Needle in the TCP/IP Stack

How I “Earned” my Shmoocon Barcode

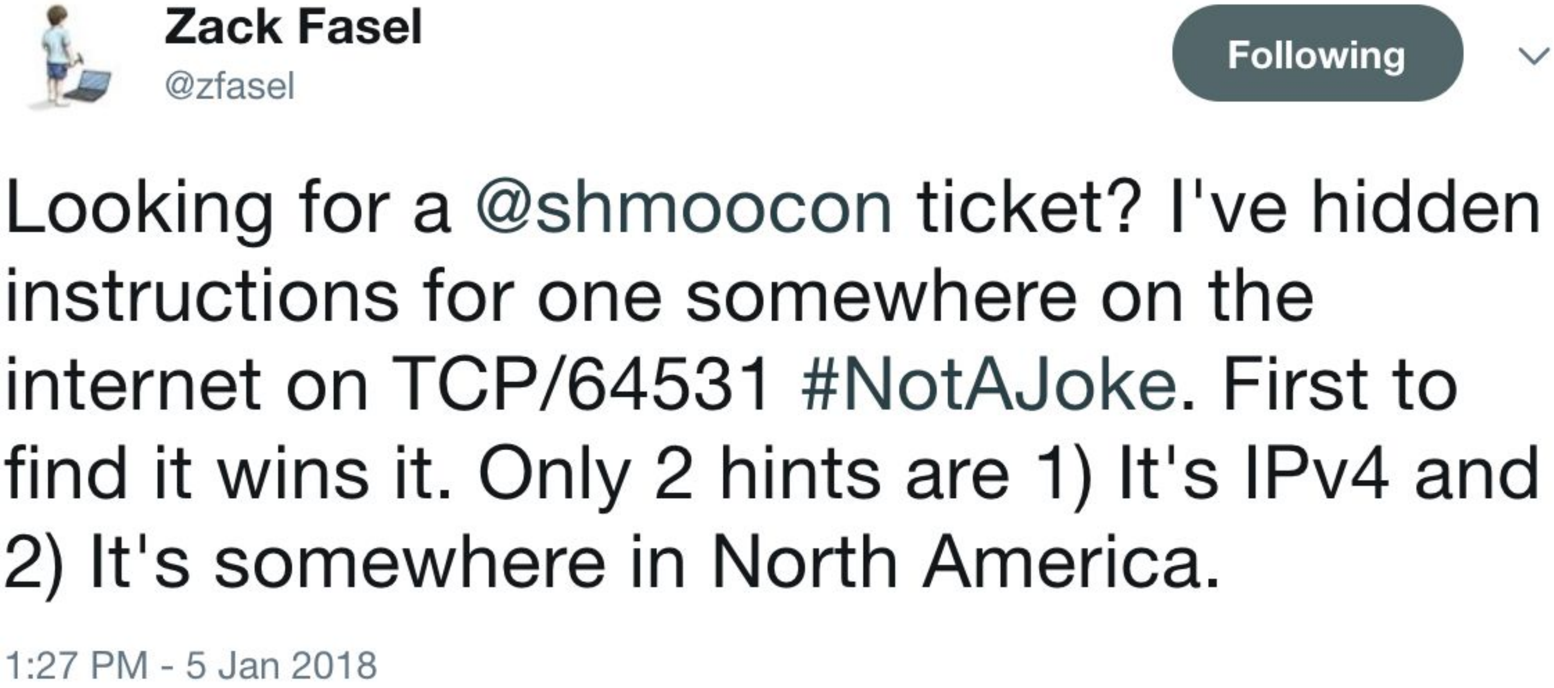
Tom Valadez (@tvldz)

Shmoocon Ticket Stats

There were 1480 tickets released in three sales rounds.

- All tickets were held in 9.50 seconds.
- The wait lists filled up .77 seconds after that.

[0] http://shmoocon.org/2017/12/16/end-of-year-ticket-stats-2018/



Zack Fasel
@zfasel

Looking for a @shmoocon ticket? I've hidden instructions for one somewhere on the internet on TCP/64531 #NotAJoke. First to find it wins it. Only 2 hints are 1) It's IPv4 and 2) It's somewhere in North America.

1:27 PM - 5 Jan 2018

An Aside: Scanning is (still) controversial?

