Hey. This is DT type at you from the corner of the convention room. As you can tell there is no freaky program this yea. There is justthis. Why? Well a few reasons but basically lots of stuff happened at the last minute and I had to make sure the shirts got done properly. The peaking list is below, and I know there will be some modifications to it. They will go on some white boards in room 3. Tomorrow we get the room accross the hall for the network and all. We have a RealAudio server going up, CuSeeMe reflector, and the T1 is actually going to work. Woah. White Knight is going to give a speecch about his Title III search warrent stuuf he has been looking into.

The shoot is happening tomorrow morning. Hacker Jeopardy is happening at 9:30 Friday and Sat night.

SPEAKERS:———————————————————————————

There will be some speaking on Friday evening before Hacker Jeopardy, all day Saturday and Sunday. About 20 people will speak, plus smaller tech sessions. If you are interested in speaking or demonstrating something please contact me.

Current speakers include:

[> Nhil - Windows NT (in)security. The challenge response system, NT 5.0 Kerb security services, man in the middle attacks on domain controllers. This will be a more technical discussion of NT related security.

[> Mudge - System Administrator for L0pht Heavy Industries. He will present a technical talk on something cool.

[> Clovis - From the Hacker Jeopardy winning team. He will discuss issues with security and networked object systems, looking at some of the recent security issues found with activeX and detail some of the
potentials and problems with network objects. Topics will include development of objects, distributed objects, standards, ActiveX, corba, and hacking objects.

[> Bruce Schneier - Author of Applied Cryptography and the Blowfish algorithm - Why cryptography is harder than it looks.

[> Richard Thieme - "The Dynamics of Social Engineering: a cognitive map for getting what you need to know, working in networks, and engaging in espionage quietly; the uses of paranoia, imagination, and grandiosity to build the Big Picture.

[> Wrangler - Packet Sniffing: He will define the idea, explain everything from 802.2 frames down to the TCP datagram, and explain the mechanisms (NIT, bpf) that different platforms provide to allow the hack.

Wrangler has been programming since seven column paper tape. He is a loner with the social skills of a California Condor. He has never been a member of LOD, MOD, or any other group. He has written no books, is not currently employed, and refuses to discuss what he refers to as "that credit card provider thing back when I used to do mainframe shit." His current projects include looking for his next Fortune 100 contract and writing the DEFCON V virus.

[> Seven - What the feds think of us.

[> Richard K. - Electronic countermeasures, counter espionage, risk management. Should include a demonstration of electronic countermeasures equipment as well as a talk on what works, what doesn't, and the industry.

[> Ken Kumasawa of TeleDesign Management - Toll Fraud in the 90s: An overview of phreaking from a hackers point of view and an industry/security consultants point.

[> Michael Quattrocchi - The future of digital cash and a presentation about the modernization and state of register-level debit cards; in effect currently throughout Canada.

[> The Deth Vegetable - "The Cult of the Dead Cow embarks on a new era of Global Domination for the 21st Century three years early — if you're not at Defcon this year, you won't be down with the master plan. Important announcements and startling new developments that will affect the entire history of the Computer Underground as you know it."

[> Ira Winkler - Real life case studies of successful and unsuccessful corporate espionage.

[> Sameer Parekh - c2.net - Why cryptography is harder than it looks, part two. A look at implementation and production problems facing people and companies wishing to develope and distribute strong encryption.

[> Carolyn P. Meinel - Moderator of the Happy Hacker Digest and mailing lists. She will preside over a seperate Happy Hacker discussion pannel that will cover the topics of wether or not "newbies" should have information handed to them, or should they learn for themselves?

[> Dan Veeneman - Low Earth Orbit satellites are nearing the launch stage, and this talk will cover the different systems that are planned and some of the services they'll offer. A bit on GPS that wasn't covered last year as well as the ever popular question and answer section.

[> Hobbit - CIFS is a load of CACA - Random SMB CIFS stuff in Microsfot products.

[> Cyber - An overview and explanation of available crypto-tools. What tools and programs do what, when to use them and on what platforms. From someone who has spent lots of time playing around with the currently available set of applications.

