From: Teresa Beamer <BEAMER@DENISON.EDU>
Subject: Minutes from August 8, 2001
To: OARTECH@LISTS.OAR.NET

OARtech Minutes, August 8, 2001

Introductions -
Question to answer what was the effect of Code Red on your campus?

Antioch University, Bruce Friend: patches in place - no impact
Clark State Community College, Hugh Evans, Jim Gossett: no effect
Columbus State, Jim Beidler: no impact
Columbus State Community College, Bart Prickurt
DAS, Department of Admin. Svcs., Mickael Yerian
Denison University, Teresa Beamer: found 2 users running IIS otherwise no impact
Heidelberg College, Kurt Huenemann, Sean Joyce: no impact
Kent State University, Kurt Eckert, Ransel Yoho: took out their router with over 200 IIS machines, caused the router to run out of memory,
Lakeland Community College, David Levine: patched no effect
Loraine County Community College, Norm Lease: patches in place no effect
Miami University, Tim Gruenhagen: Users that were running IIS were found - half a dozen effected
Mission Networks, Bob Evenson, Jon Woodland: no impact, patches in place before it happened.
NASA Glenn Research Center, Dave Pleva
NEOUCOM, Bill Mayhew: 1 users was effected - no central systems effected
OARnet, Gene Bassin, Clifford Collins, Christopher Cook, Ruth Crites, Fred Crowner, Bill Miller, Dana Rogers, Albert School, Paul Schopis, Pankaj Shah, Gene Wallis: Had patches in place before it happened. Couple servers where problem was resolved, saw a significant increase in traffic depended on the sites.
Ohio Board of Regents, David Barber: videoconference interrupted
Ohio Northern University, Bob Beer: 4 hosts affected
OhioLink, Anita Cook, Greg German: Internet slow, but otherwise no impact
Otterbein College, John Lateulere, Tim Pindell: No effect - also blocked http except to web server
Sinclair Community College, Roslyn Taylor: no impact
University of Dayton, Tim Harrington, Don Hunter: less than half a dozen effected
University of Rio Grande, Kingsley Meyer, Mike Snider: 1 IIS server effected, patched and is okay now

Urbana University, David Sullenberger: not much impact
Washingon State Comm. College, Joe Testerman: no effect
Wright State University, Shane Dawalt, Patricia Vendt: 15 machines affected
not central servers - closed off http to campus except for registered servers
Xavier University, Carl Dickhaus: 2 servers affected

Whitepaper will be sent out within 2 weeks with added sections. Vote will be taken on line.

Pankaj Shaw, OARnet
The dates have been set for the next Windows to the Future conference:
Windham Hotel in Dublin
November 27, 28, 2001
Satellite and wireless networks will be the main topic. He is talking to NASA Glen to provide a keynote speaker.

Were there some ITEC grants given out? Approved 4 grants. Topics are QoS, Measurement and Monitoring, Impact on Networks using " " stacks, also one from Wright state. There will be a second round announced shortly. They are currently in the process of hiring another engineer. Who decides the projects? I2 has a lot of input, working groups ask who can take the projects, researchers from the Universities select it, and input can also come from outside researchers, and vender partner projects.

OhioLink, Anita Cook
OhioLink's newest release came out August 1st. It is very customizable at the customer site. It uses the DOM technology to automatically bring up links when the cursor is on the item. This feature is not available in the older versions of Netscape. Older versions of Netscape show a more static screen. Database listings can include a customized list for the campuses.

New databases: Mayan Images from Oberlin. If the databases are not licensed, they can be accessed from all over the world. Digital Media Center is working with the Ohio Historical society to bring up an historical site for the bicentennial. Still working on videos. You will probably see video streaming coming in September.

