Practica 2

Vulnerabilidad en aplicación de Acceso Remoto- Telnet

Introducción

En esta práctica se configura la aplicación Telnet y se analiza su vulnerabilidad de seguridad como protocolo de acceso entre redes.

Adicionalmente en este laboratorio se utilizan analizadores de protocolos para verificar la debilidad de esta aplicación en cuestiones de seguridad.

Para obtener información adicional de conceptos y aplicaciones refiérase a las notas en clase.

GRUPO: UTVT TIC-

EQUIPO DE TRABAJO:

INTEGRANTES:

1.-

2.-

3.-

FECHA DE ELABORACION: - - 2019

FIRMA/ICE Ing. Rubén F. González.

Desarrollo de Actividades:

1. Cada equipo trabajara con su equipo vecino adyacente de acuerdo al diagrama de red configurado en practicas anteriores, el instructor le asignara el grupo al que pertenece:

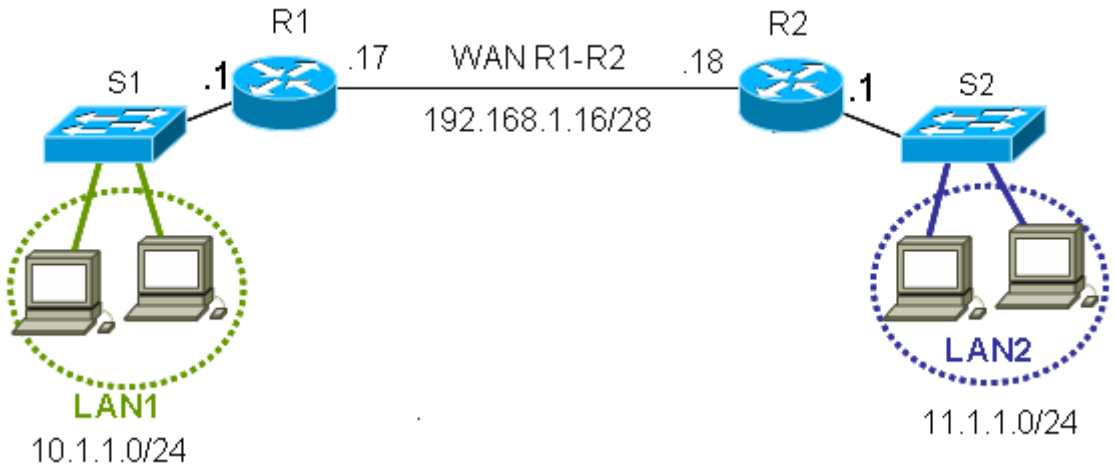


Figura 1

2. Antes de empezar cambie su dirección IP de su LAN de acuerdo al diagrama de red, lo anterior es necesario para evitar direcciones que nos pudieran crear conflictos, es imprescindible tener conectividad completa hacia los host de la red vecinas, realice las pruebas correspondientes a todos los hosts vecinos.

3. ¿Fue exitoso el acceso a todos los hosts de la red?_____, en caso contrario realice troubleshooting con sus compañeros de equipo.

4. Anote el Sistema Operativo de su PC o LapTop y su SP:

   _____

   _____

5. Crear dos cuentas nuevas de usuarios la primera con el nombre de BOGUS y password 12345; la segunda con el nombre de TELNET con el password 12345.

Notas que debe de leer:

- *Al agregar un usuario(os) al equipo se debe proporciona al acceso remoto a los archivos y programas del equipo,*
- *Recuerde que tendrá que abrir (deshabilitar) el firewall de la PC destinada como Servidor de Telnet.*

- *Telnet es un Servicio que no se recomienda tener en forma continua y configurada en inicio automático.*

6. Los pasos para realizar esta tarea varían en función si el equipo es miembro de un dominio de red o forma parte de un grupo de trabajo. (refiérase a sus clases o habilidades de Microsoft)

7. Anote si su PC esta en un Dominio o en un Grupo de Trabajo:

   _____

   _____

8. Para este laboratorio trabajaremos en el Grupo de trabajo: UTVT (Mayúsculas)

9. Para agregar un nuevo usuario al equipo, necesita tener una cuenta de administrador de equipo en la PC o Server. (Si no esta registrado – haga login como administrador para realizar esta tarea)

10. Abra Cuentas de usuario en el Panel de control.

11. Haga clic en **Crear una nueva cuenta**.

12. Escriba el nombre de la nueva cuenta de usuario.

13. Haga clic en **Administrador de equipo**, según el tipo de cuenta que desee asignar al nuevo usuario para esta práctica, haga clic en **Crear cuenta**.

