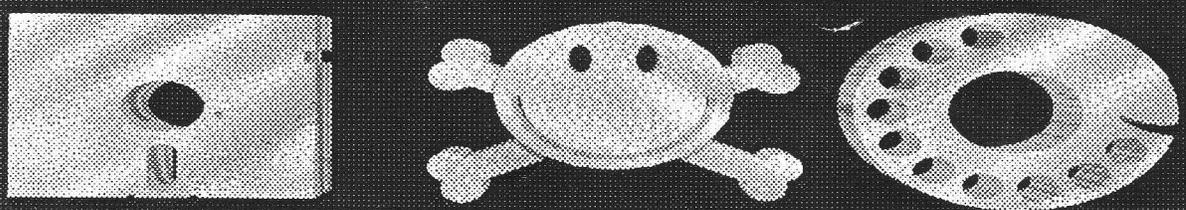# DEF CON IV

WELCOME TO DEF CON IV

As I write this I am cutting into a MRE (meal ready to eat) number eight, which is "Ham slice with accessory pack A." Anyway. You didn't want to hear about that. *This is the Anti-Program.* The first version of the program got eaten by a nasty run in with Windows NT 4.0b2. I know, I shouldn't run M$ beta nightmares. On the plus side this is being done on Page Maker 6.0a. Every Def Con in the past has been done on PM 5.0 of dubious origin. It's nice to see an update at least once every three years. Due to hotel "disagreements" we won't get the other conference room till Saturday. There will be convention updates posted on the white boards I have yet to buy, telling you of speaker changes, etc.

You might notice media this year. There has always been media, but for some reason there seem to be more tv crews this year. Don't act like an idiot in front of them or your mom will be embarassed. OK, as usual some tips: 1) Don't mess with the hotel. They have been cool about most everything, and there are plenty of other places to go and things to do. 2) Don't mess with the Goons™. They have sekret ninja like skil'z and will boot you out for dumb stuff like under age drinking, etc. Finally, knock yourself out and get crazy. I want to see string net work this year!

4TH ANNUAL SPOT THE FED CONTEST:

THE EVER POPULAR PARANOIA BUILDER. WHO *IS* THAT PERSON NEXT TO YOU?

"Like a paranoid version of pin the tail on the donkey, the favorite sport at this gathering of computer hackers and phone phreaks seems to be hunting down real and imagined telephone security and Federal and local law enforcement authorities who the attendees are certain are tracking their every move.. .. Of course, they may be right." - John Markhoff, NYT
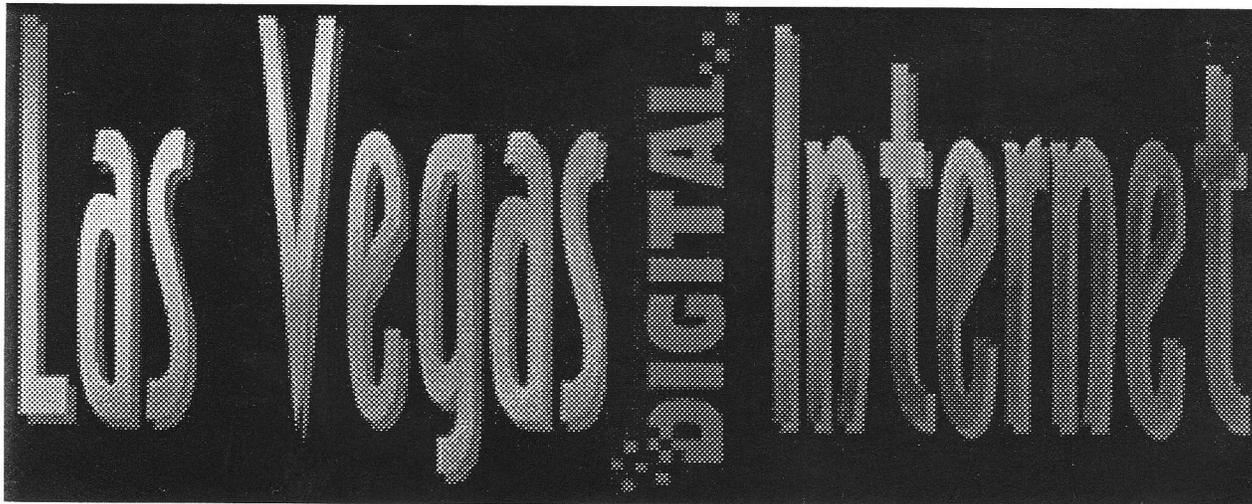
Basically the contest goes like this: If you see some shady MIB (Men in Black) earphone penny loafer sunglass wearing Clint Eastwood to live and die in L.A. type lurking about, point him out. Just get my attention and claim out loud you think you have spotted a fed. The people around at the time will then (I bet) start to discuss the possibility of whether or not a real fed has been spotted. Once enough people have decided that a fed has been spotted, and the Identified Fed (I.F.) has had a say, and informal vote takes place, and if enough people think it's a true fed, or fed wanna-be, or other nefarious style character, you win a "I spotted the fed!" shirt, and the I.F. gets an "I am the fed!" shirt.

