DEFCON 9

Las Vegas • July 13-15, 2001

DEFCON DC9

Thanks

to the following people who made DEF CON possible (In no particular order) Noid, Zac, Noid, Preist, Artimage, AX, IRA, Dead Addict, Bink, Waz, Xylorg, The People, Josh, Tina, Dianna, Ping, Major Malfunction, Metal Head, Queeg, Videoman, ArcLight, Evil Pete, Dr. Kool, Russ, Evil, Megsusa, Lockheed, The Jinx Crew, TSOK, Charel, All of the speakers who worked hard to bring you new information, The Alexis Park Staff for putting up with us, Stevyn, Penguino, Winn Schwartau, The California Car Caravan people, anyone who did something cool for the convention like set up a wireless AP or a low power micro FM station, or just helped out a fellow hacker. With out everyone working together none of this chaos would have been possible. I will have a drink and toast your studliness.

Table of Contents

Welcome to DEF CON Nine!

This is the biggest and baddest show ever. More speakers than ever, a bigger wireless network than ever, longest running show ever, and more hotel space than ever. Let me take this opportunity to put the rumors to rest. This year we have more space than H2K2 will next year, and next year we will have another 10,000 feet. If you count the entire hotel grounds we have them beat by a few acres. You are at the largest hacker party / conference on the planet!

Now none of this would not be possible with out the speakers or the staff. Unlike Black Hat, the speakers do not get paid for their time. They are doing this because they want to present neat new stuff to the community. Buy a speaker a drink for their hard work, but do it after their speech!

The staff is all volunteer, and they do a great job considering there are over 4,500 people here. Please don't mess with the staff. They are not here to make your life tough, they are here to make the show go. If a hallway is over crowded and they ask you to please move, it is not because they are out to get you. It is because they don't want the fire marshall pissed off. So buy the staff two drinks, after their shift of course!

I have selected a wide range of speakers on the most number of topics. Take some time out of your parting and see some talks this year! We have tried to make more space available to speakers so there will be less crowding.

OK, I am (as usual) up late and behind work so I am off to finish the rest of this program. Welcome to my party!

The Dark Tangent

WWW.DEFCON.ORG

Events

2ND ANNUAL DEFCON COFFEE WARS

In our second year, we're back with a caffeine-induced vengeance. The premise is simple. You wake up, likely tired and hungover, you bring us your best coffees, and we find out just who has the best coffee of all. Check it all out at coffeewars.org

New this year

- Cooler prizes
- Larger supply of of t-shirts and mugs for the populace. Expanded judging categories
- Donations of coffee from Innkeeper's Coffee
- Free scalding w/boiling water for any who bring Folgers or Starbucks
- Better organization (we've had a year to figure out how to do this right, this time)
- Rob Nielsen actually showing up and not dishing the entire event to Jay Dyson

SOCIAL ENGINEERING COMPETITION

The social engineering competition is back...this year's competition will be held by the *drunkenwhores.com crew*. It will focus mainly on celebrity deception, and harassment of a select few 24 hour help lines...we will try very hard to keep it legal, but still very fun...some of the ideas we are working on right now include the personal cell phones of some of the most popular celebrities of today, and of course the 80's....Yes, we do have Scott Baio's (Charles in Charge) home number and we are not afraid to call him up and say hello... sign ups will be at the NOC, if the response is a large as we hope the participants will be chosen by a fair method at the con... *–Humperdink*

PINGUINO'S SCAVENGER HUNT

The scavenger hunt this year is being run behalf of *FLippersmack* (project that replaced sysfail) with the help of *Kline ezine (hackcanada)* to ensure that there'll always be someone there. Stop by and pick up the rules and enter the contest! Check out the official scavenger web site.

DEFCON 9 RADIO

Defcon 9 radio. Featuring 3500+ listener selected tracks streaming Vorbis through Icecast2. Users will have the ability to vote on what they want to listen to, view who voted for what tracks, and even vote off a song if it sucks. The track that has the highest # of listeners will be broadcast to an FM frequency so those wandering around or in their hotel rooms can also listen in on what people want to hear. Our wandering reporters will be getting up to the minute reports from people @ the con and updates will be broadcast through the station randomly throughout the day. Get your scheduling information with **D-Update,** every hour during scheduled activities. A few of the lectures will also be available throughout the con through separate streams on the station.

Assistance needed: For those who have recon capabilities in the area, we need to know what FM broadcasters there are in the area, and preferably like to find a solid frequency that is not currently in use... Sponsored by DMZ Services, Inc.

THE BLACK & WHITE BALL

OK, so this year we will have more ambient music (So you can talk to the person next to you) and a bouncer at the door.... Just like all those clubs you hate in LA or NY. If you don't try to dress up in your finest threads you don't get in. This is to reverse last years trend to people showing up in the same clothing they drove out from California in. Once you get in there will be a bar (for those of you over 21), DJ action, a his / her best dressed contest and some other stuff we haven't thought of yet. *So what is acceptable to wear?* In the past there have been formal wear, fetish wear, bondage clothing, a prom dress, old zoot suits, and a full "cyber" punk on roller blades with a head mount display. Anything you want to show off or feel good wearing, basically.

THE DEF CON SHOOT

YEAR FIVE OF THE DCSHOOT IS NOW OFFICIAL!

OK people, this is what you've been waiting for.

For the first time ever, we now finally have a DC-Shoot mailing list! Use it to make defcon shoot plans, talk about guns, 2A, gun advocacy, hunting, BBQ recipes, load data, etc... Just send mail to *majordomo@23.org* with the words subscribe dcshoot in the message body.

For complete information see the official and up to date DC-Shoot website.

DJ ACTION: PERFO RMING @ DEFCON 2001

"The music is abominable" - *Winn Schwartau*

Some major changes to the event this year.

Due to the fact that Defcon is growing so large we now have to use the DJ room for speakers during the day. As of right now the **DJ room will be providing entertainment from 6pm-6am Friday and Saturday nights only.** We had hoped to start Friday evening and go straight through till Sunday, but we need the space for speakers. This is going to limit the number of acts performing this year, but it should be a good party anyways.

Big change number two is the format. Traditionally we have had Industrial/Goth/EBM music on Friday night. This year we are looking to fill the Friday slot with more live acts during the evening and some good chillout DJs for the late night. The reason for this is simply, the Industrial/Goth/EBM music really doesn't bring anyone into the room. No point in having a party if no one shows up. Go to the Official DEF CON DJ site maintained by *twentythree.org* to get the band lineup.

THE DEF CON MOVIE CHANNEL

Starting on Friday and running until Sunday evening there will be a **DEF CON Movie Channel.**

Running on the hotel's closed cable system, people staying at the Alexis Park can turn to this channel to catch up on the history of hacking movies. As many movies as we can pack in three days that are somehow related to the hacking scene. See such stinkers as *The Net* and *Hackers* and such classics as *Colossus: The Forbin Project* and *TXH1138*. Complete schedule to be available at the show.

NEW: Stevyn from *The Iron Feather Journal* will be this years VJ. He will play the movies, provide schedulle updates, sort movies, a few video interviews, and random content when not mannig his booth.

TCP/IP DRINKING GAME

Ask the panel of hackers and security types questions.. if no onecan answer the question, they drink. You see how this can get interesting quickly?

DEF CON GOES TO THE MOVIES

We are waiting to find out what movie we will try and screen at this year's show.

"BODY OF SECRETS" BOOK SIGNING

With author James Bamford and his new book, Body of Secrets, immediately following his talk, at 1PM, in the Vendor area.

CAPTURE THE FLAG CONTEST

We're changing the rules again, trying for more action, more risk & more network uptime. If you are truly confused or lost, the answers are waiting for you at the NOC.

There are 2 ways to win the contest:

Download the image disk from ctf.img . Use "dd if=/tmp/ctf.img of=/dev/fdo" or rawrite to copy this disk image to a floppy. Boot the floppy in a machine with a network card and dhcp. You've now got a web server and anonymous proxy server to attack. The goal of the contest is to deface the web site on the floppy. All methods are allowed, but the results will be judged on coolness & elegance, how small the email is, and who was the first person to mail in this type of attack.