14. El nombre que asigne a la cuenta es el nombre que aparecerá en la pantalla de bienvenida y el menú **Inicio**.

15. Para abrir, revisar y modificar cuentas de usuario, haga clic en **Inicio**, **Panel de control** y, a continuación, haga doble clic en **Cuentas de usuario**. (Recuerde que usted debe tener privilegios de administrador, de otra manera no le será posible realizar lo anterior)

Notas:

- *Debe asignar una cuenta de administrador de equipo al primer usuario que agregue.*
- *Para obtener más información acerca de las **Cuentas de usuario**, refiérase a las referencias de sus clases de Windows.*

16. ¿Cuántas cuentas aparecen en Cuentas de Usuario?

    _____

    _____

    _____

17. ¿Aparece la cuenta BOGUS y TELNET?

    _____

    _____

18. Pruebe que ambas cuentas puedan acceder como administrador a su computadora destinada para servicios de IP, para esto deberá reiniciar el equipo y acceder con usuario y password.

NO CONTINUE CON LA PRACTICA, SI LOS PASOS ANTERIORES NO FUERON EXITOSOS.

19. En esta practica una computadora realizara el servicio de **Telnet como Servidor** y otra **computadora vecina será el Cliente**, (Note que estamos utilizando el cliente del DOS aunque usted podría utilizar otro cliente que sea interoperable con el sistema operativo Windows).

Notas que debe de leer:

- *Con el Cliente Telnet, los usuarios de Windows pueden conectar con un equipo remoto que ejecute un servidor Telnet y ejecutar aplicaciones o realizar tareas administrativas en el equipo remoto.*
- *Recuerde que las aplicaciones y algunos protocolos podrían no funcionar adecuadamente si tiene activado en la PC o Servidor el Firewall, o si existe alguna lista de acceso-ACL en el router.*

20. Desde la computadora asignada como cliente ejecute un telnet hacia el Servidor, el comando para realizarlo es: telnet x.y.w.z; donde x.y.w.z es la dirección IP del host Server.

21. ¿El telnet fue exitoso, explique a que atribuye esto?

    _____

    _____

    _____

    _____

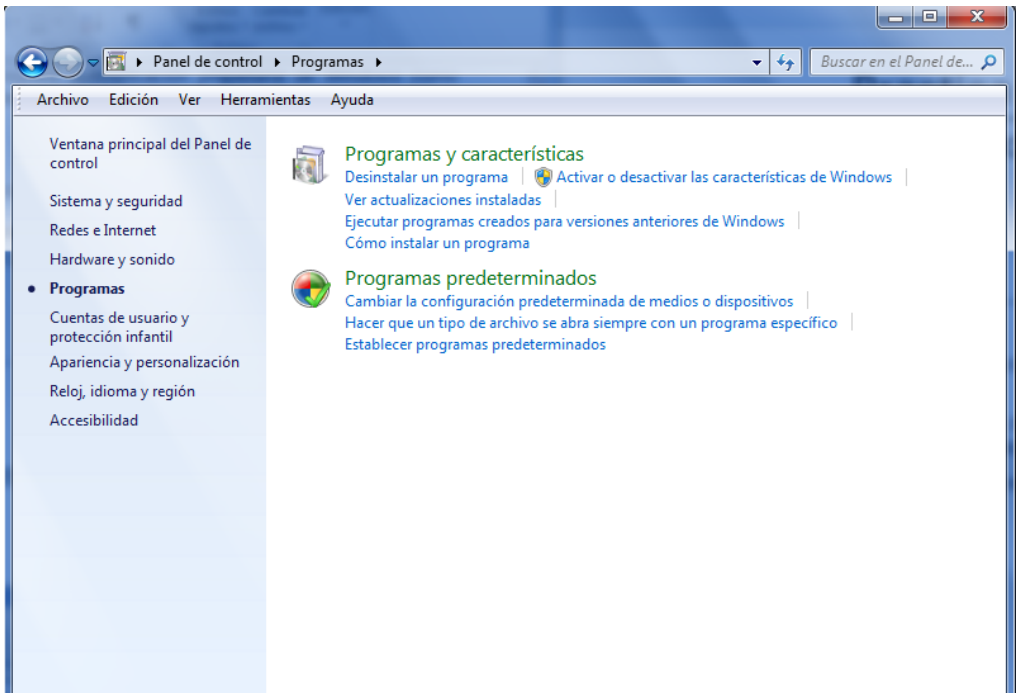
22. Ahora procederemos a revisar cual es el estado del servicio de Telnet, este servicio por default esta inactivo por cuestiones de seguridad, seria conveniente una vez iniciado el servicio y terminada la tarea con Telnet, regresarlo al estado inactivo.

