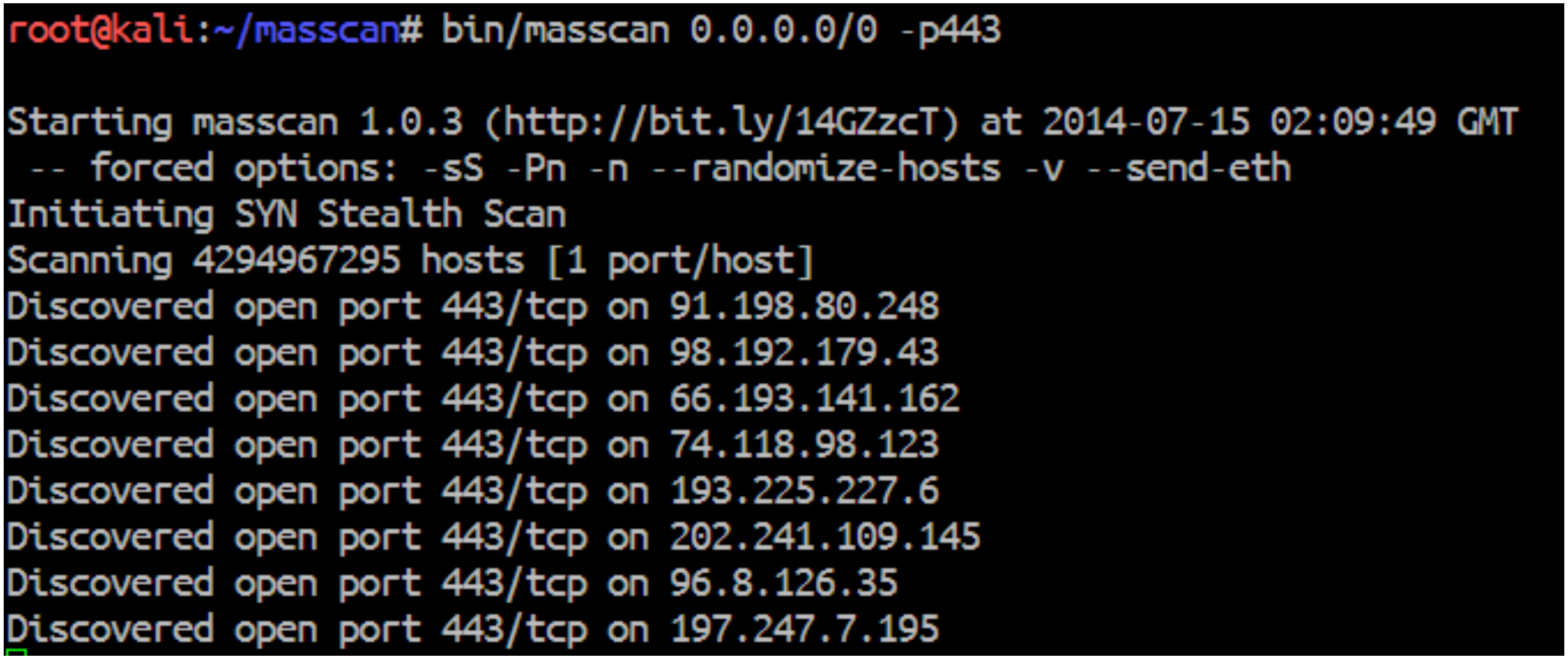
Mass Scanning the Internet

Tips, tricks, results

Robert Graham
Paul McMillan
Dan Tentler

0.0.0.0/0



```
root@kali:~/masscan# bin/masscan 0.0.0.0/0 -p443

Starting masscan 1.0.3 (http://bit.ly/14GZzcT) at 2014-07-15 02:09:49 GMT
 -- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 4294967295 hosts [1 port/host]
Discovered open port 443/tcp on 91.198.80.248
Discovered open port 443/tcp on 98.192.179.43
Discovered open port 443/tcp on 66.193.141.162
Discovered open port 443/tcp on 74.118.98.123
Discovered open port 443/tcp on 193.225.227.6
Discovered open port 443/tcp on 202.241.109.145
Discovered open port 443/tcp on 96.8.126.35
Discovered open port 443/tcp on 197.247.7.195
```

Why scan the Internet (defensive)

- How many systems are vulnerable to Heartbleed?
- How many systems can be used for NTP amplification?
- How many systems vulnerable to D-Link router vulnerability/
- Survey all SSL certificates in use

Why scan the Internet (offensive)

- Uh, it’s the deepnet
- Pick a random port, run masscan with “—banners”, and you find something hackable within minutes

Why scan the Internet (really)

- Because it's fun
- Because it's informative
  - You can't appreciate how small the Internet is until you've scanned 0.0.0.0/0
- It'll make you famous
  - Pick a target, like a Siemens control system
  - Scan the Internet for it
  - Do a BlackHat talk
  - Get in the news

Theoretical Physical infrastructure

- Packets have overhead
  - Ethernet packets have 44 bytes overhead
  - TCP SYN packets are 40 bytes
- Max rate for 1-gbps Ethernet
  - 476-mbps of actual traffic
  - 524-mbps of Ethernet overhead
  - 1,488,000 packets/second

http://blog.erratasec.com/2013/10/whats-max-speed-on-ethernet.html

ISP billing

- Some ISPs measure Ethernet rate
  – Charge you for the full 1-gbps
- Some ISPs measure WAN rate
  – Charge you for ~600-mbps
- Some ISPs don’t see the small packets
  – This one time, ISP didn’t see our outbound traffic, only inbound
- Some ISPs are unmetered
  – Yea!

