Corelan Team

:: Knowledge is not an object, it's a flow ::

Monitoring your network with Powershell

Corelan Team (corelanc0d3r) · Wednesday, January 28th, 2009

I have written a small powershell script that will help you to monitor various hosts on your network. Instead of using ping to see if a host is alive, this script will connect to tcp ports, so you can also monitor hosts behind firewalls (or hosts that cannot be pinged). In addition to this, you can also test that a port is closed (and report that this is ok if that is what you want); and only report a problem when the port is found open (instead of closed)

The script can be downloaded from the link at the bottom of this post.

This is how it works

1. **Download the script**, unzip it, and put it in a folder on a machine that

- has Powershell installed
- has access to the hosts you want to monitor

2. **Create a text file** in the same folder, containing the hosts you want to monitor. You can only put one entry per line. This is the syntax :

host:port:status (which can be 'open' or 'closed')

so suppose you want to monitor a host called www.myserver.com and verify that port 80 is open, add a line that says
www.myserver.com:80:open

If you want to monitor port 22 of host server1.mydomain.com, which should be closed by default, add a line that says
server1.mydomain.com:22:closed

Note : You can group certain servers by adding a group title between square brackets.

Example :

```
[internal servers]
www.myserver.com:80:open
dns.mydomain.com:53:open
host1.mydomain.com:139:open
server1.mydomain.com:22:closed

[external servers]
www.mycompany.com:80:open
```

3. Create a file called **smtp.cfg** and with the following entries (and replace the text surrounded by <> with your own settings)

```
smtpserver=<ip address of your smtp server>
smtpserverport=25
from=<email address>
to=<emailaddress1,emailaddress2,>
subject=[%hostname%] Port Monitor report (%events% event(s)) - %timestamp%
reportmode=2
alertmode=1
```

(all of the settings are mandatory)

As you can see, you can use 3 variables in the Subject field. (and of course, you are free to build your own subject field.)

Both "reportmode" and "alertmode" have 2 possible values :

reportmode=1 means : only show alert entries in the report

reportmode=2 means : show all entries in the report

alertmode=1 means : only send a report when something is wrong

alertmode=2 means : always send the report

How to use the script

You should have 3 files : the powershell script, the smtp.cfg file, and the file that contains the host entries.

From a powershell command line, launch the script, and use the filename of the "host entries" file as parameter. The script will assume that smtp.cfg is in the local path.

Let's say the hosts file is called hosts.txt and contains the following entries :

hosts.txt - Notepad

File Edit Format View Help

```
[Webservers]
#scan all webservers
www.corelan.be:8800:open
freetools.corelan.be:80:open

[ftp servers]
ftp.microsoft.com:21:open

[Servers that should be closed]
fw03.corelan.be:8888:closed
```

smtp.cfg is configured to send reports with all entries, to peter.ve@telenet.be and peter.ve@corelan.be, but only when there is something wrong (so alertmode = 1, reportmode = 2)

Launch the script :

```
c:\scripts> '.\pve_portmonitor.ps1' hosts.txt

--------------------------------
 pve_portmonitor.ps1
 Written by Peter Van Eeckhoutte
 http://www.corelan.be:8800
--------------------------------

[+] Reading input file
  - Connecting to host www.corelan.be to verify that port tcp 8800 is open
    Result : port is open
  - Connecting to host freetools.corelan.be to verify that port tcp 80 is open
    Result : port is open
  - Connecting to host ftp.microsoft.com to verify that port tcp 21 is open
    Result : port is open
  - Connecting to host fw03.corelan.be to verify that port tcp 8888 is closed
    Result : port is closed

[+] Writing report to report.html
```

The report is written to html, but no email is sent (because there are no unexpected results)

When you set alertmode to 2, an email will be sent every time

```
[+] Sending email to peter.ve@telenet.be,peter.ve@corelan.be
    Done.
```

The report looks like this :

Date: Today

peter.ve@telenet.be [IMLTPVEC] Port Monitor report (0 event(s)) - 28/1/2009, 17:16:34 wo 28/01/2009 17:18

[IMLTPVEC] Port Monitor report (0 event(s)) - 28/1/2009, 17:16:34

peter.ve@telenet.be

Sent: wo 28/01/2009 17:17

To: Peter Van Eeckhoutte; Peter Van Eeckhoutte (corelan)

PVE Port Monitor Report

Current date/time : 28/1/2009, 17:16:34

Host	Port	Event
[Webservers]		
www.corelan.be	8800	OPEN
freetools.corelan.be	80	OPEN
[ftp servers]		
ftp.microsoft.com	21	OPEN
[Servers that should be closed]		
fw03.corelan.be	8888	CLOSED

PVE Port Monitor - Peter Van Eeckhoutte - http://www.corelan.be:8800

Of course, you would need to schedule this script in order to be able to continuously monitor the hosts on your network. You can use the explanation at the bottom of this post to find out how to launch the script from a batch file. All that is left for you is to schedule the batch file thru Task Scheduler / Scheduled Tasks.

Download the script

You need to be logged in to download this script. Click this link to register if you don't have a useraccount yet
PVE Port Monitor (2.8 KiB)

Final notes

I don't mind that you use/change this script to suit your own environment – but don't forget to give me some credits :-)

This entry was posted
on Wednesday, January 28th, 2009 at 6:22 pm and is filed under My Free Tools, Networking, Powershell
You can follow any responses to this entry through the Comments (RSS) feed. Both comments and pings are currently closed.