Netflows
at
The University of Chicago

E. Larry Lidz,
ellidz@uchicago.edu
The University of Chicago
A few notes to start...

• This is how we use flows.
• There are other tools.
  – Some are undoubtedly better.
A brief intro to flows…

- Log flows, not connections.
  - Harder to hide traffic
  - Sometimes direction of connection unclear.
- Not an IDS, but can play one on TV.
  - No signature checking.
  - Logs unknown traffic, too.
- Forensic Tool!
  - You get logs, even if you didn’t know there was a problem.
  - Can often get date, time, method of compromise.
  - Alaska story…
What we watch

• Net Flows
  – All gateway traffic
  – Remotes

• Argus
  – Most, soon to be all, traffic through one of the core switches/routers.
Flow-tools

• Written by Mark Fulmer
  – http://www.splintered.net/sw/flow-tools/

• Capture flow exports from router

• Stored in /var/log/flow/<router>/<file> on log server.
  – Keep 3 months worth, 840GB for flow+argus
  – Merge gateways to one location, kill duplicates.
Flow-tools tools

- flow-capture to capture flows.
- flow-cat to cat a bunch of files together.
- flow-merge to merge the gateways.
- flow-stat to get statistics.
- Occasionally use other programs.
- demo of flow-cat/flow-stat:
flow-extract

• http://security.uchicago.edu/tools/net-forensics/
• Port of TAMU Netlogger’s Extract program to use flow files
  – shows fields in flows but not netlogs
  – more options with which to select
  – ICMP printed similarly to TCP/UDP
• Allows for flexible selection of flows on command line with friendly awk-like syntax.
  – DNS resolution
  – Can be used as a script with #!
Some flow-extract options

- **-b**, output in binary.
  - Useful for piping into flow-stat, etc.
- **-n**, don’t resolve IP or port names
- **-f**, use as a script
- **-D**, resolve IPs, but not port names.
- **-o**, output to `<file>`
- **-z**, compression level
  - similar to flow-cat.
flow-extract selection criteria

- net, srcnet, dstnet
- host, srchost, dsthost, hp, srchp, dsthp
- iface, srciface, dstiface
- port, srcport, dstport, proto, octets, pkts
- flag FIN|SYN|RST|PUSH|ACH|URG
- flags safrpu/safrpu
- date, time, since, before
flow-scripts

- check-scans/check-pingflood
  - flow-dscand does some of this, too…
- flhosts, flports, combo-cx
- connection reports
- doflow.sh, scaneval.sh
- check-scan/connrep output:
- scaneval.sh demo:
Argus

- QoScient’s Argus: http://www.qoscient.com/argus/
- Uses promiscuous interface
- Can export over network
- Can log application data, too!
  - We log 64 bytes… mostly header info.
- argus sends the traffic over the network, ra captures and views it.
- demo of ra.
Future Network
New Design

• Flow stuff stays about the same…
• Argus at each core switch?
  – Could export flows, but it would negatively impact performance as MLS currently uses uni-directional flows
• Connection reports moved to argus?
• …?
Questions?

• Any questions?