Practical Physical Infrastructure

- VPS can strain under the load of small packets
- Ethernet switches struggle with small packets
  - Above 500kpps is often difficult
  - Turning off flow-control may help
- Some parts may drop packets
  - Transmitting 500kpps doesn't mean all packets are reaching the Internet
- I usually do ~150kpps
  - When I don't particularly care about speed

Abuse complaints

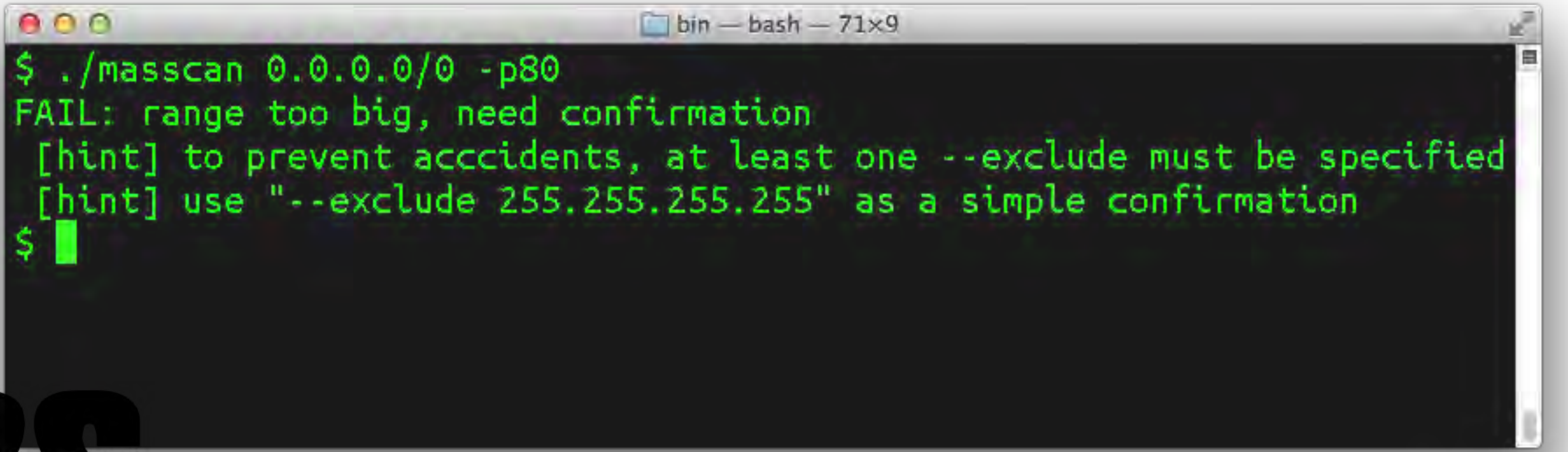
- You *will* get abuse complaints
- Your ISP *will* get upset
- Some things are worse than others
  - Heartbleed scans generate abuse complaints weeks later
  - HTTP scans get you put on fail2ban lists
  - Snort/emergingthreat rules generate a lot of complaints

ISPs must take this seriously

- Some networks react by blackholing the entire AS
- DoD gets real pissy

Maintain exclude list

- /etc/masscan/masscan.conf
- exclude = 224.0.0.0-255.255.255.255
- exclude-file = exclude.ips



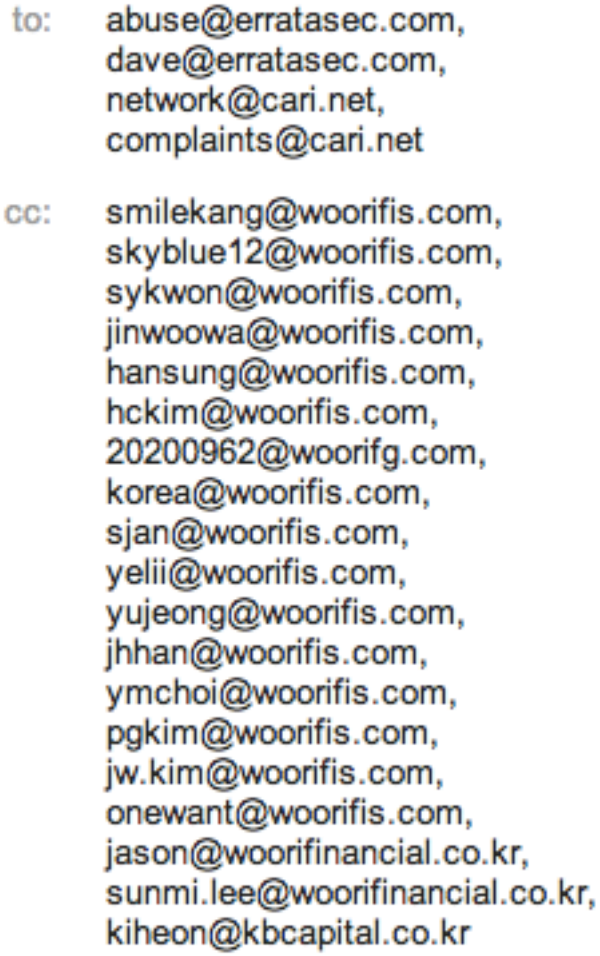
```
$ ./masscan 0.0.0.0/0 -p80
FAIL: range too big, need confirmation
 [hint] to prevent acccidents, at least one --exclude must be specified
 [hint] use "--exclude 255.255.255.255" as a simple confirmation
$ 
```

