

Freeman Geek

Introducción.

El presente laboratorio pretende estudiar lo que sucede a nivel tcp/ip en una puerta trasera desarrollando una aplicación cliente/Server con el lenguaje python.

Requisitos

Varios PC windows
ActivePython 2.5
Sniffer como Wireshark o Ethereal
Scanner como Nmap
Tener varios RFC (: Xd :)

Objetivo

Desarrollar un Backdoor (Cutdoor) usando un lenguaje de alto nivel con fines netamente educativos fortaleciendo la programación de sockets y sus bases teóricas

Desarrollo

Realizar una aplicación cliente/Server con python manejando socket TCP y modificarla a tal punto, obteniendo una puerta trasera (añadiendo entradas de registro, comandos de consola, shell system, etc.)

Nota:

Hasta el momento solo se puede conectar por Telnet al puerto que se le asigne a la escucha

Código en desarrollo

```
# socketHls.py
# Creamos un servidor al cual nos podremos conectar.
# Version inicial del Backdoor
# Gino G Viloría Pabon - freemanGeek - 26/12/2007
import socket, sys
print "\n****BackDoor Freeman Server V1.0.0!!!!*****"
port=int(raw_input("\n ingrese el puerto: "))

##Codigo para obtener ip de la maquina
hn=socket.gethostname()#Obtener el nombre de la maquina
ip=socket.gethostbyname(hn)#ip de la maquina

##Codigo Server
server = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
server.bind((ip,port))#direccion del server "" es lo mismo que localhost o 127.0.0.1
server.listen(5)
while 1:
    addr, port = server.accept()
    addr.send("****BackDoor Freeman V1.0.0!!!!*****")
    print 'Conectado con',port #puerto de quie se conecta y dirreccio ip
```

```
# socketHls.py
# Creamos un servidor al cual nos podremos conectar.
# Version inicial del Backdoor
# Gino G Viloría Pabon - freemanGeek - 26/12/2007
import socket, sys
```

```
print "\n****BackDoor Freeman Server V1.0.0!!!****"
port=int(raw_input("\n ingrese el puerto: "))

##Codigo para obtener ip de la maquina
hn=socket.gethostname()#Obtener el nombre de la maquina
ip=socket.gethostbyname(hn)#ip de la maquina

##Codigo Server
server = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
server.bind((ip,port))#direccion del server "" es lo mismo que localhost o 127.0.0.1
server.listen(5)
while 1:
    addr, port = server.accept()
    addr.send("****BackDoor Freeman V1.0.0!!!****")
    print 'Conectado con',port #puerto de quie se conecta y dirreccio ip
```