No back doors were added, but there are some questionable system administration moves that should make a remote attack easier.

Teams: Each team is going to have a color, and should use Ethernet cables of that color. (DT's going to spring for a box of red, white, blue, green, yellow, black and grey.) Each team will get an SSL client certificate that allows access to the central reporting web site.

Two weeks before defcon there was a hacking challenge involving a downloadable unix distribution or a programming problem (for the NT folks). First folks to solve the challenge got first choice on the colors. Winners from previous years are pre-qualified, they just need to come up with a new color.

Usually teams welcome new members during defcon, but you may have to show your stuff on the Grey net. Grey is Team All-of-the-Above, and is for anybody to plug into. Other teams may be added if we get more router space. If you want to plug in a machine just to see what happens, go ahead & plug it in on the grey net.

The targets: The last three IP addresses of each subnet are the target/victim IP addresses. (That should be a big hint about what to scan) Each team should have at least one machine capable of running vmWare that they're willing to leave plugged in. VMware has donated some goodies for CTF, and we'll have a license that everybody can use during Defcon. (There isn't any computer check in this year. Your team has to take care of your target machines).

How the game works:

• Each team is going to have some lUsers, some Sysadmins & probably a mess of hackers.

- Sysadmins win by getting the most points from hackers & lUsers.
- Sysadmins also get points for setting up new OSes. Sysadmins have a couple of options for how to set up hosts. Grab randomly from a bag of install disks & vmware images up on stage (20 points)
- Grab pre made vmware images from the bag, (10 points)
- Bring your own non intel architecture machines (5 points)
- Bring your own vmware images or premade intel hosts (0 points)
- Sysadmins get these points after the first lUser report. (So there's some proof that the machine worked). Sysadmins can touch the keyboard to change out services or the whole OS an hour after the first lUser report, when the machine is hacked, or when a judge takes pity on their fumbling with the install disks.
- In between setting up the OS & getting hacked, sysadmins are expected to go off & get drunk or watch the con. Go ahead & watch the console, but don't snipe attackers by hand.
- Users win by reporting on the services that that the sysadmins on other teams have set up.
- Users get 2 points for being the first to report on a new service, and 10 points for reporting the highest total.
- Users can re-report on the same service every 3 hours.
- For each service you find on another team's box, make a connection to the recording web server & report (scale of 1-10, 10 is high) how cool the service is, how hard you think it would be to implement (complexity) risk/ease of hacking. So someone who implemented a complete adventure game using forward and reverse lookups on bind4 might get 10,5,7 Reports from Grey net lUsers don't count but will influence the judges's decisions. Hackers win by putting a file on the root partition of any machine not on their team, then reporting on the hack. Hackers win the total number of points given in the lUser reports for that machine, plus any points the sysadmin may have bet, plus 20 points for the hack.
- Hackers will rank (scale of 1-10) the ease of the hack, how "risky" the service was, (yes we are setting the lUsers risk evaluation against the hackers) and coolness of the system that they hacked. So popping an ancient qpopper that turns out to be running on NT might be 2,10,8
- Betting: If a team has a positive number of points, the sysadmins can choose to bet points that their machine or service won't be cracked. They have to find someone on the other teams to take that bet & work out the terms between them. The terms should be written on paper on the wall. Hacking teams can bet points they don't have, they just go into negative points when they lose.

Still with us?

Here's the order:

- Green sysadmin grabs a vmware disk from the bag
- Sysadmin fires up the image, tweaks it to run her chosen services/site
- Red luser sees & logs the web site, (+2 points for luser)(plus 10 for sysadmin, since the site is shown to work)
- Red User's rates the site for 7,5,2 (+14 to sysadmin)
- Yellow team's luser rates it at 8,5,3 (+16 to sysadmin)
- Yellow Hacker on team 3 roots the box ((30+20)= 50 points for hacker)
- Yellow Hacker rates host as 8,5,3 (+16 to sysadmin)

So the total is Red =2, Green = 56, Yellow = 50

Rules: No coercive force, mickey finns or summoning of elder gods. No attacking the web server or central routers. Lame DOS attacks may cause the judges to disconnect your ethernet link Root partitions must have at least 64k writable. The judges may make changes to keep things moving. (think "Wait Wait don't tell me", not the olympics)

Strategy: If someone else has a cool service that's getting them a lot of points, have the hackers on your team steal it, THEN take them down.

Alliances may be profitable. Build cool (and very portable) services in advance. Pleasing the crowd on the grey net may mean you get awarded bonus points.

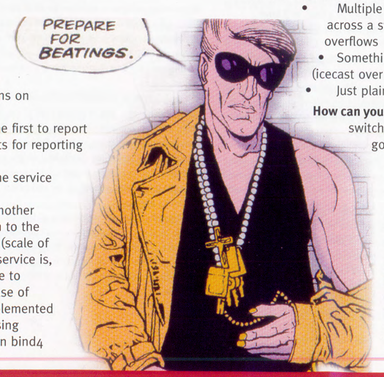
Getting hacked gives you points & the chance to change out your OS. So it is a valid strategy to put up lots of cool services that get hacked right away. A really cool server that stays up & keeps getting good lUser feedback is equivalent to installing a lot of os's & having them hacked right away. You get points for risky installs, but that costs you time. All of the scoring is tit for tat, not One round prisoners dillema so it makes sense to give people at least average points.

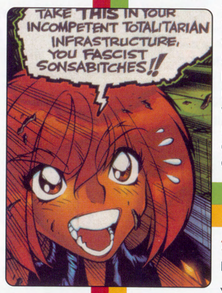
Some cool service ideas:

- Don't lock things down so that it can't be hacked, or rely on a back door that nobody will ever scan for
- Deception and confusion about where the attacker is or has connected to, but not so much that no one can get past it (hints are good)
- Multiple servers interacting Involving spoofing across a switch or router, or client with buffer overflows
- Something new with plaintext protocols (icecast over telnet with a new client)
- Just plain wrong apps (text mode quake)

How can you help? As usual, you'll need to bring switches, hubs, 10base T gear, etc. We're also going to need a lot of pre made vmware images & strange intel operating systems to put into the drawing bag , so start scrounging for windows 2.0 If anybody is willing to run book on the contest & offer dollars for points, that would be great.

In 1997 is was Team SNI, In 1998 it was the Mad Sweedish Hackers, In 1999 it was The Ghetto Hackers, In 2000 It was The Ghetto Hackers / Subterranean Security Group Combo... Who will it be in 2001?





CYBERETHICAL SURFIVOR: THE GAME

Ethics. CyberEthics. Kids. Hackers. And what about those Parents, huh? Corporations are ethical, right? ... and let's not forget Government, too!

Ethics is that gray area between Legal and Illegal...and maybe your personal or corporate ethics are different that his or hers, or of someone from a different country or culture. Yet, we all need to live in the same "Space". And that's the whole point of "CyberEthical Surfivor." **CyberEthical Surfivor** is an Interactive Game that pits 18 brave souls on two teams against each other. The object of the Game is to be...duh... the last one standing: A true Surfivor. How you get there is half the fun, but Da Judge (Jennifer Granick) and Da Time Keeper and the D'Audience will be heavily involved in who become the Surfivor! Think: Originality, Creativity, Positivity and Sticking to Time Evolve and Develop a Consistent CyberEthical Profile and Persona That Your Team Mates, Opponents and Audience Will Support Throughout the Game. Strategy? Compete with your team? Want winners or losers on your side? The other side? What does the audience want?

AUDIENCE PEOPLE: You get to play, too, by second-guessing and challenging the contestants on stage. You can pick and choose who stays and who goes. Who is the most or least ethical... in your humble opinion? We'll have roving microphones so you can get your 2-cents in! Wouldn't want our contestants to feel they're getting off easy, would we? In fact, you can make their cyberethical lives a tad miserable, if you choose.