Complainers are often dicks

- “I’m going to call the Internet Police on you”
- “We’ve blocked you at the firewall, so there! neener-neener”

Complainers are often stupid

- "The infrastructure of Woori Financial Group is classified as "National Security Objective Facility - class A" and unauthorized access to this facility is strictly prohibited by related laws and regulations."



to: abuse@erratasec.com,
dave@erratasec.com,
network@cari.net,
complaints@cari.net

cc: smilekang@woorifis.com,
skyblue12@woorifis.com,
sykwon@woorifis.com,
jinwoowa@woorifis.com,
hansung@woorifis.com,
hckim@woorifis.com,
20200962@woorifg.com,
korea@woorifis.com,
sjan@woorifis.com,
yelii@woorifis.com,
yujeong@woorifis.com,
jhhan@woorifis.com,
ymchoi@woorifis.com,
pgkim@woorifis.com,
jw.kim@woorifis.com,
onewant@woorifis.com,
jason@woorifinancial.co.kr,
sunmi.lee@woorifinancial.co.kr,
kiheon@kbcapital.co.kr

Friendly with ISP

- We work closely with our ISP
- Provide free cybersec consulting
- Handle abuse complaints ourselves
  - SWIP – Shared WHOIS Project
- Add everyone who asks to our “exclude” aka “blacklist” file

…or you can do anonymous VPS

- Pay cheap VPS provider with Bitcoin
- You can complete the scan and be done before complaints cause them to shut down your account
- A lot of them are shady operators friendly to spam and scammers anyway

masscan

-

like nmap

- *All* nmap options are parsed
  - …if only to say “this nmap option isn’t supported”
- Output formats close to nmap
  - Can be imported into some tools
- Lots of features supported
  - SCTP scanning
  - UDP nmap-payloads

unlike nmap

- *Port-at-a-Time* instead of *Host-at-a-Time*
  - Results for each port reported as soon as it's found
  - Results are not combined together per host
- …because it's asynchronous
  - Transmit thread spews out requests
  - Receive thread receives responses
- …making it 1000 times faster

Nmap is a better scanner

- NSE is way cool
- Scanning a single host is way better

- Masscan is simply a *faster* or *more scalable* scanner for large networks

It’s own TCP/IP stack!!#$%^@

- Masscan has it’s own TCP/IP stack
  - Runs side-by-side with existing stack
  - Defaults to same address
  - Causes duplicate ARPs and TCP RST
- OS RSTs prevent TCP connections from being established
  - Should spoof different IP address or filter range of ports to prevent this

Banner checking

- Establishes TCP connection
- Heuristics figure out protocols
  - Scan for port 443 of Internet reveals a lot of SSH and HTTP running on that port
- Only a few things supported right now
  - One of these days I’ll NSE-style scripting, but right now you can hard-code C stuff

Multiple sources

- --shard 1/50
  - Used when doing the same scan from multiple machines
- --source-ip 10.0.0.32-10.0.0.63
  - Spreads out a scan from multiple IP addresses from the same machine
- --source-ip 0.0.0.0-255.255.255.255
  - …for when you want to be a dick

Load testing

- ~~This will crash firewalls~~
- Great for load testing firewalls
- --infinite --banners --source-ip <range>
  - Maintains lots of open connections with target

Binary format

- Use “-oB foo.scan” instead of “-oX foo.xml”
- Then convert:

```
masscan –readscan foo.scan –oX foo.xml
```

