Using Argus and Watcher to monitor Darknets

Version 0.2

Most of this work is derived from,

http://www.cymru.com/Darknet/index.html

Many thanks!

You will need Argus, which can be found,

http://www.qosient.com/argus

See below for how to get hold of Watcher

This document looks at using Watcher scripts to monitor Argus on darknets placed within an organisation. This aims to give Network security staff an insight into the machines scanning within their netblock. We make some subtle changes, to make the Darknet box 'silent' except when it spots internal to internal scanning. We still record everything, so we can examine the data if necessary.

In our set up, a single box is monitoring two distinct subnets, making it very versatile. Our system runs FreeBSD 5.3 and Argus 2.0.6.

The first stage is to follow the instructions on the darknet pages - set up the darknet and get it running. Once the system is up and running, we make a few changes, so that the Watcher scripts can work.

We will keep the variables from the original Darknet work and add some of our own,

```
My_Darknet_1 prefix  = 10.18.18.0/24
My_Darknet_2 prefix  = 192.168.32.0/24
```

(We are monitoring the 2 different darknets on one machine)

```
Sniffer IP      = 172.16.18.2
Management IP   = 192.168.18.2
Mailhost        = 192.168.18.25

em0   - SNIFFER NIC - 172.16.18.2
fxp0  - MGMT NIC    - 192.168.18.2
```

Change 1. Change argus.conf to work with Watcher scripts

```
# Store the flows in an output file.  Rotate this file
# regularly with a script.
ARGUS_OUTPUT_FILE=//data/argus/current/argus.out
#
```

Change 2. Allow the machine to send email out, ipf.rules

```
# Permit mail out to the mailserver
pass out quick on fxp0 proto tcp from 192.168.18.2 to 192.168.18.25 = 25 keep state
#
```

Change 3. Add the watcher scripts. These should be found in the directory

contrib/Argus-perl-2.00

Of the downloaded source file. At the time of writing, argus-2.0.6 did not have the files included, so we used those from argus.2.0.4 and made the following changes ...

Change 4. Firstly we make changes to Argus.pm. This sets the variables out so, needs to be configured for your environment. Note the coupling to the argus.conf file.

```
> $Archive_root = "/data/argus/archive/";
> $Archive_dir_template = "%Y/%m/%d";   # eg  2001/03/05
```

The changes to the archive directory fit with the rotation script we add later

```
> $Def_Host = 'localhost';
> $Def_Port =  '2002';

> $My_Darknet_1 = '10.18';
> $My_Darknet_2 = '192.168';
> $Local_IP = "$My_Darknet_1|$My_Darknet_2";
> $Local_IP_re = '10\.18|192\.168';
```

Change 5. We remove the following line from ra.conf, as it is better controlled over the command line,

```
< RA_PRINT_HOSTNAMES=no
```

Change 6. As the network is dark, we can increase the sensitivity of the Watcher scripts. This is done through Watcher.pm file

Firstly decrease the reporting period to 600 seconds,

```
> $Period =  600;  ## seconds -- reporting period
```

Then lower the local interest threshold,

```
> $Local_Interest_Threshold =  50;
> $Remote_Interest_Threshold = 50;
```

The final change to this file is the ra_filter. This needs some work, as we only want the sensor to email us on actual scans, so we need to cut out the broadcast traffic. Connecting to the remote argus port and trying out various versions of the filter should give you an idea of one that works for you.

```
> $RA_Filter = "src net $Argus::Local_IP and ip and not net 224.0 and not net 255.255.255 and not net
239.255.255";
```

Change 7. Even though there are changes to Watcher.pm, argus itself changed slightly between 2.0.4 and 2.0.6. We make some changes to the file watcher.pp to reflect this

```
>     if ( defined $opt_F ) {  # read from a file
>        open(RA, "$Argus::Client_path/ra -Zs -nn -F $Argus::Home/lib/ra.conf -u ".
>             " -r $opt_F  $Argus::Watcher::RA_Filter|") ||
>        die "Can't open '$opt_F:$!";
>     }   else {  # connect to a live server
>        if (! open(RA, "$Argus::Client_path/ra -Zs -nn -F $Argus::Home/lib/ra.conf -u".
>                  " -S $ArgusHost:$ArgusPort " .
>                  "$Argus::Watcher::RA_Filter|") ) {
```

The important changes are,
the use of '-nn', this stops both resolving of hostname and protocol (and the reason we alter ra.conf)
The ra syntax changed from -S $ArgusHost -P $ArgusPort (in version 2.0.4) to, -S $ArgusHost:$ArgusPort (version 2.0.6).