LOSERS: There will be 17 losers, and they will all win something, just for playing. Nothing stupendous, but hey... you lost!

SIGN UP: Anyone can play. Kids. Spooks, Spies, Hackers, Suits. No age limits (this is a PG/PG-13 Game). Submit your name, affiliation and contact information at the NOC. We will draw names from a stupid hat at the beginning of the Game, Saturday, July 14, 2001.

WHAT THE SURFIVOR WINS:

1. $800 donation of ethics books in your name to the educational institution of your choice.
2. DefCon attendance free for life!
3. DefCon Jacket
4. Bragging Rights
5. Come back next year to defend your title!

HOST: Winn Schwartau (www.nicekids.netwww.interpactinc.com, www.infowar.com)

DA JUDGES: Jennifer Granick, Stanford Law; Chris Goggans, Counterpane; Richard Thieme, Social Commentaryist

7TH ANNIVERSARY HAXOR JEOPARDY

Hacker Jeopardy is Back!

Yup...DefCon fans just keep on coming and coming...So, for the 7th year in a row... we play Hacker Jeopardy! **It starts, as usual, at 10PM on Friday night** for two games where the teams (of up to three people each) fight it out, duke it out and drink it out with questions to our answers.

You know the Game. Winners win great gifts from Dark Tangent and DefCon. Losers get to drink. All players drink. (>21 Only) Hacker Jeopardy is rated Heavy-R, NC-17 and one year it was nearly X. You are warned.

WHO CAN PLAY? Most people play pretty lousy... but you can still try. Submit your teams at the NOC and we'll pick you out of a hat before each Game. One year a secret government group got so drunk, they didn't answer one question right. That was humiliating. For them.

AUDIENCE PLAYS: Yup! You get to play, too. DefCon ends up with tons of presents and gifts that we toss out to audience members who come up with the right questions... we got to get rid of all this stuff...one year we gave away a couple dozen Sun workstations! Plus, you can make fun of the contestants on stage. Be rowdy. A little rowdy, not a lot rowdy. Don't want anyone arrested again for being TOO rowdy.

WHEN: Friday, July 13, 2001: 11PM. Rounds One and Two. Saturday, July 14, 2001: 11PM Round Three, and then the Final Round, where the winners from the first three Games compete. Last Year's winners can play in Final Round as Team #4, if they choose.

Uber Haxor Sessions

FX, *Phenoelit*

ATTACKING CONTROL, ROUTING, AND TUNNELING PROTOCOLS

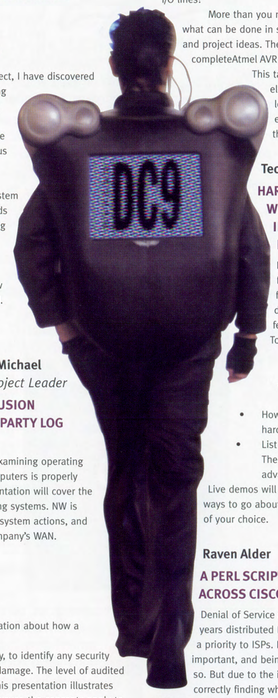
The protection of networked computers depends on the security and integrity of the underlying communication layers. In the last years, many people invested time to research bugs and exploits on the application level and less interest was on the network layers.

We are going into the realms of protocols of ISO OSI layer 2 and 3. The audience will get a quick refresher on what Layer 2 and 3 are about and which general attack approaches exist. Layer 2 will be covered quickly and attacks using the well known ARP, CDP and some more will be explained.

The primary part of the session will be focused on the abuse of ICMP and interior routing protocols (RIP & IGRP), how to scan for autonomous systems and for IP protocols other then TCP/UDP. Re-routing of packet streams for sniffing/interception will be covered as well. The finale will explain and show how to attack VPNs using GRE and how tunneling can enable you to circumvent NAT.

Thor

GRABBING USER CREDENTIALS VIA W2K ODBC LIBRARIES



Ofir Arkin, *The Sys-Security Group*

INTRODUCING X: PLAYING TRICKS WITH ICMP

During my research with the "ICMP Usage In Scanning" project, I have discovered some new active and passive operating system fingerprinting methods using the ICMP protocol. Methods that are simple, and efficient.

The active operating system fingerprinting methods were not correlated into a certain logic. A logic that would allow us to have the ability to use any available method in order to, wisely, actively fingerprint an operating system.

In this talk I will be releasing a new active operating system fingerprinting tool using the active OS fingerprinting methods with the ICMP protocol I have discovered. I will be explaining the tool's inner works and the various active OS fingerprinting methods with ICMP implemented and used with the tool.

The tool's limitations, ways to detect its usage, and how to defend our selves from its abilities will also be discussed. Future plans and enhancements, which include a different approach to OS detection, will be presented as well.

Robert Grill, *CISC, sscp, Audit Project Leader;* **Michael Cohen,** *MBA, CISA, CISSP, GCIA, CNA, Audit Project Leader*

WINDOWS NT AND NOVELL HOST BASED INTRUSION DETECTION USING NATIVE LOGGING AND 3RD PARTY LOG REPORTING TOOLS

Auditing is defined for this presentation as the process of examining operating system (OS) audit logs to assure information stored on computers is properly protected, and meets corporate security policies. This presentation will cover the Novell NetWare 4.11 (NW) and Windows NT 4.0 (NT) operating systems. NW is capable of auditing Novell Directory Services (NDS) and file system actions, and NT for domain and file systems actions, performed on a company's WAN.

Auditing tracks the following types of information:

- User Actions
- Resource Usage
- File System Security and Access Control
- Login and Logoff Activity

NT and NW also includes auditing features to collect information about how a system is being used.

These features monitor events related to system security, to identify any security breaches, and to determine the extent and location of any damage. The level of audited events is adjustable to suit the needs of an organization. This presentation illustrates the usage of NT and NW security monitoring separately; however, the concepts apply to any platform.

The costs and benefits along with the weaknesses of such logging will also be addressed. While these are two older platforms that the software vendors would love to see upgraded, they are both still used in many organizations.

Mark Grimes, *Network Security Researcher*

TCP/IP INTELLIGENT AGENTS: THE FUTURE OF ELECTRONIC WARFARE AND DEFENSE

The study of Artificial Intelligence bring many treasures to the development of both offensive and defensive network tools. Code can be designed to make "intelligent" decisions based on a presented data sample. When rules are explicitly laid out by RFC to indicate proper connection handling, these rules can be mapped and recalled. This would allow for an automated handling of network traffic with decision making enforced on next-packet injection.

The DEF CON speech will focus on Intravenous. Information will be shared with regard to overhead handling, event priority, as well as database and sensor/decoder optimizations. Examples in logic considerations will be broken down for simple attack scenarios. The IV specific design constraints and project goals will be discussed, a maillist will be announced for open discussion about the code that has been developed so far, and improvements of the overall design criteria.

The Nemesis injection routines will be used in Intravenous. The threat of Nemesis by itself will be discussed with examples sited from published sources, and then will be contrasted with the introduction of AI components, that will make up the overall study, Intravenous (an agent concept model).

photek

WRITING BACK DOORS

This talk will be about the art of creating backdoors. Starting with automated shell scripts as an example, moving quickly to suid-exec wrappers and finally an introduction into writing kernel modules, and modifying existing ones using Linux in this case. In this talk there will be non-public code written especially for the talk. I'm not sure if this is for the haxors or the uber haxors. Probably uber haxors, as you'd need to at least be able to read some C, and the major focus will be on Linux kernel module creation and modification.

Phil King

8 BITS AND 8 PINS: MORE FUN WITH MICRO CONTROLLER HACKING

"Microcontrollers" are microprocessors with additional peripherals, I/O controls, and memory all built into one chip.

Last year, Phil introduced the wonderful world of 8-bit micro controllers and showed how to set up your own project development lab. This year he looks at more fun, cute, and devious electronic devices you can build, this time focusing on micro controllers with only 8 pins. What can you do with 2K of code spaces and only a few I/O lines?