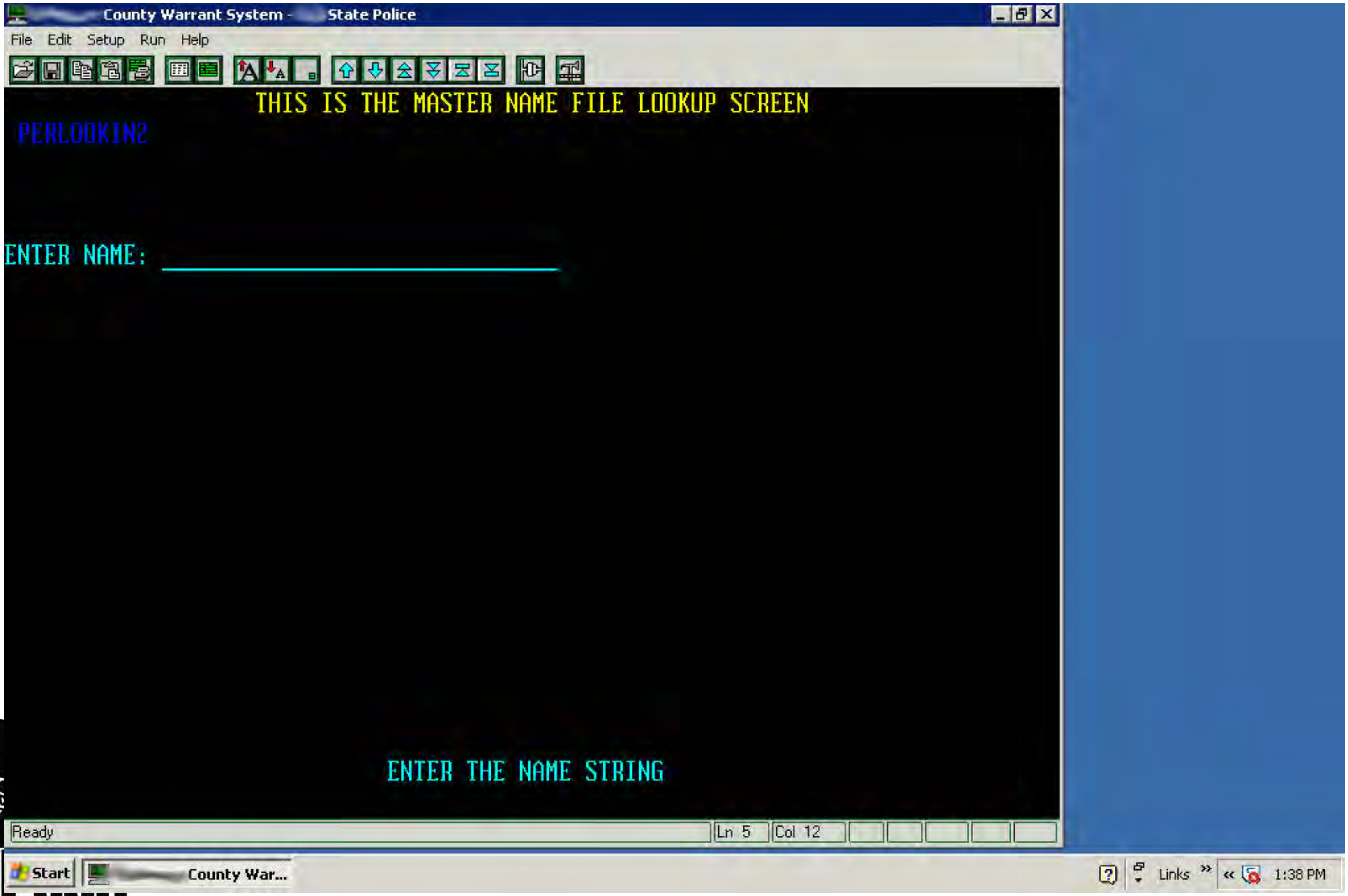
- Because
  - It’s more compact
  - If there’s bugs in output, I can fix them

Spoof scan

- Receive on one IP address
  - Such as a burner Android phone
  - Receiving packets is low-bandwidth
- Send from data center without egress filtering
  - --source-ip spoofing the other source address

results

VNC scanning



[redacted] County Warrant System - [redacted] State Police

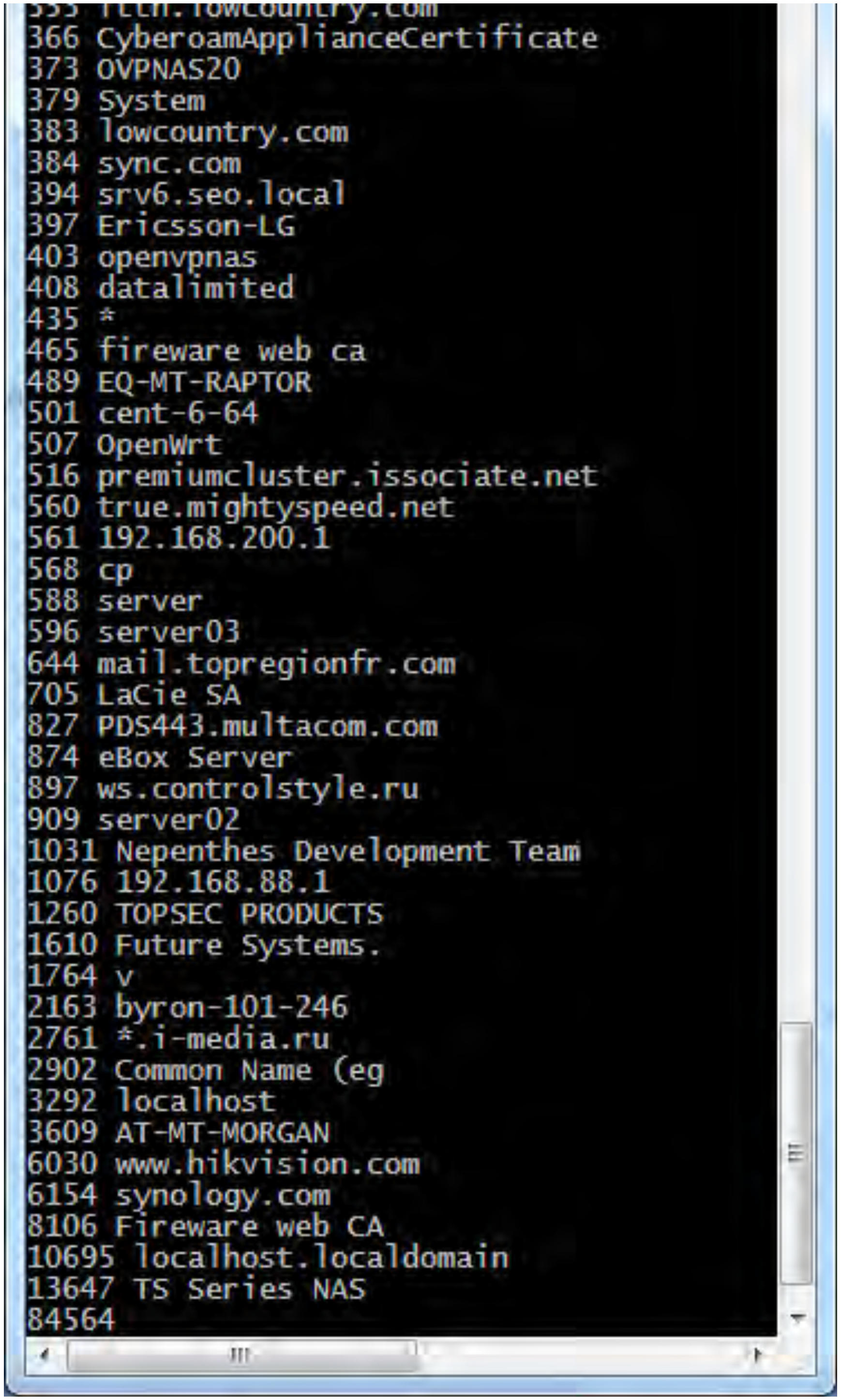
```
                    THIS IS THE MASTER NAME FILE LOOKUP SCREEN
 PERLOOKIN2



ENTER NAME: ______________________________









                              ENTER THE NAME STRING
```

