**Common Ports**

|  |  |
| --- | --- |
| PowerShell Remoting (HTTP) | 5985 |
| PowerShell Remoting (HTTPS) | 5986 |
| Dameware (on receiving end) | 6129 |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

**Task List – Starting May9th 2014**

# Example

* Get CAC Card updated. Need to update email address on file with the badge office on electron road.
  + Done
* Look into ACAS user account and why it is auto disabling. Check logs on Splunk server. Possibly contact Peter and see if there is a script somewhere.
* Gets access to ACAS using my new account created by Adam Jackson?
  + Done
* Work on SWAN licensing coagulation. Find out what we have, what we don’t have. If we have something, need to find the license for it and/or which part of the product.
* Review Licensing of current software and systems.
* Review DADUM (approved DoD software list)
  + Done

# 5/9/14 – Friday

* Create LDAP query to find all user accounts older than 120 days (or a variable amount) old
  + Currently have queries to find:
    - All users
    - All users not disabled
    - All users CLO enforced
    - All users not CLO enforced
    - All users password never expires
* Compile list of items to discuss at Monday’s roundtable meeting
  + Justin working on plugin #21745 “Authentication Failure” on group of NOC machines
  + New LDAP queries
    - ADUC queries Justin built
  + Tweaking LastLogonScript
  + Progressing through STIG checklist
  + Kyle wrote 8 GPOs for workstations
  + Need to build test VMs and STIG up.
  + Want Physical to Virtual workstation
  + Building a Windows 2012 Member Server Ops box, and sysprep it to make a template.
* Find out why Midway and other machines affected by #21745 “Authentication Failure – Local Checks Not Run”
  + Verifying that Best Practices checklist is applied on Midway
* See if Kyle’s unclass smartcard certificates have been revoked or not. Navy websites won’t allow him to authenticate.
* Created GPO-002-WS to mitigate the authentication scanning problem on Nihue and other affected machines, however it did not work. On Monday, RESTART Nihue and scan again. Why did Midway scan cleanly???
* **TO DO MONDAY:**
  + Prepare for the roundtable meeting
  + Restart Nihue and rescan (see above)
  + Get Server 2012 build sysprep document from Paul Plummer
  + Verify once more (have Kyle attempt to log onto unclass navy websites) that Kyle’s CAC certs have been revoked. If revoked, have Eva Ruiz Notify Don Ridgeway about it and get new token process started.
  + Talk with Guy about why Kyle can’t get to the SWAN share. He’s using the proper password, because he’s able to get into his email w/ it. Maybe have him try typing his MailSD1 passowrd into Notepad and copying that into the credentials box when he tries to map to SWAN share? Maybe look at other permissions that other guys in SWAN have and see if he’s missing anything. Guy copied permissions from <javery> to <klauro> so there shouldn’t be a problem.

# 5/12/14 – Monday

* Testing GPO-002-WS for plugin 21745. Midway worked when I applied these settings to the registry manually, but NIHUE did not when the GPO applied the settings. I will undo the settings on Midway and then place it in the Windows7Test OU to see if the settings being applied there will stop #21745. Will do a scan after first removing the settings from Midway to ensure that the plugin still pops up on that machine.
  + Removed registry settings from Midway, rescanned in ACAS, and it scans clean. #21745 does not show up even after removing registry settings. Will restart and scan again to see.
* Need to export query definitions to shared drive for Kyle.

# 5/13/14 – Tuesday

* Put VM for GemX in the 56 vlan, and now it works.
  + Alex says that GemX can’t be run on VM because the vendor will not support it. So that VM is now without purpose. It was good practice creating it though.
* Ran SCAP tool and built checklist for MOLOKAI
* Attended RDTE 2.0 Admin Meeting in order to understand how the RDTE Unclass. community handles management of the domain between domain admins and lab admins.
  + Stigged MOLOKAI according to checklist requirements, and marked changes in the Windows Change management spreadsheet.
* Found out that CSWF’s requirements for granting SA or SAR accounts have been relaxed. They are also getting rid of the “PA” account designation.
* TO DO WEDNESDAY:
  + Create local machine accounts on any machines being affected by the “authentication scan failure” problem, and rescan to see if the plugin still comes up. Be sure to scan machine before making any changes to ensure that it still gets a bad scan… then try the local account creation “fix.”
  + Why doesn’t EMET show up on MOLOKAI??? It’s not in the registry, nor in the Local Group Policies.

# 5/14/14 – Wednesday

* Swanscan issue: 3 bad attempts | 05/14/14 6:06:15 AM \*\*strange because I can only find bad attempts for 2 different machines, though the second machine shows multiple audit failures in its security log, for swanscan trying to authenticate.
  + Splunk log found 1 audit failure with swanscan trying to authenticate to GALAPAGOS at the time stamp listed above. Account: swanscan. Record # is 2046189. Event code 4776. Error code 0xc0000064, this error code means “user name does not exist”. Why would it not recognize the username? Is it looking for a LOCAL username instead of a domain username?
  + Splunk log found 1 audit failure with swanscan trying to authenticate to southbrother.srdte.spawar.navy.smil.mil. Audit failure, record number 73592236, event code 4776. Error code 0xc000006a, “user name is correct but the password is wrong”
  + Splunk log found 1 audit failure with swanscan trying to authenticate to southbrother.srdte.spawar.navy.smil.mil. Audit failure, record number 73592238, event code 4776. Error code 0xc000006a, “user name is correct but the password is wrong”
  + Splunk log found 1 audit failure with swanscan trying to authenticate to southbrother.srdte.spawar.navy.smil.mil. Audit failure, record number 73592239, event code 4776. Error code 0xc000006a, “user name is correct but the password is wrong”
  + Record number: 73592240 Error code 0xc000006a, “user name is correct but the password is wrong”
  + Record number: 73592241 Error code 0xc000006a, “user name is correct but the password is wrong”
  + 73592242 Error code 0xc0000234 “user is currently locked out”

# 5/15/14 – Thursday

* Check w/ Mark about the CSA checklist. Is the OS checks all I need to stig? How about applications?
* Applied GPO-002-WS back to MIDWAY to see if it could mitigate #21745. Around 07:30, I saw 6 machines with this vulnerability, but now at 08:02 it’s back down to 4 machines: HBSSMGR, NIHUE, MIDWAY, and ZANZIBAR.
  + After applying the GPO to ZANZIBA, gpudate, and reboot, it still remains.
* GemX now shows up on ACAS with 30 high vulnerabilities, the majority concerning Internet Explorer.
  + Going to try installing the fix for MS12-010. It looks like each consecutive update fixes the one behind it, but this is where the trend stops. Hopefully installing this will cover all the prior fixes back through MS11-025.
  + When I tried to install MS12-010 the installed throw an error message saying “this update does not apply to your system”. So now I’m trying to start from beginning, with installer for MS11-050, the earliest vulnerability in the list for IE. I’ve downloaded the installer for IE 8 and IE 9 just in case.
  + Nope that didn’t work either. I decided just to try to install the patch for the most recent “Zero Day” vulnerability that came out, KB2964358, and it worked for the IE 9 installer.
  + TO DO MONDAY:
    - Keep stigging GEMX, and install HBSS and Tumbleweed. Then make that thing a template!

# 5/19/14 – Monday

* GemX VM Group Policy service won’t start up. Looking at event log details.
  + First instance of the gpsvc failing was today at 7:41:28, event ID 7031
  + Today at 3:19:10am, event ID 1112 warning about Group Policy Client Side Extension.
  + Decided to roll back to snapshot from Thursday 5-15-14, and that fixed the problem.
* Continued STIGing the GemX VM.

# 5/20/14 – Tuesday

* Running into conflicting (?) inadequate-privilege problems when applying certain GPOs to GemX VM.
  + Javery.da could log on, but javery.sa could NOT. Found out that .SA account was not a member of the “domain admins” group. Once I added it, the .SA account could log in. The “Default Domain Policy” GPO

# 5/22/14 – Thursday

* Re-SCAP-scanned GEMX VM and it came back with 68 new open STIG findings… verified this by comparing to the WIP checklist that I’ve been completing.
  + The problem was that I had re-scanned using an older release version of a STIG benchmark (Windows 2008 STIG – Version6, Release 1.25). The STIG I originally used to create my first checklist was Windows 2008 MS STIG Benchmark Version6, Release 1.27).
  + Re-scanning GemX VM using the original file, Release 1.27.
* FUN FACT: “NT SERVICE\*user\_role* “ is how you can get Windows to recognize a role like “eventlog”, one of those virtual ones, when adding memberships.

# 5/27/14 – Tuesday

* Continuation of effort to STIG MOLOKAI. (75% complete).
* Assisted Todd in installing Splunk Forwarder 6.0.3 on CAICOS
* Verified w/ CSWF Randy Beam that Kyle Lauro was listed in CSWF list properly
  + Requested .SA account for Kyle Lauro on PAC domain, account was created 5/27/14
* Standing meeting w/ Dave, Chris, and Kyle regarding roaming email profiles for SWAN users
* Worked with CJ McDonough to clarify issue with KB296035 MS14-024
  + Initially we had planned to push a fix via GPO, however this is not something that can be changed with a GPO. Instead we instructed the admin to manually change the name of the file in question, adding “.old” to it. This should stop ACAS from seeing this as a vulnerability.
* Assisted Robert Yowell in clarifying issue with ATO accreditation question regarding Windows domain functionality.

# 5/28/14 – Wednesday

* Assisted Quinyon Washington in attempts to regain access to local administrative accounts for machine that could not gain network access. Failed. Recovery software could not recognize HDD partitions on machine.
* Found list of STIGs for Dave that pertained to password age and change settings.

# 5/29/14 – Thursday

* Filled out Monthly Status Report and sent it to Mike de Lira.
* SWAN Roundtable meeting 0900-1100
* Looked at the current settings of the administrative security groups, SA MA DA to decide where to start in reorganizing them.
* Where you left off, FOR MONDAY:
* Spend Monday working on fixing vulnerabilities on your systems. Put the installation of GemX on hold, it is currently NOT priority. Priority is making sure that all STIG checklist artifacts, and vulnerabilities are completed and mitigated by June 12. Let Jenny know BEFORE June 12 if there are any vulnerabilities that can’t be fixed. One of the stig requirements is making sure that the security groups on the domain are architected in a way that follows Least Privilege. Because of this you will need to unstring the mess of groupings and current architecture so that SA accounts and groups go with workstations, MA accounts and groups go with Member Servers, and DA accounts and groups go with Domain Controllers. It’s probably best to wait until you meet with Paul on Tuesday at 3:00pm so he can explain how they have it designed on the UNCLASS side. Spend Monday fixing the vulnerabilities that you have on your machines, and help Kyle with his. Work together to get this fixed ASAP. The other items that were scheduled to start in June – CLO enforcement and all that – is going to be pushed back until all priority items are completed.

