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.

```
┌──(champuser㉿kali)-[~]
└─$ ./portscanner2.sh 10.0.5 53

  HOSTS    | PORTS
_____________________

 10.0.5.22 | 53

┌──(champuser㉿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.

```
┌──(champuser㉿kali)-[~/SEC335/SEC-335]
└─$ ./portscanner2.sh 10.0.5 53 > dns-servers.txt

┌──(champuser㉿kali)-[~/SEC335/SEC-335]
└─$ 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)

┌──(champuser㉿kali)-[~/SEC335/SEC-335]
└─$ git add .

┌──(champuser㉿kali)-[~/SEC335/SEC-335]
└─$ git commit -m "Week 3 DNS SERVERS"
[main dd9b145] Week 3 DNS SERVERS
 1 file changed, 4 insertions(+)
 create mode 100644 dns-servers.txt

┌──(champuser㉿kali)-[~/SEC335/SEC-335]
└─$ git push
Enter passphrase for key '/home/champuser/.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

┌──(champuser㉿kali)-[~/SEC335/SEC-335]
└─$
```

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.shrire.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

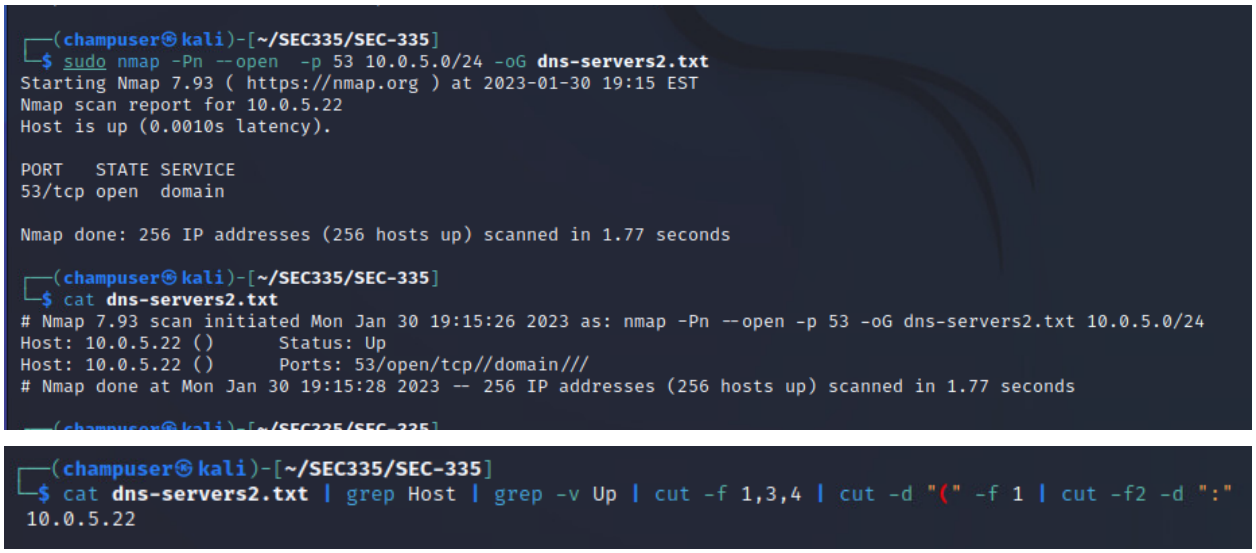
Executable File | 13 lines (7 sloc) | 124 Bytes

```
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



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.

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.