Ready   Ln 5   Col 12

[redacted] County War...

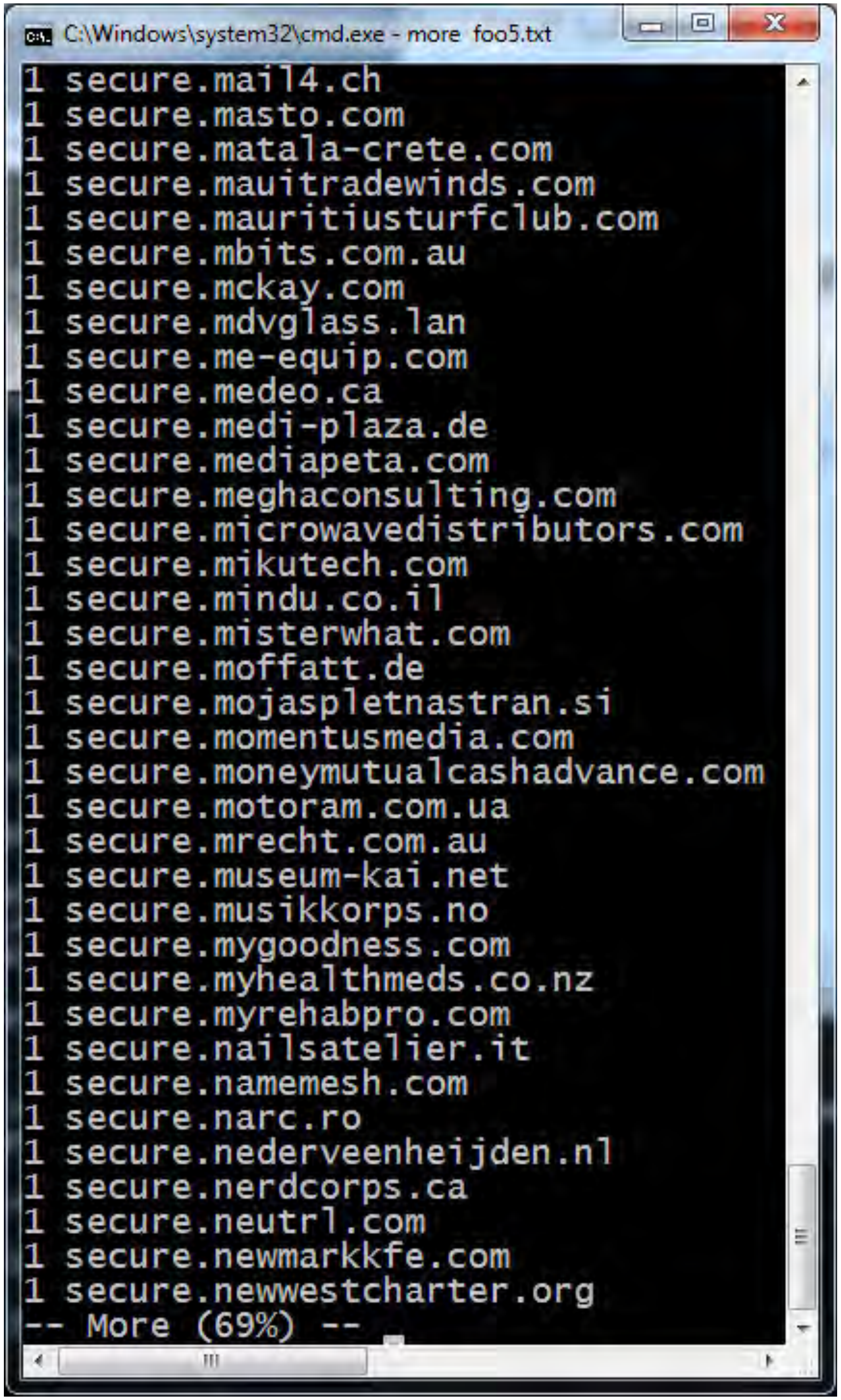
Heartbleed

- 600k systems vulnerable April 10
- 300k system still vulnerable July
  - – Mostly “devices”



