Oartech minutes
12/8/2010

Introductions

Oarnet member meeting had presentations from grant awards (BTOP).

There was a request that we get the agenda out to the entire list, not just to those that registered to attend.

Oarnet Updates
TJ Sandor

OMMC (Ohio Middle Mile Consortium) includes COMnet, OneCommunity, and Horizon

The OMMC was put together to help fund BTOP grants. It increases competition in underserved areas of the state and possibly to provide redundant connections. Its focus is not just for higher education but for the entire Oarnet backbone. It will help to bring more K12 and other connections up.

COMnet is planning to build directly through ADA. Is there any projection for the availability? They are currently in environmental assessments. Possible offerings may become available in middle of next year in their primary areas. More information will be available as the work moves along. All the members are starting up and are generally in the environmental assessments.

What is the best way to for a community, business, or tech park to get connected? Connect Ohio is their best bet. As a fall back, have them contact your Oarnet representative.

Oarnet is currently rolling out public broadcasting to Oarnet's IP service. They are also undertaking work with their sister organizations to improve connectivity.

Optical mesh architecture is being implemented. This is a full mesh lambda with 10Gb capacity. Ring 0 is complete and Ring 4 is underway with the east side of the ring complete.

Oarnet is also working on a community cloud service. This would be a virtualization service and is in the development phase with the 1st step a pilot. There are several models being piloted: Gold (fully managed), Silver (VM+OS, menu of services such as security and backup), Bronze (More Amazon like, could be bare VM or hardware resource pools which allow users to provision from the VM. Is anyone here interested in these pilot programs? A couple indicated interest. Some campuses are doing this instead of the co-location service. A cost schedule is currently being developed. The expected timeframe for the cost structure is by the next member meeting (March). An Exchange infrastructure

is being developed for the entire state of Ohio but is not on the roadmap as a cloud service. Contact your Oarnet representative if you are interested in participating in the pilots. The SLA for the various levels of VM service are being defined. Under the bronze model you are completely responsible. But the responsibilities for the other levels are still being determined.

Client Services
Mary Ann Zbydnowski

Currently there are 88 higher education members. Eastern Gateway CC is bringing up new locations; Kent State and OU are working on regional campuses; Heidelberg and Mt Vernon Nazarene are using Timewarner's ELAN.

Co-location service: OSU site is full, so they are bringing up a co-location site at Wright State and are looking for other possible locations. There are new products in VMware - Zimbra. They have sold $10.9m to date. Fusion is still $15 until the end of the year. There will be a new VMware View Demo Portal coming soon. This would give some examples, performance, etc… if you are thinking of deploying a view, desktop, infrastructure.

OMMC BTOP
ComNet is currently working on: U of Findlay, Tiffin, Heidelberg, Bluffton U, ONU, Rhodes, Northwest State, U of Northwestern Ohio. They are also working on secondary connections, remote campuses, and reconnecting where contracts are expiring.
Horizon: Rio Grande
One Community: still coming up

I2 Magpi event to be held on Dec 10th

The Oarnet website will be coming up. Please participate in the Oarnet survey: www.surveymonkey.com/s/DYULGLLW. Oarnet is moving away from Remedy to using Service Now for their ticketing system. Remedy seems to be becoming too complicated. Service Now is integrated into email, and in fact is email based. What to other sites use? One site has Service Now and has found that their first level techs are very script oriented. You have to provide scripts to reduce the number of calls that have to get escalated. Once the site got through this learning curve, they were happy with Service Now. Another site is using Footprints. It has an inventory component, but they did not get it to work. Oarnet is in the foundation data phase of implementation of the Service Now hosted solution. The BOR-CIO advisory groups are looking to see if we can get an Oarnet wide discount. Another school has implemented some phone integration into their helpdesk product using Support Desk Express.

Cyber Exercise Developer and Trainer
Overview and Cyber Security Research
Brian Wisniewski

SEI (Software Engineering Institute)
Created in 1984 and is federally funded and sponsored by the US Department of defense operated at Carnegie Mellon. The employees are actually employed by Carnegie Mellon.

There are four main areas: Acquisition Support, Networked Systems survivability, research technical and system solutions, and software engineering process. Our speaker is in the Network Systems survivability area whose areas of focus are Cyber Threat and Vulnerability analysis, Enterprise and workforce development, etc…. His specific area is the workforce development. See http://www.cert.org for publications, podcasts, and training courses for keeping up to date.

The cyber security workforce development model creates a framework that will validate security skills. Their focus is to build knowledge and skills to provide a trained security workforce. They use an optimized model which uses lecture and virtual training environment that is scripted to keep it controlled to the subject of the class. This has evolved into XNET which is an internet based synchronous web based delivery of cyber security classes.

http://vte.cert.org is the asynchronous knowledge and skill building site. This is where they start the training when they are working with an agency. They capture a class (e.g Security+) then provide it in a virtual environment to be accessed from anywhere in the world. This allows the military to use it from the field.

http://xnet.cert.org is browser based access to specific cyber training environment. It uses geographically dispersed teams together in a virtual classroom.

They use customizable scenarios based on the agency's requirements (e.g. insider threat). Using the same types of data that you would see in a production environment, they put together a timeline that is built much like a play. Is easily customized and uses real world scenarios to train analysts how to react in the event of a threat. They are currently using open source applications to provide the environment and then the analysts would interpolate from there to what they would see in the commercial tools. They use team collaboration tools like WIKI, chat, and clickable Scenario Maps and work on team projects, including tests. The users are allowed to provide feedback, take quizzes, and answer questions. The evaluator can glean information that would allow them to see the holes in knowledge that might need to be addressed in future classes.

The example he showed is the International Cyber Defense Workshop, which is an international competition with teams of 5 that work together to see who will solve the problem the fastest. They are able to manipulate the machines as part of the exercises (installing tools, etc). They can focus the scenario at whatever difficulty level they need for the team that is taking the scenario. They use widely available tools: Snort, Base, Splunk, Wireshark, etc… on 25 virtual machines, 2-site "corporate" network. They use both fixed and mobile environments using ESXi and NFS.

On a high level, the attacks are getting more malicious, is there any hope that things would become more stable? It is getting harder to introduce holes, but the fingerprinting is getting harder. The forensics is still very busy, so probably not.

We wear multiple hats, what do you recommend that we can do? One element they have found is the user security training can reduce the social engineering problems. Do user training, keep patches up to date and keep antivirus up to date. User education is very important. Best program he has seen is MOTE at Virginia Community College system.

Contact info:
Brian Wisniewski
bdwisneiwski@cert.org

Check out the cert site for more information: www.cert.org

Discussion:
Where do people buy their Cisco equipment, Smartnet? Some discussion as to whether we can talk about this in the meeting. Getting a Smartnet listing on page is almost impossible. Several VARS were mentioned. One site has bid their Smartnet contract. What other equipment are other sites using besides Cisco? Juniper, Enterasys, Impulse (clean access replacement).

Are any sites looking at reducing their wired investment and focusing their investments on wireless? Several are focusing on wireless in the dorms. Some are focusing on doing 100Mb and providing gigabit wired only when requested.

How is Packet Logic working at schools using it? Good. One school is getting close to end of the life of their current device and will be looking at another solution. Another is using Palo Alto and their Packetshaper is at end of life. Some are looking at Net Equalizer. One site has blocked peer to peer for all segments of the network and anyone that needs it must ask for it. This made to copyright notices go away.

Lunch and Tour afterword.

Meeting adjourned 12:05pm.