Agenda

WNAG

October 18, 2017 9:30 – 11:00 EC2-111

Previous Business

Nexus users not in WatIAm	Mike (notes at bottom)

New Business

New secretary	Jim
GlobalSign certs	Anton
New LDAP farm	Anton
Trickbot malware	Mike

Stalled Items

None

Standing Items

None .

Faculty Updates

<u>AHS – Lowell</u>

- No report submitted

<u>Arts – Nevil</u>

- Mobile lab on Nexus
- Faculty laptops on Nexus
- SCCM client issues – stuck downloading ##%.
- Are people monitoring security groups of interest? If so, how?

Agenda

Computer Science - Clayton

- Retail services will be replacing Xerox printer on MC 2nd and 3rd floors this week.

Engineering – Ray (Erick)

- Reduced more than 100 groups under people/academic/engineering down to 12, with work still in progress. 47 groups in other Faculties and non-academic areas need attention.

Environment – Bernie

- Resolved growing pains with Xerox printers in labs working with both Windows and Macs.
- Missing NetApp folders on N: for all incoming grads and undergrads (\\files\students$) has been resolved. Comments from IST?

IST – Dave/Anton

- Two new agenda items:
  1. Switch to a new ldap farm config, planning to go live on Oct 24th
  2. Switch to IntranetSSL certificates on Nexus DCs. No firm date yet but no later than Nov 13th

IST – Manfred

- Refer to "Additional Notes" section.

IST - Ravindri

- Nothing to report.

IST – Security – Mike

- Over 500 compromised undergraduate email accounts in September.
- We had a malware infection break out on campus last week. We determined it was Trickbot, worming about, and it seemed to have an affinity for machines with the following properties:
  1) Win7
  2) Older installations (but I sort of repeat myself)
  3) Fully patched
  4) Show vulnerable to nmap scans for MS17-010

  The combination of #3/4 is most interesting/annoying. I believe #1/2 is because the exploit used, ETERNALBLUE from the Shadowbrokers dump, works best against Windows 7.

Math – Jim

- Working through Pending Moves list and fixing user profiles. We seem to have had quite a few users' settings changed when IST fixed the "missing" profiles and home drives (or that's just when we noticed it).

Science - Allan

- Nothing to report.

Other Business

Agenda

?

- ?

Additional Notes

Regrets: Bernie

Agenda Details:

Manfred: Report from Workstation Services

- SCCM-PMM has now been upgraded to version 6.1
- MBAM client is being tested in IST. Results are interesting, showing it may be more work than originally anticipated to reach compliance. This is mainly due to incorrect BIOS versions, older non-UEFI-capable systems, and a few with incompatible TPM. At least we have a compliance report. Problems like missing system partitions, or partitions that are too small will require manual intervention.
- Acrobat Pro 11 officially reached end of life last weekend. The 2017 version has been tested and is now available via the WebStore. ($110)
- A few clients are still attempting to connect to our Netapp via NTLMv1. The number is under 20. Yesterday's list included computers in Engineering, Science and AS:

```
        10.20.117.150: v1020-wn-117-150.campus-dynamic.uwaterloo.ca.
        10.20.167.42: v1020-wn-167-42.campus-dynamic.uwaterloo.ca.
        129.97.126.79: mmejr.uwaterloo.ca.
        129.97.126.92: mmeclinic11.uwaterloo.ca.
        129.97.128.28: tlabdc1.tlab.uwaterloo.ca.
        129.97.128.89: tlabdc2.tlab.uwaterloo.ca.
        129.97.133.57: mmetech12.uwaterloo.ca.
        129.97.142.26: cclrjoneslap2.uwaterloo.ca.
        129.97.185.14: meadmin07.uwaterloo.ca.
        129.97.27.29: meprof03.uwaterloo.ca.
        129.97.36.148: solids80.uwaterloo.ca.
        129.97.36.186: mmefc45.uwaterloo.ca.
        129.97.46.29: mechpc97.uwaterloo.ca.
        129.97.46.40: meprof1.uwaterloo.ca.
        129.97.47.12: oakley.uwaterloo.ca.
        129.97.8.242: ece-public06.uwaterloo.ca.
        129.97.8.247: ece-public11.uwaterloo.ca.
        172.16.39.61: cn-vpn-172-16-39-61.campus-dynamic.uwaterloo.ca.
        172.16.43.184: 3(NXDOMAIN)
```