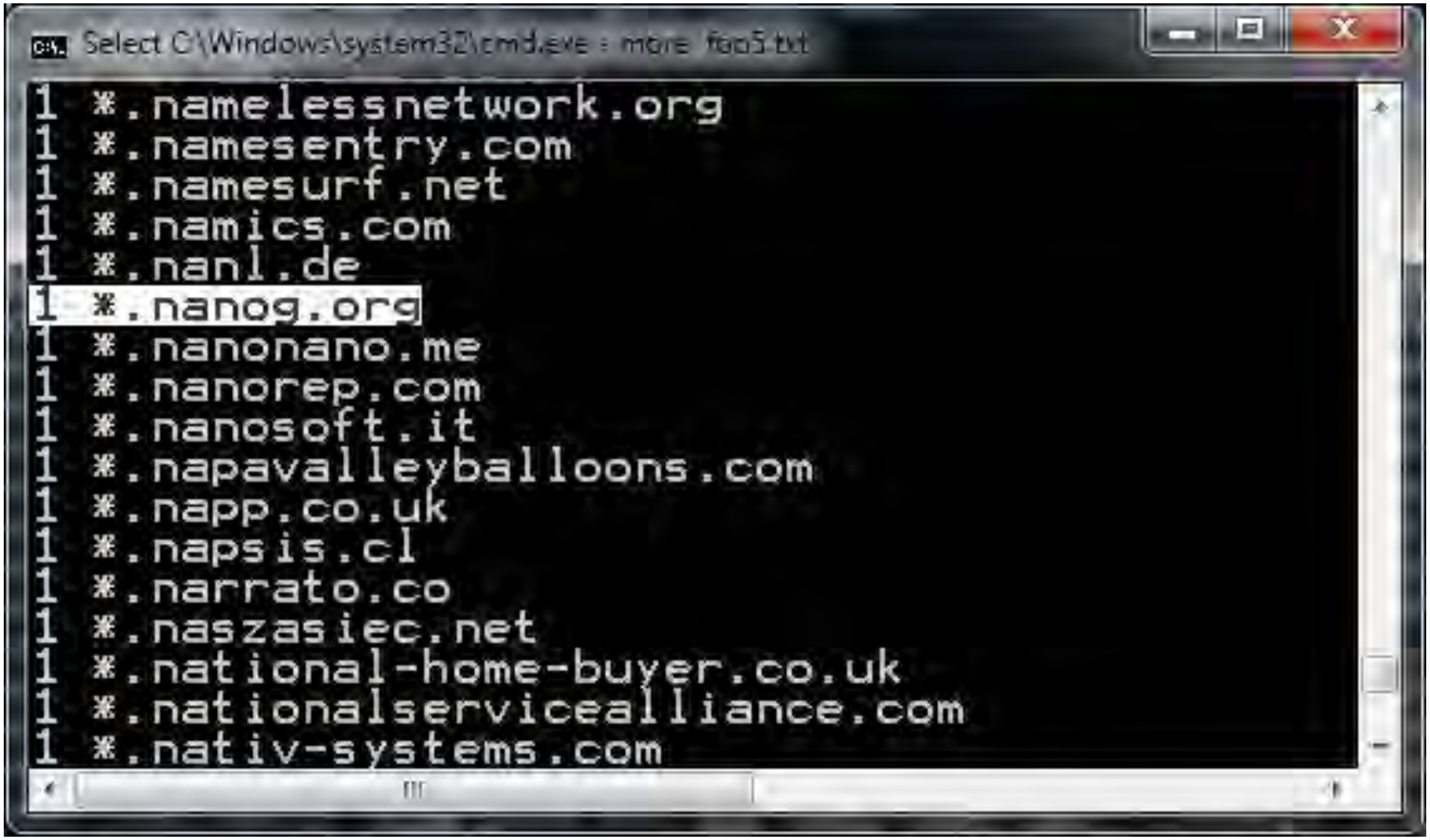
```
355 ftth.lowcountry.com
366 CyberoamApplianceCertificate
373 OVPNAS20
379 System
383 lowcountry.com
384 sync.com
394 srv6.seo.local
397 Ericsson-LG
403 openvpnas
408 datalimited
435 *
465 fireware web ca
489 EQ-MT-RAPTOR
501 cent-6-64
507 OpenWrt
516 premiumcluster.issociate.net
560 true.mightyspeed.net
561 192.168.200.1
568 cp
588 server
596 server03
644 mail.topregionfr.com
705 LaCie SA
827 PDS443.multacom.com
874 eBox Server
897 ws.controlstyle.ru
909 server02
1031 Nepenthes Development Team
1076 192.168.88.1
1260 TOPSEC PRODUCTS
1610 Future Systems.
1764 v
2163 byron-101-246
2761 *.i-media.ru
2902 Common Name (eg
3292 localhost
3609 AT-MT-MORGAN
6030 www.hikvision.com
6154 synology.com
8106 Fireware web CA
10695 localhost.localdomain
13647 TS Series NAS
84564
```

