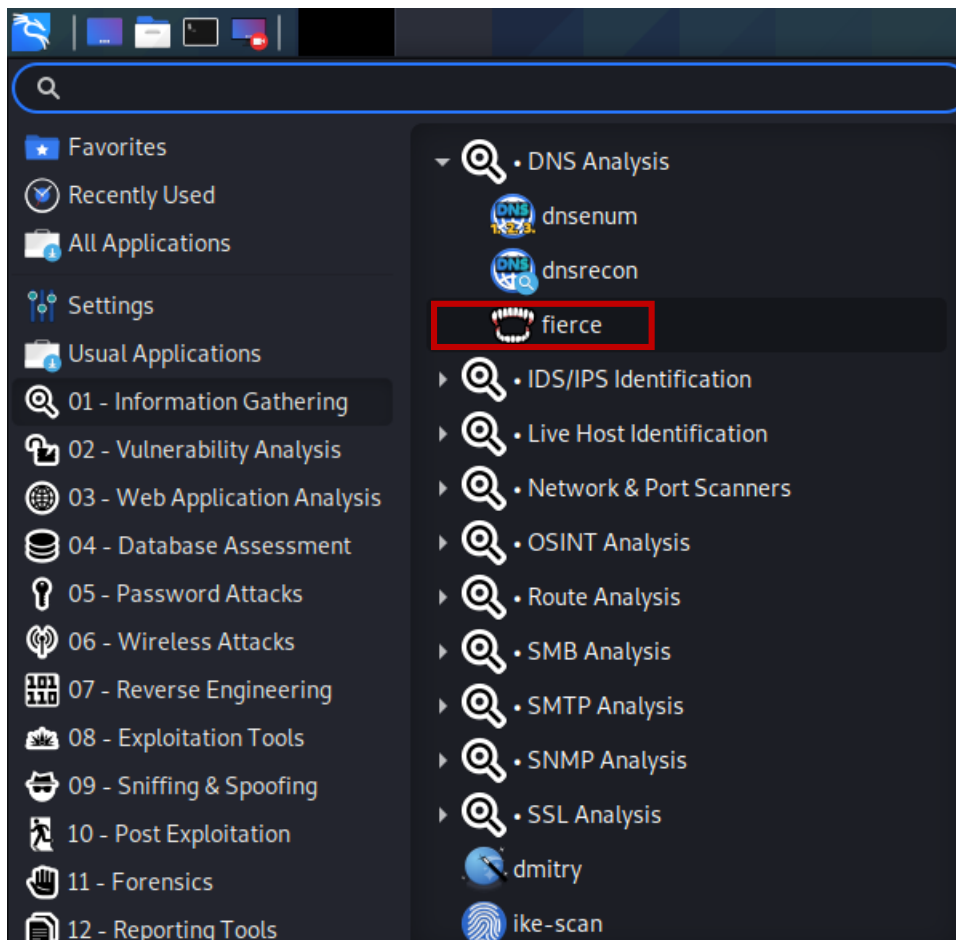
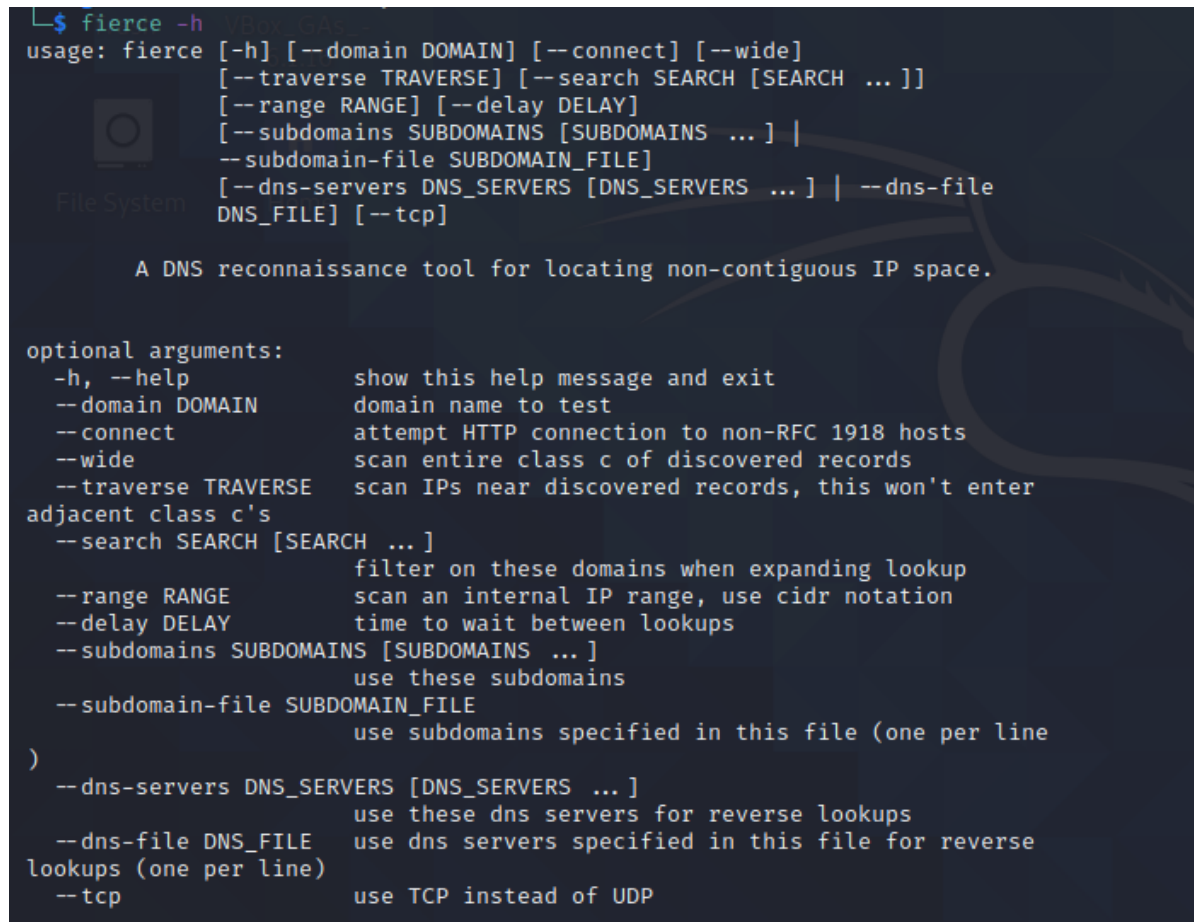