I incorrectly thought that this was now considered benign

https://nmap.org/book/legal-issues.html

HD Moore, on scanning the entire internet: “[It] drew quite a lot of complaints, hate mail, and calls from law enforcement,” he says. “ [0]

I did not, however, receive any abuse complaints.

[0] **https://www.technologyreview.com/s/514066/what-happened-when-one-man-pinged-the-whole-internet/**

~~NEVER TELL ME THE ODDS~~ I SHOULD HAVE CALCULATED THIS EARLIER

Canada, Mexico and USA IPv4 addresses are administered by ARIN and LACNIC

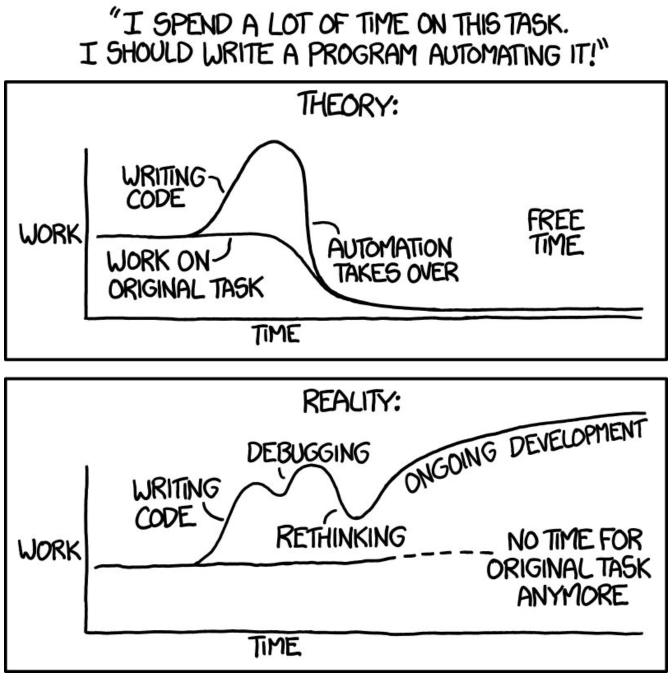
# of IPv4 Addresses Assigned to ARIN ~ 1,459,617,792

# of IPv4 Addresses Assigned to LACNIC ~ 167,772,160

1,627,389,952 IPv4 addresses, or ~37% of the total IPv4 space

It's fun to reinvent the wheel (naively)

“I can achieve this quicker with garbage Python (CTF code) than elegant, efficient code in a lower Level language”



Garbage Python

```
import socket
from threading import Thread
import time
import geoip2.database

def connect(address):
      s = socket.socket()
      s.settimeout(4)
      port = 64531
      try:
            s.connect((address, port))
            s.send("shmoo?\n\r")
            data = s.recv(1024)
            print(data)
            with open('singlehop-out.txt', 'a') as the_file:
            the_file.write(address + " " + data)
      except Exception as e:
            print("something's wrong with %s:%d. Exception is %s" % (address, port, e))
      finally:
            s.close()

with open("singlehop-in.txt") as f:
      content = f.readlines()
      for address in content:
            t = Thread(target=connect, args=(address,))
            t.start()
```

Limits and issues

- File Descriptor Limit
  - **`/etc/security/limits.conf`**
- TCP Timeouts
  - How do I know the connection lasted long enough for a response?
  - How do I minimize the number of open sockets?
- Sequential Scanning is Abusive
- How can I make this more efficient and balanced?
  - Producer-Consumer?
  - IP Randomization?
  - Maybe not Python

