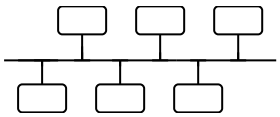


File System Security

This exercise aims to investigate an authorisation mechanism used to protect some file systems.

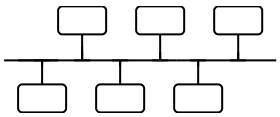
In order to experiment with Unix file security it is necessary to have "root" login permissions normally only available to the system administrator.
However some of the techniques of file protection can be implemented by the user on their personal web space storage directories.

Win 9x/NT

Aims	Procedure	Notes
For this exercise you will need to work with a partner.	Find out the hostname and IP address of the machine you are using and that of your partner. **Run… Open: cmd** C\> **ipconfig**	Own IP___.___.___.___ Your Partner IP___.___.___.___
If you have the W: drive mounted as per the last exercise you can quickly create the directories for this exercise. Otherwise use the unix commands listed in this exercise.		WinNT Directories W:\ex2 W:\ex2\personal W:\ex2\napier

Soc Unix Account

Aims	Procedure	Notes
Login to the Soc Unix service	C:\>**telnet telnet** **Login:** **Password:**	
Create a directory for this exercise and set appropriate file permissions	**> cd public_html** **> mkdir ex2** **> chmod 755 ex2** **> cd ex2**	



The behaviour of the web server can be modified on a "per directory" basis by including server directives in the directory. The file **".htaccess"** is normally used for this purpose. Note the leading "."	Create a new .htaccess file inside ex2 > **vi .htaccess** OR **> pico .htaccess**	Use the "Pico" editor if you are unfamiliar with vi.
The **ErrorDocument** directive tells the server what to do if an error occurs. The error number indicates what the problem is E.g.**404** = "Not Found"	contents of ex2/.htaccess file **ErrorDocument 404 "Sorry file gone!** **ErrorDocument 401 "Unauthorised!** **ErrorDocument 403 "Cannot Access!**	
Set the .htaccess file permissions. rwxr--r--	**chmod 755 .htaccess**	
Try and access a "missing" file within /ex2 on the web server	Use MS IE or Netscape on the desktop PC to access the URL below, user your own loginID.	
URL **http://www.dcs.napier.ac.uk/~*b18276543*/ex2/notthere.htm**		
	What error message was displayed?	Error Message: _____ _____ _____
Create 2 sub-directories and set file permissions	**> mkdir personal** **> chmod 755 personal** **> mkdir napier** **> chmod 755 napier**	
.htaccess files can also be used to restrict http access to files based on the IP address of the client or the client's domain.	Create an .htaccess file inside the "personal" directory. **> cd personal** **> pico .htaccess** Content of .htaccess, insert *your own IP address xx.xx.xx.xx* **AuthType Basic** **deny from all** **allow from** *xx.xx.xx.xx*	

Set .htaccess file permissions	**> chmod 744 .htaccess**	
Create a simple HTML file inside ex2/personal, check you can access it yourself via WWW then ask your partner to try		Self: Allowed/Denied Partner: Allowed/Denied
HTTP Access permissions can be more complex. Allow access from any machine in Napier except your partner's.	Create an new .htaccess file inside ex2/napier with the following content (remember to chmod file permissions), insert *your partner's IP address* **AuthType Basic** **allow from napier.ac.uk** **deny from** *yy.yy.yy.yy*	
Create a simple HTML file inside ex2/napier, check you can access it yourself, ask your partner to try. Finally ask another person to access it from a third machine.		Self: Allowed/Denied? Partner: Allowed/Denied? Third Party: Allowed/Denied?
HTTP access permissions can also be based on password authentication.		
Create an encrypted password file in a location outside the public_html directories.	> **cd ~** **> mkdir webadmin** **> cd webadmin** **> htpasswd -c .htpasswd** *userid*	
Add an entry for yourself and one for your partner.	**htpasswd .htpasswd** *partnerid*	
View the password file	**cat .htpasswd**	Can you identify the "salt" values for each password? Self: ☐☐ Partner: ☐☐
Modify the content of the .htaccess file in ex2/personal	**> cd ..** **> cd personal** **> pico .htaccess**	

<table>
<tr><td colspan="3">Content of ex2/personal/.htaccess.
use your own login id and IP address.

AuthUserFile /home/~b2345678/webadmin/.htpasswd
AuthName "My Personal Access"
AuthType Basic
require valid-user</td></tr>
<tr><td></td><td>Try accessing a file within ex2/personal
Ask you partner to do the same.</td><td>Self: Allowed/Denied/ Password?

Partner: Allowed/Denied/ Password?</td></tr>
<tr><td>Access permissions can also be specified as satisfying either the IP address or the userid/password</td><td>Modify the .htaccess file in ex2/napier</td><td></td></tr>
<tr><td colspan="3">ex2/napier/.htaccess content
(remember to set file permissions),
insert your partner's IP address yy.yy.yy.yy

AuthUserFile /home/~b2345678/webadmin/.htpasswd
AuthName "My Napier Access"
AuthType Basic
allow from napier.ac.uk
deny from yy.yy.yy.yy
require valid-user
satisfy any</td></tr>
<tr><td></td><td>Try accessing any file within ex2/personal
Ask you partner to do the same. Then ask a third individual to try.</td><td>Self: Allowed/Denied/ Password

Partner: Allowed/Denied/ Password

Third Party: Allowed/Denied/ Password</td></tr>
</table>