Figura 1 Hapja e vegles Fierce permes metodes GUI

Në kuadër të DNS Analysis perveq veglës Fierce janë **dnsenum**, **dnsrecon** këto vegla janë parakusht për veglat e kategorive si: nmap, unicornscan, nessus, nikto dhe të tjera të natyrës së ngjashme pasi që të gjithë këto kërkojnë që të dimë paraprakisht hapësirën e IP .

## Metoda 2 :

Hapim terminalin në sistemin operativ Kali Linux dhe shënojm komandën **fierce-h** e cila do shfaq veglën Fierce me opsionin help, opsion ky që përveq që na ofron hapjen e veglës Fierce na ofron ndihmë të dijmë më shumë rreth argumenteve se si të përdorim veglën Fierce dhe si t'i shkruajm argumentet.[4]



```

$ fierce -h
usage: fierce [-h] [--domain DOMAIN] [--connect] [--wide]
             [--traverse TRAVERSE] [--search SEARCH [SEARCH ...]]
             [--range RANGE] [--delay DELAY]
             [--subdomains SUBDOMAINS [SUBDOMAINS ...]] |
             --subdomain-file SUBDOMAIN_FILE
             [--dns-servers DNS_SERVERS [DNS_SERVERS ...]] | --dns-file
             DNS_FILE] [--tcp]

A DNS reconnaissance tool for locating non-contiguous IP space.

optional arguments:
  -h, --help                show this help message and exit
  --domain DOMAIN           domain name to test
  --connect                 attempt HTTP connection to non-RFC 1918 hosts
  --wide                    scan entire class c of discovered records
  --traverse TRAVERSE       scan IPs near discovered records, this won't enter
                             adjacent class c's
  --search SEARCH [SEARCH ...]
                             filter on these domains when expanding lookup
  --range RANGE             scan an internal IP range, use cidr notation
  --delay DELAY             time to wait between lookups
  --subdomains SUBDOMAINS [SUBDOMAINS ...]
                             use these subdomains
  --subdomain-file SUBDOMAIN_FILE
                             use subdomains specified in this file (one per line)
  --dns-servers DNS_SERVERS [DNS_SERVERS ...]
                             use these dns servers for reverse lookups
  --dns-file DNS_FILE       use dns servers specified in this file for reverse
                             lookups (one per line)
  --tcp                     use TCP instead of UDP