NOTE TO THE FEDS: This is all in good fun, and if you survive unmolested and undetected, but would still secretly like an "I am the fed!" shirt to wear around the office or when booting in doors, please contact me when no one is looking and I will take your order(s). Just think of all the looks of awe you'll generate at work wearing this shirt while you file away all the paperwork you'll have to produce over this convention. I won't turn in any feds who contact me, they have to be spotted by others.

HINTS FOR FEDS: A few hints so you can survive longer. (1) If you have to carry a firearm, don't use the "Gunny-sacks." The butt packs are easy to spot with their long zippers. (2) Try not to have a military style haircut. Dead giveaways. (3) Use of the word "Affirmative" and "Negative" don't help your undercover personae. (4) Drink a lot. I mean A LOT. No one will suspect you as a drunken agent of law enforcement! (this is one of my better tips.)

One whole slew of feds was spotted by someone when the feds' supervisor came into the hall and mentioned to their companion "One of my guys was already spotted." Doh! The contest winner just followed him to his group, and won their shirt with FOX Television from L.A. filming the whole thing. The spotted feds were cool with it, accepting their shirts.. but I think they left early.

ISP and Internet Services Provided By:

Dune: Lock picking demonstration and Q&A - There will be various tools and locks demonstrated. This will be a smaller talk at table X at x:xx on Sunday.

Koresh: A technical talk about ip spoofing, sequencing and fragmentation attacks as well as firewall penetration techniques.

Carolyn Meinel: *"Jobs are for Lusers"* - The oppressive potential of employers and the diversified marketplace results in self employment.

Andrew Black: FBI Computer Crime Division - Someone from the FBI will talk on the newly created computer crime divisions in San Francisco, Washington D.C. and New York.

HACKER JEOPARDY

Winn is back, bigger and badder with Hacker Jeopardy. The Holy Cow will help supply the beer, you supply the answers. Extra secret bonus round, and an elite challenge round make this year even better. The first round starts at 12 midnight o'clock on Friday and lasts until it is done. The second round will happen Saturday at midnight. Audience prizes! Give aways!

6 teams will be picked at random and compete for the final round. There can be only one! Strat's Team, the winners from last year, will get a chance to compete again if all the members can be found. Can they win twice in a row?

New Exciting Bonus Rule! Each team member must chug a beer before beginning the round.

Free Internet Access. Dialup: (702) 257-1111
Userid: demo, PW: free DNS: 208.129.21.2

KDNA
Voice of Mercury

FM Broadcast:
2-meter Simplex:	144.400 Mhz
2-meter Repeater:	146.940 Mhz 100hz PL, negative shift (vegas area)
2-meter Repeater:	145.190 Mhz, negative shift (vegas area backup)
Simplex Autopatch:	147.000 Mhz
Citizens' Band/CB:	Channel 26 (as in 2600)
Packet:	145.690 (K7WS-1/"LAS", 9600bps)

Please monitor CB 26 and/or 144.400 Mhz while travelling. Sending a "CQ DEFCON" message every once-and-awhile will stir up activity. Once in vegas, the 146.940 repeater works quite well, as it is on top of the Tropicana. There is, however, a bit of a "shadow" when you get too close to the Tropicana, and this might be a problem. If it is, try the 145.19 repeater. Otherwise, a new repeater frequency will be posted in the convention room. Do not abuse the Simplex Autopatch, please.