Notas:

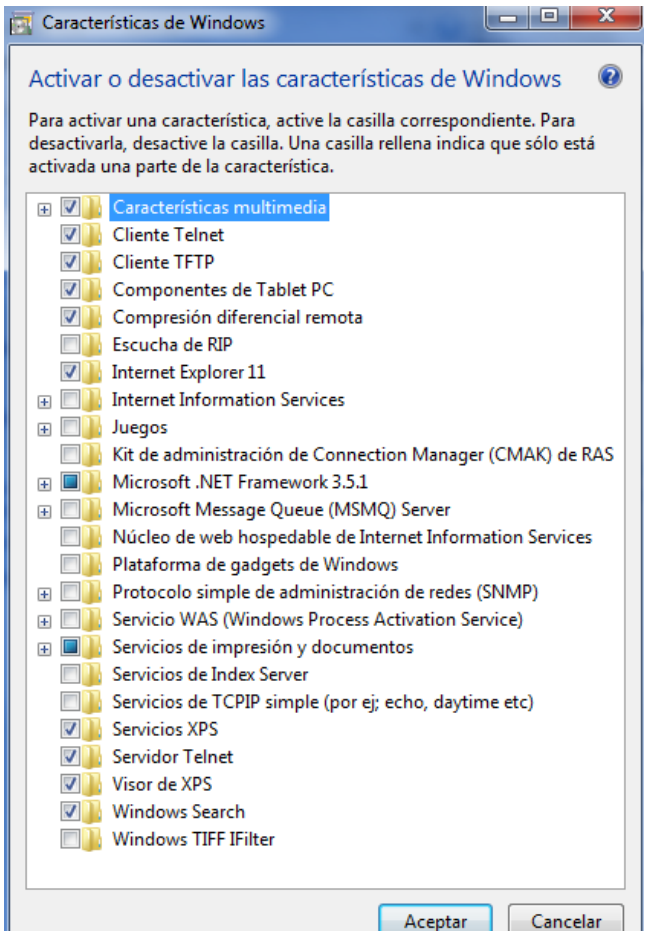
- *Con el Cliente Telnet, los usuarios de Windows pueden conectar con un equipo remoto que ejecute un servidor Telnet y ejecutar aplicaciones o realizar tareas administrativas en el equipo remoto.*
- *El procedimiento para otros sistemas operativos de Windows como Windows Server y Windows es diferente y es necesario habilitar o deshabilitar el servicio de Telnet de diferente forma además de requerir autentificación propietaria de Windows como NTLM (Paquete de seguridad que permite la autenticación entre clientes y servidores).*

23. Haga Clic sobre **Inicio** y seleccione Panel de control.

24. Haga doble Clic en **Activar o desactivar las características de Windows** usted deberá estar viendo la siguiente pantalla:



25. Seleccione activar el protocolo Telnet para el cliente y Servidor, como se muestra en la siguiente figura:



26. ¿Cuál es el estado del Servicio Telnet?

    _____

27. Ahora inicie el servicio de telnet en la ventana Servicios

28. ¿Cuál es estado del Servicio de Telnet ahora?

