NMAP 5 - NETWORK CHECKS

When previously speaking about nmap (see here), I spoke about using nmap to check your network for any changes. This will pick up new hosts, new services and changed services. Since I have already gone through what the new nmap5 is capable of doing and how cool it is, I will not repeat myself, but lets just look at the network check script. as with all scripts I put up, I make no claims to its perfection, you use it at your own risk and please feel free to make any changes you want. Call it something like *nmap-netchk* and *crontab* it to run daily...

```
##VARIABLE SETUP
BSE=/admin/check
LOGS=$BSE/logs
NMAP=/usr/local/bin/nmap
DATE=`date +%a-%b-%Y`

##REMOVE OLD LOG FILE IF NEEDED
rm -rf $LOGS/results.$DATE.txt

##CHECK TO SEE IF THIS IS THE FIRST TIME WE ARE RUNNING
if [ -f $LOGS/log.one ]
 then
  echo fine
  mv $LOGS/log.one $LOGS/log.two
 else
  touch $LOGS/log.one
fi

##THE ACTUAL CHECKING - CHNAGE IP ADDRESSES AS NEEDED
for x in 192.168.3.15 192.168.3.45 192.168.3.56
 do
  $NMAP -sT $x -n -p 1-65535 -sV -sC --reason --open -oX $LOGS/log.one >> $LOGS/
results.$DATE.txt
 done

##CHECK TO FIND ALL LIVE HOSTS
echo "Live Hosts?" > $LOGS/mail.log
echo "" >> $LOGS/mail.log
$NMAP -sP -n 192.168.3.1-254 >> $LOGS/mail.log
echo "----------------------------" >> $LOGS/mail.log

##CHECK TO FIND ANY CHANGES
echo "Any Changes?" >> $LOGS/mail.log
echo "" >> $LOGS/mail.log
/usr/bin/ndiff $LOGS/log.two $LOGS/log.one >> $LOGS/mail.log
```

What this script does is run the nmap checks against the list of ip addresses. The full results are stored in the *logs* subfolder in the *results.xxx* files while the xml results are stored in the same folder in the *log.xxx* files. The xml files are used for *ndiff*, and the *ndiff* results are also stored in the *logs* subfolder in the *mail.log* file. The idea is that you can mail yourself the *results.xxx* file to see all the nmap results, but to see just what has changed, mail yourself the *mail.log* file, this file will also have a list of all live hosts so you can see if there any other systems which should be added to the main check.

I am sure there are many ways to do this, this is just mine, and if you choose to use it, I hope it is useful. Have fun

and learn.