Light Ray

Other DEF CON Stuff

MAIL dtangent@defcon.org Send all email questions / comments to dtangent@defcon.org. It has been said that my email is monitored by various people. If you want to say something private, please do so with my pgp key (At the bottom of this announcement) I usually respond to everything, if not I'm swamped or had a system problem.

SNAIL MAIL Send all written materials, pre-registrations, etc. to: DEF CON, 2709 E. Madison, Seattle WA, 98112 If you are pre-registering for $30 please make payable to DEF CON and include a name to which you want the registration to apply. I don't respond to registrations unless you request.

DEF CON Voice Bridge (801) 855-3326 This is a multi-line voice bbs, VMB and voice conference system. There are 5 or so conference areas, with up to eight people on each one. Anyone can create a free VMB, and there are different voice bbs sections for separate topics. This is a good neutral meeting place to hook up with others.

MAILING LIST send email to majordomo@fc.net and in the body of the message include the following on a separate line each. subscribe dc-announce subscribe dc-stuff dc-announce is used for convention updates and major announcements, dc-stuff is related to general conversation, planning rides and rooms, etc.

CAPTURE THE FLAG

Killer Prizes! Dollars to be won! Round up the posse (so to speak) for it's time to bust root!

The capture the flag network is still going to have 5-9 dedicated machines. These machines will be running a variety of operating systems. The network is going to be connected to the Internet by way of a firewall. One machine on the net will be a terminal server for serial connections and people connecting from the Internet.

Seriously: The goal of the contest isn't to put messages on the console displays. Instead every machine will have a file on it called root.flag or root.flg To capture the flag, put your tag in that file. Putting messages on the console was too easy on some OSes, plus it would interfere with playing Quake.

The new simplified rules: **1)**No hacking from the console. **2)**No disabling any host for more than 3 minutes or the network for more than 30 seconds. A host is considered down if a Defcon Goon can't access a host and read the root.flag file. **3)** No crashing the terminal server. **4)** In order to be in the contest, you have to sign up your name(s) and an email address on a web page we'll have set up. Otherwise it just gets too complicated figuring out who's actually winning. (Remember, the whole Internet can play)

The Prizes: Dark Tangent is in charge of handing out prizes, and also of telling me what they are. It should include a couple hundred dollars cash and several prizes from Index Publishing, Secure Computing and anonymous donations.

Added attractions: About half of the machines on the net will be running Quake on the console. Bring your own quake machine to join in the fun.

Port-scan poker, hacking with a Las Vegas theme (details to be figured out at the last minute)

About 6 gigs of file space for all your 0day needs.

Top Ten reasons to attend Defcon 4
by Pappy 023ndorph

10. There are new hotels and PBX operators who've never heard of us.
9. You swore one year you'd see a speaker. This could be the year.
8. Even pit bosses and bondsmen can forget a face after a year.
7. That guy that told you to fuck off in IRC will be there.
6. You miss the 107 degree evenings.
5. Hookers take credit cards.
4. You go where the no-day eurowarez go.
3. We've got to find the 20+ MIA's from last year.
2. Everyone else is going, follow the heard. Moo.
1. The unbridled smut.

Here is a brief review of the new Stratosphere
Hotel Gseven posted to the mailing list: .. There is no gambling in the tower, although there is a "Stratosphere Casino" on the ground. The "King Kong" ride is part of phase two, and has not been built yet. By all reports, the "Let It Ride" roller coaster is a major yawner. The "Big Shot" by all reports is pretty wild, and is described as a reverse bungee jump. Contrary to the other report, you don't get "hauled" up and "dropped". You get shot up, by a giant slingshot but tethered by a rubber band. Supposedly if you manage to open your eyes at the top and are facing the right direction, you can see Lake Mead.