    _____

    _____

    _____

    _____

29. Solicite a su vecino de Red LAN que realice un ping hacia la PC donde acaba de configurar e iniciar el Servidor de Telnet, ¿Fue exitoso el ping?

    _____

    _____

    _____

    _____

30. Si el ping fue exitoso, proceda a abrir una sesión de línea de comando y escriba el comando telnet a.b.c.d. (Donde a.b.c.d es la dirección IP del Servidor Telnet).

Notas:

- *Es importante que el modo de autentificación llamada NTLM (Paquete de Seguridad que permite autentificación avanzada entre clientes y servidores) este deshabilitada Con el Cliente Telnet, los usuarios de Windows pueden conectar con un equipo remoto que ejecute un servidor Telnet y ejecutar aplicaciones o realizar tareas administrativas en el equipo remoto.*

31. Escriba el login y password de los usuarios que creo dentro del grupo de trabajo UTVT en el punto 13 de este laboratorio

32. ¿Tiene acceso al Servidor de Telnet?

    _____

33. Si la respuesta fue negativa realice troubleshooting y analice los valores que aparecen en la pregunta 29. (No consulte al profesor hasta que haya revisado si tiene actualizado su sistema operativo, así como haber revisado cada uno de los pasos anteriores).

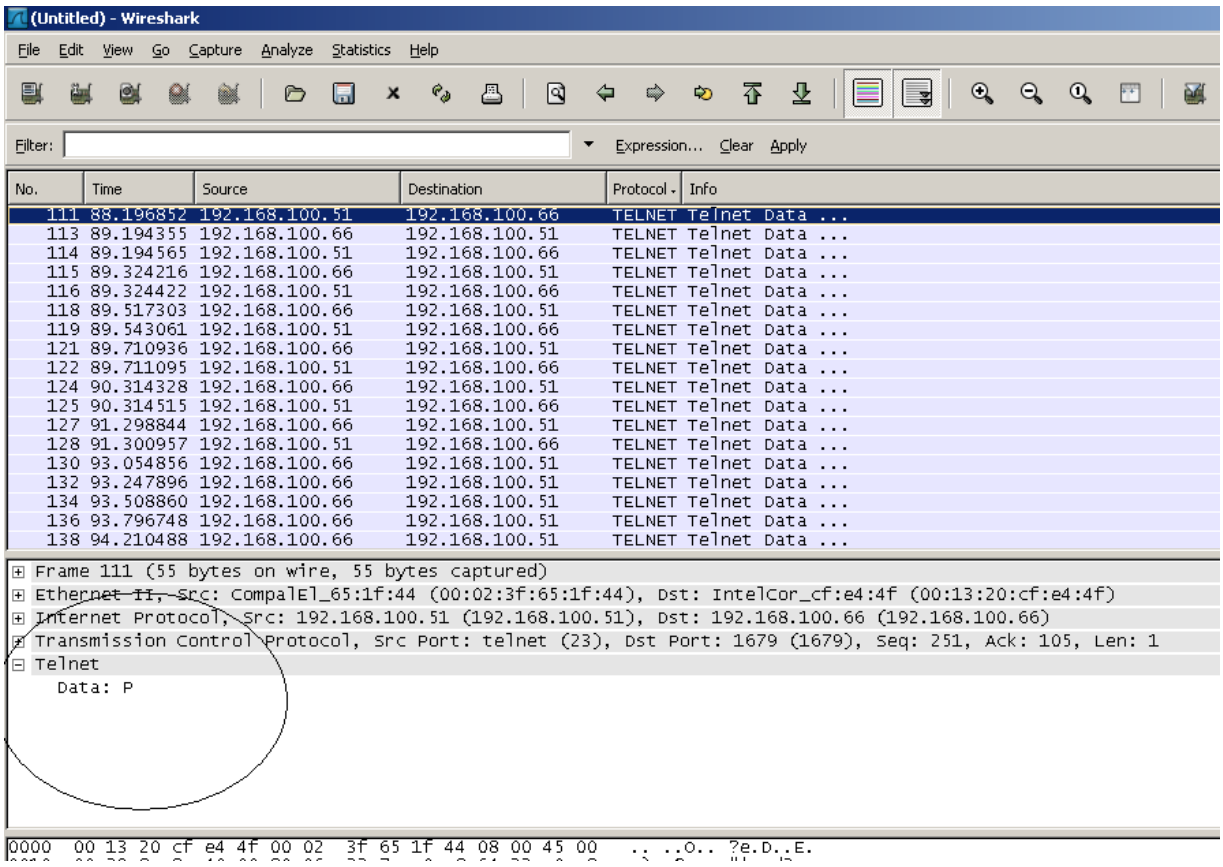
34. Cierre la sesión de telnet con el comando quit.

