NF2 – EL SERVEI FTP || UF2: WEB I FTP

CAS PRÀCTIC 2 – SERVEI FTP AMB PROFTPD

NOM DE L'ALUMNE/s: Nil Massó

OBJECTIU

- **Configurar el servei d'FTP amb ProFTPd en base a les premisses de l'enunciat per tal de complir els paràmetres establerts i fer les corresponents comprovacions.**

INSTRUCCIONS

- **L'activitat és de tipus individual.**
- **Cal realitzar-lo sobre les màquines virtuals proporcionades a l'inici del mòdul.**
- **Recordeu que caldrà configurar-les a nivell de *hostname*, usuaris, etc.**
- **Caldrà també que realitzeu les adients configuracions de xarxa amb IP estàtica dins la 'xarxa NAT' que utilitzem al MP.**
- **No hi ha problema en reutilitzar les de la UF1 o NF1 de la UF2. Tingueu en compte les configuracions que hi teniu per si us poden generar algun conflicte o variació.**
- **També podeu utilitzar les màquines de la plataforma IsardVDI degudament configurades i personalitzades.**
- **Per defecte, cal que justifiqueu les respostes amb captures de pantalla.**
- **Si a la captura no hi ha cap valor que la identifiqui de forma única, cal que es vegi el fons d'escriptori, *notepad* o eines similars amb el vostre nomcognom!**
- **Totes les captures que mostrin les comandes han d'incloure, a part del resultat, la comanda i/o els paràmetres, per tal de veure com la feu.**

Utilitzant la Ubuntu Server 22 amb el ProFTPd instal·lat, caldrà configurar-ne el servei per tal que compleixi les premisses que a continuació es descriuran, i posteriorment, fer les comprovacions corresponents segons pertoqui. Com a client, sempre que no s'especifiqui el contrari, podeu fer servir qualsevol màquina, fins i tot fer les comprovacions amb el servidor actuant com a client a través del programa *ftp* via consola.

Partirem doncs de la configuració per defecte del ProFTPd. Si pel que sigui teniu algun problema i voleu obtenir la configuració original, teniu una copia del fitxer proftpd.conf a /usr/share/proftpd/templates/proftpd.conf. Les nostres configuracions aniran directament a un fitxer dins de la carpeta */etc/proftpd/conf.d/nomcognom.conf*, de forma que ja sobreescriuran les configuracions que pertoqui.

La configuració que heu de generar ha de complir següents característiques generals:

- El sistema ha de permetre l'ús del servei per part d'usuaris de sistema autenticats i també ha de permetre l'accés anònim.
- Els usuaris (tant de sistema com anònims) han de quedar tancats al seu directori de *home*, només poden "baixar" dins el seu arbre de directoris.

- Tots els usuaris autenticats que s'especifiquin a l'activitat no han de tenir accés via terminal consola al Linux, però el *proftpd* si que controlarà que tinguin una *shell* definida.
- S'ha de configurar el servidor per tal que els ports passius siguin fixes, i han d'anar del 45665 al 45670, ambdós inclosos.
- Tots els *logins* (correctes i incorrectes) han de quedar registrats als *logs*.

A nivell de requeriments del sistema i funcionament a complir:

- Crear un parell d'usuaris nous complets dins el sistema: *nomcognom* i *cognomnom*.
- Crear un usuari de sistema que es digui *professor*.
- Els fitxers que es pengin al sistema de fitxers no es poden sobreescriure, si de cas s'ha de fer un esborrat previ per tornar a penjar el mateix fitxer.
- S'ha de limitar el servei per tal que només puguin entrar al sistema autenticat els 3 usuaris de sistema citats anteriorment, de forma que la resta d'usuaris de sistema existents no tinguin accés al servei FTP.
- L'usuari *professor* no ha de poder treballar en mode passiu.
- L'usuari *nomcognom* no podrà esborrar cap arxiu.
- L'usuari *cognomnom* no podrà crear cap nou directori.
- L'usuari professor no podrà llistar el seu directori principal, però si els diferents subdirectoris que pugui tenir.
- Els usuaris anònims no podran pujar contingut, només baixar-ne.

