CCI Web Server Configuration

Document Author: arho.virkki@tyks.fi

Server Address and Credentials

CCI Web server is hosted at https://www.shellit.org/ with IP 185.87.108.219 and Canonical domain name srv-185-87-108-219.shellit.fi. In addition, there are two vsshp.fi aliases pointing to this address (configured by Medbit)

```
$ host cci.vsshp.fi
cci.vsshp.fi has address 185.87.108.219
$ host ktp.vsshp.fi
ktp.vsshp.fi has address 185.87.108.219
```

For credentials, see the files at `ktp@ktpgit.vsshp.net:/opt/git/Common.git` under the *webserver* subdirectory.

Installed Software

Apache 2

```
sudo apt-get install apache2

sudo sh -c 'echo "ServerName ktp.vsshp.net" >> /etc/apache2/apache2.conf'
sudo systemctl status apache2
```

Manual pages and convenience tools

```
sudo apt-get install --reinstall man-db
sudo apt-get install bash-completion
sudo apt-get install kbtin # for ansi2html
```

Security Settings

Install Uncomplicated Firewall

```
sudo apt-get install ufw
sudo ufw allow ssh
sudo ufw allow http
sudo ufw allow https

sudo ufw enable
sudo ufw status
```

Review sysctl configuration

See the comments on *sysctl.conf* and turn on features accordingly. By default, everyting is commented with #.

```
sudo vim /etc/sysctl.conf
```

Install Denyhosts

Denyhosts is a basic tool which works pretty well against brute-force attacs. Install it with

```
sudo apt-get install denyhosts
```

Then, review the settings

```
sudo vim /etc/denyhosts.conf
```

Install Malware Scanner

Install the traditional malware scanners:

```
sudo apt-get install chkrootkit rkhunter
```

The utility of these tools appears to be limited, but running them periodically does not (probably) hurt, eihter.

```
sudo rkhunter --update
sudo rkhunter --check

sudo chkrootkit
```

Install Lynis Security Audition Tool

Install lynis from https://cisofy.com/

```
ssh ktp@ktp.vsshp.fi

mkdir -p ~/local
cd ~/local
wget https://cisofy.com/files/lynis-2.4.0.tar.gz
tar xvzf lynis-2.4.0.tar.gz
sudo chown -R root: lynis
```

Then run the audit

```
cd ~/local/lynis
sudo ./lynis audit system | less -R
```

To produce an html report, pipe the output through *ansi2html*

```
sudo ./lynis audit system | ansi2html > ~/$( date --iso-8601)_Lynis_Report.html
```

Extra Tweaks

Fix the locale with perl (http://askubuntu.com/questions/454260/how-to-solve-locale-problem)

```
sudo locale-gen en_US.UTF-8
sudo locale-gen fi_FI.UTF-8
```

Generate a retro banner with http://www.network-science.de/ascii/ and put it into

```
sudo vim /etc/update-motd.d/10-help-text
```

Set up Password Authentication with Apache

Intall utility called apache2-utils:

```
sudo apt-get update
sudo apt-get install apache2-utils
```

Create the Password File for user(s):

```
 # first user
sudo htpasswd -c /etc/apache2/.htpasswd <username>
 # additional users, leave -c argument out
sudo htpasswd /etc/apache2/.htpasswd <username2>
```

To View contents of the file:

```
cat /etc/apache2/.htpasswd
  #Output
username:$apr1$.0CAabqX$rb8lueIORA/p8UzGPYtGs/
username2:$apr1$fqH7UG8a$SrUxurp/Atfq6j7GL/VEC1
```

Configuring Apache Password Authentication

```
sudo nano /etc/apache2/sites-enabled/000-default.conf

  #inside the file it should look similar to this

<VirtualHost *:80>
  ServerAdmin webmaster@localhost
  DocumentRoot /var/www/html
  ErrorLog ${APACHE_LOG_DIR}/error.log
  CustomLog ${APACHE_LOG_DIR}/access.log combined

  <Directory "/var/www/html">
    AuthType Basic
    AuthName "Restricted Content"
    AuthUserFile /etc/apache2/.htpasswd
    Require valid-user
  </Directory>
</VirtualHost>
```

Before you restart the server, you can check the configuration file correct syntax with following command:

```
sudo apache2ctl configtest
  #output
Syntax OK
```

After this you can restart Apache Server

```
sudo systemctl restart apache2
sudo systemctl status apache2
```

Now, the directory should be password protected.