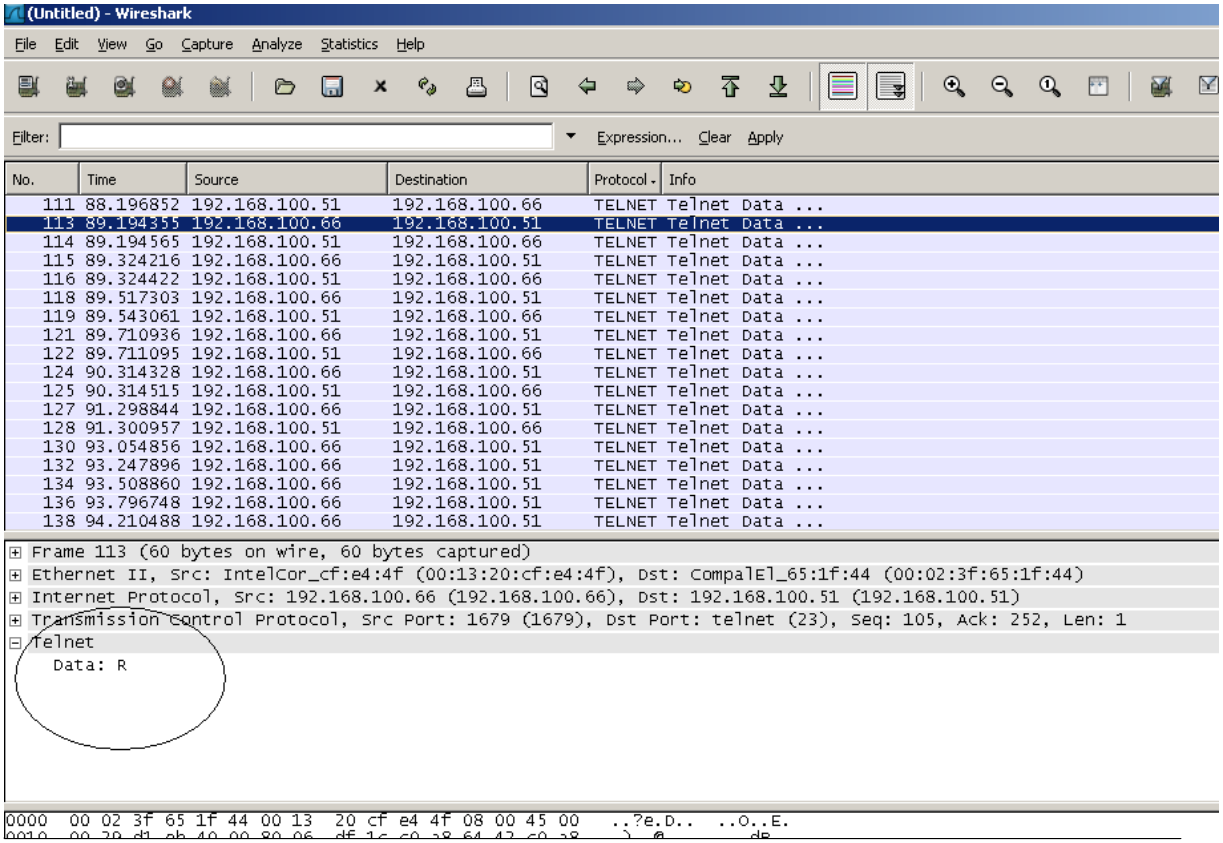
35. Abra el programa WireShark (incluye WinCap), una captura en tiempo real con el filtro telnet.

