

<https://github.com/dthomsen116/SEC-335/wiki/Activity-3.1---DNS-Enumeration>

Deliverable 1. Provide a screenshot of your /24 port scan against 10.0.5.0/24 similar to the one below.

```
(champus@kali)~$ ./portscanner2.sh 10.0.5 53

HOSTS | PORTS
-----|-----
10.0.5.22 | 53

(champus@kali)~$ cat portscanner2.sh
#!/bin/bash

host=$1
port=$2

echo
echo "  HOSTS    | PORTS"
echo "  _____"

for i in {1..254}; do
    ipaddr=$host.$i

    timeout .1 bash -c "echo >/dev/tcp/$ipaddr/$port" 2>/dev/null && echo " $ipaddr | $port "
done
```

Deliverable 2. Provide a screenshot similar to the one below that shows your directory structure and the source code of your /24 port scanner. Note, this code can be 1 liner, but I want you to go through the process of submitting source code to github.

```
(champus@kali)~$ ./portscanner2.sh 10.0.5 53 > dns-servers.txt

(champus@kali)~$ git status
On branch main
Your branch is up to date with 'origin/main'.

Untracked files:
  (use "git add <file> ..." to include in what will be committed)
    dns-servers.txt

nothing added to commit but untracked files present (use "git add" to track)

(champus@kali)~$ git add .

(champus@kali)~$ git commit -m "Week 3 DNS SERVERS"
[main dd9b145] Week 3 DNS SERVERS
1 file changed, 4 insertions(+)
create mode 100644 dns-servers.txt

(champus@kali)~$ git push
Enter passphrase for key '/home/champus/.ssh/id_rsa':
Enumerating objects: 4, done.
Counting objects: 100% (4/4), done.
Delta compression using up to 2 threads
Compressing objects: 100% (3/3), done.
Writing objects: 100% (3/3), 338 bytes | 169.00 KiB/s, done.
Total 3 (delta 1), reused 0 (delta 0), pack-reused 0
remote: Resolving deltas: 100% (1/1), completed with 1 local object.
To github.com:dthomsen116/SEC-335.git
  350a497..dd9b145  main -> main

(champus@kali)~$
```

Deliverable 3. Write a script that takes a network prefix and a specific dns server in which to perform a lookup. Assume a /24 network. Provide a screenshot similar to the one below showing the program run.

```
(champuser@kali)-[~/SEC335/SEC-335]
$ vim dns-resolver.sh

(champuser@kali)-[~/SEC335/SEC-335]
$ ./dns-resolver.sh 10.0.5 10.0.5.22
19.5.0.10.in-addr.arpa name = mail.shire.org.
20.5.0.10.in-addr.arpa name = www.shire.org.
21.5.0.10.in-addr.arpa name = bios.shire.org.
22.5.0.10.in-addr.arpa name = ns.shire.org.
23.5.0.10.in-addr.arpa name = cupcake.shire.org.
24.5.0.10.in-addr.arpa name = bifur.shire.org.
25.5.0.10.in-addr.arpa name = pippin.shire.org.
26.5.0.10.in-addr.arpa name = prancingpony.shire.org.
27.5.0.10.in-addr.arpa name = arwen.shire.org.
28.5.0.10.in-addr.arpa name = nancurunir.shire.org.
31.5.0.10.in-addr.arpa name = gloin.shire.org.
32.5.0.10.in-addr.arpa name = bree.shire.org.
250.5.0.10.in-addr.arpa name = fw-rivendell.shire.org.
```

Deliverable 4. Provide a screenshot similar to the one below that shows your directory structure and the source code of your dns resolver.

```
main ▾ SEC-335 / dns-resolver.sh

dthomsen116 dns-resolver

1 contributor

Executable File | 13 lines (7 sloc) | 124 Bytes

1  #!/bin/bash
2
3  host=$1
4  dns=$2
5
6
7  for i in {1..254}; do
8      ipaddr=host.$i
9      nslookup $ipaddr $dns | grep "name"
10
11
12
13  done
```

Deliverable 5. Use nmap to find your DNS servers. Figure out how to:

- skip host discovery
- use a grepable output to send results to dns-servers2.txt
- only scan for a single tcp port across 10.0.5.0/24
- only report "open" ports
- see if you can use a bash 1 or 2 liner to list the unique IP addresses that respond to DNS lookups.