# 6/2/14 – Monday

* Dave instructed me on how to connect to BALI through SSH.
  + Showed which directories to get to, and created a page to work from: /webhome/windows/index.html
  + Different ways to deliver this content?:
    - HTML Tables –similar to the way that the SWAN Hosts page works
    - XML? – would it be possible to display them on our page like they do in the html sheets?
    - Spreadsheet – a sheet that admins can download.
  + Categorization
    - By machine type: Domain Controller | Member Server | Workstation
      * OS

# 6/4/2014 – Wednesday

* When get back from lunch, continue trying to make sense of which groups will be affected. You figured out which GPO pushes the Workstation Admin group to machines (SRDTE Workstation Admins Group to Administrators). Good job.
* Figuring out member server problems
  + 1.) Go through every group and find any service accounts or other group accounts that look like they could be important / affected by the change. Got 8 accounts.
    - Splunk.ma – is used (probably, says Chris) by the Forwarder Client to facilitate its duties.
      * This should not be affected by any settings since it’s a member of the Member Server Admins group; as long as this .MA account is only being used on a Member Server, then it’s fine.
    - Splunk.sa - is used (probably, says Chris) by the Forwarder Client to facilitate its duties.
      * This should not be affected by any settings since it’s a member of the Workstation Admins group; as long as this .SA account is only being used on a Workstation, then it’s fine.
    - Swanroot (sscpac) - <disabled>
    - Swanroot (srdte) - apparently not super important. It’s locked.
    - Swanscan - \*\*\*the big issue\*\*\*
    - Swan\_scripts.da (sscpac)
      * Last chunks of objectSID: 1004242070-2584
      * Last authentication to sscpac-dc1 12/16/13 1:07:24PM
      * Last authentication to sscpac-dc2 <not set>
      * Last authentication to sscpac-dc3 3/13/2014 5:02:02 PM
      * This account does not appear to have been used in a long time, so it shouldn’t be anything that is scheduled. Therefore nothing should break if we remove its privileges.
      * 6/6/14 - removed from ADMINISTRATORS (sscpac builtin)
      * 6/6/14 – changed primary group from DOMAIN ADMINS to DOMAIN USERS, and removed from DOMAIN ADMINS (sscpac)
    - Swan\_Scripts.DA (srdte) – didn’t find any reference in scripts on SWAN share
      * Last chunks of objectSID: 2890315443-9722
      * Last authenticated to srdte-dc3 12/16/13 11:27:21AM.
      * Last authenticated to srdte-dc1 12/16/13 2:04:16PM.
      * Last authenticated to southbrother (srdte) 4/18/2014 3:14:59AM.
      * **runs task schedule scripts on DCs. CLO account scripts. Apparently thee was an issue with security groups not being able to run the task, and it had to be actual accounts. This swan\_scripts.da account had to be logged into the DCs at all times. Account status script was the big one that was running, it touches all the external domains and outputs that big, ugly HTML report that we use to send numbers to Anabel. The scripts should be on SRDTE DC. After speaking w/ Chris Baker I found out that this runs on the SOUTHBROTHER DC; this makes sense because SOUTHBROTHER was the only DC that the account had recently logged in to on 4/18/14. Chris had changed the script to allow it to run so long as anyone that was a member of one of the administrative security groups was logged in, and since there’s always one of us logged in the script keeps running. Go to Windows task scheduler, and look at the root to find the Windows task that references the account status script.**
      * **Script Located on SOUTHBROTHER:** C:\scripts\task\_scheduled\_scripts\AccountStatus\_remove\_users\_needing\_domain\_accounts\_modified\_to\_update\_IA\_v5b.
    - Trust – should not
    - ~~Vcbackup~~ – Vmware VCB backup user. What is this and how will it be affected?
      * 1.) see when it was last used / logged in: 6/5/2014 3:23:16… this would appear to be an automated task of some sort?
      * According to Dave Teger, this is an account that is used to facilitate the creation of snapshots in vSphere for machines.
      * Removed vcbackup from the DOMAIN ADMINS group.
      * Created a new security group called VSPHERE BACKUP on the SRDTE domain, and added Vcbackup to this group.
      * Removed vcbackup from the domain-builtin ADMINISTRATORS group.
  + 2.)
  + ENTERPRISE ADMINS group doesn’t seem like it will be a problem. It only has 5 active groups in it, all of which are just users. Myself and the other guys.
* For Thursday: Keep working on this list^above. Talk with Dave about the vcbackup group, and see if anyone knows about the others. Might be a good idea to send an email to swan and cc Peter Thung to see if he has any idea… Also find out WHERE those swan\_scripts.da account are being used, if they’re being used at all.

# 6/6/14 – Friday

* Created script to find machines based on Operating System. Located in \windows\_team\new windows team\scripts
  + Found the various Windows Server 2008 machines on SRDTE
    - SWANVCTR – be very careful with this. It’s hosting vSphere
    - SWANSADR – Nat Coil’s HBSS repository. He says “go for it”.
    - MONKEY – Bluescope app …? Not exactly sure what that is
    - SWANWSUS – the WSUS server
    - TASMANIA – non-existent machine that has been deleted from AD.
    - GEMX – my GemX VM.
* Start moving GPOs for Server 2008 into production OUs.
* Trying to get clear on why my .SA could not log in, yet my .MA can. Well the .MA was still part of the DOMAIN ADMINS (srdte) group, and I removed that. The .SA account is a member of a lot of groups, but the only offending group that should be blocking it’s access is Domain Admins…which the .MA was a part of and could still log in. Damnit. ...
* FOR MONDAY: Work on that problem w/ Paul Z’s machine : CMS1 Tumbleweed stuffs.
* Refer to chart that you drew in your notebook for B I G P I C T U R E view of what’s going on if you forget.

# 6/16/14 – Monday

* Manually applying patches to 5 systems that couldn’t be patched automatically by WSUS.
* Rebooted all systems that received updates.

# 6/17/14 – Tuesday

* Moved 9 STIGs into production OU (Windows 7 Computers) from the Test OU (Windows 7 Computers/Windows7Test/STIG)
* Built Windows 7 VM to be used for Active Directory Administration
  + IP Settings for Windows 7 VMs:
    - IP: something in the same subnet as 140.199.56.57
    - Gateway: 140.199.56.36
    - Subnet: 255.255.192
    - DNS: 140.199.56.1, 140.199.56.2
  + Install all of the updates and then CLONE IT! 🡪 Make the second one1
* Moved up 5 Windows Server 2008 GPOs from the test OU, to the production OU, in SRDTE.

# 6/18/14 – Wednesday

* Finish installing and configuring updates on SRDTE-AD1.
  + Configure all local group policies, and then clone the machine. See if these local policies persist after the change. 🡪 They did persist, along with the

# 6/23/14 – Monday

* Test smartcard login on SSCPAC – Log in successful. Tested on COZUMEL, TOBAGO, NAURU, BARBADOS, after gpupdates and a reboot. It seems that the changes Gary Delgado helped us out with just needed time over the weekend to propogate.
* Taking on the task of creating that Windows Logon notification pop-up script. This is an IA Control. Got the paper copy from Jenny.
  + Paul Plummer has not heard of this control, and does not know of a solution off-hand.
* PS Notes
  + **DISPLAY A MESSAGE BOX**
  + [System.reflection.assembly]::loadwithpartialname(“system.windows.forms”)  
      
    [system.windows.forms.messagebox]::show(“This is where the message goes”,”Title bar”)
  + **GET LastLogon**
  + Get-ADUser javery –properties LastLogon | select LastLogon
  + **GET LastLogon (DATA ONLY)**
  + get-aduser javery -properties lastlogon | foreach {$\_.lastlogon}
  + outputs: 130480421365686404  
    **CONVERT TIME FORMAT**[datetime]::FromFileTime($lastlogon)
  + **RESULTS FROM MONDAY EVENING’S WORK:**

PS C:\Windows\system32> get-aduser javery -properties lastlogon | foreach {$\_.lastlogon}

130480421365686404

PS C:\Windows\system32> $lastlogon = get-aduser javery -properties lastlogon | foreach {$\_.lastlogon}

PS C:\Windows\system32> [datetime]::FromFileTime($lastlogon)

Monday, June 23, 2014 5:08:56 PM

PS C:\Windows\system32> $MessageString = [datetime]::FromFileTime($lastlogon)

PS C:\Windows\system32> $MessageString

Monday, June 23, 2014 5:08:56 PM

PS C:\Windows\system32> $MessageString = "You Last Logged in:" + [datetime]::FromFileTime($lastlogon)

PS C:\Windows\system32> $MessageString

You Last Logged in:06/23/2014 17:08:56

PS C:\Windows\system32> $MessageString = "You Last Logged in: " + [datetime]::FromFileTime($lastlogon)

PS C:\Windows\system32> $MessageString

You Last Logged in: 06/23/2014 17:08:56

PS C:\Windows\system32> $MessageString = "You Last Logged in:" + ([datetime]::FromFileTime($lastlogon))

PS C:\Windows\system32> $MessageString

You Last Logged in:06/23/2014 17:08:56

PS C:\Windows\system32>

**FOR WEDNESDAY**

Using Active Directory modules via PS istn’ going to work since we can’t have active directory tools on workstations. Need to find a VBscript way of going about it. Also need to talk with paul to see if three’s a better way to query the data, or have the DC alerted as soon as the user logs in.

Check with Jenny about the IA Control on the new Risk Management Framework document (iase.disa.mil on the low-side), and see if perhaps this is no longer a requirement. I doubt that It isn’t but I can hope…

# 6/30/14 – Monday

* Spoke with Kayley Byrne from Splunk, on phone, about license pricing to increase currently daily log allowance.
* Received newly imaged PAC workstation. Setup email. Had Servicedesk add my .SA account
* Started to apply SecGroup lockdown stigs today:
  + Applied GPO “STIG-WINUR-000020-MS” to the Member Servers OU in SRDTE. This blocks SRDTE\Enterprise Admins, SRDTE\Domain Admins, and BUILTIN\Guests from logging on locally.
  + Also need GPO to remove Domain Admins from these machines.
* Bring up at the admin meeting: The new “Last logged in” screen.