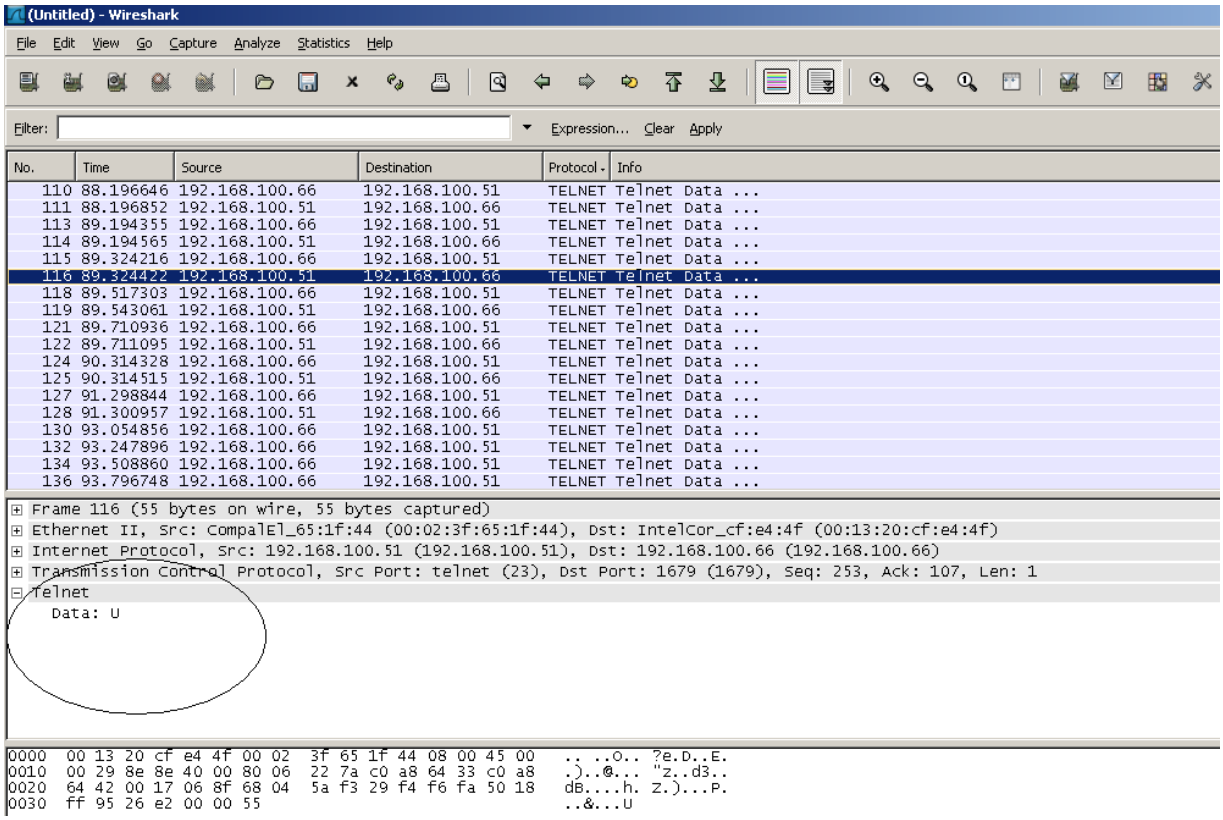
36. Nuevamente el cliente de la red local deberá iniciar la sesión de Telnet después de haber iniciado la captura con la cuenta BOGUS.

37. Revise la ventana de captura de la sesión Telnet y compruebe que el analizador esta capturando la sesión de Telnet que inicio el cliente local, revise el procotolo TCP y después localice el protocolo de aplicación Telnet

38. Usted deberá capturar el inicio de sesión, el user y el password el cual aparece en texto plano (clear text), a continuación se muestra un ejemplo de la captura de los 3 primeros caracteres del nombre del user PRUEBA en el WireShark.


