Module 2: Sniffing Password

Difficulty: Beginner
Completion Time: 20 minutes
Points: 10 points

Scenario

You are an attacker and you wish you looking for access into a machine. When you sniff the network, you noticed that one of the machines is using a FTP service, which sends unencrypted passwords over the network. You are a going to act as an attacker and sniff your own login password by connecting to a FTP server.

Introduction

Password sniffing is particularly a threat for users who log into systems over a network where the password is not encrypted. Telnet, FTP, and rlogin are usually employed when logging onto systems over a network. The problem with these services is that they do not encrypt passwords. As a result, when a user enters in his or her password, it is transmitted in the clear, meaning anyone monitoring the network can read it.

Directions

You will need Wireshark (Ethereal) to watch an FTP session from your machine to server 172.168.5.10. If you do not possess Wireshark, you can download it at http://www.wireshark.org. Also, make sure your machine possesses a 172.168.5.0/24 address.

First, run Wireshark on the interface that you are using to connect to the FTP server.

Open a terminal and type

```
~# ftp  172.168.5.10 <ENTER>
```

Use linux_class as the user, linux_class as the password. You should now be logged into the server.

Then, type

```
$ quit <ENTER>
```

to terminate the session.

Go back to the Wireshark screen and go to the menu Analyze -> Follow TCP Stream.

a) Can you see your password in the tcp data on the analyzer? (Take a screen shot)

Now repeat the process but use ssh, Start Wireshark.

Type

```
~# ssh –l linux_class 172.168.5.10 <ENTER>
```

Note: it is a lower case ‘L’ not the number 1.

You might get a prompt asking if you want to continue or not. Type “yes” here.
Enter linux_class (as the password).

Then, type

```
$ quit <ENTER>
```

to terminate the session.

b) Can you see your password in the tcp data on the analyzer? (Take a screen shot)

Submit the two screen shots to the NetSecLab website.