```

*Figura 2 Hapja e veglës Fierce permes komandes fierce -h*

Duke përdorur këtë komandë ne mund të marrim informacionet si emrin e serverit ( NS-NameServer) dhe transferimin e zonës në lidhje me një fushë të synuar (target domain).

Fierce së pari identifikon serverat autoritarë DNS për domenin e synuar që kemi specifikuar. Me pas përpiqet të realizojë transferim të zonës, si dhe të shfaq të gjeturat të domenit nga secili server autoritarë DNS. Mirëpo shumë domene nuk e lejojnë transferimin e zonës, në rastin kur fierce nuk mund të marrë transferimin e zonës atëherë automatikisht tenton të realizoj forcën brutale për të synuar domenin, por ndonjëherë mund të ndodhë që mos të jetë e mundur as realizimi përmes forcës brutale e kjo ndodhë në rastet kur kemi ndonjë defekt në Kali Linux .

## 2.2 Testimi i komandes: - fierce -dns domain threads

```
mirja@10:~$ fierce -dns uni-pr.edu threads 10
DNS Servers for uni-pr.edu:
    albert.ns.cloudflare.com
    mira.ns.cloudflare.com

Trying zone transfer first...
    Testing albert.ns.cloudflare.com
        Request timed out or transfer not allowed.
    Testing mira.ns.cloudflare.com
        Request timed out or transfer not allowed.

Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force

Checking for wildcard DNS...
    ** Found 90059215063.uni-pr.edu at 213.163.123.247.
    ** High probability of wildcard DNS.
Now performing 2280 test(s)...
```

Figura 3 Testimi i komandes fierce -dns domain threads

Argumenti threads është vendosur për të shpejtuar skanimin, pasi Fierce nëse nuk ceket ndryshe ekzekuton komandat në single threaded mode, andaj me anë të vendosjes së këtij argumenti rritet shpejtësia.[5]

Gjëja e parë që Fierce bënë është të gjejë emrat e serverëve për domenin e synuar. Në vazhdim, synon të bëjë transferimin e zonës. Nëse dështon në gjetjen e emrave të serverëve për domenin e synuar atëherë kontrollon nëse wildcard DNS është i qasshëm, pastaj performon një brute force kundër domenit duke përdorur built-in wordlist.

```
mirja@10:~$ fierce -dns uni-pr.edu -threads 10 -wordlist /usr/share/dnsrecon/namelist.txt
DNS Servers for uni-pr.edu:
    albert.ns.cloudflare.com
    mira.ns.cloudflare.com
```

