AD Tech Service Team Minutes 02/17/2017, Scott Hall, Room 216

Members: ~~Alan Surrette~~, Billy Beaudoin, Joshua Gira, Derek Ballard, Dustin Duckwall, Douglas Flowers, Jeremy Brown (Chair)

Guests: John Klein, Dave Conn, Abraham Jacob, Joe Wells, Daniel Sink, Michael Underwood, Matt Pollard, Dan Green (remote)

Voting Items

- Remove the insecure cipher suites from AD domain controllers
  - Must provide ample notification (Sysnews post/multiple emails)
  - Will test in WOLFCHOW/WOLFTEST first, then move to a single DC, then expand to all DC's
  - **Vote Passes**
- Create a NCSU-Linux Computers group to mimic the NCSU-Mac Computers group and nest it in the NCSU-Read Group Membership group
  - **Vote Passes**

New items

- SCEP is becoming opt-out starting 17 Feb 2017.
  - Reminder that Kasperksy uninstalls require a reboot. The SCEP install won't execute until Kaspersky has been removed.
  - OITWMS can provide a report to determine machines that continue to talk to the Kaspersky server.
  - Expected ~11K machines will migrate over the next week
  - You can still request custom OU policies for SCEP
    - Use for reporting and whitelisting/blacklisting
  - Current settings DO NOT allow pausing the AV. If you need to disable the AV you need to stop the Windows Defender service or add an exception to a custom SCEP policy.
  - SCEP will run a full scan once a week - Saturdays at 2AM
- Announce and disable/remove some insecure ciphers from AD domain controllers (Derek)
  - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
  - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
  - TLS_RSA_WITH_AES_128_CBC_SHA
  - TLS_RSA_WITH_AES_256_CBC_SHA
  - TLS_RSA_WITH_3DES_EDE_CBC_SHA, and all other 3DES ciphers
  - Suggestion to push domain wide if it works on the DC's
  - This would be done after scheduling testing. We do one DC, have testing done against that one for awhile. Then configure the others.
- Deployment of the new SHA256 AD PKI. We are going to begin issuing computer certs, code signing certs from the new cert server, and stop issuing these certs from the old SHA1 server.

The old server will be kept around for approximately a year, till everything has transitioned over to the SHA256 certs.
    - We need to provide new PKI certs to provide a cert bundle for non-Windows machines: Derek will publish this to https://www.ncsu.edu/crl
- We would like to start requiring LDAP signing instead of prefer LDAP signing.
    - This would be done after announcing and scheduling testing. We do one DC, have testing done against that one for awhile. Then configure the others.
    - Suggestion to not require signing but rather disable ldap and force everyone to use ldaps
    - This would allow clients that can't do signing still have connectivity since it is encrypted
    - Ldaps is only supported on the VIP. Not all machines can use the VIP. Some apps require an FQDN to a DC.
    - We are logging clients talking via unsigned. Need to make a report in Splunk to determine what machines those are
- Turn off NTLMv1 on the WolfTech domain.
    - http://www.windows-hied.org/Pages/Conference2014/Slides/turningOffNtlmV1.pptx
- Windows patches have been canceled from this past patch Tuesday
    - https://blogs.technet.microsoft.com/msrc/2017/02/14/february-2017-security-update-release/
- New Terminal Services license server has been deployed. If you are interested in using Server 2016 Terminal Services, please put in a SNow ticket to OIT_WINDOWS for support.
- Citrix support is going away 31 May. In response an RDS install is being deployed.
    - The current configuration is planned to support
        - RSAT Tools
        - SCCM Console
        - Putty, RDP, SQL Server Management Studio
    - It is expected that RDS will provide the same functionality as Citrix to begin with. Following we are looking to expand functionality as deemed needed by others on campus.
    - We are interested in others opinions on software that could/should be deployed from terminal services
    - Are they any volunteers for some early access, testing
        - Billy volunteers
    - At this point, the intent is to support OU system administrators on campus. This is not intended to be a general user desktop replacement.
- Want to add Linux boxes in the NCSU OU to NCSU-Read Group Memberships just like we do Macs
    - Linux boxes do membership lookups with the computer's permissions, not the user's
- Proposal to remove the things that were blocked from UITC way back.
    - Things requested to turn back on
        - Logon banner has been disabled. Request to set a logon banner for the domain.
        - Screen timeout for Windows 7 should be re-enabled to match Windows 10.
- There is an AD Security engagement upcoming.

    - Current scope is being ironed out
    - Previous AD Risk Assessment Programs are here
        - https://activedirectory.ncsu.edu/risk-and-health-assessment-program/

Carry Over from last meeting:

- Billy: It's unclear whether Macs in AD support pre-auth. It is not set in userAccountControl by default and there are seemingly a lot of pre-auth errors in the DC logs.
    - https://blogs.msdn.microsoft.com/muaddib/2013/10/28/how-to-find-user-accounts-with-kerberos-preauthentication-disabled/