More than you might imagine! We'll look at various tiny projects, and see what can be done in small space and on a small budget. Bring your questions and project ideas. The people with the best ideas will go home with a completeAtmel AVR micro controller hardware development package.

This talk will have a fairly high fun-factor looking at cool electronic toys, but there will be talk about and examples of low-level code and hardware design. Some programming experience and electronics vocabulary will definitely make the material more understandable.

TechnoDragon

HARDWARE MODS, HOW TO LOOK FOR THEM, WHAT TELLTALE SIGNS TO LOOK FOR, HOW TO IDENTIFY WHAT HARDWARE MOST LIKELY CAN BE MODIFIED, ETC.

Hardware mods. Have you ever wondered what special features can be enabled is your hardware, or even crippled for security reasons? Well, I will cover theory, fact and many designs covering identification and activation of hidden features wether they be hardware or software.

Topics will include:

- Identification of places to perform mods in hardware
- How to manipulate mods and features and settings to enable mods.
- How to identify what extra features can be enabled in hardware.
- List of what tools are required.

Theory behind future mods and placement of mods in advanced devices.

Live demos will be performed on the platforms covered and tutorials on ways to go about discovering what mods can be performed on the hardware of your choice.

Raven Alder

A PERL SCRIPT THATTRACKS DENIAL OF SERVICE ATTACKS ACROSS CISCO BACKBONES

Denial of Service attacks are well known in the security field, but in recent years distributed Denial of Service attacks have become more of a worry and a priority to ISPs. Recognizing when a DDoS attack is crossing your network is important, and being able to shut it down at your network's edge is even more so. But due to the increasing ease of spoofing the source IPs of a DDoS attack, correctly finding where the traffic is entering your network becomes more difficult. Rather than being able to traceroute via normal routing methods, most tracing of spoofed addresses has to be done hop by hop, one router at a time. In a large backbone, this can take hours, particularly when you consider that many DDoS attacks come from hundreds of different IP addresses.

There aren't many tools out there to aid NOCs in tracing these sorts of attacks. Indeed, many NOCs are still forced to trace attacks by hand. To address this problem, I have written a Perl script to trace DDoS attacks backwards through a Cisco-router network. The script can handle spoofed IPs, and will run both on Cisco's older routers (7500 series) and on their Gigabit Switch Routers. This talk will present the script and provide a guided tour through the code to explain how and why it works.

Robert Muncy

SECURING CISCO ROUTERS

We will begin with basic IOS Commands to secure a router, looking at unneed services and turning off seldom used protocols. From there we will look at configurations for defeating basic attacks against your network, including DDos,SMURF and other nasty things you can do to netowrks. Next we will look at some Simply Access list and nifty tricks you can do with them! I will also discuss the basics of Encryption, RADIUS and other security measures you can use when making connections to multiple sites. For this Talk I have assumed you have at least heard of TCP/IP Ports, Basic Cisco IOS Commands, and the internet and how it works! This talk is geared to Cisco noviecs but who have done basic networking already.

Thomas J. Munn, *Infosecurity Analyst*

USING OPEN BSD, SNORT, LINUX, AND A FEW OTHER TRICKS TO SET UP A TRANSPARENT, ACTIVE IDS

Basically I will cover:

- How to set up Snort Sensor in Openbsd
- How to use Perl & Rules to actively adapt rules to attacks, while keeping yourself from being "DOSSED"
- How to use ACID to make logs more easily accessible, and analyzed
- How to Use database portion to look at historical attack trends and react appropriately
- How to set up "safe" management segment on your network that is both accessible to you, but hard for "them" to get into.

Anders Ingeborn

DESIGNING SMALL PAYLOADS

This speach presents a number of ways to reduce the size when designing payloads for exploiting buffer overflows. It includes some code examples and will also give examples of situations when a small payload is needed (where the available number of bytes are restricted).

Bruce Potter & Adam

THE CAPTIVE PORTAL

Adam and I have been doing research on wireless security from a practical perspective. Basically discovering what's wrong with the current security models in 802.11 networking and how they can be fixed or worked around.

Adam has developed a system called the Captive Portal that will allow wireless networks to be setup that are resilent to problems with link-level authentication and encryption schemes. The system is still in development, but will be "released" by conference time (as much as open source software gets released ;). In the coming months we will be writing a paper on the Captive Portal; how it works, what it's strenghts and weaknesses are, and instructions on getting one going.

I will give the first part of the talk, Adam will give the second part the part that deals directly with the Captive Portal. We will also setup a wireless network at DC so folks can try and hack the portal. We're always looking for ways to improve our idea.

Kevin McPeake & Chris Goggans

FALLING DOMINOS

As the only groupware solution to meet the US DoD's standard for the Defense Messaging System, Lotus Notes / Domino is considered one of the more secure mail/groupware platforms in the world. With an installed base of more than 75 million corporate and government seats, the product is used by almost all financial institutions, Big 6 accounting firms, government's intelligence agencies and defense organizations.

At DEFCON 8, Trust Factory co-founders Kevin McPeake and Wouter Aukema presented several new vulnerabilities along with Chris Goggans, of Security Design International, who validated their research. Topics included known vulnerabilities and new ones, such as bypassing the Execution Control List, modifying Notes design elements and Digital Identity theft. Using a newly developed tool code named "Sesame", Trust Factory demonstrated weaknesses in the hashing algorithms for internet passwords as well as the validation of Notes ID-files obtained from remote networks and users.

Now, for the 2001 installment of Defcon, Kevin and Chris will be returning to Las Vegas to present "Falling Dominos" once again. Updated with all the latest tricks, tips & treats accumulated over the last year during their cooperative research together, Kevin and Chris will be demonstrating Domino Web Hacking secrets & will conduct a demonstration how all the vulnerabilities can be assembled to conduct Information Warfare.

Dan Kaminsky, *CISSP, http://www.doxpara.com*

GATEWAY CRYPTOGRAPHY: HACKING IMPOSSIBLE TUNNELS THROUGH IMPROBABLE NETWORKS WITH OPENSSH AND THE GNU PRIVACY GUARD

1) Theory of Gateway Cryptography
2) Methods of securely connecting mutually firewalled hosts
3) Turning any SSHD into a VPN termination point (without using PPP over SSH)
4) Dynamically Rekeyed OpenPGP
5) PPTP over SSH
6) Securely SUing to root
7) Robustifying live-configuration of OpenSSH
8) SFTP Compatibility Mode (implementing everything with cat, tar, and tail)

Dmitry Sklyarov, *ElcomSoft Company*

EBOOKS SECURITY – THEORY AND PRACTICE

Security aspects of electronic books and documents, and a demonstration of how weak they are:

"standard" PDF encryption,
Rot13 (used by New Paradigm Resources Group, Inc.),
FileOpen (by FileOpen Systems),
SoftLock (by SoftLock Services, Inc.),
Adobe's Web Buy,
Adobe's eBook Reader (GlassBook Reader)
InterTrust DocBox plug-in.

Documents publishing in electronic form have a lot of advantages against traditional on-paper publishing. You could easily find list of such advantages on web server of any company, which provides eBook solutions. But nobody perfects, and there is one big problem that related with eBooks. Information in electronic form could be duplicated and transmitted, and there is no reliable way to take control over that processes. There are several solutions from different companies that were developed to prevent unauthorized distribution of the electronic documents.

Optyx

KIS - KERNEL INTRUSION SYSTEM

This is the release of KIS. KIS is a self contained binary that when executed on a system installs itself so that it will be loaded on reboot and loads a kernel module. This LKM hides itself, all of its subprocesses or desired processes, all of their files, directories, and network connections automatically. The presentation will consist of demonstrating how to setup and use KIS as well as explain some of the basic design concepts.

