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

-- 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

• [Link to blog post](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`

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

26 Defcon
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.”
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

THIS IS THE MASTER NAME FILE LOOKUP SCREEN

ENTER NAME: ____________________________

ENTER THE NAME STRING
Heartbleed

- 600k systems vulnerable April 10
- 300k system still vulnerable July
  - Mostly “devices”
Secure: you keep using that word
Some I think are just honeypots
Mainframe scanning

- TN3270 Telnet-over-SSL port 992
- Look at @mainframed767 for cool pics of IBM Mainframe login screens
<other results>
<demos>