InfoSec from an ISP's Perspective

Theo Baschak

BSides Wpg 2013-11-17

Online HTML5 Slides

Presentation source/download available at
github.com/tbaschak/bsideswpg2013-ISPInfoSec

Who I Am

- Employed by VOI Network Solutions – primary administrator of Winnipeg-based commercial Internet Service Provider and carrier.
- Avid Open Source Software user/fanatic, and recently, contributor.
- Involved with both Internet Exchanges in Winnipeg.

1. Elected member on the Board of Directors for the Manitoba Internet Exchange (MBIX).
2. Also involved with the creation and technical operations of the Winnipeg Internet Exchange (WpgIX).

Notable Projects

- GENES: Assisted Genes Telecom with network upstream migrations from Cancom satellite with a /29, to MTS leased line(s), to Manitoba NetSet ethernet.
- WPGWIFI: Ran wpgwifi.com to raise awareness of wireless security.
- BCN: Built BCN's network from the ground up through second generation of network upgrades.
- VOI: Network wide upgrade from mixed vendor to single vendor core.

Overview

- Knowing Your Network
- Problems? What Problems?
- Best Current Practices

Knowing Your Network

- MANY very nice Open Source software tools in this area
- Some proprietary tools have the polish resulting from full-time development time
- Discovery Tools: nmap, metasploit framework, shodanhq
- Monitoring Tools: nagios, observium
- Logging: syslog/syslog-ng, logstash, splunk
- Documentation: IPAM (IP Address Management)

Discovery

- finding abusable services: nmap with scripts or nmap via metasploit
- ex: `nmap -sU -p 53,161 -sC <target/net>`
- metasploit can be more useful for SNMP discovery than nmap just on its own
- shodanhq is also handy, but may not necessarily be up to date
- UDP "small services" not needed, and dangerous potential for abuse as DDoS tools

Monitoring Tools

- Monitoring should be more than just simple up/down alerting
- Ex: high bw usage, packet loss, high CPU usage, high number of smtp messages/sec, BGP session dropped
- Evolution of OSS graphing suites: MRTG . . . Cacti . . . Observium
- . . . Does nothing if not acted upon

Logging

- Dealing with large volumes of logs
- Reviewing logs
- Troubleshooting using logs

Documentation

- Accurate
- Up to date
- Available to those who need it
- Available in common formats
- Easy to understand

Problems? What Problems?

- There are **many** common problems that affect ISPs and even large corporate/enterprise networks.
- To make the situation better, we all have to acknowledge and resolve all reported problems.
- Luckily there are many tools available to make this process easier.

Specific ISP-Related Problems

- 2011 Ubiquiti Worm (exploited lighttpd misconfig)
- BCP38 Filtering
- Open/Unrestricted DNS Resolvers
- Open/Unrestricted SNMP Servers with default/easily guessed credentials (public, private, admin, hp_admin)
- SMTP/SPAM issues
- Automated attacks
- BGP Leaks/Hijacking

2011 Ubiquiti Worm

December 19, 2011 - A botnet-installing worm becomes very public, gregsowell.com, UBNT forums and full-disclosure

This worm targeted the widely popular Ubiquiti ISP platform, versions 3.6.1/4.0/5.x, and downloaded a botnet client to permanent storage on the affected device itself.

Spoofed Traffic & UDP Services

- The lack of source address filtering at the edge of most networks aids spoofing attacks
- There are many, many unintentionally open DNS servers which can be abused from spoofed sources
- Also many devices with default credentials which can be probed by spoofed addresses causing large reflected DDOS attacks
- Some routers don't track these SNMP connections

Automated Attacks

- FTP, SSH, SMTP, RDP, SIP very common
- cause noticeable CPU strain on some devices
- helps to be aware of potential destinations for new attacks (know your network)
- proactive security policies can help protect the network

Significant BGP Events

1. 2008 Pakistan Youtube Nullroute BGP Leak

- AS17557 leaked a /24 which quickly went global – /22 from AS36561 (Before Google)

2. 2012 Bell/Tata BGP Leak

- Major Bell leak noticed by many Canadians

3. 2013 Spamhaus DDoS

- 300 Gbps DDoS also combined with /32 BGP leaks with a fake DNS server

The Pirate Bay ‘Moves to North Korea’

As proof that they know how the internet works better than the authoritites chasing them, The Pirate Bay hijacks some North Korean networks, and injects them into a satellite BGP session in Cambodia.

Best Current Practices

- Very few hard rules on the internet, there are suggested guidelines, but in reality it be very wild west
- "How to interoperate in the network of networks?"
- RFCs and specifically subsection of RFCs dedicated to Best Current Practices which provide guidance
- Spirit of cooperation is what has developed/carried the Internet this far, it is expected that everyone will continue to participate for the greater good

BGP Filtering

- Misconfigs can have global consequences
- Internet largely runs on trust, that trust is very easily abused
- **Always** filter your customers, ideally both on AS-path and their networks announced
- AS-path should begin with their AS, to prevent readvertising internet-learned routes
- Cisco Regex Ex: `ip as-path access-list 1 permit ^65564$`

Edge ACLs

- ACLs on Edge routers can block unknown devices in your network from becoming abusable servers (SMTP, DNS, SNMP)
- BGP, 2+ Upstreams and stateful firewall == Trouble
- Firewalls just inside the Edge are popular too w/ Enterprise networks

Communication With Other ISPs

- Receiving, tracking & acknowledging abuse/hacking/DOS/DDOS reports from other organizations
- Sending & tracking abuse/hacking/DOS/DDOS reports to other organizations
- . . . /dev/null often

The End

Presentation source/download available at
github.com/tbaschak/bsideswpg2013-ISPInfoSec