Skyler Kessenich and Grace de Benedetti

1. Passive information gathering:
   a) What domain did you investigate? friendsbalt.org
   b) What is its IP address? 54.209.77.18
   c) When does the domain's registration expire? June 6th, 2025
   d) What information, if any, did you learn about the people or corporation responsible for the domain in question? We learned the organization, got some contact information and a summary of how we registered to gain this information. We got information of the whois server, but when we use the whois website, "Statutory Masking Enabled" for most of the information.

Address and information about the organization:

```
organisation: Public Interest Registry (PIR)
address:      11911 Freedom Drive 10th Floor,
address:      Suite 1000
address:      Reston, VA 20190
address:      United States
```

Contact information for the senior director:

```
contact:      technical
name:         Senior Director, DNS Infrastructure Group
organisation: Afilias
address:      Building 3, Suite 105
address:      300 Welsh Road
address:      Horsham, Pennsylvania 19044
address:      United States
phone:        +1 215.706.5700
fax-no:       +1 215.706.5701
e-mail:       tld-tech-poc@afilias.info
```

How we registered:

```
Domain Name: FRIENDSBALT.ORG
Registry Domain ID: D172823-LROR
Registrar WHOIS Server: whois.networksolutions.com
Registrar URL: http://www.networksolutions.com
Updated Date: 2020-04-04T08:36:14Z
Creation Date: 1996-06-02T04:00:00Z
Registry Expiry Date: 2025-06-01T04:00:00Z
Registrar Registration Expiration Date:
Registrar: Network Solutions, LLC
Registrar IANA ID: 2
Registrar Abuse Contact Email: abuse@web.com
Registrar Abuse Contact Phone: +1.8003337680
Reseller:
```

Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited

2. Host Detection:

a) List the IP addresses for all the active hosts you found on the local network: 10.0.2.1, 10.0.2.2, 10.0.2.4, 10.0.2.15

b) What entities do those IP addresses represent? 10.0.2.1: router (default ip), 10.0.2.2: default gateway for virtualBox, 10.0.2.4: Metasploitable (private ip address), 10.0.2.15: Virtual Machine (this is the default gateway for guest virtual machines)

c) For each possible candidate IP address it was searching in the local network, what steps did nmap take? The local host broadcasts to all possible local ip addresses from 10.0.2.0 to 10.0.2.255 by sending an ARP protocol request saying "who has 10.0.2.# tell 10.0.2.15". If The IP address is active on the local network, it will send back a TCP protocol message with ACK flags.

d) Same question, but for the 137.22.4.0/24 network. 137.22.4.5: elegit.mathcs.edu , 137.22.4.17: perlman.mathcs.carleton.edu, 137.22.4.19: ada.mathcs.carleton.edu, 137.22.4.146: mtietest2.mathcs.carleton.edu, 137.22.4.175: awb1.mathcs.carleton.edu, we also found 137.22.4.20 and 137.22.4.20 but using nslookup did not work. We could find that these two addresses had carle.net as their providers and were located in the central time zone. Our local host sent SYN messages to every ip address on carleton's mathcs network, and waited to see if it was an active ip address by receiving an ACK message in response.

3. Port Scanning:

a) Which ports does Metasploitable have open, and what services do they correspond to (e.g. port 22 / SSH or port 80 / HTTP)?

These are all the ports that 10.0.2.4 has open:

```
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
```

```
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
```

b) What database server(s) is/are available on Metasploitable? mysql and postgresql. I think ingreslock is a database itself, but not a database server?

c) What is the value of the RSA SSH host key? What is the host key for? host key: 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 The host key is used for authentication. It verifies that the client is connecting to the correct host using an RSA key pair.

d) Pick one of the open ports that has a service you have never heard of, and explain what the service does.

port 445-- microsoft-ds is a port with type SMB which stands for Server Message Block. SMB is a protocol used mostly by window servers to give shared access to files and other items such as printers over a network and can also remotely execute commands.