THE WHEEL 2.0

MASSCAN

https://github.com/robertdavidgraham/masscan

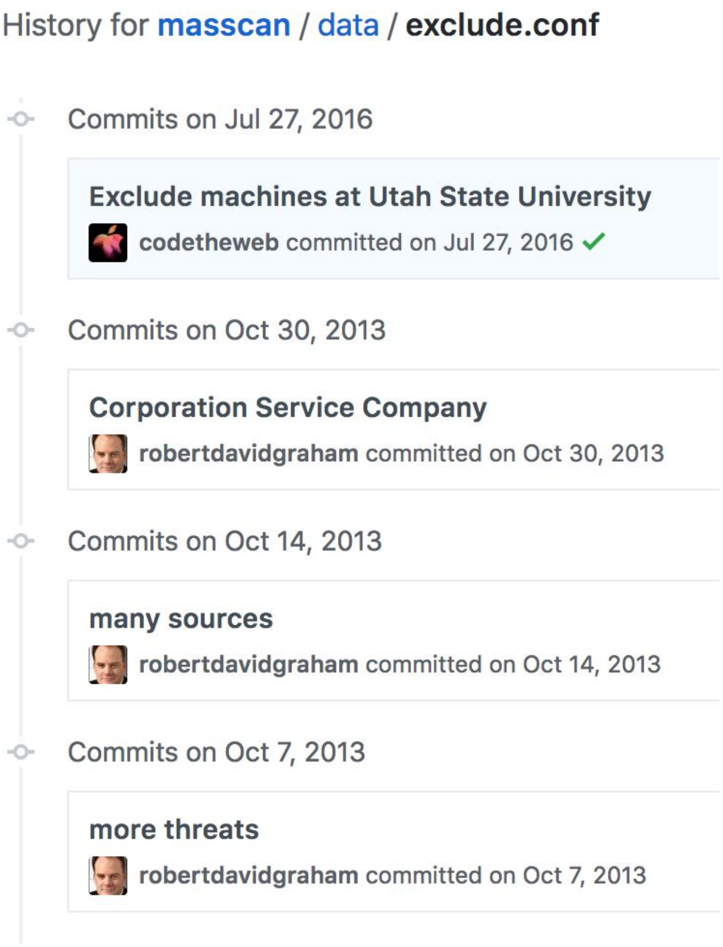
@ErrataRob

“It can scan the entire Internet in under 6 minutes, transmitting 10 million packets per second.”

- Asynchronous, with separate transmit/receive threads
- Usage similar to nmap
- Can use PF_Ring kernel modules
- Banner grabbing

Masscan Abuse Mitigation

- Masscan randomizes target IPs
- Built-in blacklist, exclude.conf



History for masscan / data / exclude.conf

Commits on Jul 27, 2016

Exclude machines at Utah State University
codetheweb committed on Jul 27, 2016 ✓

Commits on Oct 30, 2013

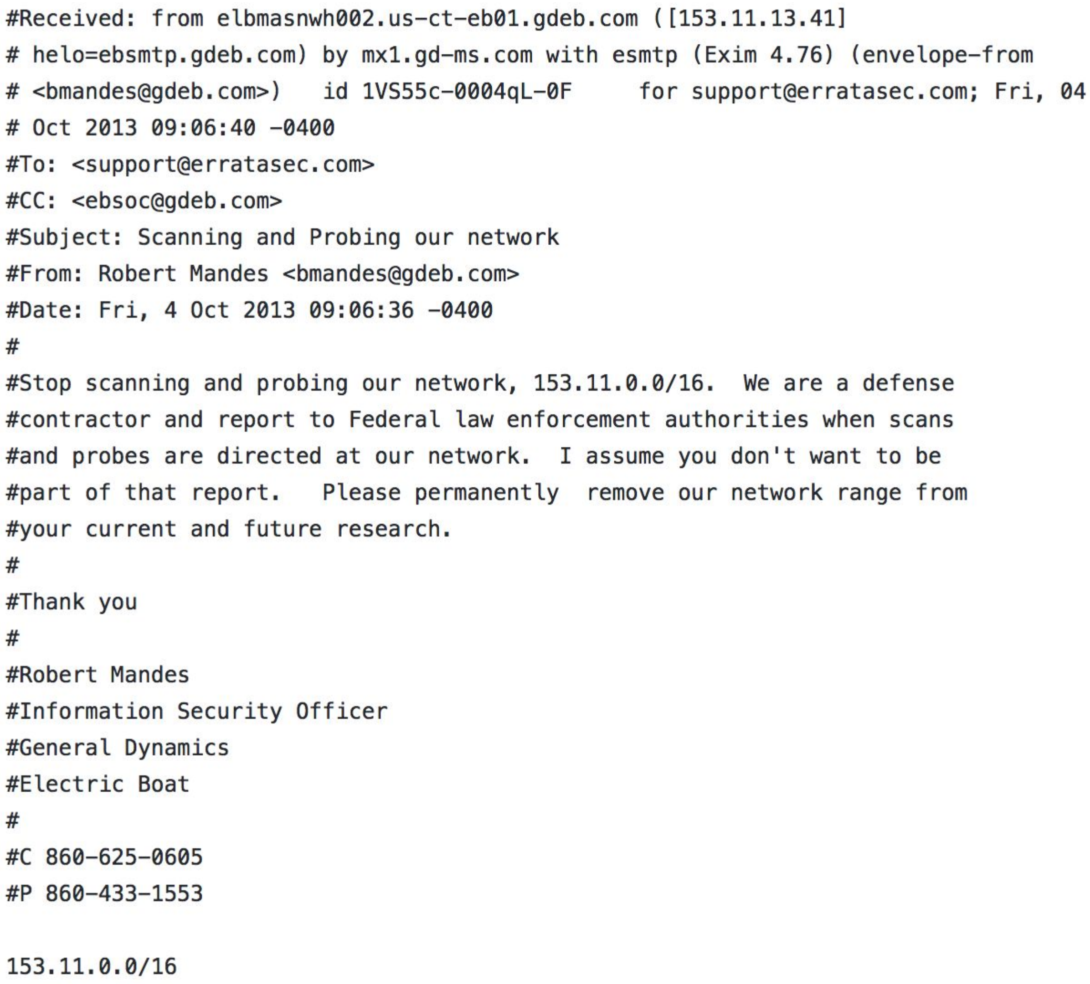
Corporation Service Company
robertdavidgraham committed on Oct 30, 2013

