

```
#!/bin/bash
```

```
CURRENTDATE=`date +%F:%H:%M`
```

```
DATE=`echo $CURRENTDATE`
```

```
## Begin Config
```

```
# The directory for autonmap data/scans
```

```
RUN_DIRECTORY="/usr/local/autonmap/"
```

```
# The directory you want the web report to live in
```

```
WEB_DIRECTORY="/var/www/autonmap/"
```

```
# The subnets you want to scan daily, space separated.
```

```
SCAN_SUBNETS="Insert Subnets to Scan"
```

```
# The full path (http) to where the report will be hosted by your webserver. This is included in the email report.
```

```
# I suggest setting up auth using htpasswd etc, in which case you can include the auth in the URL for simplicity if you want.
```

```
WEB_URL="http://website/scan-$DATE.html"
```

```
# The full path to your chosen nmap binary
```

```
NMAP="/usr/local/bin/nmap"
```

```
# The path to the ndiff tool provided with nmap
```

```
NDIFF="/usr/local/bin/ndiff"
```

```
# The email address(es), space separated that you wish to send the email report to.
```

```
EMAIL_RECIPIENTS="email address"
```

```
## End config
```

```
echo $DATE"- Welcome to AutoNmap2. "
```

```
# Ensure we can change to the run directory
```

```
cd $RUN_DIRECTORY || exit 2
```

```
echo "`date` - Running nmap, please wait. This may take a while. "
```

```
#$NMAP --open -T4 -PN $SCAN_SUBNETS -n -oX scan-$DATE.xml > /dev/null
```

```
#$NMAP --open -sn -n $SCAN_SUBNETS -oX scan-$DATE.xml > /dev/null
```

```
$NMAP --open -T4 -Pn -sS $SCAN_SUBNETS -n -oX scan-$DATE.xml > /dev/null
```

```

echo "`date` - Nmap process completed with exit code $?"

#Convert the xml into html - added by Damien Hull
xsltproc scan-$(DATE).xml -o scan-$(DATE).html

# If this is not the first time autonmap2 has run, we can check for a diff. Otherwise skip this
section, and tomorrow when the link exists we can diff.
if [ -e scan-prev.xml ]
then
    echo "`date` - Running ndiff..."
    # Run ndiff with the link to yesterdays scan and todays scan
    DIFF=`$NDIFF scan-prev.xml scan-$(DATE).xml`

    echo "`date` - Checking ndiff output"
    # There is always two lines of difference; the run header that has the time/date in. So we can
discount that.
    if [ `echo "$DIFF" | wc -l` -gt 2 ]
    then
        echo "`date` - Differences Detected. Sending mail."
        echo -e "AutoNmap2 found differences in a scan for '${SCAN_SUBNETS}' since last
scan. \n\n$DIFF\n\nFull report available at $WEB_URL" | mail -s "AutoNmap2"
$EMAIL_RECIPIENTS
    else
        echo "`date` - No differences, skipping mail. "
    fi

else
    echo "`date` - There is no previous scan (scan-prev.xml). Cannot diff today; will do so
tomorrow."
fi

# Copy the scan report to the web directory so it can be viewed later.
echo "`date` - Copying HTML to web directory. "
cp scan-$(DATE).html $WEB_DIRECTORY

# Create the link from today's report to scan-prev so it can be used tomorrow for diff.
echo "`date` - Linking todays scan to scan-prev.xml"
ln -sf scan-$(DATE).xml scan-prev.xml

echo "`date` - AutoNmap2 is complete."
exit 0
root@sec9mgt:/usr/local/autonmap#

```