Jason Peel

CYPHERPUNK-GRADE COVERT NETWORK CHANNELS

Two parties, both operating in hostile network territory, need to communicate covertly via an internetwork. They need to do so in a manner such that a well-resourced attacker cannot gain knowledge of the content of their transactions, nor even gain evidence beyond plausible deniability that discrete communication is taking place. The assumptions made are extreme; it is understood that lives may be at stake.

An initial r+d implementation in library form as well as proof-of-concept code built upon it will be presented. By taking advantage of peculiarities in many fielded protocols, steganographic techniques applied to the network layers, and using dynamic polymorphism based on local traffic patterns and cryptographic control, the channel is effectively able to resist detection and attack. Discussion concerning the theory, implementation, and political ramifications is welcomed.

K2

POLYMORPHIC SHELLCODE API

Polymorphism has been around for years in the form of virus attacks. There is a wealth of information pertaining to this. This presentation will concern itself with the implementation of an API designed to place some black-box code (probably shellcode) within an encoded structure and deliver it against a number of Architectures (SPARC,HP,IA32,more soon).

This code has been tested thoroughly against a number of popular NIDS Sensors (ISS, snort, dragon, NFR,), and has proven that as of yet, the code itself can NOT be detected at all. There are some possible methods of detection and that will be analyzed and future modifications to further evade these measures.

D-Krypt

WEB APPLICATION SECURITY

Rob Shein

EVALUATING VPN SOLUTIONS

This session will detail a methodology by which security professionals may independently examine the security of a VPN. We will cover basic concepts of key exchange and management, leading into a description of good and bad ways by which the two ends of a VPN connection arrive at the necessary shared secret. We will discuss common mistakes such as improper random seeding or key exchange, and step through a checklist of things to check. Finally, we will apply this methodology before the audience in the testing of a running VPN system, and demonstrate two vulnerabilities that exist.

Nick Farr

DESIGNING SECURE INTERFACES "FOR DUMMIES"

"The old addage holds there is an inverse relationship between usability and security. The more user-friendly the system, the less secure it is. However, recent user heuristics research may lend insight into how to design more usable, more secure operating system interfaces—independent of the underlying OS architecture, AND the gullibility of the user.

By highlighting the graphical and subtexual cues recently highlighted in popular OS interfaces, the speech will cover how users are betrayed by them, either into a state of paranoia or a false sense of security. The speech will show how both states can be used to exploit the system through the user.

As well, five guidelines for future interface design will be presented, showing how increasing the security of the interface can actually be used to increase, instead of restrict usability. While the talk is theoretical, each guidline will be applied as integrated into the design of a work-in-progress Kiosk package currently under development.

Adam Bresson

DATA MINING WITH PHP

Biing Jong Lin; Chieh Chun Lin; Jan Che Su

SURVEY OF COUNTRY-WIDE WEB SERVER SECURITY

This presentation describes how we did the country-wide web server security evaluation in 1999 and 2001. It covers methodology and results. Also, we compared the difference between these 2 surveys, make some conclusion on current status and advisories to the government. Vulnerable web servers by type and percentages as well as trends are covered.

General Sessions

Richard Thieme

HACKING A TRANS-PLANETARY NET: THE ESSENCE OF HACKING IN A CONTEXT OF PAN-GLOBAL CULTURE, THE WETWARE / DRYWARE INTERFACE, AND GOING TO EUROPA

When Richard Thieme spoke at DefCon 4, he said hacking was practice for trans-planetary life in the 21st century. Well, guess what? It was. But a changing context has also changed what hacking looks like. Context is content, and what was hacking at MIT on a PDP-6 just doesn't cut it any more. The essence of hacking is the same, but the game is played differently. When space war involves holographic image projection, cloaking devices, multispectral camouflage, micro-know-bots and the creation of synthetic environments that an adversary thinks are real ... when cells are switched on to conduct heat and electricity ... and the exploration of Titan and Europa make Mars and the moon look like inner suburbs ... hacking means more than knowing how to spray paint a website or shut down a server. Hacking means an artist's imagination, an obsessive hunger for knowledge, and a deep understanding of cyborg humanity. Thieme illuminates the topography of that weird landscape.

Key concepts: context is content, i.e. what makes sense in one context no longer makes sense in another, what is wise in one context is insanity in another; hacking in its essence is a way to approach life with identifiable qualities and characteristics—some are innate and some can be learned. the ones that can be learned and how to learn them are spelled out; the attributes of hacking as it evolved in the sixties, if translated whole hog into the 21st century, make you look like a dork; it's not about being a script kiddie, doing ddos attacks, or leaving graffiti—it is about the tools of imagination, the weapons of the mind, in a world of widespread deception; the practice of deception—the creation of illusion, the use of misdirection, the lethality of ridicule—are examined in relationship to hacking as the quest to know the truth; specific scenarios will be described, using the most current human resources, including war in space; the fusion of information war and space war through the "information web;" the changing definitions of humanity at the wetware/dryware interface, with emphasis on materials science and advances in brain enhancement; how life in space changes people and changes the species; and the bottom line—how the real attributes of hacking can be ported into this Borg world and used imaginatively, mischievously, and with a light touch to give real style to one's hacking and transform one's cyberlife into a work of art.

Peter Shipley

802.11B WAR DRIVING

Michael Wilson

HACKER DOCTRINE IN INFORMATION WARFARE

It is now an accepted fact that computer hackers, crackers, hacktivists, virus writers, and other politically-aware individuals in the computer underground are 'taking matters into their own hands.' Whether through website defacementsor full-scale denial-of-service attacks, non-governmental, non-aligned individuals and groups are conducting what the military refers to as 'information operations' of increasing sophistication.

What is clearly missing in these independent operations, however, is a complete and thorough understanding of how to think about attacks, how to undertake'mission planning,' and how to be truly effective. Based on our own understanding of practical applications in information warfare, 7Pillars Partners will present educational material on information operations that canhelp fill in these 'gaps' in a hacker's comprehensive understanding.

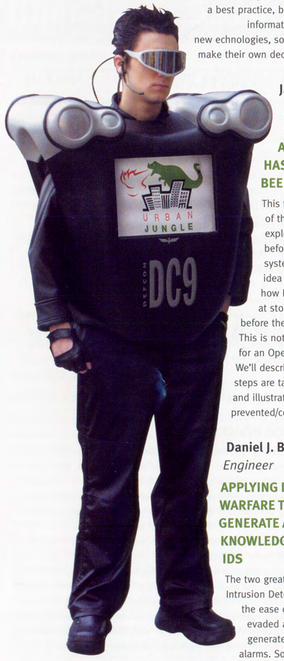
Marcus Andersson

FIREWALLING WIRELESS DEVICES

The different technologies today for providing IP-access over the air to handheld devices all pose some interesting questions about traditional securitywork. How to firewall? What is the physical differences of being on the "inside" versus the "outside" of the firewall? How to implement prudent securitymeasures if there is no security on the physical layer? Today, we can conclude that most base-stations used for Radio LAN:s, regardless of technology (Bluetooth or IEEE 802.11) have coverage outside the building. This means that if someone is in the parking lot, with a PC and a RadioLAN connection, one is connected to the office LAN.

The presentation suggests some architechtureal workarounds to some of these problems, namely for example to put all handheld devices on their OWN "demilitarized" network, and not on the "inside" of the firewall. Other suggestions are made on how to implement some security on the handheld devices themselves, in order to protect them from compromising the whole network, as an unsecured "endpoint" in such a network would do. The topic of personal firewalls and automated virus-scanners for handheld devices comes in at this level.

Some issues regarding implementing cryptography in different layers of the OSI-model are discussed, as is both risks and verified securityholes with current cryptographical implementations on the link-layer (such as WEP). A brief discussion on cryptographical protection and the impact on intrusion detection (the sensors can't see what happens if the traffic is encrypted) and virus-scanners (scanners can't scan encrypted mail) in included as well.



It is not in the scope of the presentation to suggest a best practice, but rather to give some information on the threats of these new echnologies, so that risk management can make their own decisions based on that.