# 7/1/14 – Tuesday

* Created matrix to visualize the sec group membership changes. See [\\140.199.56.11\windows\_team$\new windows team\task list\javery\DomainGroupRestrucutre.xlsx](file:///\\140.199.56.11\windows_team$\new%20windows%20team\task%20list\javery\DomainGroupRestrucutre.xlsx)
* Scanning results seen on ACAS this morning were successful, even after implementing the “Deny Logon Locally” to SRDTE member servers. Initially we were wondering why the scan wasn’t being affected, however a closer look showed that the “swanscan” account was still a member of “SRDTE Member Server Admins”. That is why the ACAS scan was successful. To test, I have applied the rest of the stig lockdowns to SRDTE-OPS-001, added it to the temp test OU “STIG Security group lockdown settings”, and removed “swanscan” from “SRDTE Member Server Admins”.
  + Re-scanning with “swanscan” after changes were made: FAILED.
  + Re-scanning with “swanscanner.ma” after changes made:
* Tried to run a script against SRDTE-OPS-001 from my desktop, Galapagos, running an administrative PowerShell prompt with my javery.sa credentials. Tried:

Get-WmiObject win32\_computersystem -Computer $ComputerName | select username

And Windows returned error:

Get-WmiObject : Access is denied. (Exception from HRESULT: 0x80070005 (E\_ACCESSDENIED))

At line:1 char:1

+ Get-WmiObject win32\_computersystem -Computer srdte-ops001 | select username

+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

+ CategoryInfo : NotSpecified: (:) [Get-WmiObject], UnauthorizedAccessException

+ FullyQualifiedErrorId : System.UnauthorizedAccessException,Microsoft.PowerShell.Commands.GetWmiObjectCommand

So, unauthorized access to a member server, when trying to run a script with .SA credentials.

Next I tried running the same script from a PowerShell that I opened as “Run as different user…” with my .MA credentials, and it worked. However HBSS did pop up a warning alert citing that I was attempting to access another user’s directory. Clicking “ignore” made it go away and still let me use PowerShell.

* Next, trying to narrow down which GPO is blocking scripts.
  + I unlinked STIG-WINUR-000018 “Deny logon as batch job” and restarted SRDTE-OPS001. Will try to run script against it and see what happens.
    - Still get “unauthorized access exception” error.
  + Unlinked STIG-WINUR-000017 “Deny acces to this computer over network”. Gpupdate, and reboot.
    - Still “unauthorized access”
  + Unlinked STIG-WINUR-000019 “Deny logon as a service”
    - Still “unauthorized access”
  + Unlinked STIG-WINUR-000020 “Deny logon locally”
    - Still “unauthorized access”
  + Unlinked STIG-WINUR-000020 higher up, at the “Member Servers” OU…
    - Still “unauthorized acces”
  + Unlinked STIG-WINUR-000021 “Deny logon through terminal services”
  + SOLUTION: it depends on the groups that are in the built-in “Administrators” group. Since my .SA account was not in the built-in “Administrators” on SRDTE-OPS001, nor was any security group it is associated with, it did not have the credentials to access the machine via PowerShell script.
* The plan for Wednesday 7/2/14:
  + Admin meeting at 9AM.
  + Check to see how the scans went on the SRDTE member servers, hopefully all is well. Also make sure that there are no problems with any other accounts or scans since we started scanning with **swanscanner.ma**, alongside **swanscan**.

# 7/2/14 – Wednesday

* Need to check with Adam or Chris, but it appears that the member servers were scanned successfully. They show in ACAS as having a good scan this morning.
* Need to start moving GPOs over to the SSCPAC domain.
  + Decided that we would copy / paste them over, instead of cross-domain linking.
  + Since SSCPAC does not organize the OU structures based on machine type, we will need to filter the GPOs with WMI filter. Time to Google how WMI filtering works…
  + Found out about the win32\_operatingsystem class that can be used to write queries in WMI, along with the ProductType attribute to differentiate between workstations, member servers, and domain controllers.

Select \* from win32\_operatingsystem where ProductType = “1”

* + So that should work. Now to test it…
  + To test, I’ve added SRTDE-OPS001 to the SSCPAC domain, and put it in a test OU. In this test OU, I copied over GPO STIG-WINGE-000200 (you can copy GPOs from one domain to another, and according to Kyle this prevents cross-domain linking problems) and applied it to SRDTE-OPS001. It created “denynetworkaccess” local group on the machine. I applied a WMI filter on the GPO so that it will only apply to Domain Controllers, and rebooted SRDTE-OPS001.
* Got WMI to work properly. Time to start moving stable GPOs over to SSCPAC!
* Need to be able to export or get a list of the GPOs in a specific OU
  + Solution is “get-gplink” function that I found on technet forums. Saved to Scripts folder, and my Documents folder.
  + Run command :

**get-gplink -path "OU=Windows 7 Computers,OU=Computers,OU=SRDTE users and computers,DC=srdte,DC=spawar,DC=navy,DC=smil,DC=mil"**

* + You can pipe specify the exact OU you need, and PIPE it into **Format-Table –Property <the property>**
  + Or further filter results with **Where-Object {$\_.gponame -like 'stig\*'} | Format-Table**
  + Was able to copy 1 GPO over from SRDTE to SSCPAC by using copy-gpo:

**Copy-GPO -SourceName stig-2.006-ws -SourceDomain srdte.spawar.navy.smil.mil -TargetName stig-2.0 06-ws -TargetDomain sscpac.srdte.spawar.navy.smil.mil**

* + That –TargetName switch is required… so if I want to make this an automatic process, I’ll need to find a way to automatically tell it that the –TargetName should be exactly the same as whatever was entered in for –SourceName. Some kind of **For Each…** statement, probably.

# 7/3/14 - Thursday

* Can put the results into a PowerShell object.
  + 1. Define the object: **$objectname = @{}**

2. Put all the output into it: $objectname = **get-gplink -path "OU=Windows 7 Computers,OU=Computers,OU=SRDTE users and computers,DC=srdte,DC=spawar,DC=navy,DC=smil,DC=mil"**

* + Woo!
  + Now we can reference each of the properties that get-gplink gives up: Path, GPOGUID, GPOName, with the syntax $objectname.property ($objectname.gpoguid). !!!
  + This command successfully copies the specified GPOs form the specifiec OU, from one domain to another:

**get-gplink -path "OU=Windows 7 Computers,OU=Computers,OU=SRDTE users and computers,DC=srd**

**e,DC=spawar,DC=navy,DC=smil,DC=mil" |Where-Object {$\_.gponame -like 'stig\*'} |ForEach-Object {Copy-GPO -SourceName $\_.gponame -sourcedomain srdte.spawar.navy.smil.mil -TargetName $\_.gponame -TargetDomain sscpac.srdte.spawar.navy.smil.mil}**

* Ran this command to copy all GPOs from SRDTE that started with the word “STIG”, and place them in SSCPAC:

**get-gpo -all -domain srdte.spawar.navy.smil.mil | Where-Object {$\_.displayname -like 'stig\*'} | ForEach-Object {Copy-GPO -SourceName $\_.displayname -SourceDomain srdte.spawar.navy.smil.mil -TargetName $\_.displayname -TargetDomain sscpac.srdte.spawar.navy.smil.mil}**

* Just realized that we’re going to need more WMI filters than just “Workstations, Member Servers, Domain Controllers” . Going to need to be more granular with:
  + Member Servers 2008
  + Member Servers 2012
  + Domain Controllers 2008
  + Domain Controllers 2012
  + Maybe something like:
    - SELECT \* FROM Win32\_OperatingSystem WHRE (version like ‘6.0%’ OR version like ‘6.1%’)

**For Monday:**

Work on developing a calendar-like solution (or something) so we can track the GPOs that we’re applying to the enclave. We have all our STIG GPOs migrated to SSCPAC, now we just need to track what we’ve linked, and when we’ve linked them.

# 7/7/14 – Monday

* Came in this morning and Dave said that SRDTE-DC1 was hung up on Friday evening, and he had to come in on Saturday to restart it. When I looked at the System logs on DC-1, it showed many of the usual errors for TCP/IP, but also numerous Schannel errors, eventID 36874. The last error message that popped up before the system hung indefinitely was eventid 109, Kernel power manager initiated shutdown transition. Then nothing else was seen in the logs until Dave rebooted the DC and things started to show back up on Saturday 7/5/14 approx 2:00pm.
* The plan for today:
  + Implement .SA lockdowns for workstations on SRDTE. The .MA lockdowns have so far been successful, so now it’s time to expand over to .SA and be sure to let Adam and Chris know so that they can prepare the scans accordingly. .
  + STIG-WINUR-000017, STIG-WINUR-000018, STIG-WINUR-000019, STIG-WINUR-000020, STIG-WINUR-000021 have been added to OU “Windows 7 Computers/Windows7Test/STIG” .
  + NIHUE is in this OU, and having updates applied prior to testing.
  + Tried logging in with SRDTE\javery.sa, got denied. Turns out that javery.sa was still a member of Domain Admins, so I removed that. Tried logging in again with success.
  + Requested that Adam try scanning NIHUE with swanscanner.sa credentials.
  + **GOOD SCAN!!! – OH YEAH!**
  + Almost every .SA account on SRDTE is a member of Domain Admins, and this cannot be allowed once workstations are locked down, otherwise .SA accounts would not be usable.
* We found out why our VMs have been maxing out the CPUs
  + The Splunk service on the hosts starts going crazy and causes the CPU to max. The fix we’ve found so far, is stopping and re-starting the Splunk service.

# 7/8/14 – Tuesday

* SSCPAC-DC1 and SSCPAC-DC2 are running around 50% CPU again… Dave says that he wants to try and play around with one of those DCs and Splunk to try resolving the issue.
* Is swanscanner.sa ready for prime-time? Need to make sure that either “SRDTE\SRDTE Workstation Admins” is in local administrators group.
* Created GPO to add “SRDTE\SRDTE Workstation Admins” to BUILTIN\Administrators on all SSCPAC Workstations
* Working on filter on DC3, PS script. Trying to cycle through all servers, and get the wmi property for producttype = 3, member server.
* Created GPO to add “SRDTE\SRDTE Member Server Admins” to BUILTIN\Administrators on all SSCPAC Member Servers
  + Let’s get a list of all servers on SSCPAC:

**Get-ADComputer –filter {operatingsystem –like “\*server\*”} –Property \* | Format-Table Name, OperatingSystem –auto**

* Next, try to get the WMI filter object win32\_operatingsystem producttype:

**For Wednesday:** Every machine on SSCPAC should have SRDTE\Workstation Admins now in its BUILTIN Administrators group. Adam can now start scaning using swanscanner.sa . YAY Progress!