Figura 4 Testimi i komandes -wordlist

Pasi që të përfundojë skanimi, shfaqen të gjitha nëndomenet(subdomains) që gjenden, së bashku me subnet-et, të cilat mundemi pastaj t'i kontrollojm përmes veglës nmap ose ndonjë skaneri tjetër të portave. Fierce zakonisht përdor listën e fjalëve(wordlist) që janë paraprakisht të integruara, por kemi mundësinë t'a specifikojmë vetë listën e fjalëve që do e përdorim. Ndonjëherë fitojmë më shumë rezultate duke përdorur lista të ndryshme të fjalëve. Më poshtë si shembull kemi përdorur listën që vie me “dnsrecon”.

```

Checking for wildcard DNS...
  ** Found 90059215063.uni-pr.edu at 213.163.123.247.
  ** High probability of wildcard DNS.
Now performing 2280 test(s)...
104.24.121.140 groups.uni-pr.edu
104.24.120.140 groups.uni-pr.edu
172.67.191.171 groups.uni-pr.edu
172.67.191.171 mail.uni-pr.edu
104.24.120.140 mail.uni-pr.edu
104.24.121.140 mail.uni-pr.edu
172.67.191.171 mail2.uni-pr.edu
104.24.121.140 mail2.uni-pr.edu
104.24.120.140 mail2.uni-pr.edu
104.24.120.140 ns3.uni-pr.edu
172.67.191.171 ns3.uni-pr.edu
104.24.121.140 ns3.uni-pr.edu
104.24.120.140 smc.uni-pr.edu
104.24.121.140 smc.uni-pr.edu
172.67.191.171 smc.uni-pr.edu
104.24.121.140 student.uni-pr.edu
172.67.191.171 student.uni-pr.edu
104.24.120.140 student.uni-pr.edu
104.24.120.140 support.uni-pr.edu
172.67.191.171 support.uni-pr.edu
104.24.121.140 support.uni-pr.edu
172.67.191.171 www.uni-pr.edu
104.24.120.140 www.uni-pr.edu
104.24.121.140 www.uni-pr.edu

Subnets found (may want to probe here using nmap or unicornscan):
  104.24.120.0-255 : 8 hostnames found.
  104.24.121.0-255 : 8 hostnames found.
  172.67.191.0-255 : 8 hostnames found.

Done with Fierce scan: http://ha.ckers.org/fierce/
Found 24 entries.

Have a nice day.

```

Figura 5 Rezultati i komandes : *fierce -dns uni-pr.edu -threads 10*

Pasi që të përfundojë skanimi, shfaqen të gjitha nëndomenet(subdomains) që gjenden, së bashku me subnet-et, të cilat mundemi pastaj t'i kontrollojmë përmes veglës nmap ose ndonjë skaneri tjetër të portave. Fierce zakonisht përdor listën e fjalëve(wordlist) që janë paraprakisht të integruara, por kemi mundësinë t'a specifikojmë vetë listën e fjalëve që do e përdorim. Ndonjëherë fitojmë më shumë rezultate duke përdorur lista të ndryshme të fjalëve. Më poshtë si shembull kemi përdorur listën që vie me “dnsrecon”.<sup>[2]</sup>

### 2.3 Testimi i komandes : - *fierce -dns domain -threads -connect path*

Me anë të komandës **-connect** mundësohet konektimi në domenet e zbuluara, dhe tenton të kthejë prapa HTTP Headers për cdo web server që është duke u ekzekutuar.

Kjo teknikë mund të na japë më shumë informata, të tilla si tipi dhe versioni i web serverit që është duke u ekzekutuar, që më pas mundemi t'i targetojmë.

Nëse së bashku me këtë komandë e përdorim komandën **-fulloutput** atëherë si rezultat do të shfaq cdo gjë që webserveri kthen.<sup>[1]</sup>

Testimi i skenimit duke përdorur komandën **-connect** duket si në vijim :



```

mirja@10:~$ fierce -dns uni-pr.edu -threads 10 -connect ~/Desktop/uni-pr.txt
DNS Servers for uni-pr.edu:
    mira.ns.cloudflare.com
    albert.ns.cloudflare.com

Trying zone transfer first...
    Testing mira.ns.cloudflare.com
        Request timed out or transfer not allowed.
    Testing albert.ns.cloudflare.com
        Request timed out or transfer not allowed.

Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force

Checking for wildcard DNS...
    ** Found 97499925841.uni-pr.edu at 213.163.123.247.
    ** High probability of wildcard DNS.
Now performing 2280 test(s)...
172.67.191.171 groups.uni-pr.edu
104.24.120.140 mail.uni-pr.edu
104.24.120.140 mail2.uni-pr.edu
172.67.191.171 mail2.uni-pr.edu
104.24.120.140 groups.uni-pr.edu