Commits on Oct 14, 2013

many sources
robertdavidgraham committed on Oct 14, 2013

Commits on Oct 7, 2013

more threats
robertdavidgraham committed on Oct 7, 2013



```
#Received: from elbmasnwh002.us-ct-eb01.gdeb.com ([153.11.13.41]
# helo=ebsmtp.gdeb.com) by mx1.gd-ms.com with esmtp (Exim 4.76) (envelope-from
# <bmandes@gdeb.com>)   id 1VS55c-0004qL-0F     for support@erratasec.com; Fri, 04
# Oct 2013 09:06:40 -0400
#To: <support@erratasec.com>
#CC: <ebsoc@gdeb.com>
#Subject: Scanning and Probing our network
#From: Robert Mandes <bmandes@gdeb.com>
#Date: Fri, 4 Oct 2013 09:06:36 -0400
#
#Stop scanning and probing our network, 153.11.0.0/16.  We are a defense
#contractor and report to Federal law enforcement authorities when scans
#and probes are directed at our network.  I assume you don't want to be
#part of that report.   Please permanently  remove our network range from
#your current and future research.
#
#Thank you
#
#Robert Mandes
#Information Security Officer
#General Dynamics
#Electric Boat
#
#C 860-625-0605
#P 860-433-1553

153.11.0.0/16
```

