DNS Reconnaissance :

DNS foreward lookup Bruteforce

Try commonly used hostname
$sudo apt-get install dnsutils
$host www.checkpoint.com
$host ftp.checkpoint.com
$host pop3.checkpoint.com
Task :
Collect commonly used hostname and do bash scripting in such a waythat it takes input one by one from this file and runs it iwl command , I.e loop the list with command .

Automating the search :

shuhari@debian: ~

```
  GNU nano 3.2                                                dns.sh

#!/usr/bin/bash
cat hostname | while read line
do
        host "$line.checkpoint.com"
done
```

shuhari@debian: ~

```
shuhari@debian:~$ sudo ./dns.sh
smtp.checkpoint.com is an alias for michael.checkpoint.com.
michael.checkpoint.com has address 194.29.34.68
michael.checkpoint.com mail is handled by 10 tls2.checkpoint.com
Host telnet.checkpoint.com not found: 3(NXDOMAIN)
ftp.checkpoint.com has address 194.29.38.122
Host mime.checkpoint.com not found: 3(NXDOMAIN)
Host pop.checkpoint.com not found: 3(NXDOMAIN)
Host http.checkpoint.com not found: 3(NXDOMAIN)
Host dns.checkpoint.com not found: 3(NXDOMAIN)
www.checkpoint.com is an alias for d4epvaz4tpdrm.cloudfront.net.
d4epvaz4tpdrm.cloudfront.net has address 18.161.125.125
d4epvaz4tpdrm.cloudfront.net has address 18.161.125.95
d4epvaz4tpdrm.cloudfront.net has address 18.161.125.78
d4epvaz4tpdrm.cloudfront.net has address 18.161.125.75
ns1.checkpoint.com has address 209.87.222.140
ns2.checkpoint.com has address 209.87.212.242
Host http.checkpoint.com not found: 3(NXDOMAIN)
Host https.checkpoint.com not found: 3(NXDOMAIN)
host: '.checkpoint.com' is not a legal name (empty label)
shuhari@debian:~$
```

The while read loop. Here, cat reads each line from standard input and writes the line to standard output.

Remove unwanted information aslo :

shuhari@debian: ~

```
  GNU nano 3.2                                          dns.sh

#!/usr/bin/bash
cat hostname |while read elem
do
        host "$elem.checkpoint.com" >> result.txt
        grep -E -o "([0-9]{1,3}[\.]){3}[0-9]{1,3}" result.txt > output.txt
        cat output.txt
        break
done

```

grep command :

-E, --extended-regexp

Interpret PATTERNS as extended regular expressions (EREs, see below).

-o, --only-matching

Print only the matched (non-empty) parts of a matching line, with each such part on a separate output line

shuhari@debian: ~

```
shuhari@debian:~$ sudo ./dns.sh
194.29.34.68
194.29.38.122
18.161.125.75
18.161.125.78
18.161.125.125
18.161.125.95
209.87.222.140
209.87.212.242
194.29.34.68
194.29.38.122
18.161.125.75
18.161.125.95
18.161.125.125
18.161.125.78
209.87.222.140
209.87.212.242
194.29.34.68
194.29.34.68
194.29.34.68
194.29.34.68
shuhari@debian:~$
```

DNS reverse lookup bruteforce :

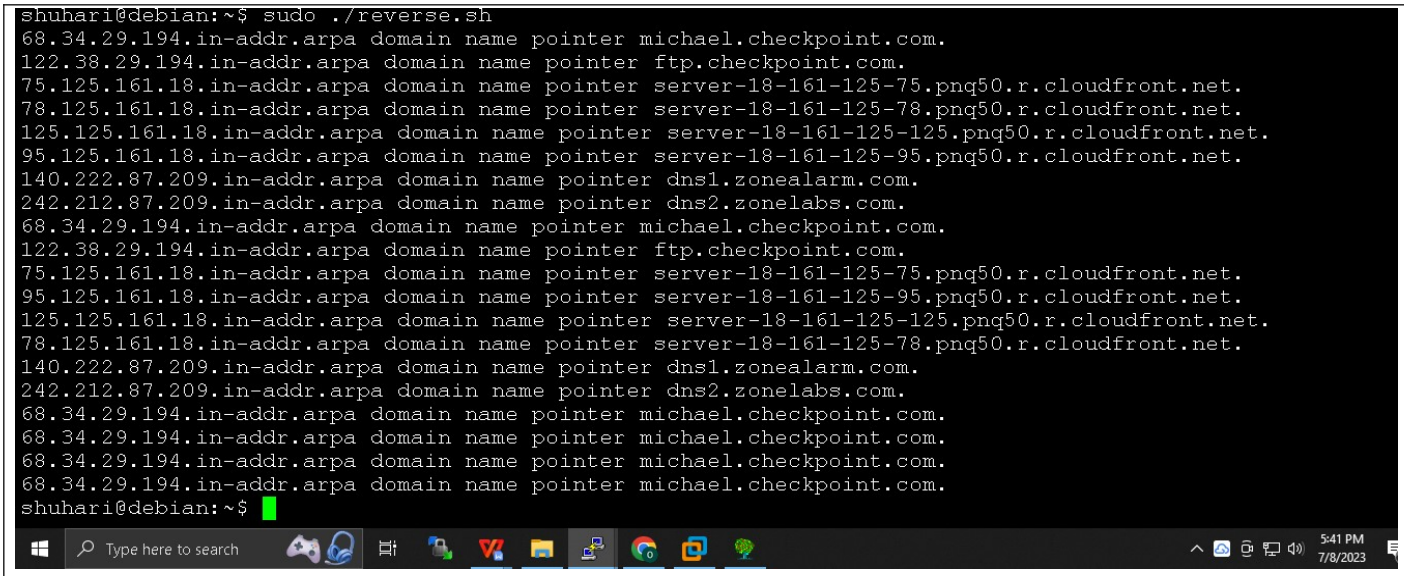
Ip to name :

In previous practical we have saved our outpit in output.txt file which contains all ip address of checkpoint.com now we shall do reverse of that run a ascript which shall take line from that file as input to host command and show domain of that .

shuhari@debian: ~

```
  GNU nano 3.2                                          reverse.sh

#!/usr/bin/bash
cat output.txt | while read elem
do
        host "$elem"
done
```



Run a a script which shall take input from user I.e network id and then run the script and after that remove unwanted things I.e nxdomain -> again run diff script which shal reomve the field ->
Expected output -> paste it in treepad .