# 7/9/14 – Wednesday

* Still having Splunk “over-indexing” problems on SSCPAC-DC1 and SSCPAC-DC2. Dave is looking into it.
  + Looks like Splunk Forwarder 6.1 is going to be our solution to the “over-indexing” problem.
  + Assisted Dave with the install for that on SSCPAC-DC1. Further testing with ACAS scans shows, so far, that the CRIME Vulnerability that was present with 6.0.3, does not get flagged with 6.1 .
  + New edition of Splunk Forwarder(6.1) has been installed on SSCPAC-DC1.
* Working on Applications General Checklist STIGS
  + STIG-DTGW005-WS : should set the specified file types to only “open” in notepad, have their filepaths displayed in windows explorer, and have “confirm after download” enabled. T
    - Testing first on NIHUE. Created a HelloWorld.vbs script. Currently it will run when double-clicked, and its file type is not visible in windows explorer.
    - NIHUE is a bitch to work with and takes too long. I’m using SRDTE-AD1 as my test machine for this. As such, I have moved it into the STIG OU.
    - SRDTE-AD1 runs the .vbs script automatically and does not show its file extension by default. Good, time to apply the GPO and see if it makes a difference.
      * It does! The .vbs script opens with Notepad by default, however the problem I now see is that running the script with the Windows Based Script Host application is not so easy. It does not pop up under the “open with…” options when you right-click the .vbs file. But I suppose people will rarely need to run such files so it’s acceptable.
* User Gary Burnette <burnette> called in complaining that he was getting the same logon error message that plagued us a few weeks back “…smartcard logon is not supported…”. He was able to log back in by the time the call was transferred to me, and said that he got a Windows pop-up telling him his info was out of sync, and to log off or lock the screen. His machine is 140.199.18.82, and his logon server at the time was SSCPAC-DC2. He also said that he had not received any email messages in a while, but that suddenly he had email in his inbox. I was able to ping his machine from mine (GALAPAGOS). It seems that he had some lapse in connectivity and that may have been the root cause.

# 7/10/14 – Thursday

* Called Splunk support for unlock license. Karey Byrne is sending unlock license via email. Received 07:52.
* Installed splunk license. Restarted the Splunk Indexer application via the web interface.
* Upgrade SplunkForwarder on NIKOA, SRDTE-AD1, SOUTHBROTHER, SSCPAC-DC3
* Monkey, Anitgua, SRDTE-DC1
* Does the server.conf patch file that we had to add to all forwarders get updates when you install Splunk 6.1 over the old instance? On SRDTE-AD1 the last date modified on etc\system\local\server.conf was 6/26/14 10:33am.
* I’m installing over the old instance now.
* SRDTE-AD1 finished installing SplunkForwarder 6.1 . Rebooting.
* The server.conf file date modified remains the same: 6/26/14 10:33am. And the added lines “disableDefaultPort=true” and “supportSSLV3Only=true” are present.
* I’m going to uninstall SplunkForwarder on SRDTE-AD1, and reinstall the updated version to see if there are differences in the server.conf file.
* SplunkForwarder has been uninstalled. Rebooting.
* SplunkForwarder has been reinstalled, rebooting.
* Turns out that the files ARE different when you do a fresh install of the SplunkForwarder 6.1 .
* Uninstalling old SplunkForwarder on SRDTE-AD1. Uninstall complete. Rebooting.
* Installed SplunkForwarder on Southbrother. Rebooting.
* Created new shared drive for Windows Admins
  + Created 12GB partition on FS-01
  + Shared this as \windows\_admins$
  + Set permissions to:
    - Authenticated Users – Read & Execute
    - All javery accounts – Full Control
    - All klauro accounts – Full Control
  + Migrated all data from “New Windows Team” to the windows\_admins$ share
  + Migrated all old data from Windows\_team$ share to a folder in windows\_admins$ called “Old Windows Team”
  + Stopped sharing windows\_team$
* Researching SPLUNK search query language.
* Source = WinRegistry Trying to find hosts that are forwarding useless info and bloating the indexer. WinRegistry should not be logged for instance.
  + The hosts that this is coming from are: ~~swanscan91~~ | ~~ANTIGUA~~ | sscpac-dc3 | ~~southbrother~~| srdte-web1
* Uninstalling the old SplunkForwarder 6.0.0 from ANTIGUA . Going to update the forwarder so it’s only sending correct logs.
  + Searching SPLUNK by host=”Antigua” source=WinRegistry shows that the last recorded event of WinRegistry was 4/11/2017 15:25:26.
* **Fun Fact:** running appwiz.cpl from a **Run** windows brings up Programs and Features.
* Piping data to get a sum of the kb :

**index="\_internal" source="\*metrics.log" per\_host\_thruput series=swanscan91 | stats sum(kb)**

…lets convert that to MB:

**index="\_internal" source="\*metrics.log" per\_host\_thruput series=swanscan91 | stats sum(kb) as kb | eval MB =round(kb/1024,1)**

* So the plan now is to do “clean” installs (uninstall completely and reinstall) of SplunkForwarder 6.1 on the offending machines listed above. This should cut down on the amount of WinRegistry data logged, hopefully.x
* Finished clean installing SplunkForwarder on Monkey 5:57 PM. Rebooting. The last visible even that Splunk logged for **swanscan91**  should be 4/11/2017 16:27:15
* Uninstalling splunkForwarder from srdte-web1 4/11/2017 5:57 PM.
* Finished clean install of SplunkForwarder on SRDTE-web1. Rebooting 4/11/2017 5:57 PM
* Looks like there’s only SSCPAC-DC3 left that forwards “WinRegistry” events to SPLUNK. Just did a search for **Source=WinRegistry** with a time span of “Last 15 Minutes” and only SSCPAC-DC3 came up.
* For Monday : Do a clean install of SplunkForwarder 6.1 on SSCPAC-DC3.
  + Check to see how the quotas are doing over the past few days.

# 7/14/14 – Monday

* 81.6% of SSCPAC-DC3 logs just this morning up until were WinRegistry.
* Going to do a clean install of the updated SPLUNK Forwarder. Taking a snapshot of SSCPAC-DC3 now.
* Removed philipm from CLO Exemption list.
* Clean install of SPLUNK Forwarder on SSCPAC-DC3 complete. Rebooting.
* Last observed log of source=WinRegistry on SPLUNK was 08:20:37 AM.
* Sscpac-dc3 is checking in successfully, with no recent instance of WinRegistry logs.
* Uninstalling old SplunkForwarder from SRDTE-AD2.
* Finished clean install of SplunkForwarder on SRDTE-AD2. Rebooting.
* SRDTE-AD2 is checking in with SPLUNK.
* MrPatch is having issues authenticating swanscan credentials through Shavlik. I’m unlinking STIG-WINUR-000017 through STIG-WINUR-000021.

# 7/15/14 – Tuesday

* Splunk got a massive spike in logged crap this morning thanks to windows\_snare\_syslog, and its coming from stor.spawar.navy.smil.mil.
* Starting to link GPOs in the SSCPAC domain, and keep track of exactly which ones were linked in my document: DomainGroupRestructure.xlsx.
* Group Memberships
* STIG GPOs

## IWEB Site Stuff

* + Connect to Bali using Tectia SSH
  + The directory is /webhome/web
  + Created CSS for Windows page. Windows.css
  + Setup page for posting.
  + Login is the same as mail login. No more key involved, just password.

### VI Commands

* Vi *filename* edit filename starting in vi
* i insert
* :x exit and save
* :q! exit w/o saving

Testing COZUMEL to see if it got the 12 GPOs I pushed to SSCPAC today.

# 7/16/14 – Wednesday

* Troubleshooting SWANSCANNER.DA w/ Adam.
  + It works! Was able to successfully scan all domain controllers
* Applying Lockdown STIGS to workstations on SRDTE
  + Need to remove some users from the Domain Admins group. Removing:
    - Adamj.sa
    - Baker.sa
    - Coil.sa
    - Mcmahon.sa
    - Trangj.sa
    - Thungp1.sa
* Unlinked the “add\_SWAN\_SEC\_Group\_to\_Administrators\_Group” GPO from SSCPAC San Diego\Bayside\SWAN. That group did not contain any necessary user accounts, and was deleted to clean out unnecessary accounts.
* Trying to do a gpupdate /force on COZUMEL and ANACAPA, but keep getting the error message that references a GPO. The GPO it references is SITG-WINUR-000005-WS, I’m unlinking it and seeing what happens.
* SCM – GPO tool!
* For some reason COZUMEL and ANACAPA won’t update the GPOs… each one of the GPOs I added to SSCPAC was causing it to fial, and then once I unlinked all of those, preexisting GPOs started to cause It to fail, like Remediation\_Plugin\_55915… fuck. Hopefully something replicates and this stops. This is even stranger because TOBAGO and BARBADOS updated their GP just fine… no errors, and their in the same damn OU!

# 7/17/14 – Thursday

* Got COZUMEL and ANACAPA to get pull down GPOs successfully by rejoining them to the domain. Gpupdate will still fail if you try it with srdte credentials, for some reason.
* COZUMEL has an account in BUILTIN\Administrators that is only referenced by its SID: S-1-5-21-2009968954-2146312033-1004242070-1884 . This appears to be an unknown account…
* Linked STIG-1.010-WS and it updated ok. Went ahead and linked all the GPOs I had unlinked yesterday, and suddenly gupudateing on COZUMEL fails again, citing the GUID for the last GPO in the list. Unlinked the last 5 in the list, rebooted and was able to gpupdate. So I linked those 5 again, rebooted, and was able to gpupdate.
* Have been trying to gpupdate NAURU, but keep getting failures. Removed the unknown account that was in the BUILTIN\Administrators group, privilege
* **After deleting that account and rebooting NAURU, gpupdate worked.**u
* **Sd**
* So if we enforced the WINUR policies, what would this lock down, or effect on SSCPAC?
  + Take a look and see how the Project Admins would be affected.
* SRDTE-AD1 and SRDTE-AD2 are logging many times more logs in SPLUNK than anyting else, even the DCs. So I’ve moved those 2 machines into the “Blocking” OU in SRDTE to (hopefully) remove any STIG GPOs that may be setting over-restrictive auditing policies and causing the Security logs to fill up with “Failure” events like it has been. Let’s see how that affects everything.