Scan Everything

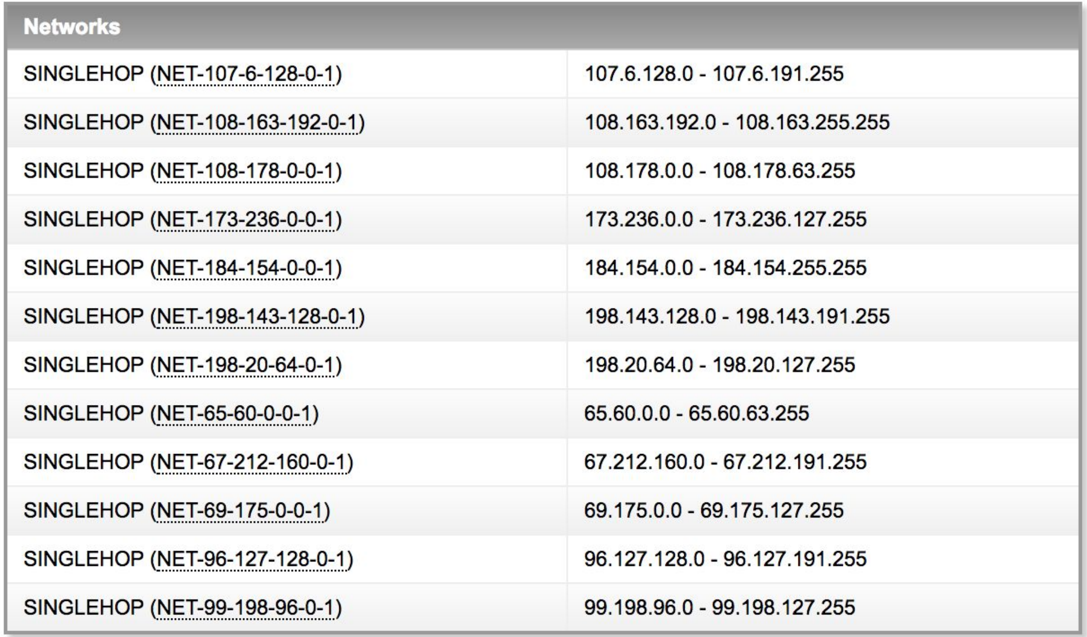
It’s still way too much

- Too many addresses
- Too much data to parse
  - Weird responses that need follow-up
- Actual malicious actors
  - Two fake services discovered containing the string “shmoocon”
- Intuitively abusive

WHERE WOULD THE TARGET HIDE THE FLAG?

- zfasel.com
  - 192.30.252.153
  - GitHub (Pages?)

- urbanesecurity.com
  - 96.127.157.27
  - SingleHop



Networks	
SINGLEHOP (NET-107-6-128-0-1)	107.6.128.0 - 107.6.191.255
SINGLEHOP (NET-108-163-192-0-1)	108.163.192.0 - 108.163.255.255
SINGLEHOP (NET-108-178-0-0-1)	108.178.0.0 - 108.178.63.255
SINGLEHOP (NET-173-236-0-0-1)	173.236.0.0 - 173.236.127.255
SINGLEHOP (NET-184-154-0-0-1)	184.154.0.0 - 184.154.255.255
SINGLEHOP (NET-198-143-128-0-1)	198.143.128.0 - 198.143.191.255
SINGLEHOP (NET-198-20-64-0-1)	198.20.64.0 - 198.20.127.255
SINGLEHOP (NET-65-60-0-0-1)	65.60.0.0 - 65.60.63.255
SINGLEHOP (NET-67-212-160-0-1)	67.212.160.0 - 67.212.191.255
SINGLEHOP (NET-69-175-0-0-1)	69.175.0.0 - 69.175.127.255
SINGLEHOP (NET-96-127-128-0-1)	96.127.128.0 - 96.127.191.255
SINGLEHOP (NET-99-198-96-0-1)	99.198.96.0 - 99.198.127.255

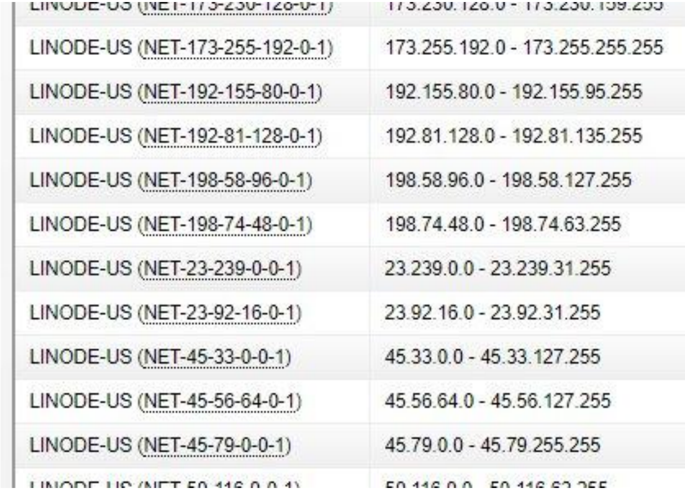
Where Would I Hide The Flag?

