Subject: Re: Co-op?
Posted by theplague on Mon, 13 Jun 2005 01:04:08 GMT
View Forum Message <> Reply to Message

ok heres what to do:

note: first backup server.dat
1) W32Dasm (deassemble server.dat), find the locations of the decisions ("Gameplay Pending")
2) HIEW it (hex editor + debugger), use the debuger view and change the location to the ones found from above
3) Change the 'je' or 'jl' to 'jne' or 'jae' for each desition

EDIT: pr download and read this..
http://www.hnc3k.com/hncfilez/The%20complete%20C.R.A.C.K.I.N
.G%20G.U.I.D.E%20for%20newbiez.rar?PHPSESSID=8742814d9887164
72202a72cc7996513&PHPSESSID=a2a76035bbe142198793266faf7c
a362&PHPSESSID=529864ac65a7aedd9d5911b879826b69&PHPS
ESSID=082019a4ea38b992b09b6a37c12cafc9&PHPSESSID=95d6bca
0ab82abdf557a74c7c5326503

(use attached image for reference)

File Attachments

1) untitled.GIF, downloaded 454 times

HEX:	ASM:	Meaning:
EB	jmp	jump
90	nop	no operation
75 or 0F85	jne	jump if not equal
74 or 0F84	je	jump if equal
77 or 0F87	ja	jump if above
0F86	jna	jump if not above
0F83	jae	jump if above or equal
0F82	jb	jump if below
0F83	jnb	jump if not below
0F86	jbe	jump if below or equal
0F8F	jg	jump if greater
0F8E	jng	jump if not greater
0F8D	jge	jump if greater or equal
0F8C	jl	jump if less
0F8D	jnl	jump if not less
0F8E	jle	jump if less or equal