Patty Vendt - France World Internet Security Conference
People attended this international conference from all types of businesses. The biggest difference Patty noticed was all the people there used Pine to read their email. The information on the incidence response process was very good. Previously we had had discussions for starting a security group to begin providing information on security incidences with the idea of creating a "first team". OSU does have a first team. What is the interest? Do we want

to determine best practices? There seemed to be about 10 hands raised. Please send an email to Patty if you are interested. The Dayton IT alliance is trying to get a security special interest group going as well. (First Team - Incidence response team)

Bob Evenson and John Woodland, Mission Networks
They are a Greenfield company. The goal in creation of Mission was to provide networks going to tier 2 locations instead of tier 1 locations. They can create the economies of scale to make the project possible in the tier 2 areas. They are the regional operation company that provides a broad range of services. This is a planned network that is not in the ground yet. They are trying to find those early adopters to find out what the customers want. They are a fiber optic company and building an exclusively packet based network that is standardize on IP. The network will be going into about 83 cities with 120 central offices with access to over 70% of the population and 80% of the university and major colleges in Michigan and Ohio. They started in Michigan about 9 months ago.

They "Bridge the digital divide by" expanding existing services and enabling new services for sites that are off the beaten path. Their list shows 35 cities in Ohio that are in the first stage. They are still developing the list. Once they start installing the list represents an 18-month build. Once done in Ohio they will then move into neighboring states staying in the areas with the tier 2 cities.

They have defined several suites of services that they will provide. The Commercial Suite will have class 4/5 dial tone services, PRI, integrated T1, and VPN. These lists are still being developed. Some will go in some areas, and not in others, depending on customer needs. The Data Center Suite will include email, radius/authentication, web casting/streaming, news feeds, firewall, managed DNS, data storage, and disaster recovery. Not as competitor to OARnet but to provide commercial services. ISP Suite will include managed modem services, NAP connectivity, and prioritization of service, DSL, and managed route services. The Network Suite includes dedicated private networks, shared private networks, lambda leasing (DWDM), carrier traffic, collocation, NNI capability for frame relay and ATM. The lambda leasing will eventually allow very quick turn up and turn down of bandwidth.

The 3 Layers of the technology
Optical Layer
Their model has 3 layers to make the provisioning, etc much faster. At the lowest level, the Optical layer is all Cisco based using Dense Wave Division Multiplexing (DWDM). The way they are setting out the network they will not

need to have many regeneration modules. They will be using optical routing. They are bringing out a long haul net and adding the short haul pieces, as opposed to the pinning a lot of short haul pieces together.

Packet Layer
Allows easier management because it doesn't require manual crawling out to see the cross connects. It will be an all IP packet based network with an ATM Edge. The ATM is only for compatibility use with legacy connectivity. They will be using IP QoS, and looking at congestion avoidance, QOS Queues and Diffserv/RSVP, and provide voice quality connections. They will be using MPLS and will be using Cisco products to allow soft switching that can done centrally, and then send the traffic path directly through the network. Mission will be using SS7 to look at the type of call coming in and set the line appropriately.

Management Layer
Using software that will allow immediate setup/teardown of connections. Billing can be taken down to a small time period, or by number of packets. It can be very flexible.

They are developing a scalable and customizable data center. They found that many of the ISPs did not have hardened sites, and found the Tier 1 sites would not allow access to data centers unless you were using their products. Mission is trying to provide a secure hardened data center. First data center is in Michigan and they would like to add a second one in Ohio.

Why would you be using PKI for security over biometric for entrance security? He feels it more secure as it require physical and something you know to enter. In some cases the security person will have to put their card in as well. The data center concept came up in March. They are currently in development of this concept.

Hardened/Carrier class data center needs a hardened bunker with the power, and environmental controls that supports 99.999 % availability, and backup.

Their products will include Bandwidth, Storage, Hosting - collocation, Managed OS, Managed web services, managed applications. They are focusing on collocation and managed OS at this time.