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
111 88.196852 192.168.100.51 192.168.100.66 TELNET Telnet Data ...
113 89.194355 192.168.100.66 192.168.100.51 TELNET Telnet Data ...
114 89.194565 192.168.100.51 192.168.100.66 TELNET Telnet Data ...
115 89.324216 192.168.100.66 192.168.100.51 TELNET Telnet Data ...
116 89.324422 192.168.100.51 192.168.100.66 TELNET Telnet Data ...
118 89.517303 192.168.100.66 192.168.100.51 TELNET Telnet Data ...
119 89.543061 192.168.100.51 192.168.100.66 TELNET Telnet Data ...
121 89.710936 192.168.100.66 192.168.100.51 TELNET Telnet Data ...
122 89.711095 192.168.100.51 192.168.100.66 TELNET Telnet Data ...
124 90.314328 192.168.100.66 192.168.100.51 TELNET Telnet Data ...
125 90.314515 192.168.100.51 192.168.100.66 TELNET Telnet Data ...
127 91.298844 192.168.100.66 192.168.100.51 TELNET Telnet Data ...
128 91.300957 192.168.100.51 192.168.100.66 TELNET Telnet Data ...
130 93.054856 192.168.100.66 192.168.100.51 TELNET Telnet Data ...
132 93.247896 192.168.100.66 192.168.100.51 TELNET Telnet Data ...
134 93.508860 192.168.100.66 192.168.100.51 TELNET Telnet Data ...
136 93.796748 192.168.100.66 192.168.100.51 TELNET Telnet Data ...
138 94.210488 192.168.100.66 192.168.100.51 TELNET Telnet Data ...
Frame 111 (55 bytes on wire, 55 bytes captured)
Ethernet II, Src: CompalEl_65:1f:44 (00:02:3f:65:1f:44), Dst: IntelCor_cf:e4:4f (00:13:20:cf:e4:4f)
Internet Protocol, Src: 192.168.100.51 (192.168.100.51), Dst: 192.168.100.66 (192.168.100.66)
Transmission Control Protocol, Src Port: telnet (23), Dst Port: 1679 (1679), Seq: 251, Ack: 105, Len: 1
Telnet
Data: P
0000 00 13 20 cf e4 4f 00 02 3f 65 1f 44 08 00 45 00


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
111 88.196852 192.168.100.51 192.168.100.66 TELNET Telnet Data ...
113 89.194355 192.168.100.66 192.168.100.51 TELNET Telnet Data ...
114 89.194565 192.168.100.51 192.168.100.66 TELNET Telnet Data ...
115 89.324216 192.168.100.66 192.168.100.51 TELNET Telnet Data ...
116 89.324422 192.168.100.51 192.168.100.66 TELNET Telnet Data ...
118 89.517303 192.168.100.66 192.168.100.51 TELNET Telnet Data ...
119 89.543061 192.168.100.51 192.168.100.66 TELNET Telnet Data ...
121 89.710936 192.168.100.66 192.168.100.51 TELNET Telnet Data ...
122 89.711095 192.168.100.51 192.168.100.66 TELNET Telnet Data ...
124 90.314328 192.168.100.66 192.168.100.51 TELNET Telnet Data ...
125 90.314515 192.168.100.51 192.168.100.66 TELNET Telnet Data ...
127 91.298844 192.168.100.66 192.168.100.51 TELNET Telnet Data ...
128 91.300957 192.168.100.51 192.168.100.66 TELNET Telnet Data ...
130 93.054856 192.168.100.66 192.168.100.51 TELNET Telnet Data ...
132 93.247896 192.168.100.66 192.168.100.51 TELNET Telnet Data ...
134 93.508860 192.168.100.66 192.168.100.51 TELNET Telnet Data ...
136 93.796748 192.168.100.66 192.168.100.51 TELNET Telnet Data ...
138 94.210488 192.168.100.66 192.168.100.51 TELNET Telnet Data ...
Frame 113 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: IntelCor_cf:e4:4f (00:13:20:cf:e4:4f), Dst: CompalEl_65:1f:44 (00:02:3f:65:1f:44)
Internet Protocol, Src: 192.168.100.66 (192.168.100.66), Dst: 192.168.100.51 (192.168.100.51)
Transmission Control Protocol, Src Port: 1679 (1679), Dst Port: telnet (23), Seq: 105, Ack: 252, Len: 1
Telnet
Data: R
0000 00 02 3f 65 1f 44 00 13 20 cf e4 4f 08 00 45 00



39. ¿Fue exitosa la captura del user y password para el servicio de telnet utilizando el analizador de protocolos, explique porque?