Start Update by DT and Crew. We went up there the other night, and just missed the last ride. It closes at 1 AM and the last chance to buy tickets is at about 12:30pm. You get about a 5g acceleration going up, and about 3g going down. The view is awesome, but the roller coaster ride is shut down. Seems a few wheels and bolts shot loose and broke a eindow. It's down pending a new safty review.

Netta "grayarea" Gilboa: *Sex, Lies and Computer Crimes: The Truth Behind The Indictment Of "Computer Genius" Christopher Schanot* - On March 25, 1996 Christopher Schanot was arrested based on an 11 day old warrant which stemmed from an indictment in Missouri for five counts of computer and access fraud involving Bellcore, SRI, Sprint and Southwestern Bell.

Gilboa is the publisher of the award-winning publication *Gray Areas* (http://www.gti.net/grayarea) and is the author of "Elites, Lamers, Narcs and Whores: Exploring The Computer Underground" which recently appeared in the Seal Press book *Wired_Women: Gender And New Realities In Cyberspace.* She has also been published in *Phrack, Computer underground Digest, Cult of the Dead Cat, Empire Times, Dupree's Diamond News,* and many other paper magazines and electronic publications. Gilboa holds an M.S. in Advertising and an M.A. in Sociology from Northwestern University and a B.A. in Journalism from State University College of New York at New Paltz.

Attitude Adjuster: "Windows 95 viruses and the Internet: How public API's and crafty code make for wild potential viruses." The speech will get people's attention, though. There are "security holes" big enough to drive early 70's model Chevy's through.

AA is an 80x86 assembler programmer, formerly a virus writer for the Virulent Graffiti virus group, and writes articles for Phalcon/SKISM and do virus disassemblies.

Great news here... Monday morning, 2AM, my friend's apartment burnt down. The machine that I was going to bring for the keysigning is now a pile of ashes. I'm gonna update the keysigning page begging for a machine... I doubt it'll be a problem, but, I thought I'd mention it. I had to get out of the building through a less-than-intended exit, that being a second floor window, and broke me left leg in two places below the knee. Barring surgery (which I find out about next week), I'm gonna be at the Con... Now, I'll relax and watch my foot turn blue.

Bootleg :*"The problems with counterfeiting"* - Sure to be a favorite with our federal "MIB" guests. Learn the technologies of reproducing money, and how the new $100 bills have already been forged.

Eric Hughes : Founder of Cypherpunks List - Keynote Speech Saturday morning. Digital Banking and Currency issues.

Dan Veeneman: *"Satellite Vulnerabilities: Present and Future"* - talking about controlling satellites, jamming and spoofing, GPS systems, future LEO systems, etc. Dan can be reached at: system@decode.com (Dan Veeneman) or on the Cryptography, Security, Privacy BBS +1 410 730 6734   Data/FAX

Yobie Benjamin & The Grinch: The Java session is an overview of Java's security - both its strength and weaknesses. It will cover Java's security architecture and also talk about Jvav's future from a h/p perspective. This session IS NOT a technical session or a "Introduction to Java" class. Technical sessions may be held off-line depending on the parties going on @ DefCon.

Yobie Benjamin is an Associate Director and Strategic Technologies Consultant with Cambridge Technology Partners (CTP), an international professional services firm that specializes in the development information technology solutions. Previous to CTP, Yobie has worked for and consulted with a number of firms including Lotus Development Corporation, Bank of America, GTE Information Systems and the American Automobile Association. Yobie specializes in large scale information systems/application architecture and emerging technologies.
The Grinch regularly publishes technical articles in the magazine Java World, an IDG publication. The only guys better than grinch in Java programming are the people who wrote Java themselves.