Jay Beale

ATTACKING & SECURING RED HAT AKA HOW EFFECTIVE HAS BASTILLE LINUX BEEN?

This talk will demonstrate each of the major (widely available) exploits against Red Hat 6.x, before and after hardening the system with Bastille Linux. The idea is to show, very concretely, how Bastille Linux was effective at stopping/containing attacks, before the exploit was ever written. This is not simply a "product demo" for an Open Source tool, though! We'll describe exactly what hardening steps are taken to combat each attack and illustrate how these prevented/contained a compromise.

Daniel J. Burroughs, *Research Engineer*

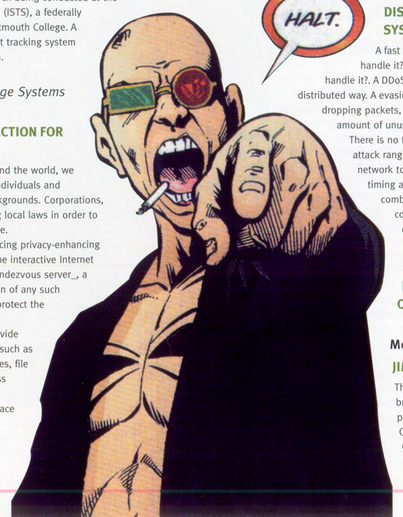
APPLYING INFORMATION WARFARE THEORY TO GENERATE A HIGHER LEVEL OF KNOWLEDGE FROM CURRENT IDS

The two greatest weaknesses of Intrusion Detection Systems (IDS) are the ease of which they may be evaded and their tendency to generate vast amounts of false alarms. Sophisticated attackers are able to easily avoid detection, maintaining a low profile by spreading out the attack both in time and (network) space. Meanwhile alerts are generated by normal user activity. IDS have not yet reached a level where they can reliably detect and assess advanced attacks while being able to separate normal user activities.

This presentation discusses the use of Information Warfare theory, combined with multiple target tracking algorithms to generate a higher level of knowledge from current IDS. Instead of looking at IDS as the final stage in attack determination, it becomes the first stage. The IDS are treated as sensors on our network gathering information that is fed into a data fusion engine. By gathering information from different types of IDS and other sensors distributed throughout one or more networks, we aim to generate a higher level of knowledge, a situational awareness, that paints a much clearer picture of the activity on out networks.

By combining and fusing data gathered from many independent networks, it is possible to move away from the traditional defensive posture of network security. In its place we are given more of bird's eye view of the scene, and are able to see the activity of individual attackers spread out across many networks.

This presentation is based on research being conducted at the Institute for Security Technology Studies (ISTS), a federally funded research institute housed at Dartmouth College. A demonstration of the data fusion / target tracking system will be provided during the presentation.



Dr. Ian Goldberg, *Zero-Knowledge Systems*

ARRANGING AN ANONYMOUS RENDEZVOUS: PRIVACY PROTECTION FOR INTERNET SERVERS

As the Internet grows in popularity around the world, we are beginning to see clashes between individuals and governments from different cultural backgrounds. Corporations, organizations, and legislatures are using local laws in order to enforce their wishes on others worldwide.

Much work has been put into producing privacy-enhancing technologies that protect clients of online interactive Internet services. In this talk, we present the _rendezvous server_, a primitive which allows the transformation of any such technology into one which can equally protect the providers of those services.

It is our hope that being able to provide privacy for providers of online services, such as mailing lists, discussion groups, web sites, file servers, and chat rooms, they will be less susceptible to attack, and so will help prevent the Internet from becoming a place where the powerful can control the availability of content worldwide.

William L. Tafoya, Ph.D., *Professor of Criminal Justice, Governors State University*

GENERAL SESSION OPENING TALK

Keith Nugent

WINDOWS 2000 SECURITY: HOW TO LOCK DOWN YOUR WIN2K BOXES

Windows 2000 provides a lot of new security features that were previously not available in earlier versions. The NT line, however, has never been considered very secure right out of the box. We'll be talking about how to use NTFS permissions, Default Security templates, Custom Security templates, and Group Policy to lock down a Win2k box.

We'll look at what level of security is applied by default on a Win2k box, how to analyze these settings against proposed settings, and how to apply identical settings across multiple boxes.

Brenno de Winter, *CEO, DeWinter Information Solutions*

IP V6 SECURITY

What's new. What are new risks? What are new opportunities. HC NTFS Alternate Data Streams

Windows NT (WNT) and Windows 2000 (W2K) have powerful graphical user interfaces that make the job of assessing the security condition of and securing these operating systems considerably easier. Changing the bad logon limit is, for example, relatively easy to both understand and do in both of these Windows operating systems.

Providing adequate security does not, however, always involve working with mainstream features of applications, operating systems, and networks. Alternate data streams (ADSs) are an example. This little-known feature available with the NT File System (NTFS) in WNT 4.0 and Win2K (RICH98) has been available since the advent of NTFS in the first WNT release, WNT 3.1. Although this feature is relatively unknown by the vast majority of WNT users and administrators, it provides a potentially very powerful attack mechanism for malicious individuals intent on compromising and exploiting WNT and W2K systems.
What is an ADS? How can ADSs be created and how can executables be run in them? How can they be misused (e.g., by having malicious executables run in them)? How can they be found? This paper addresses these and other related issues concerning ADSs and security considerations.

James Bamford, *author, researcher*

RESEARCHING SECRETS

Bryan Glancey

WEAKEST LINK

Presentation and demonstration of attack attempts against common security software. Highlighting use of common hacking tools to attack Boot Protection, File Encryption, and other misplaced ideas. Seeking out the weakest section of security architecture and attacking based upon it
Demonstrations including:

- sector editors
- Windows based password attack programs (password grenadiers)
- Windows window password broadcasting (the **** thing)

Simple Nomad

WIDDERSHINS: DE-EVOLUTION AND THE POLITICS OF TECHNOLOGY

Enrique Sanchez

DISTRIBUTED INTRUSION DETECTION SYSTEM EVASION (DIDSE)

A fast connection is the new era, but your IDS system can handle it?, your Operating System can handle it?. Can you handle it?. A DDoS is not the worse thing that an attacker can do in a distributed way. A evasion attack can take place while your IDS is just dropping packets, while it is just there checking an innumerable amount of unused packets with unused connections.
There is no tool such as this, or is it? DIDSE distributes the attack ranging the amount of packets to be sent to the network to cause a flood to even modem connections in a timing and hidden way the is virtually impossible to hide it, combined with some accuracy in penetration an attacker could easily bypass the new era security systems. He can bypass your IDS.

Bruce Schneier

BRUCE SCHNEIER ANSWERS QUESTIONS

Meet The FED Panel

JIM CHRISTY WILL BE MODERATING

This years panel will build on last years format: A brief introduction and statement from each of the panel memebers, and then right into Audience Questions and Answers. So far the Panel includes: OSD - Paul Smulian (Information Assurance); GAO - Keith Rhodes (Chief Tech Officer); Arizona State Representative Wes Marsh; NSA - Ray Semko, Interagency OPSEC Support Staff

Newbie Sessions

Lile Elam

RENAGADE WIRELESS NETWORKS, CREATING CONNECTIVITY ON DEMAND

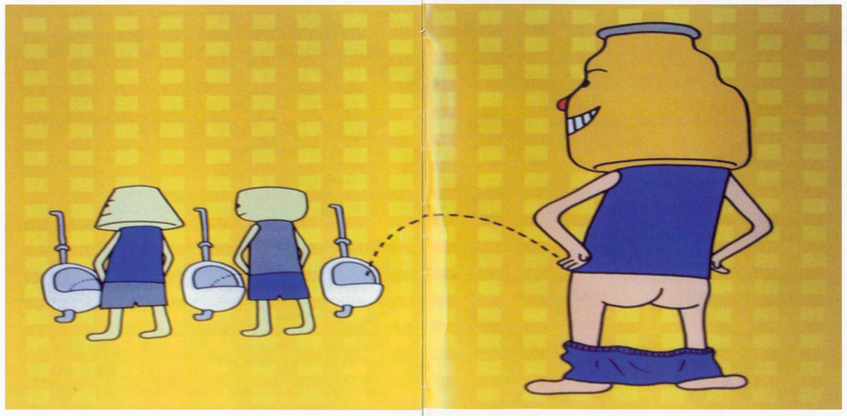
A panel of wireless hackers will describe how adhoc open wireless networks have been successfully set up for various events and places. From small/large happenings to local neighborhood access, learn how to create open wireless networks for all to use. After all, what is hacking without connectivity!