My personal shell/VPS progression:

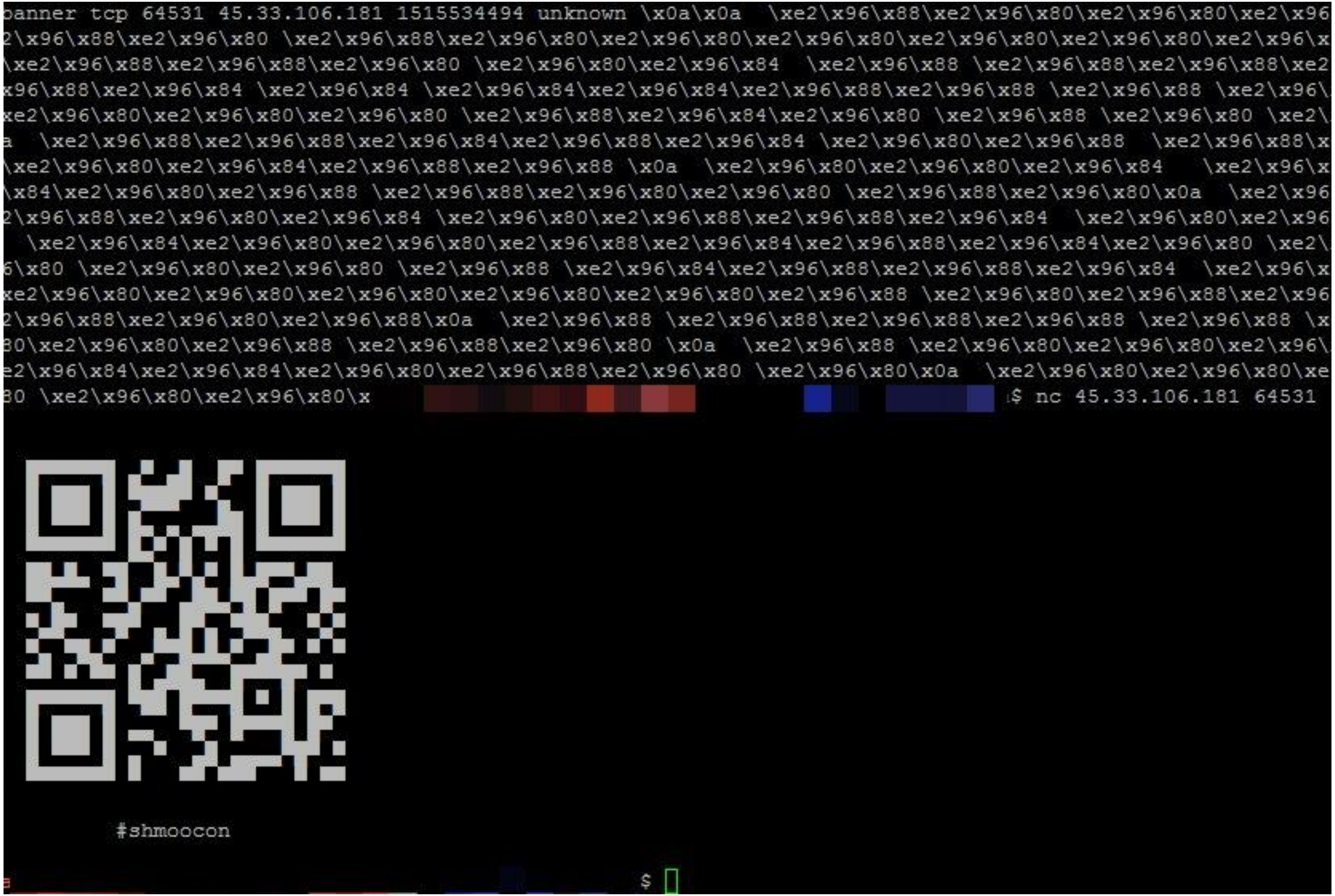
Dreamhost > Linode > Digital Ocean > AWS/Lightsail

Others:

Azure, RackSpace Cloud, SoftLayer?