    _____

    _____

    _____

40. ¿Cual es el puerto fuente y el puerto destino que esta utilizando su aplicación telnet en este momento?

    _____

    _____

41. Porque en el analizador en las líneas del protocolo Telnet a veces aparece el puerto fuente como puerto destino y viceversa. ¿Explique?

    _____

    _____

    _____

42. Repita nuevamente desde el punto 35, ahora utilizando el programa **Putty** el cual trae un cliente estándar de telnet y funciona con el Server Telnet de Windows.

43. ¿Fue exitosa la captura del user y password utilizando el cliente Putty de telnet utilizando el analizador de protocolos, explique porque?

_____

_____

_____

_____

44. ¿Cuál es la diferencia de usar el Cliente Telnet de Windows y el que trae el programa Putty?

_____

_____

_____

45. Cual serían sus recomendaciones para utilizar esta aplicación en ambientes de Microsoft Windows.

_____

_____

_____

_____

46. Mencione una opción que se pueda utilizar casi como telnet pero con nivel de seguridad.

_____

_____

47. Ahora escriba cuales son los valores que tiene actualmente su localhost para este servicio, para realizar lo anterior en la pantalla de línea de comandos (command prompt) escriba : tlntadm

- Tecla Alt asignada a "CTRL+A" :
- Tiempo de espera de sesión inactiva :
- Número máximo de conexiones :
- Puerto Telnet :
- Intentos erróneos (máx.)de inicio sesión :
- Finalizar las tareas al desconectar :
- Modo de operación :
- Mecanismo de autenticación :
- Dominio o grupo predeterminado :
- Estado :

48. Modifique los valores anteriores como se muestra a continuación:

- Tecla Alt asignada a "CTRL+A" : sin cambio
- Tiempo de espera de sesión inactiva : 5 minutos
- Número máximo de conexiones : 3
- Puerto Telnet : sin cambio
- Intentos erróneos (máx.)de inicio sesión : 2
- Finalizar las tareas al desconectar : sin cambio
- Modo de operación : sin cambio
- Mecanismo de autenticación : sin cambio *
- Dominio o grupo predeterminado : sin cambio
- Estado sin cambio

49. Para realizar el punto anterior utilice el siguiente comando desde la línea de comandos: **tlntadmin**

50. Es útil en todo momento el comando ***/?*** cuando requiera asistencia del sintaxis de comandos en el sistema operativo de Windows XP.

Notas:

- **NO intente modificar los parámetros de autentificación si no ha llevado un curso de seguridad IP avanzado o tiene amplia experiencia en sistemas operativos de Microsoft.*
- *Si requiere mayor información consulte algún Curso de Seguridad IP Avanzado .*

51. Asegúrese que tenga conectados a 3 usuarios a su servidor de Telnet, uno local y dos remotos con cualquier cliente utilizado anteriormente.

52. ¿Cuál es el comando que muestra cuantas sesiones tiene activas en su Servidor de Telnet?

_____

_____

_____

53. ¿Cual es la información desplegada por el comando anterior?

_____

_____

_____

_____

_____

_____

_____

_____

_____

54. Ahora elimine las dos sesiones remotas de clientes telnet, mantenga activa la sesión de su cliente local.

55. ¿Cuál es el comando que utilizo para eliminar las sesiones de los clientes remotos de telnet?

_____

_____

_____

56. ¿Cual es el significado del ID en la sesión activa del Telnet, explique?

_____

_____

_____

57. ¿Cual es el significado del Dominio en la sesión activa del Telnet, explique?

_____

_____

_____

58. ¿Cual es el significado del Dominio en la sesión activa del Telnet, explique?

_____

_____

_____

59. Nuevamente pida que realicen la conexión los usuarios remotos y envíeles el siguiente mensaje “It´s time to go home guys”

_____

_____

_____

60. Con esto finaliza esta práctica, avise a su profesor.