Dennis Salguero

THE BUSINESS SIDE OF STARTING YOUR OWN CONSULTING FIRM AND HOW THEY CAN SUCCEED

I currently run my own computer consulting firm and I think that I can help others. I don't specialize in security, but obviously, there are similar tasks that need to be done. I would cover things like:

- Incorporation
- Taxes
- Marketing
- Keeping the client happy
- Billing and getting paid



Robert Graham, CTO/Network ICE

PRINCIPLES OF CYBER ANARCHY THE DEFENDANT: SO YOU GOT YOUR LAME ASS SUED: A LEGAL NARRATIVE

"The Defendant" put up a website critical of his ex-employer, and within a week found himself in the center of a $120,000 lawsuit, facing some of the most powerful lawyers and largest firms in the country. With a week to fight the restraining order put against him, he had to learn everything he needed to know about legal procedures, presenting a defense, and speaking to the press. Through this, he kept the website up, answered many questions, and became the lightning rod for hundreds of angry, mistreated employees. Come listen to what he learned, and get some ideas in case it's ever you in the courtroom.

Barry J. Stiefel

NAT FOR NEWBIES AND NOT-SO-NEWBIES: A TUTORIAL

Network Address Translation (NAT) is a cheap and simple method for boosting the effectiveness of your firewall. Properly configured NAT can help hide your internal network structure from outsiders, enforce "outbound only" connections from internal hosts, and preserve scarce IPv4 addresses. This tutorial moves quickly through the basics, discusses a typical NAT configuration, describes NAT in action, enumerates the benefits of NAT, explains several potential pitfalls and shows how to configure DNS to accommodate the translated addresses.

Dario D. Diaz, Esq.

DIGITAL MILLENNIUM COPYRIGHT ACT

A presentation of the DMCA, a discussion of the terms and meanings with specific reference to the technical aspect of the Act, a case law study of specific cases around the country (not many as the law is very new and untested), and the repercussions of specific "hacking" acts that may result in a violation of the Act.

Dr. Cyrus Peikari

AN OPEN-SOURCE, INTERNATIONAL, ATTENUATED COMPUTER VIRUS

The unchecked proliferation of global information networks has left society vulnerable to a digital Armageddon. Computer viruses can counter this vulnerability by stabilizing and strengthening information systems. Using analogies from medicine, this paper demonstrates the pressing need for well-designed computer viruses. This paper also proposes the design, implementation, and distribution of an open-source, international, attenuated computer virus.

Shatter

FAQ THE NEWBIES: INFORMATION FOR PEOPLE NEW TO SECURITY,HACKING OR DEFCON.

ETTIQUITE: How to approch people, talk with people, introduce yourself and how not to be a lamer. Example will include real life anecdotes, stories from past cons, and even things that happened the night before.
PHILOSOPHY: Why are you here, and what are you doing? What is your motivation to be here? Why do you hack?

Also included in this section is the concept of ethics: How your actions effect yourself, others, and the net at large, responcibility for your actions, and the differences of white/grey/black hat hacking, and why real hackers don't wear hats.
LEARNING: Where to go to learn, proper steps to true knowledge, and how to avoid the trappings of being a script kiddie. Knowing the difference from downloading a useful tool for your set and grabbing a script and wrecking havok.
REAL WORLD: What the media dosn't tell you, why hacking is easier on tv and the movies, and the you don't get 6 figure jobs by getting busted for hacking a .gov installation. Debunking some of the myths that the gov't and private sector look for the best hackers to hire from the lists of convicted hackers.
WHERE TO GO FROM HERE: What you can get out of defcon, what you can learn, and where to go after you nurse a major hangover.
This is the general idea of the lecture, same overall concept from last year, but the content is dynamic and updated to always remain current.

Len Sassaman, *Security Architect & Technology Consultant*

WHAT IS SSL, A CA AND FREECERT?

The goal of FreeCert is to provide free or low-cost certificate authority services to individuals and organizations with limited budgets, as well as raise awareness of the services that CA's actually provide.

Many users of the Internet today are unaware of what role a CA plays in the process of secure website viewing. In my presentation, I intend to give a brief explanation of how SSL works and what it is that a CA does. I will explain what the browser warning messages mean to the user, and what to do when encountering them. I will discuss the dangers of trusting CAs, and methods of ensuring that certificates are valid when the CA cannot be ultimately trusted.

Following this, I will present details about FreeCert: what it does and does not intend to accomplish, who can benefit from it, and how it will execute these goals. Information on becoming involved in the development of FreeCert will be provided, and questions about FreeCert will be answered.

Jennifer Granick

EUROPEAN CYBERCRIME TREATY

Ryan Lackey

HAVENCO: ONE YEAR LATER

HavenCo provides secure colocation in the Principality of Sealand, in the North Sea, to a wide range of clients. We've gotten a lot of press in the past year, still, we get a lot of questions:

- Why do people go offshore in the first place?
- What can they gain?
- Aren't they all just software pirates and pornographers?
- Can existing companies restructure offshore after they get sued?
- What is life like on Sealand?
- Do you have photographs?
- Can I visit?
- Why don't you offer shell accounts?
- Is Sealand really a country? Is the UK going to invade?
- Are you going to set up other datahavens?

I will try to answer these questions, and will present a slideshow walkthrough of Sealand, information about our network and physical infrastructure, and information about current clients. In addition, I'll discuss some of our current development projects, and how our services can be useful to pro-liberty forces around the world.

David Gessel\Super Dave, of the DoC

INTRODUCTION TO QUANTUM CRYPTOGRAPHY

The subject is Quantum Cryptography, and the scope of the paper will be targeted toward a lay audience with a basic understanding of physics (what is an electron, a photon, etc.), computers (that they deal with binary information), and cryptography (that combining data with noise makes the data unreadable unless the noise is removed).

I will move quickly and at a basic level through the quantum physics involved and the cryptographic principles and leave the audience with an understanding of the state and potential of quantum computing and quantum cryptography.

John L. Dodge, Bernadette H. Schell

LAURENTIAN UNIVERSITY HACKER STUDY UPDATE

Laurentian University's Hacker Research Team from Sudbury Ontario Canada interviewed and surveyed self-professed hackers at Def Con 8 in Las Vegas and H2K in New York City in July 2000. The objective of the study was an attempt to give a balanced view on hackers - including the "white hats" and the "back hats". Its intent was to collect information that would give a realistic picture of the way hackers think, feel, and behave rather than some unbalanced and contrived picture based on the media or innuendo. The 22-page questionnaire had five parts:(I) hacker demographics, (II) health and mind-body symptoms, (III) routine behaviors, (IV) respondents' likes and dislikes and (V) decisions regarding work and/or school.

The media and academic writers have created many hacker myths based on their feelings or observations. Are they supported by fact or are they just fiction? Of the 20-hacker myths investigated we will present which are supported by the questionnaire data and which are not. We begin to crack the myths with a balance view.

Sharad

SECURITY & PRIVACY ARE CRITICALLY IMPORTANT ISSUES IN TODAYS DIGITALLY CONNECTED AGE

The typical netizen is blissfully unaware of the dangers that lurk each time he or she gets connected. Others consider security to be a "black art", too complex to understand - and therefore studiously avoid anything to do with it.

This session serves as an introduction to the dangers that abound in today's networked existence. Besides presenting an overview of various attacks, the talk tries to demystify them by explaining the "how it works" of the attacks.