Secure: you keep using that word



```
1 secure.mail4.ch
1 secure.masto.com
1 secure.matala-crete.com
1 secure.mauitradewinds.com
1 secure.mauritiusturfclub.com
1 secure.mbits.com.au
1 secure.mckay.com
1 secure.mdvglass.lan
1 secure.me-equip.com
1 secure.medeo.ca
1 secure.medi-plaza.de
1 secure.mediapeta.com
1 secure.meghaconsulting.com
1 secure.microwavedistributors.com
1 secure.mikutech.com
1 secure.mindu.co.il
1 secure.misterwhat.com
1 secure.moffatt.de
1 secure.mojaspletnastran.si
1 secure.momentusmedia.com
1 secure.moneymutualcashadvance.com
1 secure.motoram.com.ua
1 secure.mrecht.com.au
1 secure.museum-kai.net
1 secure.musikkorps.no
1 secure.mygoodness.com
1 secure.myhealthmeds.co.nz
1 secure.myrehabpro.com
1 secure.nailsatelier.it
1 secure.namemesh.com
1 secure.narc.ro
1 secure.nederveenheijden.nl
1 secure.nerdcorps.ca
1 secure.neutrl.com
1 secure.newmarkkfe.com
1 secure.newwestcharter.org
-- More (69%) --
```

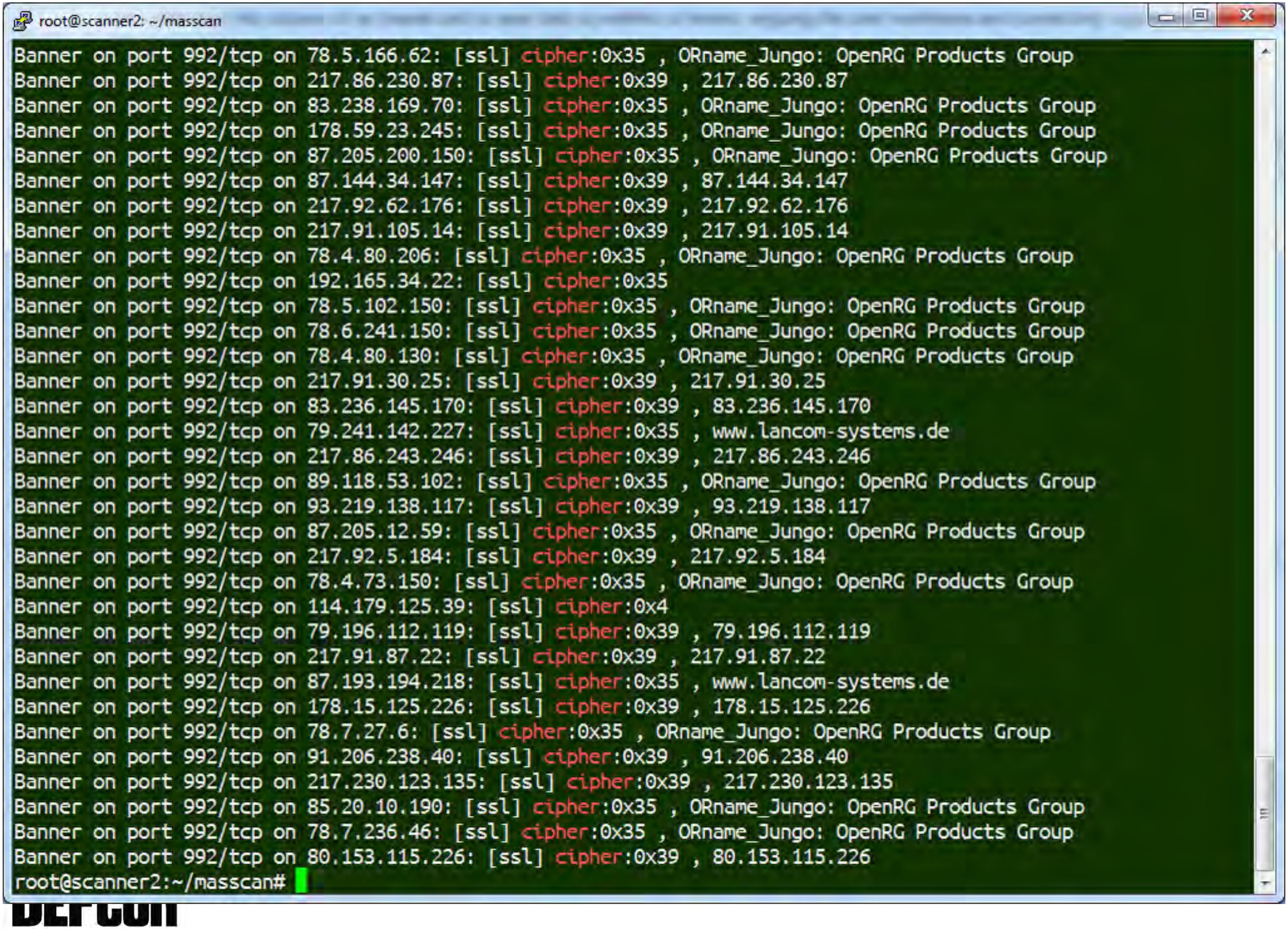
Some I think are just honeypots



```
1 *.namelessnetwork.org
1 *.namesentry.com
1 *.namesurf.net
1 *.namics.com
1 *.nanl.de
1 *.nanog.org
1 *.nanonano.me
1 *.nanorep.com
1 *.nanosoft.it
1 *.napavalleyballoons.com
1 *.napp.co.uk
1 *.napsis.cl
1 *.narrato.co
1 *.naszasiec.net
1 *.national-home-buyer.co.uk
1 *.nationalservicealliance.com
1 *.nativ-systems.com
```

