

Distributed IDS on JANET

John Green
JANET-CERT
30th June 2004



By analysing traffic sites can...

- Monitor new threats
- Detect misconfiguration
- Spot compromised machines within
- Capacity planning
- Draw pie charts
- Contribute information to community



Current coordination

- Scan reports by email from 2 JANET sites, and one MAN
- Inserted into database for trend analysis
- JANET sources are reported to sites
- Other .edu sources are alerted if time allows
- Very concise. Source IP, Destination Net, Number of Flows, Port, Time/Date



Sources of data



SNMP

- Data retrieved using SNMP
- MRTG, Cricket
- Netsight
- Easy to install and configure
- Useful for spotting odd traffic volumes
- Limited use for finding out what is causing it
- Difficult to automate



Netflow

- Used for
 - Traffic Accounting
 - Billing
 - Network Monitoring
 - Capacity Planning
- Collects flows, not packet contents
- Contains
time,srcaddr,dstaddr,input,output,srcport,dstport,
tcp_flags, proto,tos,nexthop,src_as,dst_as and
many more



Uses

- Processing can identify
 - Dos attacks
 - Large upstream flows
 - Rogue FTP servers
 - P2P usage
 - Flows to ports running no known services
 - Large numbers of outbound SYN
 - Find command and control routes
- Provide much more detail than SNMP
- Argus also popular



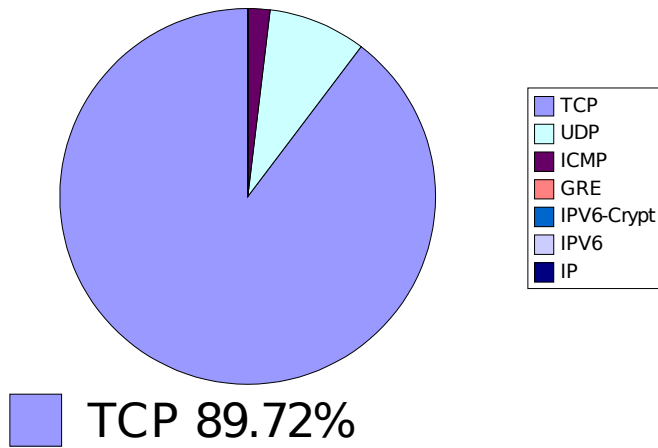
Netflow on the core

- Quantity of data much greater than at site level
 - 1.5GB/hour on global (level3/sprint) transit
- Lack of knowledge about site configuration
- Data storage and access is a bottleneck
- Can spot
 - Flows to known C&C servers
 - Machines scanning
- Administrative overhead

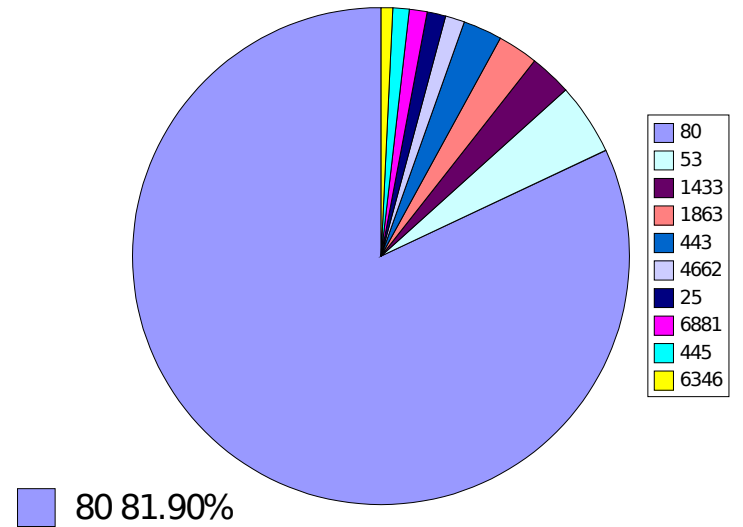


Even simple analysis provides....

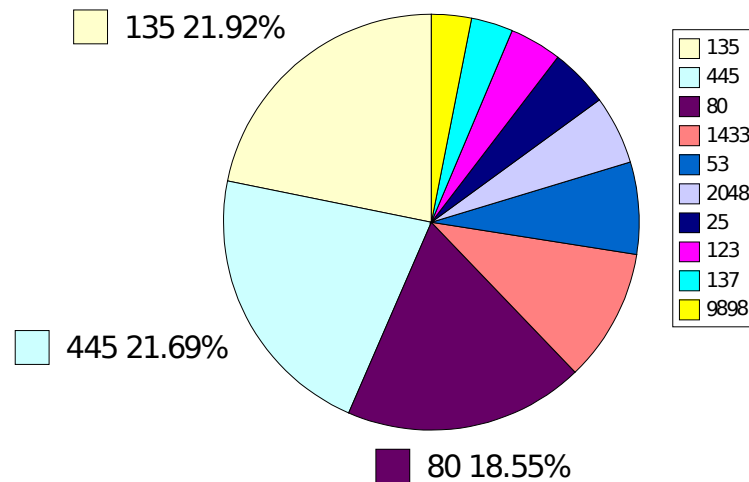
Protocol



Outbound Port



Inbound Port



Packet Level

- Only feasible at site
- IDS useful. Needs to be careful configured
 - False positives, site specific configuration (firewall)
 - Alerts contain sensitive data
 - Packet contents considerably more private
- Easy to get overwhelmed with alerts
- With careful tuning useful to find
 - FTP servers on high ports
 - Infected machines



Note!

- Not interested in systematically collecting IDS and firewall logs
- Privacy
- Site custom configuration skews data
- Other commercial offering available
- ***** Are interested in specific reports *****
 - JANET sources
 - Other “Important” sources



Darknets

- A use for unused address space
- Unpolluted by real network activity
- Only see malicious traffic and backscatter
- Spot new threats and attacks
- Identify infected machines elsewhere (possibly other JANET sites)
- The larger the network the more useful
- Diverse netblocks (/8's) useful



Collaboration

- Collect traffic locally and contribute aggregated or raw (tcpdump?) logs to central repository
- Configure tunnels to route unused space to central collection point
- Data useful to spot new scanning methods
- Correlation with high level (netflow) data



Dim networks and honeypots

- Darknets only see part of the picture
- Useful to
 - Make the network look used
 - Elicit more than just a SYN from attacking machine
 - Spot more than just large scale scanning
- escirt.net sensor uses honeyd and prelude
- More realistic honeypots require a great deal more effort (probably too much)



Recap

- Network flows provide very high level picture
- Can be operated on backbone or MAN
- Packet inspection only realistic at site
- Privacy a concern. IDS often log too much
- Useful for identifying compromised machines
- Darknets useful for spotting attacks
- Honeypots can make it look more realistic



Aggregation

- Data far more valuable if aggregated across the network
- Volume of data likely to be huge
- Require standard format
 - IETF “standard” is IDMEF
 - Useful for single alerts, less good at aggregated
- Prelude comes with robust IDMEF messaging infrastructure and API



Sending IDMEF

- Prelude has C, Perl and Python API
- Or XML easily generated with scripts
- Send by
 - Email
 - Using Prelude messaging layer
- Parsed and inserted into DB



Using the data

- Identifying compromised JANET hosts
- Spotting new trends and patterns
- and....

?

Way forward

- Basic IDMEF reporting system in place
- Require beta testers
- Contact j.green@ukerna.ac.uk
- Mailing list?
- Looking for demand for other services



?