Dave Banisar: *"Tales from inside the Beltway: truly scary stories on privacy, censorship and watching Congress and the President work"* Dave is a policy analyst at EPIC and previously at CPSR and have been working on fighting big bro for about 5 years now.   He can be reached at: Banisar@epic.org or 202-544-9240. The Electronic Privacy Information Center * 202-547-5482 (fax) 666 Pennsylvania Ave, SE, Suite 301 * HTTP://www.epic.org Washington, DC 20003   * ftp/gopher/wais cpsr.org

The Institution: Today's hacker underground has lost the sense of community and mutual respect that was prevalent in the 80's. There is too much elitism in the scene, and as a result, the wheel has been invented too many times. Many of the new breed think hacking is mailbombing, running scripts, or crashing machines, which has given rise to new and unjust laws, and given ALL hackers a bad name. The Institution has been formed to remedy this by creating a loose association of 'old-school' hackers. This fraternity has been organized to promote the Hacker Ethic and open some of the doors closed by the elitism movement, and to foster a environment of learning and understanding throughout the community. During this session we'll discuss more of the philosophy and design behind the Institution.

Mudge: Operator of l0pht.com - Vulnerabilities in OTP's - SecurID and S/key. Dictionary, Spoofing, Hi-Jacking and Race Condition attacks.

Emmanuel Goldstein: Editor and publisher of 2600 Magazine - Panel discussion with Scott Skinner- "Why the E.F.F. Sucks"

Richard Thieme: *"the symbiotic relationship between networked computers and humans - a dialectic constituting a rising spiral of mutual transformation"* - Richard Thieme has lived in Chicago, Madrid, London, Salt Lake City, Lahaina (Maui) and now Milwaukee. Taught literature at the University of Illinois, wrote fiction. Worked as an Episcopal priest for sixteen years in three cultures. Now speaks, consults, and writes about the human dimension of computers. His focus is transformation - individual, organizational, global - and the transformation of spirituality online.

Hacking redefines how we think of ourselves. Redefines how we understand out possibilities for action in the world. It's also a metaphor for new opportunities available to human beings now and in the next century. Hacking is one way to practice living in transplanetary society. That's why hackers are pathfinders for the next generation. Spirituality is simply the way getting connected online translates into new kinds of community life.

Thieme consults on change, technology, and diversity for banks, insurance companies, law firms, schools, associations, government, etc. "The Stock Market, UFOs, and Religious Experience" is done frequently for investment and financial people.

Ira Winkler: has performed penetrations that rival the best of the hacker community. He is in the very enviable position of being paid to hack into some of the largest companies in the world. While he holds the unpopular opinion that hackers should be prosecuted for their actions, he believes that hackers can "outgrow their ignorance and be valuable members of the information security community." His advice for wannabe computer security professionals is that, "If you want to do what I do for a living, you have got to stop what you are doing." Come and see what he means.

Ira Winkler is the Director of Technology for the National Computer Security Association. He runs the NCSA laboratories, Firewall and Anti-Virus Product Certification programs. He also investigates information-related crimes. He is considered an expert in Social Engineering, Industrial Espionage, Penetration Testing and Information Warfare. For samples of his penetration work, look at http://all.net/journal/csi/xsocial.html, the June 3, 1996 Forbes ASAP (p.80), and the May/June 1996 issue of InfoSecurity News.

Mike Peros: I have some great war stories to share with everyone about some illegal Japanese Intelligence bugs that i found at an DOD contracting facility which was working an US Air Force contraction involving the F 18 fighter jet.

US Goverment Illegally Wire Tapping Innocent American Citizens And how I Caught them.

Data Tapping Through the Switch. Compromising the sub frame rooms, cross connecct boxes, and the many uses of liquid solder. The use of a cell phone as an eavesdropping device.

Stephen Cobb: *"101 Things to do with an Ex-Hacker"* - Could we or should we develop a process for "sanitizing" people who want to make the transition from illegal hacking to legitimate employment?

Stephen is an employee of the National Computer Security Association, is Co-Chair of the Computer Ethics and Responsibilities Campaign. He is also, by birth, a Libra, and thus given to weighing both sides of everything. He has been using a modem since 1983, but has never attempted unauthorized access. He believes in gun control but practices target shooting. He doesn't believe in income taxes, but pays them anyway. He is British by birth, but holds an American passport. A former Rugby player, he is an ex-member of Mensa and the National Organization for Women. In 1970, while still in high school, he charged police lines in protest at the all-white South African Rugby tour. In 1995 he cheered the multi-racial South African victory in the Rugby World Cup.

