Stefan Knott
TLEN 5833 UNIX Admin
Lab 5 Writeup

1. Email to Jim on password security

Jim,

I will be glad to grant the access you wish once you make a few changes to your account. To begin with, you should never use the company's name in your password, nor should you reuse company passwords. See the below company password policies and let me know if you have any questions.

SysAdmin

Password Policies:

Unique password for each account
Never share your password
Do not store your password online
Report immediately if your password has been compromised
Avoid common words and the company name
Passwords require 10 characters consisting of: 2 upper case letters, 2 digits, and 1 non-alphanumeric character
Change your password every 4 months

2.

Give mpalmer access to service vsftp restart on Machine C

```
visudo
mpalmer ALL=(ALL) NOPASSWD: /usr/sbin/vsftpd restart
```

give mpalmer permission to modify files and directories under /var/ftp/ on Machine C

```
setfacl -m u:mpalmer:rw /var/ftp/
```

3.

pbeesly kapok and abernard must be allowed to restart the http daemon on Machine B through sudo, modify all files under /var/www/html/

```
visudo
pbeesly ALL=(ALL) /sbin/apachectl restart
kkapoor ALL=(ALL) /sbin/apachectl restart
abernard ALL=(ALL) /sbin/apachectl restart
setfacl -m u:pbeesly:rw /var/www/html
setfacl -m u:kkapoor:rw /var/www/html
setfacl -m u:abernard:rw /var/www/html
```

4.
adjusted default umask in /etc/profile to allow users, groups, to rwx and for others to have no permissions on Machines A,B,C,D,E

umask 007

checked via:

logout
login
umask —> 0007

5. restrict server access by user
to restrict access..modify the /etc/security/access.conf file and add “account required pam_access.so” to each /etc/pam.d/login file as pam will draw information from …/ access.conf

add to /etc/pamd.d/login of servers A-D:
account required pam_access.so

in /etc/security/access.conf:
Machine A:

-:ALL EXCEPT sknott mscott : ALL

Machine B:

-:ALL EXCEPT root sknott mscott pbeesly kkapoor abernard : ALL

Machine C:

-:ALL EXCEPT root sknott mscott mpalmer : ALL

Machine D:

-:ALL EXCEPT sknott mscott : ALL

6.
Granted dschrute sudo access on all machines by editing etc/sudoers/ on each machine via:

visudo
dschrute ALL=(ALL) ALL

checked via:

sudo -l -U dschrute —> User dschrute… (ALL) ALL

7.

Allow Michael Scott to shut down, and cancel pending shut downs on all machines

visudo
mscott ALL=(ALL) /sbin/shutdown -h now
mscott ALL=(ALL) /sbin/shutdown -hc now

8.

I ensured new password changes are 10 characters long, contains at least 2 digits, 2 uppercase, and 1 non alphanumeric character by editing each machines /etc/pamd.d/ system-auth file password requisite line to:

password requisite pam_pwquality.so try_first_pass retry=3 minlength=10 ucredit=2 dcredit=2 ocredit=1