```

Figura 6 Testimi i komandes -connect

Rezultati nga ekzekutimi i komandës **-connect**:

```

    104.24.121.0-255 : 8 hostnames found.
    172.67.191.0-255 : 8 hostnames found.
IO::Socket::INET=GLOB(0x55fadb094170)

HTTP output for 104.24.120.140 groups.uni-pr.edu
IO::Socket::INET=GLOB(0x55fadb090a68)

HTTP output for 104.24.120.140 mail.uni-pr.edu
IO::Socket::INET=GLOB(0x55fadb087d48)

HTTP output for 104.24.120.140 mail2.uni-pr.edu
IO::Socket::INET=GLOB(0x55fadb090a68)

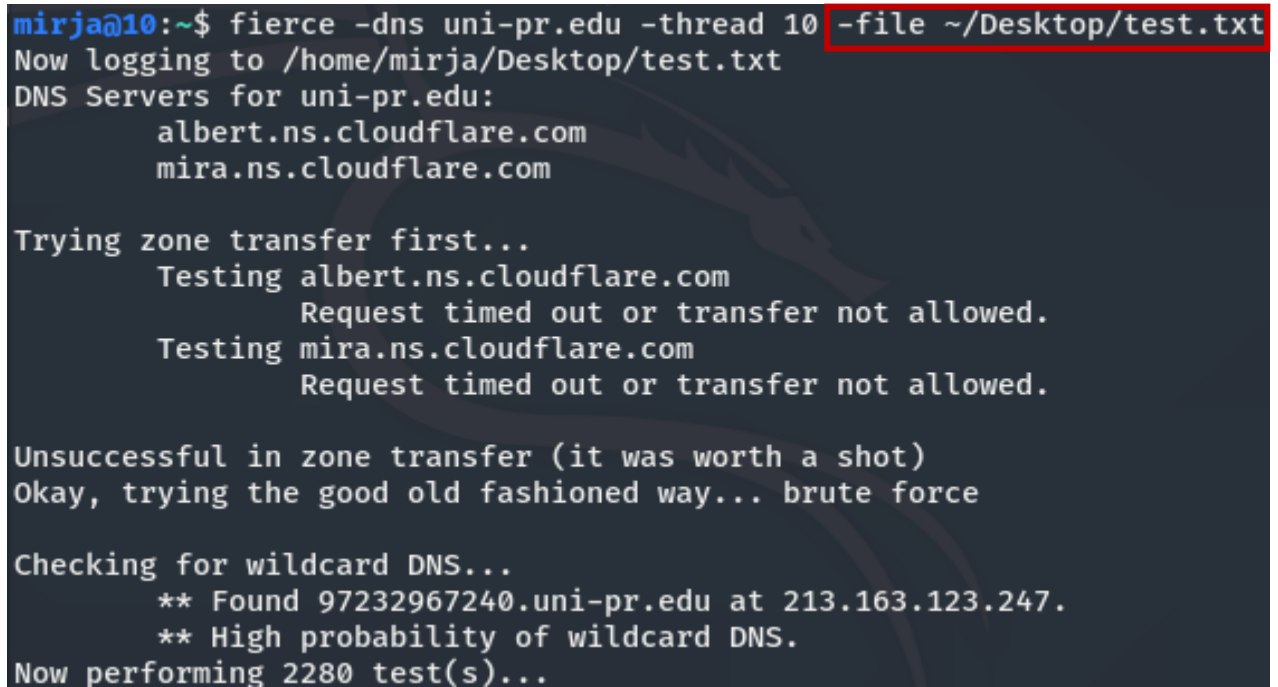
```

Figura 7 Rezultati i komandes : -connect

Nga figura e më sipërme shihet se komanda **-connect** bënë përpjekje për lidhje me adresën publike të domenit në rastin tonë Universitetit të Prishtinës dhe si dalje jep HTTP Header-in, për shkak të natyrës së kësaj komande realizimi i saj merr shumë kohe .