# 7/18/14 – Friday

* SRDTE-AD1 was filling up SPLUNK with a lot of failure security audits. Here is the search query I used to find info about it:
* **host=srdte-ad1 source="WinEventLog:Security" Process\_ID=0x240 eventtype="windows-security-4656-failure"**
* SRDTE-AD2 is in the blocking OU. Gpresult /R shows that it is not getting any GPOs. Good.
* SRDTE-AD1 is in the blocking OU.
* TOBAGO still logs too much to SPLUNK, and it’s because it still has the old Forwarder.
  + Doing a clean uninstall and reinstall.
* SPLUNK Stuff Today:
* Query all hosts and have the stats show in Gigabytes.
* **index="\_internal" source="\*metrics.log" per\_host\_thruput series=\*| stats sum(kb) as kb | eval MB =round(kb/1024,2) | eval GB = round(((kb/1024)/1024),2)**
* Query throughput of all hosts
* **index="\_internal" per\_host\_thruput | stats sum(kb) as kb by series | eval MB =round(kb/1024,2) | eval GB = round(((kb/1024)/1024),2)**
* Query the total throughput of all hosts
* **index="\_internal" per\_host\_thruput | stats sum(kb) as kb | eval MB =round(kb/1024,2) | eval GB = round(((kb/1024)/1024),2)**
* hklm\software\microsoft\windows\currentversion\installer\folders

# 7/21/14 – Monday

* Had roundtable meeting, led by Chris
  + Need to create Splunk logs projections based on the baseline data usage of the current workstations. Allow atleast 1.5 weeks of solid data being logged to Splunk so that I have a good data set to work from.
  + Need to install GemX by August 4th.

# 7/22/14 – Tuesday

* Fixing Plugin # 76464 Unauthorized Digital Certificates Could Allow Spoofing
  + The rvkroots.exe fixes the vulnerability
  + How can I deploy this to my machines?
  + Automated solutions are taking too long to develop. I have wasted enough time, could have installed this manually by now. Using a manual solution instead.
* Can’t finish connecting trust to JAOC.RHINO
  + Error message: “Cannot Continue | The trust relationship cannot be created because the following error occurred: The operation fialed. The error is: A device attached to the system is not functioning. “
  + Possible causes:
    - STIG Settings?
    - Firewall settings on *their* side?
    - Firewall settings on *our* side?
      * John Harmon is adding their DC IP addresses to a group in our firewall.
* Working on print server separator page. This uses separator page files, refer to support.microsoft.com/kb/102712 , or support.microsoft.com/kb/131714 for more information about the “escape codes” scripting language for this.
* **How to set separator pages from SRDTE-FS01:**
  + From SRDTE-FS01 open a windows explorer and navigate to: [\\140.199.56.11](file:///\\140.199.56.11)
  + Right-click on Papergirl2 and choose “Open”
  + Click on the “Printer” menu and select “Open as Administrator”
  + Enter credentials
  + Click on the “Printer” menu and select “Sharing”
  + On the “Advanced” tab click on “Separator Page…”
  + Click “Browse…” to choose the separator page file (.sep)
* For Wed:
  + Finish the printer STIG, reset the printer so we can set the password for it. Lock it down again…

# 7/23/14 – Wednesday

* Moved GemX VM out of the “Test STIGs” OU and up to its parent OU “Server 2008”. Then deleted the “Test STIGs” OU.
  + Keeping a document for all the settings that I’m doing to PaperGirl2, also going to save and export a configuration file that can be imported next time.
* Installing GemX on the GemX VM. Installing updates and rebooting first.
* Taking snapshot of GemX VM
* Need to create local login credentials on GemX with the approved account information found in the GemX binder.
  + Credentials created.
* Troubleshooted the RPITEL.SA account issue with Kyle on the phone after he met up with Rod Pitel at Topside.
* Finished write-up for printer configuration of PaperGirl2 titled “HP Laserjet 400 colorMFP M475dw Configuration Guide.docx” and saved it to “\\SWAN\change management\networkd\_devices”
* FOR THURS: Fix the IE problem Alex was having on GEMX VM. Supposedly a STIG or something is preventing him from opening a browser.

# 7/24/14 – Thursday

* Helped Jack Mcnabb out with his mcnabbjr.sa account. He said that he was receiving a logon error citing no logon servers available, but it looked like his machine SWAN.62.14 wasn’t on the network so it probably couldn’t talk to any of the DCs.
* ~~KB2592687 that Todd was having problems installing, apparently can be successfully installed by unplugging the network cable, starting the Windows firewall service, installing the patch, and rebooting the machine. Be sure the plug the network cable back in.~~ It came back…
* Enabled Telnet on SRDTE-AD1. Trying to connect to PaperGirl2 so I can complete the security config lockdowns. Looking up the manual for it to see how exactly I’m supposed to connect to it.
* Never mind, that didn’t work. Disabled Telnet.
* Printer checklist finished and submitted to Jenny’s ATO folder in the [\\SWAN](file:///\\SWAN) drive.
* Windows Update Issues on NIHUE
  + After telling NIHUE to install update and shutdown, it appears that the update is gone. Checking for updates now to make sure.
  + It’s still there: “Update for Microsoft Visio 2010 (KB2553444) 32-Bit Edition” 18.8 MB.
  + VISIO 2010 isn’t installed!!! WTF?!
* Installing Java 7\_65 on NIHUE.
* NIHUE showing Plugin# 74154 “MS KB2927432: Visual Studio Update 2 for Debug Interface Access SDK”
  + The fix is to install Visual Studio 2013 Update 2… just install a whole new piece of software
* Fix plugin 63155, Unquoted service path enumeration: go to registry **:Local machine /SYSTEM/current control set / services** and fix the file paths so that they’re enclosed in quotes.
  + Edited the following registry entries in HAWAII so they’re enclosed in quotes:
    - jhi\_service : C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\DAL\jhi\_service.exe
    - Intel(R) ME Service : C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\FWService\IntelMeFWService.exe
    - LMS : C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\LMS\LMS.exe
    - pdfcDispatcher : C:\Program Files (x86)\PDF Complete\pdfsvc.exe
  + Time for a scan!
  + Didn’t work. Had Todd restart it. Scanning again.
  + Still not working. Tried turning off a service that ACAS says had an unquoted path, the only one I could narrow down was “PDF Document Manager”
* Fix Plugin 62758 : rename “C:\Windows\SysWOW64\msxml4.dll” to “msxml.dll.old”
  + Rescannig MIDWAY to see if the changes remove the hit in ACAS.
  + 62758 still shows up in Midway, so it doesn’t look like an immediate fix.
  + /jj152146(v=vs.85).aspx

## cob

Have been trying to fix **63155** Unquoted Service Paths, and **62758** XML Parser, for half of the day now with no results. I was able to make the XML parser go away on my machine, GALAPAGOS, a few days ago by adding “.old” to the file and the ACAS finding disappeared. However I could not make it go away on NAURU, CAICOS, MIDWAY, NIKOA, BORABORA, or LANAI. The one thing I haven’t tried is changing the name of the other “msxml4” file that’s listed, nor have I tried deleting both of them. It might be a good idea to keep a copy of the files on a shared drive once I delete them, just in case they need to be restored. I will try to delete the files on Monday if they’re still showing up in ACAS.

With **63155**, it seemed like I did something correct on GEMX, because the finding disappeared. Unfortunately I have not been able to fix the finding on HAWAII. I haven’t tried much with SRDTE-AD1 or SRDTE-AD2 because they’re in the blocked OU. With HAWAII, I tried adding quotes to the beginning and end of each of the service paths that ACAS listed. I did go back and move the ending quotation mark on one of the service paths because there were other parameters after the .exe .

**GEMX**. Alex is having a problem where IE doesn’t display the website because the URL isn’t in the Trusted Sites. The machine is being locked down, probably by GPO, and doesn’t allow you to add to the trusted sites. Look into creating a GPO that pushes that URL to trusted sites, or eases up the security on the browser so you can add to Trusted Sites. Refer to the screenshot that Alex emailed to my SIPR email.

# 7/28/14 – Monday

* **63155** no longer shows up in ACAS on HAWAII. It looks like adding the quotes fixed the problem, though I’m not sure why it wouldn’t clear when I scanned the machine directly after, and needed to cook over the weekend. Either way, prob solved.
* **63155** still appears on SRDTE-AD1 and SRDTE-AD2 as expected. I have not done anything on those machines to fix the problem, so adding the quotes should fix it and clear the ACAS findings by tomorrow. Both machines are being hit on C:\Program Files\Tumbleweed\Desktop Validator\DVService.exe, so I will go into the registry and add quotes around that path. NOTE: These machines are still in the blocked OU, and there’s prob some GPO that fixes this that is being applied to other machines.
  + SRDTE-AD1, added quotes and rebooted.
  + SRDTE-AD2, added quotes and rebooted.
* I looked in Configuration-Tumbleweed-Standard-4.10-conf and Configuration-Tumbleweed-Standard-4.11-conf, but no registry settings were present.
* **62758** no longer shows up in ACAS for any of my machines!
* **GEMX** Content being blocked from Internet Explorer. “If you trust this website, you can lower security settings for the site by adding it to the Trusted sites zone. If you know this website is on your local intranet, review help for instructions on adding the site to the local intranet zone instead. To add this site to Trusted sites zone: Select the Tools menu, then Internet Options. On the Security tab, select Trusted Zone and then Sites.”
  + <http://localhost:8080/taclane/flex/Gemx_flex.html>
  + Created GPO-011-WS to add that url ^ to the trusted sites. GPO path Computer Configuration > AdministrativeTemplates > Windows Components > Internet Explorer > Secure page > Site to zone assignment list.
  + Still doesn’t let you open up GEMX. I’m putting GEMX into the Blocking OU and seeing how it works after that. If I can actually get INTO the trusted sites list, then I can manually add it myself, instead of the GPO doing it, and verify that it works or not.
  + I can see the security details in IE now. Removing <https://localhost> from Local intranet. Adding it to Trusted Sites.
  + Fuck it. Try upgrading IE to ver 11 on GEMX, and then put it in the same OU that KUKULA is in.
  + Changed the password for the .\postgres account. Same as swannet. Now the postgres service can start. Once that starts, you can start the GemX service successfully.
    - THEN the webpage is available via Firefox, however it needed Flash.
    - Installed Flash v. 13 because that was the version available on IWEB that had both the Plugin and ActiveX installers. V. 14 did not have the plugin. That will need to be updated later.
    - The GemX login page now displays! Login cred are gemxadmin and gemxadmin. That loads too! Now I think Alex just needs to setup the configuration info for the hardware and we should be done with GemX.
* **TDANG** called saying that he emailed his DC firewall configurations to Nat on Thursday. Check with Nat to see if he received that email and if he responded to TDANG at all.
* Tobago already had KB2677070 and KB2813430 installed, even before I had ran the rvkroots.exe last week. I ran rvkroots.exe just now, and checked for Windows Updates. KB2917500 showed up. I installed the update, and now running a scan. I will run it on SNOOP next if it works.
  + **76464** still shows up on TOBAGO after the Windows Update. Installing rvkroots.exe again.
  + Time for another scan!
  + **76464** is still there… it shows up when I look at the dashboard, and in the vulnerability list, however it does not show up in the scan results directly after a scan.
    - I’m doing a scan on SNOOP to see if it shows up in the scan results for IT.
* Scanned **SRDTE-AD1** and **SRDTE-AD2**, and the **63155** “Unquoted service path” vulnerability no longer shows up in the scan results. Though it still shows under “Vulnerabilities” and “Dashboard”.
* **Tobago** upgraded **WinSCP** on the workstation and rebooted. Scanning…
  + Doesn’t show up anymore in Scan Results, looks like it’s gone!
* **SNOOP** upgraded **WinSCP** on workstation and rebooted.

