ITSP Aufgabe 1

- Wer gab dem Verdächtigen Zugriff?

  " I need to change the password on the gnome account that Jeremy gave me."

- Welche Art von Zugriffen hatte der Verdächtige?

  Account für einen Server der Uni. of New Orleans

- Wie lauten die Zugangsdaten des Verdächtigen?

  Login: gnome Passwort: gnome123

- Wie tauschte er sich mit Seinesgleichen aus?

  Textdateien im home von 'gnome'; evtl. MSN/Google Groups

- Welche relevanten Dateien können aus den Netzwerk-Traces gewonnen werden?

  2 Rihno Bilder über http, 2 über FTP, 1 in verschlüsseltem Archiv über FTP (Passwort:'monkey')

- Was ist mit der Festplatte passiert?

  " I zapped the hard drive and then threw it into the Mississippi River."

- Was geschah mit dem USB-Stick?

  "I'm gonna reformat my USB key after this entry, but try not to destroy the good stuff. Stuffed one fatty even between disks ;)"

  Über den Trace lässt sich eine .exe finden, mit der vermutlich der USB Stick bearbeitet wurde.

- Welche relevanten Dateien können von dem USB-Stick gewonnen werden?

  4 Rhino Bilder + 1 versteck in Aligatorbild; .jar mit f5 Ver-/Entschlüsselung, um das Steganographie Bild zu extrahieren (Passwort:'gator'); Textdatei des Täters

- Wie kann der USB-Stick mit den Netzwerk-Traces in Verbindung gebracht werden?

  In der Textdatei schreibt der Täter, dass er Zugriff auf den 'gnome' Account hat.

Bilder

`rhino1.jpg` -> rhino.log (filtern nach FTP-DATA -> Follow TCP Stream bei entsprechenden Ausgaben -> in RAW Format speichern)

`rhino2.jpg` -> rhino.log (FTP-DATA -> Zip -> Entschlüsseln mit 'monkey')

`rhino3.jpg` -> rhino.log (filtern nach FTP-DATA -> Follow TCP Stream bei entsprechenden Ausgaben -> in RAW Format speichern)

`rhino4.jpg` -> rhino2.log (File -> Export Objects -> HTTP)

`rhino5.gif` -> rhino2.log (File -> Export Objects -> HTTP)

`rhino6.gif` -> USB Stick

`rhino7.jpg` -> USB Stick, stegdetect auf Alig.-Bilder, ein Bild mit f5 versteckt -> mit der .jar extrahieren

`rhino8.gif` -> USB Stick

`rhino9.jpg` -> USB Stick