- We've been asked to look into the Microsoft and Office Stores for W10 (modern apps). Are investigating feasibility of hosting on campus. Already know we can deploy "Store" apps via SCCM
- Working on a better vanguard process to properly test new W10 releases, as they will be coming out twice a year
- We have created a virtual Excel app for ENV, since Mac users there found the Mac version was not as feature rich as the PC version

Agenda

NOTES ON non-WatIAm accounts in Nexus

I had an item from last meeting - provide some stats on unsponsored (by WatIAm) accounts in NEXUS. JasonT provided me with some data and I did some db things. Hopefully the numbers are interesting and their meaning is obvious. I can expand/explain a bit in a few hours.

```
mpnexus=> select count(*) from unsponsored_account;
 count
-------
  6624
(1 row)

mpnexus=> select ou, count(*) as count from unsponsored_account group by ou order by count desc limit 15;
                          ou                          | count
------------------------------------------------------+-------
 OU=Users,OU=Math,OU=Academic                         |  1032
 OU=Users,OU=Orphaned,OU=Administration               |   809
 OU=Users,OU=Expired,OU=Administration                |   678
 OU=Legacy,OU=Mechanical,OU=Engineering,OU=Academic   |   420
 OU=Users,OU=Guests,OU=Administration                 |   305
 OU=Support,OU=Info Systems & Technology,OU=Academic Support |   298
 OU=Legacy,OU=Engineering,OU=Academic                 |   286
 OU=Guests,OU=Administration                          |   267
 OU=Support,OU=Academic Support                       |   229
 OU=Legacy,OU=Chemical,OU=Engineering,OU=Academic     |   166
 OU=Generic,OU=Science,OU=Academic                    |   137
 OU=Legacy,OU=Electrical and Computer,OU=Engineering,OU=Academic |   123
 OU=Legacy,OU=Civil and Environmental,OU=Engineering,OU=Academic |   112
 OU=Users,OU=AHS,OU=Academic                          |    91
 OU=Legacy,OU=Engineering Computing,OU=Engineering,OU=Academic   |    88
(15 rows)

mpnexus=> select count(*) from unsponsored_account where samaccountname like '!%';
 count
-------
   614
(1 row)

mpnexus=> select count(*) from unsponsored_account where pwdlastset < '2010-01-01';
 count
-------
  1990
(1 row)

mpnexus=> select samaccountname,ou from unsponsored_account where whencreated is null;
 samaccountname |                          ou
```

Agenda

```
----------------+---------------------------------------------------------------------------------------------------------
 !d24lau        | OU=Local Admin Super User Group,OU=SuperUsers,OU=Accounts,OU=Engineering
Computing,OU=Engineering,OU=Academic
 engmachdb      | OU=EngComp-Service.Accounts,OU=SuperUsers,OU=Accounts,OU=Engineering
Computing,OU=Engineering,OU=Academic
 eng_graddb     | OU=EngComp-Service.Accounts,OU=SuperUsers,OU=Accounts,OU=Engineering
Computing,OU=Engineering,OU=Academic
 !!steph        | OU=DomainAccounts,OU=SuperUsers,OU=Accounts,OU=Engineering
Computing,OU=Engineering,OU=Academic
 !administrator | OU=DomainAccounts,OU=SuperUsers,OU=Accounts,OU=Engineering
Computing,OU=Engineering,OU=Academic
 !!smcarr       | OU=DomainAccounts,OU=SuperUsers,OU=Accounts,OU=Engineering
Computing,OU=Engineering,OU=Academic
 !m3griffi      | OU=OUAccounts,OU=SuperUsers,OU=Accounts,OU=Engineering
Computing,OU=Engineering,OU=Academic
 !delattre      | OU=OUAccounts,OU=SuperUsers,OU=Accounts,OU=Engineering
Computing,OU=Engineering,OU=Academic
 !dwalsh        | OU=OUAccounts,OU=SuperUsers,OU=Accounts,OU=Engineering
Computing,OU=Engineering,OU=Academic
 !tmo           | OU=OUAccounts,OU=SuperUsers,OU=Accounts,OU=Engineering
Computing,OU=Engineering,OU=Academic
 !erick         | OU=OUAccounts,OU=SuperUsers,OU=Accounts,OU=Engineering Computing,OU=Engineering,OU=Academic
 archinstall    | OU=Architecture Install Account,OU=SuperUsers,OU=Accounts,OU=Engineering
Computing,OU=Engineering,OU=Academic
(12 rows)

mpnexus=> select count(*) from unsponsored_account where ou like '%Legacy%';
 count
-------
  1468
(1 row)
```