John Q. Newman: The Paper Trail - John will reveal what kind of information is legally available to anyone, how to build a "file" on someone, and how to try and protect yourself from this privacy threat.

John is the most prolific and respected author of false identification books in the country. His titles include: Understanding US Identity Documents, Reborn in the USA, Reborn in Canada, Reborn with credit, Reborn Overseas, Heavy Duty Identity, and Be You Own Dick. Many of these books are used by the FBI and the Royal Canadian Mounted Police as reference material for their agents. Mr. Newman is continuing his research in this area and will have three new books published this year.

Se7en and group discussion: "Hack The Lies" - This was created to give a voice to the once-silent hacker community. Over the years, popular misconceptions have arisen about the hacking community and its motives, which are now taken as fact by the general populace. "Hack The Lies" is here to dispell this misinformation and to educate the public on who we are, what we do, why we do it, and more. Come join us for discussion during Defcon IV and make your views known.

David I. Brussin: Information Systems and Security Consultant - David will discuss security issues involved in the changes in global networking and commerce. He will address the concerns that corporations and individuals will face doing business electronically over the next five years.

Richard K.: Specialist in Kidnap & Ransom negotiations, electronic surveillance counter measures and international trade - Will talk about what's real and what isn't, plus a Q&A session that should be very interesting. Sorry! Current law prohibits show and tell of the more controversial technology.

WWW Site http://www.defcon.org/ Convention updates and archives from previous conventions are housed here. Past speakers, topics, and stuff for sale. Also a growing section of links to other places of interest and current events.

Light Ray has been going crazy with support www pages, so take advantage of them!

Room and Ride Sharing Page: Plan for sharing a ride from around the country, post the availability of floor space in your hotel room or just see what people are up to. www.defcon.org or direct at http://exo.com/~fricke/dc-ride.html

The Con Page http://exo.com/~fricke/conpage.html

Who's Bringing What Page. Find out what people are bringing and what is needed. Very interesting mix of stuff. http://exo.com/~fricke/dc-bring.html

The Las Vegas Radio Frequency Page. Perfect for hours of fun with a scanner. http://exo.com/~fricke/vegasradio.html

CDC CELEBRATES TWELVE YEARS AS A CANDLE IN THE DARKNESS

We knew it would happen. We just didn't think we'd live long enough to see it.

CULT OF THE DEAD COW (cDc) celebrates twelve years of existence this month at DEFCON IV in Las Vegas! cDc will also introduce a series of music and audio releases, a new prestigious award for the telecommunications industry, and a new batch of text articles this month (#'s 321-330).

FESTOONS. PARTY FAVORS. ROOM SERVICE.

CULT OF THE DEAD COW will be celebrating their TWELFTH ANNIVERSARY at DEFCON on July 26-28th as befits their HEAP OF ELITENESS as the oldest organized group in the computer underground. Don't miss out on the fun. SWAMP RATTE' will give several impromptu workshops on crowd control and the appropriate use and maintenance of stun guns, WEASEL BOY will read from his gripping work in progress, _UNIX Sluts_, and THE DETH VEGETABLE will amaze you all with his professional impersonations of Buddy Greco, hand soap, and the color gray. These celebrations will be the talk of DEFCON and a tribute to your good taste. Make plans to attend now. Wear something special, bring plenty of fake I.D. and watch the herd show Nicolas Cage what getting liquored up in Vegas is all about.

Freqs!