Mainframe scanning

- TN3270 Telnet-over-SSL port 992
- Look at @mainframed767 for cool pics of IBM Mainframe login screens



```
Banner on port 992/tcp on 78.5.166.62: [ssl] cipher:0x35 , ORname_Jungo: OpenRG Products Group
Banner on port 992/tcp on 217.86.230.87: [ssl] cipher:0x39 , 217.86.230.87
Banner on port 992/tcp on 83.238.169.70: [ssl] cipher:0x35 , ORname_Jungo: OpenRG Products Group
Banner on port 992/tcp on 178.59.23.245: [ssl] cipher:0x35 , ORname_Jungo: OpenRG Products Group
Banner on port 992/tcp on 87.205.200.150: [ssl] cipher:0x35 , ORname_Jungo: OpenRG Products Group
Banner on port 992/tcp on 87.144.34.147: [ssl] cipher:0x39 , 87.144.34.147
Banner on port 992/tcp on 217.92.62.176: [ssl] cipher:0x39 , 217.92.62.176
Banner on port 992/tcp on 217.91.105.14: [ssl] cipher:0x39 , 217.91.105.14
Banner on port 992/tcp on 78.4.80.206: [ssl] cipher:0x35 , ORname_Jungo: OpenRG Products Group
Banner on port 992/tcp on 192.165.34.22: [ssl] cipher:0x35
Banner on port 992/tcp on 78.5.102.150: [ssl] cipher:0x35 , ORname_Jungo: OpenRG Products Group
Banner on port 992/tcp on 78.6.241.150: [ssl] cipher:0x35 , ORname_Jungo: OpenRG Products Group
Banner on port 992/tcp on 78.4.80.130: [ssl] cipher:0x35 , ORname_Jungo: OpenRG Products Group
Banner on port 992/tcp on 217.91.30.25: [ssl] cipher:0x39 , 217.91.30.25
Banner on port 992/tcp on 83.236.145.170: [ssl] cipher:0x39 , 83.236.145.170
Banner on port 992/tcp on 79.241.142.227: [ssl] cipher:0x35 , www.lancom-systems.de
Banner on port 992/tcp on 217.86.243.246: [ssl] cipher:0x39 , 217.86.243.246
Banner on port 992/tcp on 89.118.53.102: [ssl] cipher:0x35 , ORname_Jungo: OpenRG Products Group
Banner on port 992/tcp on 93.219.138.117: [ssl] cipher:0x39 , 93.219.138.117
Banner on port 992/tcp on 87.205.12.59: [ssl] cipher:0x35 , ORname_Jungo: OpenRG Products Group
Banner on port 992/tcp on 217.92.5.184: [ssl] cipher:0x39 , 217.92.5.184
Banner on port 992/tcp on 78.4.73.150: [ssl] cipher:0x35 , ORname_Jungo: OpenRG Products Group
Banner on port 992/tcp on 114.179.125.39: [ssl] cipher:0x4
Banner on port 992/tcp on 79.196.112.119: [ssl] cipher:0x39 , 79.196.112.119
Banner on port 992/tcp on 217.91.87.22: [ssl] cipher:0x39 , 217.91.87.22
Banner on port 992/tcp on 87.193.194.218: [ssl] cipher:0x35 , www.lancom-systems.de
Banner on port 992/tcp on 178.15.125.226: [ssl] cipher:0x39 , 178.15.125.226
Banner on port 992/tcp on 78.7.27.6: [ssl] cipher:0x35 , ORname_Jungo: OpenRG Products Group
Banner on port 992/tcp on 91.206.238.40: [ssl] cipher:0x39 , 91.206.238.40
Banner on port 992/tcp on 217.230.123.135: [ssl] cipher:0x39 , 217.230.123.135
Banner on port 992/tcp on 85.20.10.190: [ssl] cipher:0x35 , ORname_Jungo: OpenRG Products Group
Banner on port 992/tcp on 78.7.236.46: [ssl] cipher:0x35 , ORname_Jungo: OpenRG Products Group
Banner on port 992/tcp on 80.153.115.226: [ssl] cipher:0x39 , 80.153.115.226
root@scanner2:~/masscan#
```

<other results>

<demos>