# 7/29/14 – Tuesday

* **SNOOP** installed rvkroots.exe, checked for windows updates and **KB2917500** popped up. Time to install.
* **NAURU** installed rvkroots.exe. Installed existing updates. After reboot, **KB2917500** shows up.
* **ANTIGUA** installed rvkroots.exe. Installed existing updates, and rebooted. **KB2917500** appears. Installing. Rebooting.
* **SRDTE-AD1 SRDTE-SD2**, tried Windows Updates but they failed. Probably caused by the Blocked OU.
* **73983 Microsoft Common Controls** Tried installing all the update files that I had installed from DISAs patch repository. **Kb2810073** said it was already installed, however when I looked at my installed updates (via control panel) the install date lists today, 7/29/14. So now I’m re-scanning on ACAS.
  + **MSCCOMCTL.OCX** was present in System32 with a version number of 6.1.98.34. It is also present in SYSWOW64 with a version number of 6.1.98.39. I’ve cut the file from System32, and placed it in my javery folder on the SWAN share just in-case. Rescanning. Vulnerability Gone
  + Rescanning **TOBAGO** to verify the vulnerability in the scan results, apply the fix, rescan, and (hopefully) see the vulnerability disappear.
  + To fix ACAS vulnerability plugin 11457, I changed the value of HKLM\Software\microsoft\windows nt\currentversion\winlogon, from 2 to 0.
* Launching a scan on **GEMX** after applying a vulnerability fix for plugin 57608. It got a bad scan last time, let’s see how it does this time. I wonder if the GEMX software and it’s extra applications is preventing the scans, just like on KUKULA.
  + Clean scan!
* **SRDTE-AD1** was getting hit for the same SMB vuln that GEMX had. Changed the local group policy on the machine according to the solution given by ACAS. Rescanned, but it doesn’t come back with a successful scan. It only shows **Authentication Failure**.
* **LANAI** getting BAD scan. Authentication failure. Rescanning…
* **The new Win7 stig mentions something about AUDITING. Paul Plummer has some things already setup that takes care of it from a domain level.**
* **LANAI** updating VSphere client.
  + also fixed the **MS Common Controls** vulnerability by removing the old version of mscomctl.ocx from System32, after ensuring that KB2880971 and KB2810073 were already installed.

# 7/30/14 – wednesday

* **CAYMAN** installed the fix for rvkroots.exe
* **BARBADOS** installed fix for rvkroots.exe. Also installed update for vSphere client.
* **SWAN-VCTR** got funky and stopped allowing us to connect through the client on 7/30/14 around 2:00pm. Restarted the server, and that fixed the problem.
* **TORTA-PC** troubleshooting WMI Installer issue w/ **Aaron Gould**. Added his machine to a Blocking OU to rule out the possibility of GPO interference as the cause of his problem. The problem remained after blocking all GPOs. The problem is on his end.
* **LAST LOGON TIMESTAMP** tested and create a write-up for the process of enabling Last Logon Timestamp info on user logon, on stand-alone machines, using local group policy settings.
* **.MA / Security Group Planning** the plan is to create a test “Lab OU” on SSCPAC. Create an OU, create an .SA account just like a lab admin would have, then set it so that the .SA account can create .MA accounts if needed.
* **Caicos**  Todd got a **Temporary Profile** message when he logged in. Probably because he deleted his old directory on that machine. Look into the fix that Josh Bregler had given me about deleting the user profile’s SID from the registry, or at least renaming it.
* **Continue the Stark Lab test proj. create users and move CAICOS**

# 7/31/14 - thursday

* Wrote monthly status report and emailed to Mike Delira.
* How to make .MA groups for each project Lab OU work??? We’re only considering SSCPAC and SWAN, not all the other domains.
  + Look at how we’re currently implementing it with SRDTE: what is the “SRDTE Member Server Admins” group currently used for?
    - Currently just a way to grant administrative rights to .MA accounts on machines. The GPO “SRDTE Member Server Admins Group to Administrators” is pushed to all machines in the “Member Server” OU.
  + If we follow the same structure that is currently used in SSCPAC, then there would have to be some kind of Project Lab *Member Server* Admin group added to *each* lab’s OU. There are **59 Project Lab OUs** currently, so 59 of these individual Lab Member Server Admin groups would need to be created, and then considered each time a new OU was made.
    - Probably add these Project Lab Member Server Admin groups to the “SSCPAC Groups” containter.
    - Do they need to be a member of “Project\_Admins” ?
    - Should we rename “Project\_Admins” to something like “Project\_Workstation\_Admins” and create a “Project\_Member\_Server\_Admins” group?
      * If we do this, do we then need to create a parent Group to hold all the types of Admin groups in? Would this ever be necessary?
      * **Probably go with this solution. If Admins need .MA accounts, they notify us**
  + Just to make sure that I’m seeing all member servers, do a WMI query on the Product type (was that it?) #3
    - Get all AD machines | show only machines where producttype == 3
* **CAICOS** doesn’t seem like it’s talking to HBSS properly. Getting McAfee virus definitions notice on ACAS
* **Create a Member Server Admin group for Stark Lab. Create an MA account and test to see if the MA account can then create other MA accounts. This would allow Mas to create other MAs and not need to bug Service Desk or SWAN constantly.**

# 8/1/14 – Friday

* Time to start creating the Project Lab Member Server Admin groups.
  + …Member\_Server\_Admins groups have been created for each project lab.
* Keep in mind that each OU has a GPO that pushes the System Administrators group to the BUILTIN\Administrators. Each of these will need to have WMI Filtering applied so that they only affect workstations.
* **Add\_<NAME>\_Member\_Server\_Admins\_to\_Administrators**
* **Make sure that all the Member Server Admins groups are also members of their Lab\_Users group.**
* As Kyle said, a good idea would be to use a phased approach, and allow the Lab Admins to Administrators Group GPOs to apply to all machines – workstations and member servers, so that the admins have time to get used to using their .MA accounts to access their member servers. During this time, the .SA accounts will still be in the BUILTIN\Administrators group. After some time, we can apply WMI Filtering to the Lab Admins to Administrators Group GPOs to only apply to workstations. This should remove the .SA accounts from BUILTIN\Administrators on any member servers beneath the GPO.
* **Things needed for blog announcement:**
  + STIG ID Numbers and any special details about the stigs.

**START WINDOWS BLOG. Remember to discuss integrating IAVA ACAS fixes with the windows page as discussed w/ Adam. Work on the redesign of IWEB.**

# 8/4/14 – Monday

* Had roundtable meeting, here’s my To Do List:
  + Remove SPLUNK client from SRDTE-AD1 and SRDTE-AD2, and place them back into the proper OUs.
  + Molokai checklist for Jenny.
  + Create .MA accounts for the necessary admins, and make sure that they have permissions to create other .MA accounts and add to the proper groups.
  + Find what CAT severity level that STIG is that requires no more than 2 admins be allowed to connect to a server at one time.
    - The GPO involved is “Terminal Services – 2 Sessions” and it sets the setting for “Windows Components > Terminal Services > Terminal Server > Connections > Limit number of connections > Enabled (2).”
    - Still haven’t found if there is a GPO that requires this, otherwise I’m not sure why this setting was enabled.
* Currently .SAs do not have the ability to add other users to their own …Admins\_Group. To do so without granting “Full Control,” give access to:
  + - Read
    - Write
    - Create all child objects
    - Delete all child objects
* Have adjusted the Group Permissions on “SELF” to allow: Read, Write, Create all child objects, Delete all child objects

## COB

You still need to create the .MA accounts for all the admins in SSCPAC that administer Member Servers. Decide on how you will alert them – email or announcement at the meeting.

