Sniffen

für

Noobs

>by crashmind

>soon !

powered by:

Der Autor übernimmt keine die Verantwortung für diesen Text. Dieser Text dient einschliesslich zur Informataion und ist keine Aufforderung zu einer Illigalen Handlung.

Einleitung

Ich diesem Tutorial möchte ich euch beschreiben wie man den FTP Datenverkehr eines Programms (Leecher) „snifft", es wird mit dem Sniffer „Ethereal" gearbeitet.
Viel Spaß beim Sniffen ....
mfg
Crackkind

Definition: Sniffer

Sniffer lauschen an einem Netzwerkinterface, z.B. einer Ethernetkarte, und protokollieren den gesamten Verkehr mit. Damit sind z.B. unverschlüsselt übertragene Passwörter wie bei Telnet oder FTP erlauschbar.

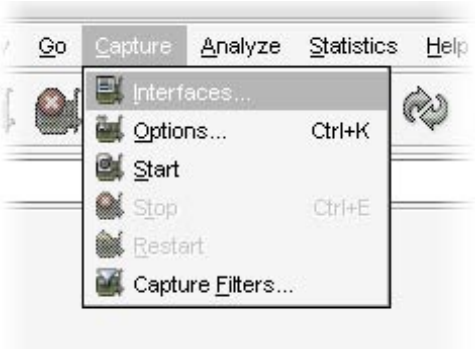
Tool

Das verwendete Sniffer-Tool ethereal steht auf http://www.ethereal.com/ zum Download bereit.

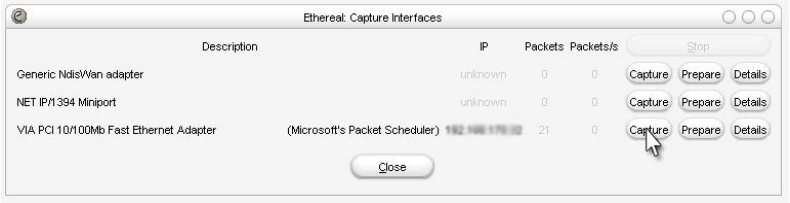
Anleitung

1.Nach der Installation, starten wir erstmal ethereal.

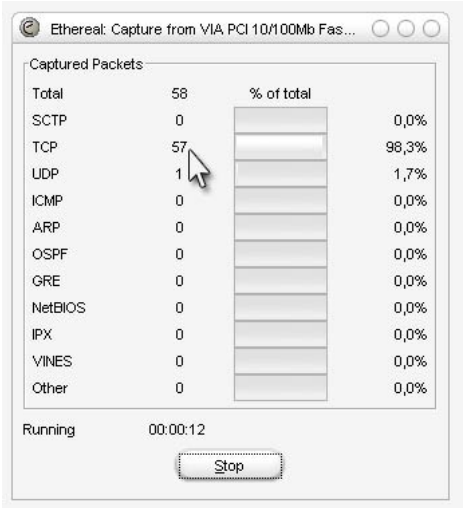
2.Um nun den Datenverkehr zu sniffen gehen wir oben in der Leiste auf Capture > Interfaces.



3.Es öffnet sich nun ein neues Fenster wo du deine Netzwerkkarten sehr können. Nun musst du die Karte sniffen mit der du ins Internet gehst, dafür klicke auf capture.



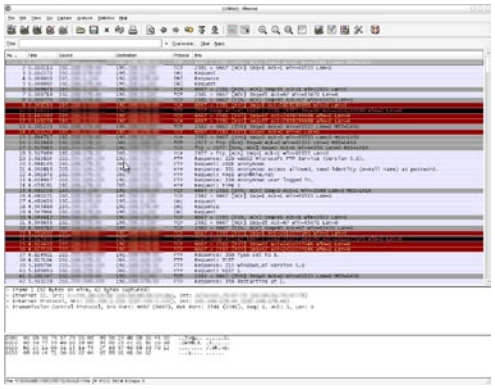
4.Im neuen Fenster wird nun der Datenverkehr deines PC angezeigt.

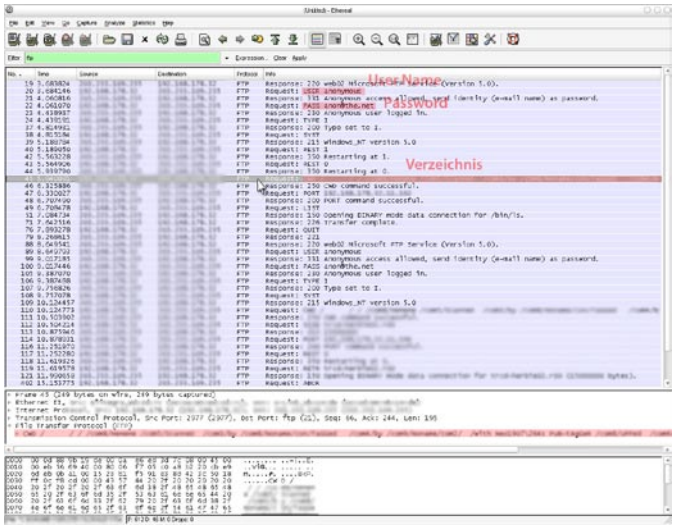


5.Jetzt startest du das Programm (Leecher) und fängst an zu downloaden. Nach dem der Leecher angezeigt, dass er sich auf dem FTP- Server eingeloggt hat und die ersten Dateien läd, brichst du einfach den Download ab und schließt das Programm.

6.Nun welchselst du wieder zu ethereal. Hier klickst du auf Stop um das protokollieren des Datenverkehrs abzubrechen und die „Aufnahmen" zu sehen.

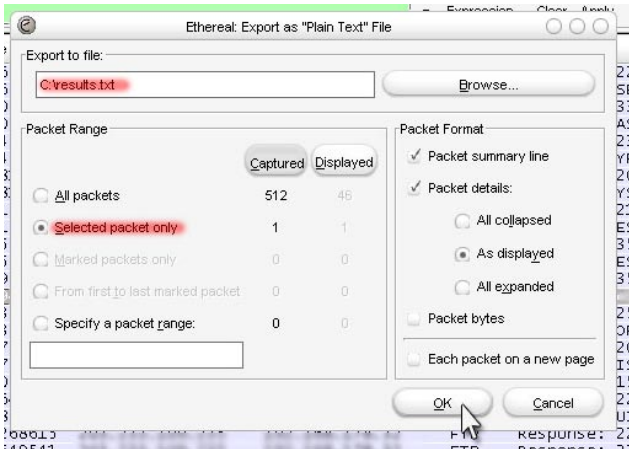
7.Der aufgezeichnete Datenverkehr sieht auf der ersten Blick sehr ungeordnet aus, um dem Abhilfe zu verschaffen nutzen wir die Filter-Fuktion, dort geben wir das Protokoll ein, in diesem Fall FTP.





8.Nun sieht das ja schon besser aus! Jetzt kannst du den gesamten Verbindungsaufbau des Programms zum FTP Server sehen, hier klickst du auf der Liste auf die Zeile wo im der Info Spalte steht „Request: CWD …".

9.Als letztes klickst du auf File > Export > as „Plain Text" File. Markiere „Selected packet only" und klick auf „OK". Öffne die Textdatei. Hier steht nun die IP des Servers und der Pfad, zusammengesetzt einfügen in einem FTP Programm und Connecten!!



Ich hoffe das Tutorial hat deinen Wissensstand erweitert!! Konstruktive Kritik an mich !

Autor: Crackkind
Datum:02.09.2005
Email: crackkind@mail.ru
hp: crackkind.dl.am