They don't have legacy gear to worry about, can provide abundance of bandwidth, and provide an all IP network that is built with today's technology and designed for tomorrow's. They have joint ventures and partnerships with Cisco Systems, and EMC. They expect 20% of first lit capacity will be filled

on day 1. They are currently working to get funding from the market. Because of the market slow down, it looks like they will start with the fiber build after the beginning of the year after the market picks up. They are going ahead with the data center in Michigan and will become income producing this fall. The last mile partnerships will be very important. Part of the contract will be to bring the fiber directly to the campus at good price bypassing the current Telco last mile issues.

How soon will you be able to determine the last mile cost for each campus so we can begin letting our campus know the costs? The information is available from them via the web site to find how the fiber needs to get to the campus. Sometimes the fiber is there and they just need to find the owners and request dark fiber that they can light.

Christopher Cook, OARnet
Coming H.323 video conferencing seminars:
August 21 for SEGPs
August 23 for others
The directory services workshop is full. They have a waiting list. Call and get your name on the waiting list if you are still interested.

Lunch

Gene Wallis, OARnet
Logical maps of the I2 Gigapop were available as a handout. The pop has a Gig Ethernet line to the OARnet AS600 to connect OARnet to tie in the SEGPs that have less than a DS3 bandwidth. They have added the I2 Commons video service for I2 H.323 video MCU's. Also, They have added an IPV6 router to allow researchers to begin testing with Ipv6. So far there are no restrictions on the Ipv6, you request a tunnel and they'll set one up for your users to test.

Gene showed a map of the Internet 1 network. They are beginning to put OC-12 to the major access points (Cleveland, Qwest, Cable and Wireless, etc...). They have added redundancy and added bandwidth to the Chicago NAP. The connection to Washington DC goes through Pittsburgh PA. They have contracted with NAP PAX (vender independent NAP) in between the MayEast and other vender specific NAPs (Network Access Point). The Chicago NAP is the one of 3 major peering points in the country. MayEast is the 2nd major NAP. The 3rd major NAP is on the west coast.

What scares you about the beginning of the school year? The traffic is running high and it's the summer. Chicago NAP is running a lot of traffic

right now and when schools start up they may have to adjust the routes the traffic may run. Looking to bring up added OC3 in September. They will continue to add bandwidth to try and stay ahead of the site needs.

Ameritech has come out with a product called GigaMan. They run fiber to the site and use the device to connect fiber to the pop. It is being offered in most of Ameritech's major population areas. Point to point gigabit Ethernet (sort of) across Ameritech lines. Pricing is very attractive (1800-1900/month). Distance it runs is about 40 miles. Rumor has it that it is cheap now and Ameritech will raising the cost.

What about the GigaMan connectivity? Designed for campus connections, does not allow DC power, client side is multimode fiber, and on the pop side uses single mode fiber. OARnet worked with Qwest, Ameritech, etc... to get it in. The gotchas: not Telco equipment, no redundancy. How well it will work is dependent on how well Ameritech supports it.

Is the competitive pricing available for the last mile issues? Call Ruth.

Bill Wilson, OARnet
They are looking at adding a remedy product that will allow you to see your site ticket information. It will probably use the same username/password sites use for accessing site ticket information. Should see something by the next OARtech meeting.

Paul Schopis, OARnet
He is building a weather map for sites to see the status of links within the network. Should see something by the next OARtech meeting.

Clifford Collins, The Humble University Network
Slides are available on the their web site (http://www.enss.net/education/presentations/) How do you investigate how to deploy a new security feature? Read vendor literature and trade rags, or you can look it up on HumbleNet. HumbleNet is a test bed for network equipment. "A Fictitious institution with a real network" that is designed like a campus network and not like a corporate network and is limited by real-life constraints. Will be documented with population, policy, architecture and configurations (parts, priced and sourced).

The equipment on it on this net: Cisco 3640 router with IOS firewall feature set and Netflow, PIX 515 firewall, BSD firewall, etc.... It will have several of the most common servers (e.g. WWW, SSL, Webmail, LDAP, Oracle, CVS, SecureID, etc...). They will several access equipment - wireless, dialup,

vlan, as well some traffic generators that will generate typical campus traffic. The network is separated into AdAcNet, Internet, DMZnet, MZNet, ITNet, and Resnet. They have been coming in via remote office or home and access the resources they need just like they are right on campus.

