Network Management & Monitoring

Log management, part II : Using swatch

Notes:
------
* Commands preceded with "$" imply that you should execute the command as
  a general user - not as root.
* Commands preceded with "#" imply that you should be working as root.
* Commands with more specific command lines (e.g. "RTR-GW>" or "mysql>")
  imply that you are executing commands on remote equipment, or within
  another program.

Exercises
----

0. Log in to your PC or open a terminal window as the root user:

        $ sudo bash

1. Let's enable logging of everything to a single file:

        # editor /etc/rsyslog.d/30-routerlogs.conf

        - Find the line

        local0.*   -?RouterLogs

        ... and add a new line below:

        local0.*   /var/log/network/everything

... this will enable logging of ALL messages to a single file, so that we
can run a monitoring script on the messages.

        - Now restart rsyslog:

        # service rsyslog restart

2. Enable a daily automated script to truncate the log file so it doesn't
grow too big:

        # editor /etc/logrotate.d/everything

        - In the file add the following:

/var/log/network/everything {
  daily
  copytruncate
  rotate 1
  postrotate
      /etc/init.d/swatch restart
  endscript
}

2. Install swatch

        # apt-get install swatch

3. Create the file /etc/swatch.conf and add the following rules in the file:

        # editor /etc/swatch.conf

watchfor /PRIV_AUTH_PASS/
        mail=sysadm,subject=Enable mode entered
        threshold type=limit,count=1,seconds=3600

watchfor /CONFIG_I/
        mail=sysadm,subject=Router configuration
        threshold type=limit,count=1,seconds=3600

watchfor /LINK/
        mail=sysadm,subject=Link state change
        threshold type=limit,count=1,seconds=3600

watchfor /SSH/
        mail=sysadm,subject=SSH connection
        threshold type=limit,count=1,seconds=3600

        Save the file and exit

4. Start swatch:

        # swatch -c /etc/swatch.conf --daemon -t /var/log/network/everything

        Check that it is running:

        # ps ax | grep swatch

5. Log in to your router, and run some "config" commands (example below):

        # telnet 10.10.X.254   [where "X" is your router number]
        rtrX.ws.nsrc.org> enable
      Password: <password>
        rtrX.ws.nsrc.org# config terminal
        rtrX.ws.nsrc.org(config)# int FastEthernet0/0
        rtrX.ws.nsrc.org(config-if)# description Description Change for
FastEthernet0/0 for Swatch
        rtrX.ws.nsrc.org(config-if)# ctrl-z
        rtrX.ws.nsrc.org# write memory
        rtrX.ws.nsrc.org# exit

        Just as in the previous exercise, attempt to shutdown / no shutdown
        a loopback interface

6. Verify that you are receiving emails to the sysadmin user from Swatch

        $ su - sysadmn
        $ mutt -f /var/mail/sysadm

7. Let's add some ACLs to the router

    ```
    rtrX# conf t
    rtrX(config)# access-list 123 deny tcp any host 10.10.X.254 eq 23 log
    rtrX(config)# access-list 123 permit ip any any
    rtrX(config)# interface fastEthernet 0/1
    rtrX(config-if)# ip access-group 123 in
    rtrX(config-if)# exit
    rtrX(config)# exit
    ```

    (remember, X is the number of your group)

    Explanation: we are now filtering Telnet to the router, on the inside
    interface, explicitly, but we allow anything else. The "permit"
    statement is required or we will be disabling all IP access to the
    router!

8. Test that it works:

    From your PC:

    ```
    $ telnet 10.10.X.254
    Trying 10.10.X.254...
    telnet: Unable to connect to remote host: No route to host
    $
    ```

    Notice that it says "No route to host" instead of "Connection refused"

    This is because, although we have disabled Telnet already by enabling
    SSH on the routers, an active ACL will respond differently than a
    Closed port (TCP RST vs. ICMP Host Unreachable)

    Now look at the logfile:

    ```
    $ tail /var/log/network/everything
    Jun  2 13:46:14 rtrX 6133: *Jun  2 15:46:13.552: %SEC-6-IPACCESSLOGP:
    list 123 denied tcp 10.10.X.37(43523) -> 10.10.X.254(23), 1 packet
    ```

    Hint: if your log is filled with "SSH-5-*" messages, ignore them like
    this:

    ```
    $ grep -v SSH-5 /var/log/network/everything | tail
    ```

    ... you should see SEC-6-IPACCESSLOGP messages

9. Add a new swatch rule to detect these events

    ```
    # editor /etc/swatch.conf, and add this:
    ```

    ```
    watchfor /SEC-6-IPACCESS/
        mail=sysadm,subject=Blocked connection
          threshold type=limit,count=1,seconds=3600
    ```

10. Kill swatch, and restart it:

    ```
    # ps ax |grep swatch | grep -v grep
    ```

```
12345 ?          Ss      0:00 /usr/bin/swatch -c /etc/swatch.conf --daemon -t
/var/log/network/everything
```

The number on the LEFT is the number you need to kill - here 12345

```
# kill 12345    (the number YOU got!!)
```

11. Restart swatch

```
# swatch -c /etc/swatch.conf --daemon -t /var/log/network/everything
```

12. Try to telnet to the router again, and check your mail!