[> Keith - Has some experience writing firmware for embedded microcontroller applications, and is giving a technical talk on applications of microcontrollers in the h/p community.

[> James Jorasch - Hacking Vegas - How to games the gamers. From someone who used to deal with hotel casino security. What really goes on?

SCHEDULE:———————————————————————————

10:00 - Doors open, sign in starts
10:00 - Movies start in main conference room
16:00 - Capture the Flag II starts

James Jorasch - "Hacking Vegas" how to beat the system in Vegas by someone who knows it inside and out.

21:30 - 24:00 Hacker Jeopardy Starts.

SATURDAY:

10:00 - 10:50 Richard Thieme - The Dynamics of Social Engineering.
11:00 - 11:50
12:00 - 12:50 Clovis - issues with security and networked object systems.
13:00 - 13:50 White Knight - Illegal wiretaps by the US Government.
14:00 - 14:50 Deth Veggie - Global Domination, cDc style.
15:00 - 15:50 Seven - What the feds think of us.
16:00 - 16:50 Bruce Schneier - Why Cryptography is harder than it looks.
17:00 - 17:50 Ken K. - Toll Fraud in the 90s: Two perspectives.

Saturday Breakout Tech Sessions:

Mudge - Secure Coding.
Hobbit - Why CIFS is CACA.
Wrangler - Packet Sniffing.
Keith - firmware for embedded microcontroller applications.

24:00 (Midnight) Final rounds of Hacker Jeopardy.

SUNDAY:

10:00 - 10:50 Ira Winkler - Take the Lamer test.. how bad are you?

11:00 - 11:50 Sameer - Why cryptography is harder than it looks, part two.
12:00 - 12:50 Cyber - An overview and explanation of available crypto-tools.
13:00 - 13:50 Carolyn Meinel - Happy Hacker Panel.
14:00 - 14:50 Michael Q. - The future of digital cash.
15:00 - 15:50 Dan Veeneman - Low Earth Orbit satellites.

Sunday Breakout Tech Sessions:

Happy Hacker track
Panel: "The Newbie Experiments"

Moderator is Carolyn Meinel, author of the Guides to (mostly) Harmless Hacking series. Other panel members are:

- Matt Hinze, editor of the Happy Hacker Digest.
- Bronc Buster, who runs a Web forum, IRC server and the New Buckaroos Web site for his fast-growing band of newbies.
- Mark Biernacki of Shellonly.com will talk about this new ISP which is designed to make it easy for newbies to learn to hack. Just say "Telnet port 22!"
- Jericho, who will hold forth on "Let the newbies fend for themselves."

We will allow each panel member to open with a brief presentation of his or orer work, followed by debate first among panel members, followed by Q&A from the audience. We expect some intense debate:-)

Then if the Aladdin hotel hasn't yet been demolished yet by riots, we will continue with a series of individual presentations:

- Jon McClintock, editor of Happy-SAD (Systems Administrator Digest) will demonstrate how to install Linux.
- Bronc Buster will hold forth on the Windows 95 denial of service programs his Web site offers.
- Carolyn Meinel will demonstrate how to read email headers, create, and decipher forged email.

Breakout Tech Sessions:

16:00 Awards for Capture the Flag
End of it all, cleanup, etc. See you all next year!

EVENTS:———————————————————————————————

[> HACKER JEOPARDY:

Winn is back with Hacker Jeopardy!! The third year in the running! Can the all-powerful Strat and his rypto-minion Erik, whose force cannot be contained, be defeated?! Will the powers that be allow Strat-Meister to dominate this beloved event for the third year in a row?! Can Erik continue to pimp-slap the audience into submission with a spoon in his mouth?!? Only Skill, Time, and booze will tell the tail!

The Holy Cow will help supply the beer, you supply the answers. The first round starts at 12 midnight o'clock on Friday and lasts until it is done. The second and secret rounds will happen Saturday at midnight.

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 defend if all the members can be found.