LINODE-US (NET-173-230-128-0-1)	173.230.128.0 - 173.230.159.255
LINODE-US (NET-173-255-192-0-1)	173.255.192.0 - 173.255.255.255
LINODE-US (NET-192-155-80-0-1)	192.155.80.0 - 192.155.95.255
LINODE-US (NET-192-81-128-0-1)	192.81.128.0 - 192.81.135.255
LINODE-US (NET-198-58-96-0-1)	198.58.96.0 - 198.58.127.255
LINODE-US (NET-198-74-48-0-1)	198.74.48.0 - 198.74.63.255
LINODE-US (NET-23-239-0-0-1)	23.239.0.0 - 23.239.31.255
LINODE-US (NET-23-92-16-0-1)	23.92.16.0 - 23.92.31.255
LINODE-US (NET-45-33-0-0-1)	45.33.0.0 - 45.33.127.255
LINODE-US (NET-45-56-64-0-1)	45.56.64.0 - 45.56.127.255
LINODE-US (NET-45-79-0-0-1)	45.79.0.0 - 45.79.255.255
LINODE-US (NET-50-116-0-0-1)	50.116.0.0 - 50.116.63.255



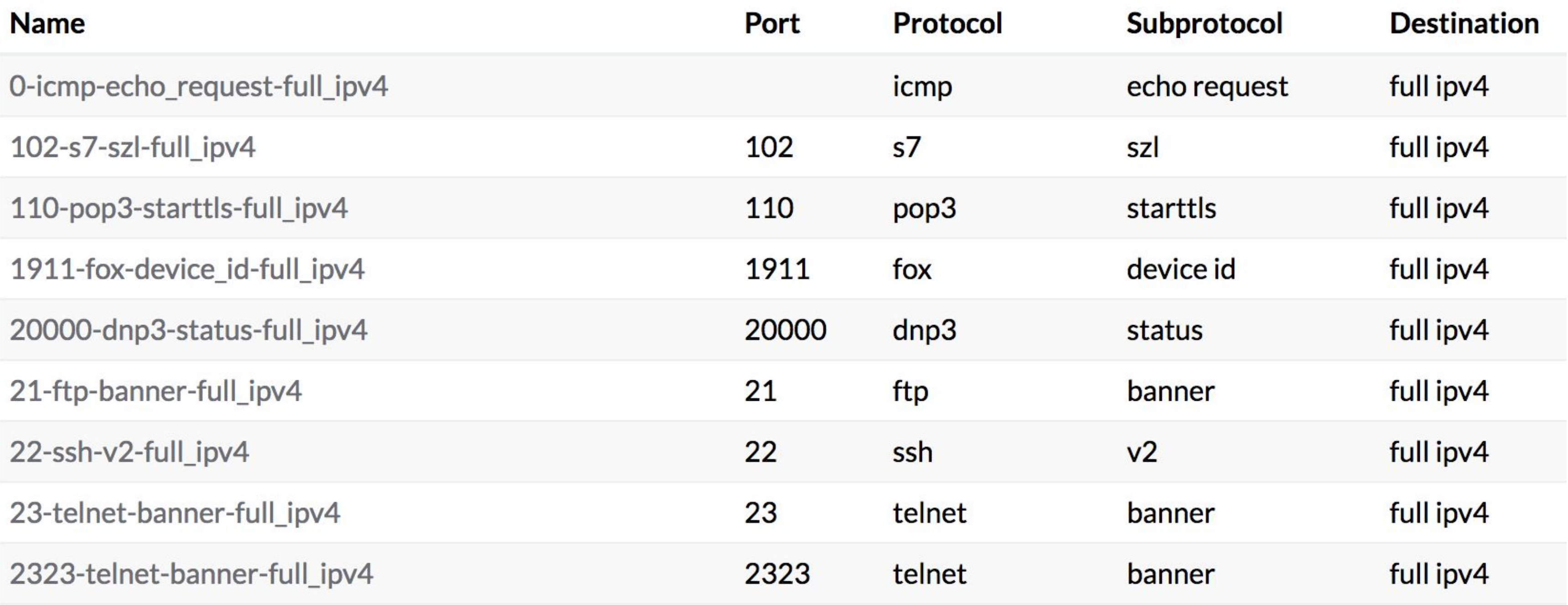
```
banner tcp 64531 45.33.106.181 1515534494 unknown \x0a\x0a  \xe2\x96\x88\xe2\x96\x80\xe2\x96\x80\xe2\x96
2\x96\x88\xe2\x96\x80 \xe2\x96\x88\xe2\x96\x80\xe2\x96\x80\xe2\x96\x80\xe2\x96\x80\xe2\x96\x80\xe2\x96\x
\xe2\x96\x88\xe2\x96\x88\xe2\x96\x80 \xe2\x96\x80\xe2\x96\x84  \xe2\x96\x88 \xe2\x96\x88\xe2\x96\x88\xe2
x96\x88\xe2\x96\x84 \xe2\x96\x84 \xe2\x96\x84\xe2\x96\x84\xe2\x96\x88\xe2\x96\x88 \xe2\x96\x88 \xe2\x96\
xe2\x96\x80\xe2\x96\x80\xe2\x96\x80 \xe2\x96\x88\xe2\x96\x84\xe2\x96\x80 \xe2\x96\x88 \xe2\x96\x80 \xe2\
a  \xe2\x96\x88\xe2\x96\x88\xe2\x96\x84\xe2\x96\x88\xe2\x96\x84 \xe2\x96\x80\xe2\x96\x88  \xe2\x96\x88\x
\xe2\x96\x80\xe2\x96\x84\xe2\x96\x88\xe2\x96\x88 \x0a  \xe2\x96\x80\xe2\x96\x80\xe2\x96\x84   \xe2\x96\x
\x84\xe2\x96\x80\xe2\x96\x88 \xe2\x96\x88\xe2\x96\x80\xe2\x96\x80 \xe2\x96\x88\xe2\x96\x80\x0a  \xe2\x96
2\x96\x88\xe2\x96\x80\xe2\x96\x84 \xe2\x96\x80\xe2\x96\x88\xe2\x96\x88\xe2\x96\x84  \xe2\x96\x80\xe2\x96
  \xe2\x96\x84\xe2\x96\x80\xe2\x96\x80\xe2\x96\x88\xe2\x96\x84\xe2\x96\x88\xe2\x96\x84\xe2\x96\x80 \xe2\
6\x80 \xe2\x96\x80\xe2\x96\x80 \xe2\x96\x88 \xe2\x96\x84\xe2\x96\x88\xe2\x96\x88\xe2\x96\x84  \xe2\x96\x
xe2\x96\x80\xe2\x96\x80\xe2\x96\x80\xe2\x96\x80\xe2\x96\x80\xe2\x96\x88 \xe2\x96\x80\xe2\x96\x88\xe2\x96
2\x96\x88\xe2\x96\x80\xe2\x96\x88\x0a  \xe2\x96\x88 \xe2\x96\x88\xe2\x96\x88\xe2\x96\x88 \xe2\x96\x88 \x
80\xe2\x96\x80\xe2\x96\x88 \xe2\x96\x88\xe2\x96\x80 \x0a  \xe2\x96\x88 \xe2\x96\x80\xe2\x96\x80\xe2\x96\
e2\x96\x84\xe2\x96\x84\xe2\x96\x80\xe2\x96\x88\xe2\x96\x80 \xe2\x96\x80\x0a  \xe2\x96\x80\xe2\x96\x80\xe
80 \xe2\x96\x80\xe2\x96\x80\x    [redacted]    [redacted]$ nc 45.33.106.181 64531



        #shmoocon

                    [redacted] $ 
```