# 8/5/14 – Tuesday

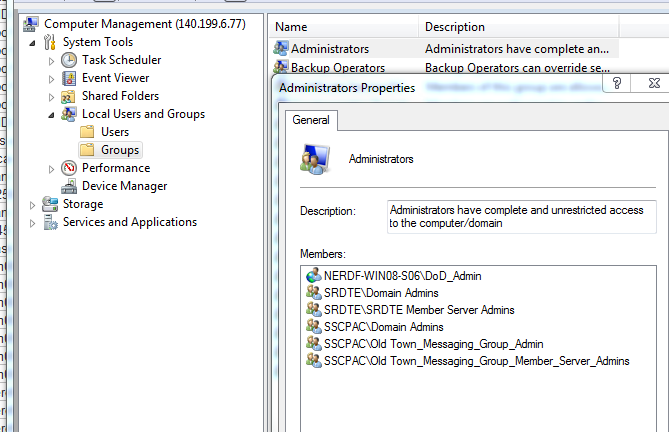
* Creating the .MA accounts. I should probably add each of them to the CLO Exempt – Privileged user accounts group since they are an .MA account and will not have a token or CLO enforced.
  + I see that some users are members of a group called CLO Exempt – SWAN PKI List and the description for this group says “users documented with PKI team.” What is the purpose of this group?
  + Created 17 .MA user accounts, added them to their Project\_Lab\_Member\_Server\_Admins groups and to CLO Exempt – Privileged user accounts:

|  |
| --- |
| * + - sronge.ma |
| * + - bhoskins.ma |
| * + - hintz.ma |
| * + - duclos.ma |
| * + - luna.ma |
| * + - laura.ma |
| * + - patryan.ma |
| * + - greg.ma |
| * + - tamj.ma |
| * + - ktrieu.ma |
| * + - lep.ma |
| * + - ntran.ma |
| * + - nphuong.ma |
| * + - rwill.ma |
| * + - woldeyes.ma |
| * + - tuanlong.ma |

* + How should these uses be notified? Be sure to notify the helpdesk as well!!!
* Communal Workstation for project admins to remote into (this workstation would have RDP documented and turned on) then they can do their ADUC stuff and be compliant with the STIG.
* The idea is to allow admins a 1 month adjustment period to start using .MA credentials on member servers. We will announce this at the admin meeting on 8/7/14, and the cut-off date for using .SA accounts on Member Servers will be the next admin meeting on 9/4/14.

# 8/6/14 – Wednesday

* Changed the “Default domain controller policy” on SRDTE, for the setting ComputerConfiguration > Policies > windows settings > security settings > local policies > audit policies > Audit directory service access, from “No auditing” to “success”.
* Change SACL for the OU “SRDTE Users and Computers”. Set the policy for Advanced > Auditing, added Principal: Everyone, Type: Success, Applies to: This object and all descendant objects.
* Looks like I can connect in to nerdf machines, some host names:
  + Nerdf-win08-s06
  + Nerdf-win08-s07
  + Nerdf-win08-s08
  + Nerdf-win08-s02



Screenshot 1: The BUILTIN\Administrators for 140.199.6.77 (nerdf-win08-s06)

* Finish and post the blog announcement, and see about how we get administrative account credentials to work on other DCs since we can’t add them to the BUILTIN\Administrators… we must need the admins to add our account to *their* “Domain Admins” group.

# 8/7/14 – Thursday

* Ran SCAP scan on MOLOKAI 🡪 95.54% [Green]
  + The plan is to fix any open issues in the checklist, and then re-scan. Then provide the SCAP results for Jenny.
* Blog Announcement for the Administrator accounts separation has been posted to the SWAN blog on the low-side.
* I gave the Service Desk the email announcement to send to the 16 users that I created .MA accounts for.
* **BGInfo**
  + the batch file:
    - start [\\xxx.xxx.xxx.xxx\netlogon\bginfo\bginfo.exe](file:///\\xxx.xxx.xxx.xxx\netlogon\bginfo\bginfo.exe) [\\xxx.xxx.xxx.xxx\netlogon\bginfo\bginfo.bgi /timer:0](file:///\\xxx.xxx.xxx.xxx\netlogon\bginfo\bginfo.bgi%20/timer:0) /accepteula
    - save as a .bat file somewhere in SYSVOL
    - Create a GPO (the tutorial does it in users)
      * User configuration > policies > windows settings > scripts > loogn > add that batch file from SYSVOL to the batch scripts tab
  + **Created** sysvol directory location \\srdte\sysvol\srdte.spawar.navy.smil.mil\scripts\bginfo
* KB555324 – CD Lockdown via gpo that Dave had us research into a little bit. We’re probably not going to implement it, but I wanted to record the KB number before I erased it off the white board.

# 8/12/14 – Tuesday

* Updated McAfee on KUKULA. Had to start the “McAfee Framework Service,” and the “McAfee Task Manager” to do so. Do these need to be stopped after the machine reboots? Were they turned off deliberately?
* Fixed **63155** on HONSHU. Placed quotes around registry path for C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\LMS\LMS.exe
* Installed patch to fix **73992** on HONSHU
* Fixed **76464** on HONSHU.
* Windows Last Logon
  + Computer Configuration > Policies > AdministrativeTemplates > Windows Components/ Windows Logon Options > Display information about previous logons during user logon ENABLED.
  + Applied GPO “Display\_Last\_Logon” to SSCPAC Domain controllers, and to COZUMEL via the “test” OU.
* WINUR-000005 “Allow log on locally” mandates that only “Adminstrators” and “Users” should be granted allow log on locally. For this to be applied in our environment without subsequently killing every normal domain user’s access, I would need to create a GPO that pushes the “SSCPAC Domain Users” and “SRDTE Domain Users” into the local Users group on all workstations.
* Moved GEMX vm to Blocking OU.
* Moved KUKULA from the KUKULA\_Exceptions OU to Blocking OU.
* Rolled JAVA on KUKULA back to v. 55. Now the GemX application loads in the browser. Have Alex do his migrations TOMORROW! While everything still works.

# 8/13/14 – wednesday

* Spoke with Anabel, Dave, and Kyle about the process for limiting admin account creation only to the Service Desk. We decided that we’d have the “delegators” for each OU listed in the description field for the OUs. This way, whenever someone sends the service desk a request for an admin account, they can first check to make sure that that person has the rights to request an administrative account be created. Then the service desk would check CSWF and the rest of the things they do.
* Went through and rolled back the administrative privileges for each of the security groups so that they no longer have the right to add members to themselves. I did this by editing the privileges for “SELF” on each group, and limiting it to the default options which are “Read” and “Read phone and mail options”.
* Put EMET 4.1 up on IWEB on the patches page for Guy Anderson to access. He says that upgrading from 4.1 to 4.1 upgrade 1 will screw the machine up and cause all browsers to crash. We might as well just skip to EMET 5.0 since it’s out, though it is going to need testing.
* **How to prevent project Admins from being able to change the description field?**
  + In Advanced Permissions in the security of the OU, under the entry for the appropriate security group, I unchecked “Write adminDescription”. I wonder if this will prevent admins from editing the description fields for users. That would be bad, since they need to be able to edit that for CLO purposes.
    - Unchecking that property DOES prevent the admin from altering the description field of any of their user’s in the OU. That’s a problem.
* The Pre-Scan best practices document on IWEB says to set LocalAccountTokenFilterPolicy to 1, however the STIG WINRG-000003 requires that it be set to 0.
  + 0 – Enables UAC remote restrictions.
  + 1 – Disables UAC remote restrictions.
  + More info at support.microsoft.com/kb/951016

## I spent most of the day trying to get the permissions setup properly to deny admins the rights to edit the description fields on their project OUs. The idea was to put the “Delegator” names in this description field, and that would be the authoritative source that the service desk would take requests from for .SA or .MA accounts. WELL, it turns out that this would cause a big mess with the permissions, so we’re not doing that. Instead, we’re going to add the names of the “Delegators” to the description fields of the Administrative Groups. Bayside\_Stark\_Lab\_Admins would have the names of its delegators in the description field, for example. To Do Thursday: - Get the names of the delegators and add them to these description fields.

# 8/14/14 – Thursday

* Bad ACAS scans on : MrPatch, SRDTE-AD1, PUKAPUKA, Galapagos, Midway, Nikoa, Lanai
  + What do all of these machines have set for LocalAccountTokenFilterPolicy?
  + HKLM\software\microsoft\windows\currentversion\policies\system\...
  + PukaPuka: 0
  + Galapagos: 0
  + Midway: 0
  + Nikoa: 0
  + Yet, other machines that had successful scans also have it set to **0**.
  + **Swanscan** account is locked out, and according to the attribute editor, it has been locked out since 8/6/14 17:30:02. Ask Chris if we are still using SWANSCAN for any scanning purposes, cause it’s not going to be working if we are.
  + It has only been 42 days since the password was set, so it shouldn’t be a password lockout issue.
  + 14.50 deleted dec 23 ’13, same with 14.51. . bldg. Barracks 365, 108.
* JAOC.RHINO
  + Thomas Dang sent an email with the new DC IP addresses, and DOM GUID. We will be using the same administrative account for his domain that we used previously: domadmin, pswd: Abcd\_123Abcd\_123. He is still going over the pre-scan checklists with his systems and will email us once they’re online so we can establish the trust.
* How should we decide who the delegates of .MA accounts are? Should it just be the same people in the .SA admins group? What if someone in the .SA admins group doesn’t have an IAT-2 cert? Does that matter?
* TO DO: cont. drafting process for Admin account creation by service desk. If Dave is here, see if he can update DNS info for JAOC, and then try to setup domain.

# 8/15/14 – Friday

* Created local group policy on GEMX to disable screensaver. That machine will be used as a monitoring system, so that’s why the screensaver needs to be disabled.
* Forcibly rebooted SRDTE-WSUS because it appeared to be locked up.
* Cont’d drafting Admin Account Creation Process document for the service desk. We will need to go over this with Anabel.
  + Email distro list issue: There is a SWAN\_Admins email distro list on the UNCLASS that is used to communicate with all SWAN Admins. Anyone receiving a new admin account on SSCPAC would need to be added to this distro list on the UNCLASS.
    - Apparently there is also a second email list that is used to notify “interested parties” as Todd called them, of events occurring on SWAN or meetings. These people aren’t necessarily admins but still want to be kept in the loop.
* Called DISA Helpdesk about the broken STIG download links for Windows 7.
  + Helpdesk guy said that DISA is no longer supplying STIG files on the classified network?
    - Doubtful, since they announced the new stigs on the STIG page with recent dates.
    - Helpdesk guy told me to email Webmaster, which I did. Will wait for reply.
* Researched some SCAP issues for Tien Nguyen, and replied back to his email.
* Moved the Win7 STIG v1r16 over to the high-side since I can’t download it from DISA at the moment. Running a scan on that.
* Installed RETINA engine on MOLOKAI.
* Emailed a list of domain controller ports to Thomas Dang. He needs to make sure that his firewall has them opened up so that we can try to establish the trust.

## to do monday: - check how thomas dang is doing on his firewall settings. Retry trust when he finishes configuring it. - check with chris about service desk procedure document. See if anything needs changing. - create updated documents to list the “swanroot” and “swanscan” and “trangj” and “ganzer” accounts in for MOLOKAI. - go back over MOLOKAI with manual stig and make sure everything is perfect for the audit. - Check and see if the Webmaster from DISA responded to my email.

