Michael Forrest (michael.forrest@abdn.ac.uk)

The application of StealthWatch in AbMAN

Tuesday 31st March 2009
Networkshop 37

Previous Monitoring

Michael Forrest (michael.forrest@abdn.ac.uk)

- Basic flow viewing via :-
  - Inmon Traffic Sentinel (2006+)
  - Foundry IronView (2002-2005)
- Interface Traffic Stats via :-
  - MRTG (old)
  - Cacti (new)

University of Aberdeen ©2009
http://www.abdn.ac.uk

Monitoring limitations

Michael Forrest (michael.forrest@abdn.ac.uk)

- Only a viewer of the flow data and very basic extras.
- Inmon has a customised snort based backend, so potential to craft rules as needed.
  - Downloadable rule set for snort didnt really work, since only the packet headers were available from flow data.
  - Supplied with zero rules, up to user to create.
- Cacti is more a historical tool for looking at traffic levels on interfaces.

University of Aberdeen ©2009
http://www.abdn.ac.uk

Monitoring limitations (2)

Michael Forrest (michael.forrest@abdn.ac.uk)

- Requires near constant monitoring to get anything useful out.
- Inmon fits more as a post event tool for looking at what happened.
- Almost need to know what your looking for.
- Too many alerts and these can become like white noise (alerts based on absolute interface thresholds which are user defined).

University of Aberdeen ©2009
http://www.abdn.ac.uk

StealthWatch Features

Michael Forrest (michael.forrest@abdn.ac.uk)

- Uses flow data from Netflow/sflow and/or port mirroring.
- “learns” the normal running environment of the flow data/network.
- Performs Behaviour-based Anomaly Detection.
  - Can detect network issues.
  - Prioritise events using a Concern Index (CI).
- Can perform mitigation on events/alarms.

University of Aberdeen ©2009
http://www.abdn.ac.uk

StealthWatch Features (2)

Michael Forrest (michael.forrest@abdn.ac.uk)

- Track/monitor host behaviour over time.
- Point of View reporting.
  - Based on user/addressing and permissions.
- Can be used for root cause determination after network event outages.
- Useful in capacity planning.
- Able to alert/track worms through network.

University of Aberdeen ©2009
http://www.abdn.ac.uk

StealthWatch RN Deployment

Michael Forrest (michael.forrest@abdn.ac.uk)

- Managed centrally by AbMAN.
- Institutes point NetFlow exporters towards central collector.
- Users login with permissions to see only their own data and associated reports/alarms and events.
- Users can customise the thresholds per zone and event actions.

StealthWatch Architecture

Michael Forrest (michael.forrest@abdn.ac.uk)

- Typical deployment would require two appliances.

SMC – Management Console
Xe1000 – Netflow Collector
(20,000 flows per sec, 100 routers)

- Larger appliance Xe2000 , which doubles the above flow capacity (up to 1000 routers).

StealthWatch GUI

Michael Forrest (michael.forrest@abdn.ac.uk)

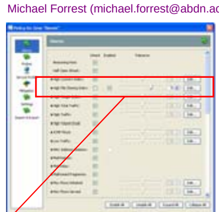
Basic Zone Configuration

Michael Forrest (michael.forrest@abdn.ac.uk)

Per Zone Alarm Policies

Michael Forrest (michael.forrest@abdn.ac.uk)

- Options can be inherited or not.
- Tolerances can be specified.
- Disabling of zone options as required.

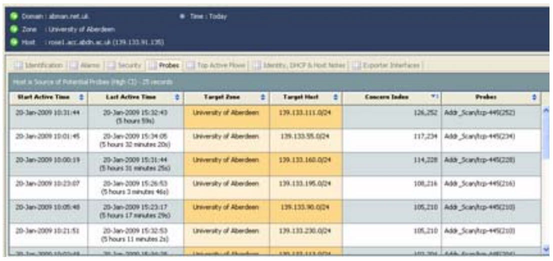


Setting Tolerances per Zone

Michael Forrest (michael.forrest@abdn.ac.uk)

Host Probing

Michael Forrest (michael.forrest@abdn.ac.uk)

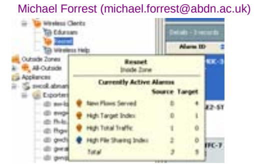


Start Active Time	Last Active Time	Target Zone	Target Host	Concern Index	Probes
20-Jan-2009 10:31:44	20-Jan-2009 15:32:43 (5 hours 59s)	University of Aberdeen	139.133.111.0/24	126,252	Addr_Scan/tcp-445(252)
20-Jan-2009 10:01:45	20-Jan-2009 15:34:05 (5 hours 32 minutes 20s)	University of Aberdeen	139.133.55.0/24	117,234	Addr_Scan/tcp-445(234)
20-Jan-2009 10:00:19	20-Jan-2009 15:31:44 (5 hours 31 minutes 25s)	University of Aberdeen	139.133.160.0/24	114,228	Addr_Scan/tcp-445(228)
20-Jan-2009 10:23:07	20-Jan-2009 15:26:53 (5 hours 3 minutes 46s)	University of Aberdeen	139.133.195.0/24	108,216	Addr_Scan/tcp-445(216)
20-Jan-2009 10:05:48	20-Jan-2009 15:23:17 (5 hours 17 minutes 29s)	University of Aberdeen	139.133.90.0/24	105,210	Addr_Scan/tcp-445(210)
20-Jan-2009 10:21:51	20-Jan-2009 15:32:53 (5 hours 11 minutes 2s)	University of Aberdeen	139.133.230.0/24	105,210	Addr_Scan/tcp-445(210)

An Active Alarm

Michael Forrest (michael.forrest@abdn.ac.uk)

- Drill down to examine host that triggered alarm.
- All alarm info visible in one view.



Alarm/Event Mitigation

Michael Forrest (michael.forrest@abdn.ac.uk)

- The response can be either :-
  - None
  - Authorize – passed to a person to authorise (email/alert)
  - Automatic – action is just performed
- Can mitigate in the following ways :-
  - SNMP (disable a network port switch for example).
  - Cisco (PIX/Guard/IOS Router)
  - Foundry
  - Custom Script (uses an expect script).

StealthWatch Interface

Michael Forrest (michael.forrest@abdn.ac.uk)

- Flow data seen from outside and inside the network.
  - Will show connections that may not have got through.
- Interface is very feature rich, lots of options still to be investigated.
- First few weeks can be intensive, whilst the appliance learns the "normal" operation of a network.
- Historical data can be kept as long as required and sufficient disk space exists.

Possible Future Directions

Michael Forrest (michael.forrest@abdn.ac.uk)

- Integration with Active Directory/RADIUS to see who's been using which IP address.
  - Requires a Stealthwatch ID appliance be installed
- Emailing of staff/students who are detected using FSI above a certain threshold.
- Mitigation of DoS events by ACL insertion onto the router to block traffic.
- Define inter-zone relationships and alert when these zones are crossed.

Questions

Michael Forrest (michael.forrest@abdn.ac.uk)