Provide a screenshot similar to the one below that shows the nmap run and output as well as the parsing of dns-servers2.txt

```
(champus@kali) - [~/SEC335/SEC-335]
$ sudo nmap -Pn --open -p 53 10.0.5.0/24 -oG dns-servers2.txt
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-30 19:15 EST
Nmap scan report for 10.0.5.22
Host is up (0.0010s latency).

PORT      STATE SERVICE
53/tcp    open  domain

Nmap done: 256 IP addresses (256 hosts up) scanned in 1.77 seconds

(champus@kali) - [~/SEC335/SEC-335]
$ cat dns-servers2.txt
# Nmap 7.93 scan initiated Mon Jan 30 19:15:26 2023 as: nmap -Pn --open -p 53 -oG dns-servers2.txt 10.0.5.0/24
Host: 10.0.5.22 ()      Status: Up
Host: 10.0.5.22 ()      Ports: 53/open/tcp//domain///
# Nmap done at Mon Jan 30 19:15:28 2023 -- 256 IP addresses (256 hosts up) scanned in 1.77 seconds

(champus@kali) - [~/SEC335/SEC-335]
$ cat dns-servers2.txt | grep Host | grep -v Up | cut -f 1,3,4 | cut -d "(" -f 1 | cut -f2 -d ":"
10.0.5.22
```

Deliverable 6. The following nmap command will use -sL (list targets) while specifying a dns server. See if you can do some magic with grep and cut or awk to produce output similar to the one below. Provide a screenshot showing your modified nmap run. Note, you may have different hosts listed as our target environment changes and grows over time.

```
(champus@kali) - [~]
$ sudo nmap -sL 10.0.5.0/24 -dns-server 10.0.5.22 --open | grep "shire" | cut -d " " -f5-6
mail.shire.org (10.0.5.19)
www.shire.org (10.0.5.20)
bios.shire.org (10.0.5.21)
ns.shire.org (10.0.5.22)
cupcake.shire.org (10.0.5.23)
bifur.shire.org (10.0.5.24)
pippin.shire.org (10.0.5.25)
prancingpony.shire.org (10.0.5.26)
arwen.shire.org (10.0.5.27)
nancurunir.shire.org (10.0.5.28)
gloin.shire.org (10.0.5.31)
fw-rivendell.shire.org (10.0.5.250)
```

Deliverable 7. zt.txt should have some useful information, see what you can do to parse it in a manner that we have a hostname and associated ip address. Provide a screenshot similar to the one below. Note, the screenshot below is not quite perfect as not every host has an IP address.

```
(chamuser@kali)~$ cat zt.txt | grep -E "([0-9]{1,3}[.]){3}[0-9]{1,3}" | grep "zonetransfer.me" | awk {'print $1','$5'} | grep -v ";"
zonetransfer.me.,5.196.105.14
14.105.196.5.IN-ADDR.ARPA.zonetransfer.me.,www.zonetransfer.me.
asfdbbox.zonetransfer.me.,127.0.0.1
canberra-office.zonetransfer.me.,202.14.81.230
dc-office.zonetransfer.me.,143.228.181.132
email.zonetransfer.me.,74.125.206.26
home.zonetransfer.me.,127.0.0.1
intns1.zonetransfer.me.,81.4.108.41
intns2.zonetransfer.me.,167.88.42.94
office.zonetransfer.me.,4.23.39.254
owa.zonetransfer.me.,207.46.197.32
alltcpportsopen.firewall.test.zonetransfer.me.,127.0.0.1
vpn.zonetransfer.me.,174.36.59.154
www.zonetransfer.me.,5.196.105.14
zonetransfer.me.,5.196.105.14
14.105.196.5.IN-ADDR.ARPA.zonetransfer.me.,www.zonetransfer.me.
asfdbbox.zonetransfer.me.,127.0.0.1
canberra-office.zonetransfer.me.,202.14.81.230
dc-office.zonetransfer.me.,143.228.181.132
email.zonetransfer.me.,74.125.206.26
home.zonetransfer.me.,127.0.0.1
intns1.zonetransfer.me.,81.4.108.41
intns2.zonetransfer.me.,52.91.28.78
office.zonetransfer.me.,4.23.39.254
owa.zonetransfer.me.,207.46.197.32
alltcpportsopen.firewall.test.zonetransfer.me.,127.0.0.1
vpn.zonetransfer.me.,174.36.59.154
www.zonetransfer.me.,5.196.105.14
```