The HumbleNet web site: Send e-mail to Ccollins@enss.net and provide your daytime phone number and unique code word to verify you on the phone. Your username will be your e-mail name.

They are using this network to test the PKI and Certificates as well as other equipment. Security services from ENSS includes Audits, Security , etc..

Albert School, DEFCON trip report, PKI Update
Wright State is working on a single password sign on for their campus. Albert came down and gave a 3rd party type of presentation on the authentication methods out there. They were able bring different ideas and discuss them to come up a real solutions. They are looking at Iplanet directories server working with Novell's LDAP to provide single sign on.

PKI Update
General Government
PKI Portal http://src.nist.gov/pki/
Bridge CA, http://csrc.nist.gov/pki/fbca/welcome.html
Recent SANS Article, http://www.sans.org/infosecFAQ/country/fed_infotech.htm

State Government is currently working on policy issues as well as the digital signatures, etc… Has begun using the bridge model for checking digital credentials.

Internet 2, http://middleware.internet2.edu , the group doing work with this is HEPKI-TAG Group and have labs at Dartmouth and Wisconsin Labs where they are looking at what would be used 5 years out. OARnet would like to collaborate with involved member institutions and can help in providing consulting to help with the emerging technologies.

Do you have a reference for how PKI and directory services fit together?
There is a book call PKI that would be good. See the ENSS web site for recommended readings. You don't have to have an LDAP server to do PKI. LDAP is only one method.

Defcon9 (defcon.org) Notes are in http://www.enss.net/education/presentations
Defcon9 is a conference to allow users to get together and discuss security issues. What he brought back is that there are a lot of smart talented

people out there that can crack your systems and you won't know it. Some URLS that are off the beaten path of security URLS:

HTTP BruteForcer - trys to log in to hotmail or web based authentications, http://www.hackology.com
NT Rootkits - can install to allow a backdoor - http://www.rootkit.com/
Security Library, http://www.vitalsecurity.net/library.html
Packetstorm security tools, http://www.packetstormsecurity.org/pssabout.html
General (in) Security, http://www.astalavista.com

Whisker - scans for CGI vulnerabilities
rain.forest.puppy - wrote an article for Phrack Magazine on how to make more security CGI scripts. A lot of hacker tools could have other things imbedded in them so you can put them on a test network like HumbleNet to see what would happen.
Some of the things in a root kit change many of the main files so that they don't work the way they did. Sends information off, turns off logging on things that you normally would see so that they hide their processes.

Summary - security is an ongoing process not a project and stop. Do Nmap scans, Ndiff scans to check for new files where you don't expect it. Watch for anomalies. Intercept is the product for NT that looks for abnormal behavior on a server and only allows predefined activities. It is primarily used for commercial sites.

What's the typical way that hackers get into your Linux to install the rootkit? Albert couldn't answer directly, as he is not up on that type of things. Comment from the listeners - not keeping up with patches. You can use checksums, but the database needs to be in a read only database, the checksum program as well. The Unix operating system may have a way to set an "immutable" bit that won't allow you to make a change to the file even with root unless the system is in single user mode. This could be used on things like the Kernel to prevent unauthorized changes.

Minutes were approved.

A reminder that in the next 2 weeks we will have the vote on the whitepaper. The majority of those sending in a vote (email) will carry.

Next meeting we will be looking at various tools that may be available to help look at your network. We would like to see the network weather map and the remedy logins. If anyone has packages that you would like to see discussed, send the information to Patty (vendt@wright.edu) A Code Red scanner is available on Norton's site. Patty saw lots of false positives from the script

provided by Sans.

Patty talked about her experience this last month that taught if you don't set up your security policies before hand and coordinate them with your security and legal staff you could find yourself being read your Miranda rights.

Meeting was adjourned.