Another Tool: Zmap Project (zmap.io)

ZMap / ZGrab / ZDNS / ZBrowse / ZAnnotate

```
$ zmap -p 443 --output-fields=* | ztee results.csv | zgrab
--port 443 --tls --http="/" --output-file=banners.json
```

Existing Data sets: Scans.io & Censys.io



Name	Port	Protocol	Subprotocol	Destination
0-icmp-echo_request-full_ipv4		icmp	echo request	full ipv4
102-s7-szl-full_ipv4	102	s7	szl	full ipv4
110-pop3-starttls-full_ipv4	110	pop3	starttls	full ipv4
1911-fox-device_id-full_ipv4	1911	fox	device id	full ipv4
20000-dnp3-status-full_ipv4	20000	dnp3	status	full ipv4
21-ftp-banner-full_ipv4	21	ftp	banner	full ipv4
22-ssh-v2-full_ipv4	22	ssh	v2	full ipv4
23-telnet-banner-full_ipv4	23	telnet	banner	full ipv4
2323-telnet-banner-full_ipv4	2323	telnet	banner	full ipv4

Lessons Learned

- It’s fun and informative to re-invent things
- Masscan and Zmap are the right tool for mass scanning
- Don’t take a problem at face value, think of possible targets
- Don’t always trust scanner output
- IPv4 is still pretty small.

Questions?