[> BLACK AND WHITE BALL:
We've talked it over, and the verdict is in. For the last two years at DEF CON there has been a sort of unspoken Saturday night dress upevent. People have worn everything from party dresses and Tuxedoes to AJ's ultra pimp Swank outfit with tiger print kilt. This year it is official. Wear your cool shit Saturday night, be it gothic or PVC vinyl or Yakuza looking black MIBs. No prizes, just your chance to be the uber-bustah pimp.

[> THE TCP/IP DRINKING GAME:
If you don't know the rules, you'll figure 'em out.

[> CAPTURE THE FLAG:
ALL NEW, ALL IMPROVED, MORE CONFRONTATIONAL,
1997 ILLUMINATI INVITATIONAL,
CAPTURE THE FLAG, HACKER STYLE.

The goal is to take over everybody else's server while protecting your own. To cut down on lag time and federal offences we're providing a playing field of 5 flag-machine networks connected by a big router in the middle. The rules:

1) No taking the network down for more than 60 seconds. 2) No taking any flag machine (including your own) down for more than 3 minutes. 3) In order to be counted in the game, a team's flag machine must
- be directly connected to the network;
- have a text file flag on the machine readable by at least 2 accounts,
- keep at least 3 *normal* services running in a way that a client could actually get their work done using them.
- run a web server if technically possible.

4) No goonery/summoning of elder gods/Mickey Finns/physical coercion... you get the idea. (You had the idea, but we're trying to prevent you from using it.)

The field of play :
Each network will have a "server" of some kind on it, called the flag machine. At the start of the game, these servers will be stock installations a lot like what you'd see on the average academic/secret cabal/military/megacorp network. Each of these machines will have a PGP private key, named root.flag, and a web server.

There will also be a machine to provide DNS, called the scoreboard.

Teams: Teams can be one human or more. In order to be a team, you have to generate 20 256bit PGP key pairs, have a DEFCON goon pgp-sign them and put the public keys on the scoreboard webserver. We'll generate a hundred key pairs in advance, so the first five teams can just grab a floppy disk (if they're trusting).

To prove that you've hacked a flag machine, PGP - sign a message with the root.flag from the hacked machine, then with one of your own. Post the doubly-signed message on the scorekeeper web server, and you've captured that flag (and invalidated the captured root.flag).

When you've captured a flag, decide between conquest and condescension: either take over the server yourself, or hand it backto its not-so-eleet owners. To conquer, put one of your PGP private keys on the captured server to become the next root.flag. (Of course, you have to properly secure the server to maintain your new territory.)

To condescend, just wait until the original owners see their shame spread across the scoreboard. (It would sure be a pity if they had to put up a new key before they figured out how you got in last time, wouldn't it?)

Two Ways to Win:
#1 EVIL EMPIRE: Whoever has the most servers responding with their teams' private keys at the end wins.

#2 PIRATE: Fabulous prizes will also be given to whoever racks up the highest total number of flags captured.

Rough game mechanics (why is everyone so untrusting?): Once every 5 minutes or more, the scoreboard machine will post a plaintext challenge. Every team that claims to own a server has toPGP-sign that challenge with the private key registered for that server and post the signed version on their machine. If a server can't respond within 3 minutes, then nobody owns it, and it's fair game to be taken back over by the goons.

Specific rules will be available in print at DefCon before the game begins.

This was a message from The People.

[> 5th 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 LA 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.

DOUBLE SECRET NOTE TO FEDS: This year I am printing up extra "I am the Fed!" shirts, and will be trading them for coffee mugs, shirts or baseball hats from your favorite TLA. If you want to swap bring along some goodies and we can trade. Be stealth about it if you don't want people to spot you. Agents from foreign governments are welcome to trade too, but I gotta work on my mug collection and this is the fastest way.

[> RAIL GUN DEMONSTRATION: (Friday)
The rail gun demo is not going off unless you have a 15,000W capacittor (I can't spell now!@#) but Ming will be talking about what he did, the problems he found and the power supply limitations.

[> OMNIDIRECTIONAL CELL PHONE JAMMER DEMONSTRAITON: (Friday)
[> RADIO BURST CANNON DEMONSTRATION: (Friday)

Due to extenuating stuff they won't go off. Maybe I will get them to talk about the problems.