#### 2.4 Testimi i komandes: fierce -dns domain -file

Me anë të kesaj komande ne i ruajm rezultatet nga skanimi i domenës së caktuar në një file të dëshirueshëm, në shembullin konkret në fajllin test.txt



```
mirja@10:~$ fierce -dns uni-pr.edu -thread 10 -file ~/Desktop/test.txt
Now logging to /home/mirja/Desktop/test.txt
DNS Servers for uni-pr.edu:
    albert.ns.cloudflare.com
    mira.ns.cloudflare.com

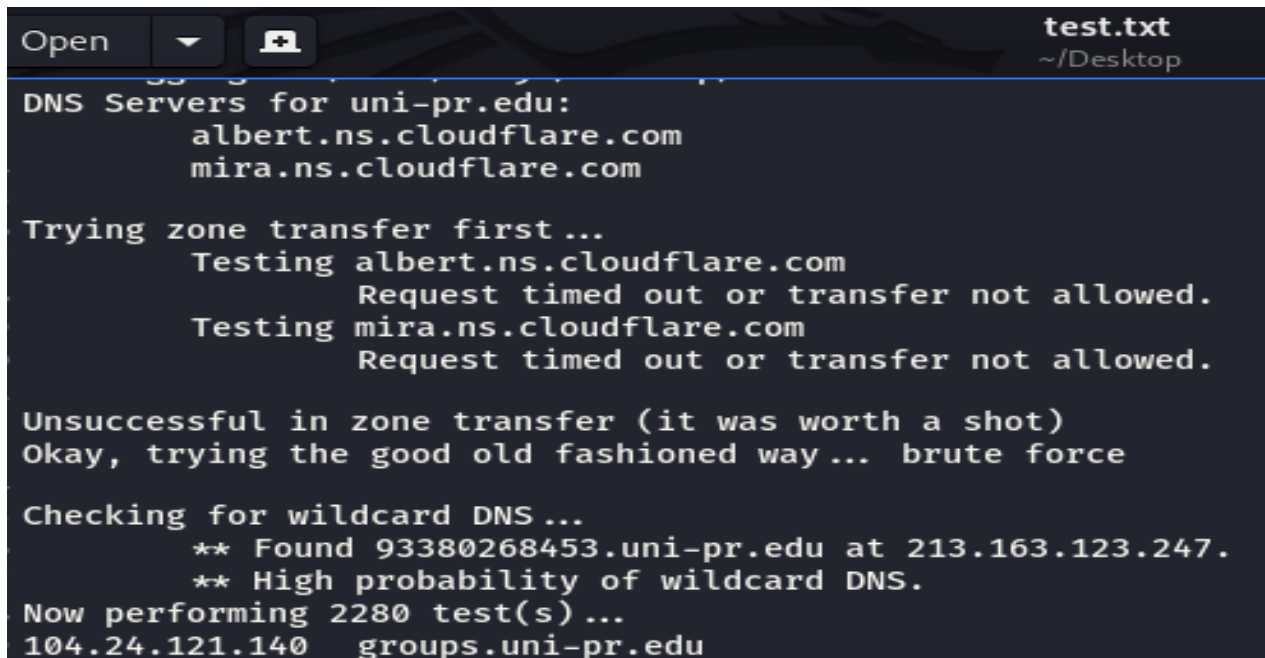
Trying zone transfer first...
    Testing albert.ns.cloudflare.com
        Request timed out or transfer not allowed.
    Testing mira.ns.cloudflare.com
        Request timed out or transfer not allowed.

Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force

Checking for wildcard DNS...
    ** Found 97232967240.uni-pr.edu at 213.163.123.247.
    ** High probability of wildcard DNS.
Now performing 2280 test(s)...
```

Figura 8 Ekzekutimi i komandes : -file

Rezultatet e testimit të komandës file janë ruajtur në fajllin e dëshiruar test.txt në të njëjtin format ashtu siq janë të paraqitura edhe në terminal.



```
Open test.txt
~/Desktop

DNS Servers for uni-pr.edu:
    albert.ns.cloudflare.com
    mira.ns.cloudflare.com

Trying zone transfer first...
    Testing albert.ns.cloudflare.com
        Request timed out or transfer not allowed.
    Testing mira.ns.cloudflare.com
        Request timed out or transfer not allowed.

Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force

Checking for wildcard DNS...
    ** Found 93380268453.uni-pr.edu at 213.163.123.247.
    ** High probability of wildcard DNS.
Now performing 2280 test(s)...
104.24.121.140 groups.uni-pr.edu
```