Aneu fent les comprovacions a mida que aneu complint els requeriments, però quan acabeu de tot, feu una nova comprovació final per tal de veure que tot funciona correctament i no heu modificat indirectament alguna cosa que funcionava prèviament. Algunes d'elles s'hauran de demostrar amb captures.

Així doncs, el primer que caldrà fer es adjuntar una captura del contingut del fitxer de configuració que heu fet.

a) Adjunteu doncs el resultat de la comanda *[cat /etc/proftpd/conf.d/nomcognom.conf | grep .]* canviant nomcognom pels vostres valors. Per demostrar que no heu tocat res del fitxer per defecte mostreu la captura d'executar [*sudo diff /etc/proftpd/proftpd.conf /usr/share/proftpd/templates/proftpd.conf]* també. 6,5 punts.

Els comentaris de la captura rosa no són importants, són els teus enunciats, pots ignorar-los.

```
root@us-nmc:~# sudo diff /etc/proftpd/proftpd.conf /usr/share/proftpd/templates/proftpd.conf
root@us-nmc:~#
```

```
ServerName "US-nmc"
#Els usuaris (tant de sistema com anònims) han de quedar tancats al seu directori de home, només poden "baixar" dins el seu arbre de directoris.
DefaultRoot ~
#El sistema ha de permetre l'ús del servei per part d'usuaris de sistema autenticats i també ha de permetre l'accés anònim.
#Tots els usuaris autenticats que s'especifiquin a l'activitat no han de tenir accés via terminal consola al Linux, però el proftpd si que controlarà que tinguin una shell definida.
RequireValidShell off
#S'ha de configurar el servidor per tal que els ports passius siguin fixes, i han d'anar del 45665 al 45670, ambdós inclosos.
PassivePorts 45665 45670
#Tots els logins (correctes i incorrectes) han de quedar registrats als logs.
LogFormat default "%t %u %a %m %r %s %b"
TransferLog /var/log/proftpd/xferlog
SystemLog /var/log/proftpd/proftpd.log
<Directory ~>
#S'ha de limitar el servei per tal que només puguin entrar al sistema autenticat els 3 usuaris de sistema citats anteriorment, de forma que la resta d'usuaris de sistema existents no tinguin accés al servei FTP.

<Limit LOGIN>
    DenyUser *
    AllowUser nilmasso massonil professor
</Limit>
#L'usuari professor no ha de poder treballar en mode passiu.
<Limit PASV>
    DenyUser professor
</Limit>
#L'usuari nomcognom no podrà esborrar cap arxiu.
<Limit DELE>
    DenyUser nilmasso
</Limit>
#L'usuari cognomnom no podrà crear cap nou directori.
<Limit MKD>
    DenyUser massonil
</Limit>
#L'usuari professor no podrà llistar el seu directori principal, però si els diferents subdirectoris que pugui tenir.
<Limit LIST>
    DenyUser professor
</Limit>
</Directory>
#Els usuaris anònims no podran pujar contingut, només baixar-ne.
<Anonymous ~>
    RequireValidShell off
    <Limit STOR>
        DenyAll
    </Limit>
</Anonymous>
```

b) També cal una captura del contingut de /etc/shells amb la comanda cat i llançar la següent comanda per cadascun dels 3 usuaris creats al cas pràctic [*sudo getent passwd user* | *cut -d : -f1,6,7*] on cal substituir *user* pel nom d'usuari a comprovar. 0,5 punts.

```
root@us-nmc:~# cat /etc/shells
# /etc/shells: valid login shells
/bin/sh
/bin/bash
/usr/bin/bash
/bin/rbash
/usr/bin/rbash
/usr/bin/sh
/bin/dash
/usr/bin/dash
/usr/bin/tmux
/usr/bin/screen
```

```
root@us-nmc:~# sudo getent passwd nilmasso | cut -d : -f1,6,7
nilmasso:/home/nilmasso:/bin/bash
root@us-nmc:~# sudo getent passwd massonil | cut -d : -f1,6,7
massonil:/home/massonil:/bin/bash
root@us-nmc:~# sudo getent passwd professor | cut -d : -f1,6,7
professor:/home/professor:/bin/bash
```