We move from basic to more sophisticated attacks, cover a "proof of concept" case study and consider the counter measures possible. The session aims to serve as a starting point for all those interested in safe guarding their online existence, for those responsible for their organiztion's security issues and for just about anyone who is interested in security.

Dan Moniz

THE IMPACT OF P2P ON SECURITY IN THE ENTERPRISE

Increasing democratization of the network means more and more users are finding interesting things to do with the resources at their disposal. In the wake of watershed decentralized applications such as Napster, many commercial and open source efforts are producing so-called "peer-to-peer" (P2P) or decentralized applications and computing frameworks. The genesis of P2P, decentralization, and distributed computing as a fundamental architecture has serious implications for the way security is handled, not only in the wilds of public networks like the Internet, but also in closed enterprise environments. Like it or not, users will be using these apps and participating in these networks. It behooves every security administrator to become familiar with the nature of P2P systems and to understand both the potential threats and possible benefits of such systems, as well as to anticipate user adoption and related issues.

John Q. Newman

HOW BACKGROUND INVESTIGATIONS ARE CONDUCTED & HOW THEY CAN BE DEFEATED

Freaky

OS/X AND MACINTOSH SECURITY

Macintosh Security has gone unnoticed by the public for many years, only recently it has become a topic due to the release of Apple's Mac OS X. With BSD functionality there is a whole new realm of security issues to be discussed.
This years discussion will include the following:

- Secure Installation of Mac OS X
- Configuring the firewall functionality
- SSH on Mac OS X
- Mac OS X Virus/Protection
- Mac OS X Security Bugs/Fixes
- sudo security risk 101
- Obtaining Root
- Denial of Service attacks
- Mac OS X Hacks & Cracks

You will also learn about the latest Macintosh security / hacking tools and see demonstrations of new apps. Plus Q&A at the end, and a guest speaker from the Macintosh Underground group Team2600 have a special announcement!

Go to http://www.defcon.org/html/defcon-9-speakers.html for speaker biographies.

Defcon 2001 Schedule

FRIDAY • JULY 13

	Uber Haxor	General	Newbie
10:00 - 10:50	Biing Jong Lin, Chieh Chun Lin, Jan Che Su **A Survey of Country-Wide Web Server Security**	William L. Tafoya **General Session Opening Presentation**	Freaky **OS/X and Macintosh Security**
11:00 - 11:50	Jason Peel **Cypherpunk Grade Covert Network Channels**	Bruce Schneier **Bruce Schneier Answers Questions**	Sharad **Security & Privacy–An Introduction To Some Interesting Concepts**
12:00 - 12:50	FX **Attacking Control, Routing & Tunneling Protocols**	James Bamford **Researching Secrets** (Book signing immediately following)	Shatter **FAQ For The Newbies: Information For People New To Security, Hacking or Defcon**
13:00 - 13:50	Mark Grimes **TCP/IP Intelligent Agents: The Future of Electronic Warfare & Defense**	Simple Nomad **Widdershins De-evolution & the Politics of Technology**	Dennis Salguero **The Business Side of Starting Your Own Consulting Firm and How They Can Succeed**
14:00 - 14:50	photek **Writing Back Doors**	Kevin McPeake & Chris Goggans **Falling Dominos**	Robert Graham **Principles of Cyber Anarchy**
15:00 - 15:50	TechnoDragon **Hardware Mods, How To Look For Them**		Barry J. Stiefel **NAT For Newbies and Not-So-Newbies: A Tutorial**
16:00 - 16:50	Raven Alder **A Perl Script that Tracks Denial of Service Attacks Across Cisco Backbones**	Marcus Andersson **Firewalling Wireless Devices**	
17:00 - 17:50			**DJ Area Set-up**
18:00 - 18:50	Adam Bresson **Data Mining with PHP**	**CyberEthical Surfivor: The Game**	**DJ Area Opens 'till 6AM**
19:00 - 19:50	Nick Farr **Designing Secure Interfaces "for Dummies"**		
20:00 - 20:50		**Movie: TBA**	
23:00 - 23:50		**Haxor Jeopardy Round 1**	

SATURDAY • JULY 14

10:00 - 10:50	Optyx **KIS–Kernel Intrusion System**	Daniel J. Burroughs **Applying Information Warfare Theory to Generate a Higher Level of Knowledge From Current IDS**	Dr. Cyrus Peikari **An Open-source, International, Attenuated Computer Virus**
11:00 - 11:50	Bruce Potter & Adam **The Captive Portal**	Dr. Ian Goldberg **Arranging an Anonymous Rendezvous: Privacy Protection for Internet Servers**	Lile Elam **Renagade Wireless Networks**
12:00 - 12:50	Ofir Arkin **Introducing X - Playing Tricks with ICMP**	Jay Beale **Attacking & Securing Red Hat AKA How Effective Has Bastille Linux Been?**	Len Sassaman **What is SSL, a CA & FreeCert?**
13:00 - 13:50	Robert Grill, Michael Cohen **Windows NT and Novell Host Based Intrusion Detection Using Native Logging & 3rd Party Log Reporting Tools**	Thor **Grabbing User Credentials via W2k ODBC Libraries**	Dario D. Diaz **Digital Millennium Copyright Act**
14:00 - 14:50	D-Krypt **Web Aplication Security**	**cDc Hacktavism Panel**	John Q. Newman **How Background Investigations Are Conducted & How They Can Be Defeated**
15:00 - 15:50		Jim Christy **Meet the FED Panel**	Michael Wilson **Hacker Doctrine in Information Warfare**
16:00 - 16:50	Thomas J. Munn **Using Open BSD, Snort, Linux & a Few Other Tricks To Set-up a Transparent, ACTIVE Ids**	Bryan Glancey **Weakest Link**	The Defendant **So You Got Your Lame Ass sued: A Legal Narrative**
17:00 - 17:50			**DJ Area Set-up**
18:00 - 18:50	K2 **Polymorphic Shellcode API**	Peter Shipley **802.11b War Driving**	**DJ Area Open**
19:00 - 19:50	Rob Shein **Evaluating VPN Solutions**	Enrique Sanchez **Distributed Intrusion Detection System Evasion**	
20:00 - 22:50		**Social Engineering Contest**	**Black & White Ball**
22:00 - 22:50		**TCP/IP Drinking Game**	**DJ Area Opens 'till 6AM**
23:00 - 23:50		**Haxor Jeopardy Round 2**	

SUNDAY • JULY 15

10:00 - 10:50	Anders Ingeborn **Designing Small Payloads**	Richard Thieme **Hacking a Trans-Planetary Net: The Essence of Hacking in a Context of Pan-global Culture, the Wetware / dryware Interface, and Going to Europa**	David Gessel **Intro to Quantum Cryptography**
11:00 - 11:50	Robert Muncy **Securing Cisco Routers**	Brenno de Winter **IP V6 Security**	Jennifer Granick **European Cybercrime Treaty**
12:00 - 12:50	Phil King **8 Bits and 8 Pins: More Fun With Micro Controller Hacking**	Keith Nugent **Windows 2000 Security: How To Lock Down Your Win2k Boxes**	Ryan Lackey **HavenCo**
13:00 - 13:50	Dan Kaminsky & Andy Malyshev **Gateway Cryptography: Hacking Impossible Tunnels Through Improbable Networks with OpenSSH & the GNU Privacy Guard**		John L. Dodge & Bernadette H. Schell **Laurentian University Hacker Study Update**
14:00 - 14:50	Dmitry Sklyarov **eBooks Security–Theory and Practice**	HC **NTFS Alternate Data Streams**	Dan Moniz **The Impact of P2P on Security in the Enterprise**
15:00 - 15:50	**DEF CON Awards Ceremony: CTF, Scavenger Hunt, Coffee Wars & Social Engineering Contest Prizes Awarded**		
16:00 - 16:50	**Thanks for coming! DEF CON closes up, but feel free to hang out**		