Figura 9 Ruajtja e skenimit ne fajllin test.txt

## 2.5 Testimi për transferim të zonës

Transferimet e zonës janë të rralla këto ditë, ato na bëjnë të mundshme marrjen e celësive për DNS dhe një ndër serviset më të përdorshme për testim të transferimit të zonave është `zonetransfer.me`. Zone transfer (transferimi i zonave) e përdor Transmission Control Protocol (TCP) për transport, dhe merr formën e transaksionit client-server. Me anë të komandës në vijim shihet se çfarë rezultatesh do të fitohen në rast të përdorimit të “zone transfer.me”. [2]

Në shembullin që e kemi testuar shihet se jemi duke e realizuar me sukses transferimin e zonës.

```
mirja@10:~$ fierce -dns zonetransfer.me -threads 10
DNS Servers for zonetransfer.me:
    nsztml.digi.ninja
    nsztml.digi.ninja

Trying zone transfer first...
Testing nsztml.digi.ninja

Whoah, it worked - misconfigured DNS server found:
zonetransfer.me.      7200    IN      SOA      ( nsztml.digi.ninja. robin.dig
ninja.
                        2019100801    ;serial
                        172800    ;refresh
                        900      ;retry
                        1209600   ;expire
                        3600     ;minimum
)
zonetransfer.me.      300     IN      HINFO    "Casio fx-700G" "Windows XP"
zonetransfer.me.      301     IN      TXT      (
google-site-verification=typ28J7JAUHA9fw2sHXMgcCC0I6XBmmoVi04VlMewxA )
zonetransfer.me.      7200    IN      MX       0 ASPMX.L.GOOGLE.COM.
zonetransfer.me.      7200    IN      MX       10 ALT1.ASPMX.L.GOOGLE.COM.
zonetransfer.me.      7200    IN      MX       10 ALT2.ASPMX.L.GOOGLE.COM.
zonetransfer.me.      7200    IN      MX       20 ASPMX2.GOOGLEMAIL.COM.
```

Figura 10 Testimi për transferim të zonës

## 3. Konkludimi

Fierce është një vegël shumë e përshtatme dhe e pajisur me shumë komanda të cilat i japin efikasitet më të lartë dhe rëndësi më të madhe në krahasim me disa vegla të tjera të Kali Linux. Çfarë e bënë këtë më të veçantë është aftësia të skanoj domenet brenda pak minutash, kjo e bënë atë të jetë një ndër mjetet më të preferuara për kryerjen e kontrolleve të cënueshmërisë në rrjetet e mëdha. Por ndonjëherë në disa domene nuk mundësohet zone transfer dhe automatikisht Fierce tenton të startoj brute force që të targetoj domenin, nëse gjatë startimit na shfaqet ndonjë defekt i Kali Linux-it atëherë do ndalohet procesi i brute force dhe do dështoj skenimi.

#### 4. Shtojca e figurava

<i>Figura 1 Hapja e vegles Fierce permes metodes GUI</i> .....	5
<i>Figura 2 Hapja e vegles Fierce permes komandes: fierce -h</i> .....	6
<i>Figura 3 Testimi i komandes fierce : -dns domain threads</i> .....	7
<i>Figura 4 Rezultati i komandes : fierce -dns uni-pr.edu -threads 10</i> .....	7
<i>Figura 5 Testimii i komandes : -wordlist</i> .....	8
<i>Figura 6 Testimi i komandes : -connect</i> .....	9
<i>Figura 7 Rezultati i komandes : -connect</i> .....	9
<i>Figura 8 Ekzekutimi i komandes : -file</i> .....	10
<i>Figura 9 Ruajtja e skenimit ne fajllin test.txt</i> .....	10
<i>Figura 10 Testimi per transferim te zones</i> .....	11

#### 5. Referencat

- [1] <https://tools.kali.org/information-gathering/fierce>
- [2] <http://knoxd3.blogspot.com/2013/06/how-to-use-fierce-in-kali-linux.html>
- [3] [https://linuxhint.com/fierce\\_network\\_scanning\\_tutorial/](https://linuxhint.com/fierce_network_scanning_tutorial/)
- [4] <https://cliuser.blogspot.com/2020/05/dns-analysis-tools-dnsenum-dnsrecon.html>
- [5] <https://www.youtube.com/watch?v=5fCU1YsF2Cs>