Pla de treball sessió 2 - Anàlisis dels protocols Telnet i FTP

Per a seguir aquest pla de treball haureu fer servir les següents comandes:

- Per obtenir informació les connexions hosts:
  - Linux: netstat o ss
  - Windows: netstat
- Analitzador de protocols Wireshark

Si no heu fet servir mai aquestes comandes o software, seria bo que les provéssiu abans de venir al laboratori i que consulteu els seus manuals.

Primera part - Preparació de l'escenari

Repetiu el muntatge de la sessió anterior. Utilitzeu l'usuari "entel" per accedir als serveis de Telnet i FTP.

Segona part - Anàlisi del protocol Telnet

1. Obriu Wireshark en el PC Linux
2. A la VM executeu netstat per a que us mostri i refresqui les connexions TCP de manera permanent.
3. Obriu un terminal i feu un telnet a la VM.
4. Observeu com canvies les connexions TCPs a la VM. Busqueu a la VM i al PC la connexió que comparteixen. Fixeu-vos en les adreces IPs i ports d'origen i destí.
5. Mireu a la VM quantes sockets/connexions hi ha relacionades amb telnet i el seu estat. Raoneu si això hauria de permetre que hi hagi connectat més d'un client al servidor o no i feu les proves pertinents per a esbrinar-ho.
6. Escriviu alguna comanda del sistema operatiu i espereu-ne la resposta i tanqueu la sessió escrivint "exit"
7. Torneu a observar la consola de la VM. Mireu per quins estats passa la connexió fins desaparèixer. Comproveu també els ports si són els que apareixen a la captura.
8. Atureu la captura i poseu un filtre adequat que mostri només els paquets corresponents a la sessió de telnet. Comproveu que el que veieu es correspon amb la informació obtinguda amb netstat.
9. Busqueu els segments TCP que corresponen amb l'establiment de la connexió. Fixeu-vos en els flags que tenen activats. Anoteu, el nº de seqüència i reconeixement de cada segment i les opcions de TCP que es negocien i els seus valors. Nota: recordeu que els números de seqüència que utilitzen tots dos extrems de la connexió haurien de ser aleatoris. Per comprovar-ho mireu la seva codificació en hexadecimal.

10. Fixeu-vos com s'envia entre client i servidor tot el que escriviu a la consola. Fixeu-vos en una comanda, el login i el password.
11. Fixeu-vos en el tancament de la connexió, en quants segments s'envien i amb quins flags activats.

Tercera part - Anàlisi del protocol FTP

1. Modifiqueu la configuració del servidor per a que us deixi pujar fitxers: obriu el fitxer /etc/vsftpd.conf i descomenteu la línia que posa "write_enable=yes". Usar el editor vi. Para borrar un carácter colocar el promtp sobre el carácter y pulsar x. Para ir al modo comando ejecutar Esc. Para guardar y salir en modo comando pulsar ZZ

   Reinicieu el servidor, como root ejecutar:

   - service vsftpd stop. (lo para)
   - service vsftpd start (lo arranca)
   - service vsftpd restart (lo reinicia)

2. Repetiu el procediment seguit abans amb Telnet però ara feu un FTP, executeu la comanda "ls" per veure el contingut del directori i tanqueu la connexió i la captura.
3. Poseu un filtre adequat que permeti només veure els paquets corresponents a la sessió de FTP
4. Busqueu la comanda que heu escrit i després la resposta del servidor. Si no la podeu veure, modifiqueu el filtre que heu posat al Wireshark.
5. Compareu respecte al cas de Telnet com s'envien les dades, ie. les respostes a una comanda.
6. Respecte a la connexió per on s'envien les dades, mireu qui estableix la connexió i com sap el port que cal fer servir.
7. Contrasteu amb netstat (o ss) la informació que veieu al Wireshark relativa a la connexió de dades.
8. Busqueu les comandes per a pujar i baixar fitxers del servidor. Pugeu un fitxer de més de 1MB al vostre servidor. Feu una captura descarregant-lo. Fixeu-vos en la velocitat de descàrrega que us dóna el client en acabar la transferència. Raoneu si el seu valor és coherent amb la velocitat de la xarxa Ethernet que ens proporciona el router.
9. Busqueu un segment de dades i el seu ACK, mireu si es compleix la relació que toca entre nº seqüència, dades transportades i valor del ACK.
10. Un cop feta la captura, apliqueu les eines d'anàlisi i representació que ofereix Wireshark al menú "Statistics=>"TCP Stream Graphs" a la connexió de dades. Raoneu que es representa en cada casa i els valors que apareixen. Penseu d'on surt la informació per a fer aquestes representacions gràfiques.
11. Feu una captura amb Wireshark mentre feu servir una aplicació del vostre PC que utilitzi TCP. Com abans, apliqueu-li les eines que es troben a "Statistics=>"TCP Stream Graphs" i compareu amb el que heu trobat abans.