Changes 8. These changes alter the way the email works given in Support.pm

Firstly change the mailhost to the correct place,

```
>    my $mail = new Net::SMTP('192.168.18.25');
```

And some minor syntax changes, We will list the old - new file diffs at this point, for clarity,

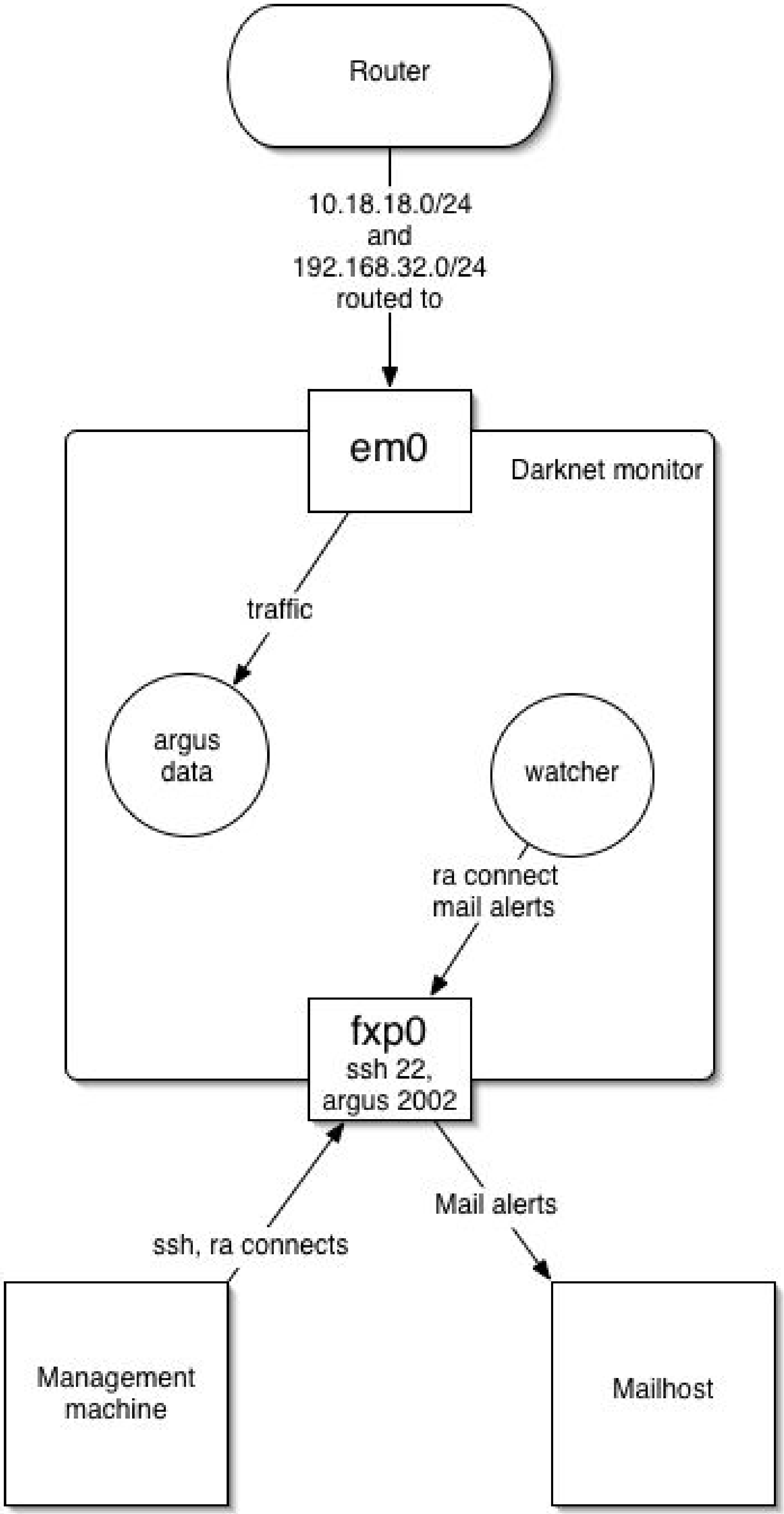
```
78,79c78,79
<     my (@a) = split(/\./, $::a);
<     my (@b) = split(/\./, $::b);
---
>     my (@a) = split('.', $a);
>     my (@b) = split('.', $b);

133c134
<     @$udp = sort {$::a <=> $::b} @$udp;
---
>     @$udp = sort {$a <=> $b} @$udp;

145c146
<     @$tcp = sort {$::a <=> $::b} @$tcp;
---
>     @$tcp = sort {$a <=> $b} @$tcp;

256c257
<     @tcpports = sort {$::a <=> $::b} @tcpports;
---
>     @tcpports = sort {$a <=> $b} @tcpports;
```

Change 9. Finally we add a script to rotate the argus files. For this we use the supplied script, which can be found in,

support/Archive/argusarchive

In the downloaded distribution

Change 10. Don't forget to change the other variables in Argus.pm to suit your environment!


Router
10.18.18.0/24
and
192.168.32.0/24
routed to
em0
Darknet monitor
traffic
argus
data
watcher
ra connect
mail alerts
fxp0
ssh 22,
argus 2002
ssh, ra connects
Mail alerts
Management
machine
Mailhost