I figured some scanner frequencies could prove useful for some of you who will be attending Def Con IV. If anyone has any 144/440 Mhz repeater frequencies they could share with me please let me know. - cracked@primenet.com

Scanner Frequencies for Las Vegas

Hotels & Casinos ——————————
151.665	Airport Casino
158.46	Riverboat Casino
460.95	Showboat Hotel & Casino
461.425	California Hotel & Casino
154.515	Aladdin Hotel
154.54	Hotel International
461.225	Airport Inn
461.55	Golden Nugget Hotel
461.70	Caesars Palace
461.90	Horseshoe Club
462.825	Bally's Grand Hotel
462.875	Golden Gate Casino
462.90	Sand's Hotel & Casino
463.45	Aladdin Hotel & Casino
463.60	Grand Resorts
464.225	Barbary Coast
464.375	Caravan Travel Lodge
464.425	Desert Inn
464.90	Vegas World Hotel

Police ———
F1 Info	159.150	F2 South	159.090
F3 Southwest	158.970	F4 North	158.745
F5 Detective	159.210	F6 Northwest	159.030
F7 Detective	158.790	F8 Special Event	156.210
F9	158.850	F10	158.850
F10 SWAT	159.910	F11	158.850
SWAT	156.030		

Fire ———
F1	453.150				
F4	453.400	453.100	458.700	154.430	154.370

Autographs

What's Happening

FRIDAY SUNDAY

REGISTRATION AND GETTING TO KNOW PEOPLE

TIME	EVENT
10:00-	CONVENTION ROOM OPENS
17:00-	CAPTURE THE FLAG STARTS
MIDNIGHT	HACKER JEOPARDY- FIRST ROUND!
02:00	CONVENTION ROOM CLOSES

TIME	EVENT
10:00-10:40	RICHARD THIEME: KEYNOTE
10:45-11:25	IRA WINKLER
11:30-12:10	MUDGE
12:15-12:55	JOHN Q. NEWMAN
13:00-13:40	ATTITUDE ADJUSTER
13:45-14:25	STEPHEN COBB
14:30-15:10	KORESH
15:15-15:55	EMMANUEL GOLDSTIEN
16:00-16:40	DETH VEGGIE
16:45-17:25	THE INSTITUTION

AWARDS FOR CAPTURE THE FLAG, FINAL PRIZE GIVEAWAYS & THE END OF IT ALL, CLEANUP, ETC.

SATURDAY

SPEAKING WILL OCCUR NON-STOP ALL DAY LONG IN ORDER TO FITT ALL SPEAKERS IN. EAT AND SLEEP AT YOUR OWN RISK. THERE WILL BE STRICT ADHIERENCE TO THE LENGTH OF TALKS SO YOU CAN BETTER PLAN WHAT YOU WANT TO HEAR.

TIME	EVENT
10:00-10:40	ERIC HUGHES: KEYNOTE
10:45-11:25	YOBIE BENJAMIN
11:30-12:10	ANDREW BLACK
12:15-12:55	MIKE PEROS
13:00-13:40	DAVE BANISAR
13:45-14:25	BOOTLEG
14:30-15:10	CAROLYN MEINEL
15:15-15:55	DAVID BRUSSIN
16:00-16:40	HACK THE LIES
16:45-17:25	DAN VEENEMAN
17:30-18:10	VAMPRELLA
18:15-18:55	NETTA GILBOA
MIDNIGHT	HACKER JEOPARDY- FINAL ROUND!
02:00	CONVENTION ROOM CLOSES

Special Events

HOLY COW FREE BEERS WITH TICKET

HOLY COW: While not really an event, the Holy Cow is sponsoring DEF CON this year with massive doses of their great beer! That's right! If you are over 21 you get a free beer ticket. Tickets will be randomly given away on Friday and Saturday. Over 500 tickets will be available! Ask any seasoned Con goer for the location of the Cow. It is down the strip about a mile. Take a $1.50 bus or a $4.00 taxi ride to get there.

VIRTUAL WORLD $2 OFF WITH NAMEBADGE

We will have a discount at Virtual World, and you will be able to play the various Red Planet or Battle Mech games. Full pod immersion! Up to eight people/pods per group. Virtual World will give any DEF CON IV attendee a $2 discount on any and every game. Just show 'em your name badge and your in! Look for the flyers around the convention hall for directions.

SEE YOU ALL NEXT YEAR!