Ara és el moment de fer totes les comprovacions per tal de veure que tot funciona com pertoca. Algunes d'aquestes comprovacions caldrà que les adjunteu a continuació:

c) Adjuntar una captura conforme s'ha pogut fer login via FTP a través d'un client per comandes amb l'usuari *nomcognom* i amb l'usuari anònim. *0,75 punts.*

```
nil@UCLI-NMC:~$ ftp nilmasso@172.25.35.180
Connected to 172.25.35.180.
220 ProFTPD Server (US-nmc) [::ffff:172.25.35.180]
331 Password required for nilmasso
Password:
230 User nilmasso logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> exit
221 Goodbye.
nil@UCLI-NMC:~$ ftp anonymous@172.25.35.180
Connected to 172.25.35.180.
220 ProFTPD Server (US-nmc) [::ffff:172.25.35.180]
331 Password required for anonymous
Password:
530 Login incorrect.
ftp: Login failed
ftp>
```

d) Amb els mateixos usuaris que a l'apartat anterior, demostreu que estan "tancats" dins el seu directori arrel. *0,75 punts.*

Prova .txt s'ha creat fent proves abans, ignoral.

Comprovo que esta tancat fent un ls, després pujo directori i veig que segueix en el mateix, per tant esta aillat.

```
ftp> ls
229 Entering Extended Passive Mode (|||45667|)
150 Opening ASCII mode data connection for file list
-rw-r--r--   1 nilmasso nilmasso        0 Dec 11 21:58 prova2.txt
-rw-r--r--   1 root     root            0 Dec 11 21:55 prova.txt
226 Transfer complete
ftp> cd ..
250 CWD command successful
ftp> ls
229 Entering Extended Passive Mode (|||45667|)
150 Opening ASCII mode data connection for file list
-rw-r--r--   1 nilmasso nilmasso        0 Dec 11 21:58 prova2.txt
-rw-r--r--   1 root     root            0 Dec 11 21:55 prova.txt
226 Transfer complete
```

Ara toca que agafeu el client de Windows 10, i hi instal·leu Wireshark i el client de Filezilla si encara no li teníeu. Un cop fet, cal que el configureu perquè es connecti en mode passiu al servidor amb Proftpd i adjunteu una captura de la part on, via el canal de control es negocia el servei sota passiu, i després, del canal de dades, on es veu per quins ports es transfereix el fitxer.

e) No obstant tot això ha d'anar amb el mateix filtre. Podeu fer servir el filtre que vulgueu sempre i quan s'adeqüi al que es demana, per tant, no son dues captures separades. *0,75 punts.*

f) Cal també que adjunteu una captura d'executar [*sudo cat /var/log/proftpd/proftpd.log | grep -i login*] on, com a mínim, s'ha de veure l'autenticació correcta de l'usuari anònim i d'un dels 3 usuaris utilitzats al cas pràctic. *0,75 punts.*

Per altra banda, no cal realitzar-les, però us animo a comprovar el que queda per demostrar, que corresponen a :

- Els fitxers que es pengin al sistema de fitxers no es poden sobreescriure, si de cas s'ha de fer un esborrat previ per tornar a penjar el mateix fitxer.
- L'usuari *professor* no ha de poder treballar en mode passiu, la resta si.
- L'usuari *nomcognom* no podrà esborrar cap arxiu.
- L'usuari *cognomnom* no podrà crear cap nou directori.
- L'usuari professor no podrà llistar el seu directori principal, però si els diferents subdirectoris que pugui tenir.
- Els usuaris anònims no podran pujar contingut, només baixar-ne.