# 8/18/14 – Monday

Trying to figure TBMCS stuff out

## to do tuesday - get with Thomas and have him allow me access to DC1. He probably needs to edit the local security policy on DC1 to allow access via terminal services and grant it to the proper group. Reference the error message that is displayed when attempting to log on to DC1 to see which group that is… - Once in, maybe try to reconfigure the time server.

# 8/19/14 – tuesday

* Get OU structure diagram for Scott
* Create a read-only account for Active Directory. Scott wants to get LDAP info.
* Local Computer Policy > Computer Configuration > Windows Settings > Security Settings > Local Policies > User Rights Assignment > “Allow Log on through Terminal Services” 🡪 Administrators
* The operation failed. The error is: A device attached to the system is not functioning.
* Error message when attempting to log in to DC1.jaoc.raptor.spawar.navy.smil.mil using domadmin:
  + “to log on to this remote computer, you must be granted the allow log on through terminal services right. By default, members of the remote desktop users group have this right. If you are not a member of the remote desktop users group or another group that has this right, or if the remote desktop user group does not have this right, you must be granted this right manually.”
  + Still couldn’t get in after Thomas configured “Allow log on through terminal services”. I had him try it from his workstation, and he couldn’t get in, so he’s working on figuring out what is preventing that.
* ~~Changing IDLE time out on SMB connections:~~
  + ~~Local Security Policy > security settings > local policies > seucirty options > Microsoft network server: amount of idle time required before suspending session. The default is 15 minutes.~~
* Changing IDLE limit for RDP
  + Local Computer Policy (gpedit.msc) > Computer configuration > administrative templates > windows components > terminal services > terminal server > session time limits > set time limit for active but idle terminal services sessions.
* Now to turn off screen lock…

## For Wednesday: ~~-Mark needs to sign off on the Privileged Account Letter that I had sent to Anabel. She felt that it would be more appropriate for him to sign off as the SDREN manager.~~ ~~- Check and see if the RDP window from SWANMONITOR to GEMX stays up. Everything will be great if you come in tomorrow morning, turn the TV on, and see the GemX app login screen!~~ ~~-Double-check with the Pauls that the Groomlake domain trust works. We set it up on our end, let’s see if they can do the same on theirs without it erroring out.~~ ~~-Setup Adam’s new token. ##########.C is his number. This will be associated with his normal user account only. Be sure to change the description field if there’s anything in it.~~ -Check with Chris and see where he’s at on the status of the Service Desk Admin account creation process doc. -change the password on SWANROOT on MOLOKAI and see about storing that password in the safe. -Separate Active Directory servers for people to log in to…

# 8/20/14 – wednesday

* Setup SWANMONITOR and TV w/ Alex. Alex will have to play with the resolution to get it how he wants it displayed.
* Received GPO from Guy Anderson for .Net Framework 4. This settings changes the “nibbles” in the registry regarding software publishing state rules. Created GPO in SRDTE called “DotNetFramework4\_software\_publishing\_state” and pushed it to NOC systems to test.
* Re-established the **trust with Groomlake**, working with Paul Zalesny.
* HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing\State, REG\_DWORD, value=0x00023c00 (146432).

# 8/21/14 – thursday

* **Completed DTA training!!! Emailed DTA training to Jenny, she will have to sign off and submit to the IAM.**
* Patched a bunch of systems.
* Brought Kukula and Gemx back into the proper OUs, and pulled down GPOs.
* Setup Alex so he can remote into SWANMONITOR through DameWare using his Oregela account and CAC card.

## For Monday: -1.) Check inbox for MOLOKAI Retina report that Chris sent me. Review the report, check the settings, expect some false-positives, and report back to Chris. -2.) Scott’s Win7 VM needs to have the proper firewall exceptions made so that it can talk to the DCs…maybe? At first we couldn’t ping srde.spawar.navy.smil.mil, and it seemed like DC4 being in the DNS records was the problem. But eventually we could ping the domain. The system still couldn’t join the domain, giving an error message saying that a domain controller could not be contacted. Troubleshoot, with Dave. -3.) See how Chris is doing with WSUS. I need to have patches done, and WSUS is preventing me from being able to pull the correct MS patches. There are a bunch of vulnerabilities… -4.) See if Anabel received my email and has reviewed the Service Desk Admin Account creation process…. -5.) Setup Todd for alt token.

# 8/25/14 – monday

* Performing rolling snapshots
* **KUKULA** was still showing up on ACAS with out-of-date McAfee definitions. According to ACAS, the DAT version should have been 7528, while its signature showed as 7526. Once I applied a successful update, the DAT version was 7539, significantly higher than what ACAS said it should have been. I also turned on the McAfee McShield, McAfee Framework, and McAfee Task Manager services to facilitate the update. I’m leaving the system on and screen-locked for a day so a good scan can verify that everything is current.
* **Todd’s Token** has been re-associated with his account. The letter was all that changed.
* **SRDTE-Web1** investigating problems with crash/lock-up. Looking through logs.
* **TCAC** OU built for Keith Hanson, with accounts, and GPOs. Finally got his machine connected
* **GemX / SWANMONITOR** potentially (finally) got RDP to NOT idle-timeout the session. There was a conflicting GPO from when Johnny was here that was setting the idle timeout at 15 minutes. I set that to unlimited. Also set it so that disconnected sessions never timeout.

# 8/26/14 – tuesday

* We could probably setup GemX’s web application to be reachable outside of GemX, and have it act as just the server. But that’s a project for a later date.
* **SWANSCAN** **KILL DATE – SEP. 4TH** :
  + Turn off GPO on SSCPAC, “add\_SRDTE\_DOMAIN\_ADMINS\_TO\_ADMINISTRATORS\_GROUP”
  + .
* Updated SWAN Lab/Project Standard Operating Procedures (SOP) document to v.15 and uploaded to IWEB.
* **Ask Dave how to set permissions so “webmaster” is listed**
* **SPLUNK**
  + What is the avg. workstation log usage? : ~150MB/day 🡪 2.5% of daily limit (5.997GB)
  + What is causing peak logging on Fridays? : logging from stor
  + 7 more machines to add to SPLUNK. 7 x 150MB = 1050MB 🡪 1.02GB extra on average extra will be logged daily.
  + Total logged daily avg : 2.5GB (42% of quota)
  + Projected increase to: 3.52GB logged daily (59% of quota)
  + Add 10 more machines (10 x 150MB = 1500MB = 1.46GB) 3.52GB + 1.46GB = 4.98GB (83% of quota)
  + Find avg indexed per DC: ~230MB/day 🡪 3.7% of daily limit (5.997GB)
  + Add 1 DC (.224GB + 4.98GB = 5.20GB) 86.7% of quota
  + Command Supposedly to get indexed by host:
  + **index=\_internal source=\*/metrics.log\* group=per\_host\_thruput | chart sum(kb) by series | sort - sum(kb)**
* make files in BALI available to the webmaster: **chgrp webmaster <filename>**

## TO DO WED: -put above data about SPLUNK into an excel matrix for better visibility**GOOD** -~~Check and make sure GemX is still up and good on SWANMONITOR~~**GOOD** ~~-search splunk logs on Thursday evening, or Wednesday morning, on keyworkd “shutdown” to look for unexpected shutdowns and crap…~~

# 8/27/14 – wednesday

* Drafted SPLUNK logging projection report
* Starting script project
  + What is the purpose of this script? : To auto-enforce CLO on accounts.
  + Peter’s IA Account Status Report shows CLO enablement and enforcement, what is the difference?
  + User accounts / attribute editor / userPrincipalName = [1464051615.E@smil.mil](mailto:1464051615.E@smil.mil) . Maybe this can be used to distinguish whether or not an account is CLO enabled.
* Reading up on ADSI for PowerShell. Low-side PC, firefox bookmarked in “Domain” folder under “Managing Active Directory…”

# 8/28/14 – thursday

* Wrote up Deletion process for service desk with SA and MA accounts, got it approved by Anabel, and added it to Pat’s SOP document.
* Applying a handful of patches to Molokai, had to migrate them over via IWEB. 051 didn’t install… so far the others are fine. 49, 47, and 46 have installed.

# 8/29/14 – Friday

* Cleared up problems with Retina report
* Wrote POAM for open and false-positive findings
* There are accounts on SSCPAC that are set for **Password Never Expires .** Here’s what I’ve done.

|  |  |  |
| --- | --- | --- |
| sAMAccountName | Display Name |  |
| 1112360332.C | Eroica Johnson | Unchecked psw never expires. Checkbox is already checked to require smartcard. |
| 1249550791.E | Derek A. Fox | Unchecked psw never expires. Checkbox is already checked to require smartcard. |
| 1295989820.E | Patrick W. Kingsland | Unchecked psw never expires. Checkbox is already checked to require smartcard. |
| Ktrieu | Kim T. Trieu | Unchecked psw never expires. Checkbox is already checked to require smartcard. |
| Test123 | Test test | Unchecked psw never expires. |
| Tingley | Gary Tingley | Unchecked psw never expires. Checkbox is already checked to require smartcard. |
| 1135772379.C | Mark Zeigler | Unchecked psw never expires. Checkbox is already checked to require smartcard. |

KEEP Working On Script.  
Talk with Todd to try and understand the entire CLO smartcard process, and where the HECK the legit, authoritative exemptions list is, how people get on it, and what the process for updating it is…

# 9/3/14 – Wednesday

* Still working on CLO exemptions / enforcement script
* Worked with Mark Darrieulat of the NCTSI external domain to setup a temporary 2-way trust, so he could pull over the swanscanner.[SA/MA/DA] credentials .

## To Do: - check if Don responded to email with Draycor account # - check if Thuy responded back about CLO exception list questions. Call her if not 553-4691 - Prep for Admin Meeting! - Finish script. - Double-check that checklist for MOLOKAI is up-to-date -Map out in pseudo-code the IF THEN logic of the existing IA Report script. That way I have a better idea of what to filter out for

# 9/4/14

* Admin meeting.

TO DO Monday:

* Check and see if Marc Wilson emailed me the price quotes. Cc’d Allison Dray.
* Assisted Scott with moving SCAP files over to his NEXCAN VM

# 9/8/14 – Monday

* Assisted Scott with moving SCAP files over to his NEXCAN VM
* Corresponding with Marc from SPLUNK, and Allison from Draycor.

# 9/10/14 – wednesday

* Changed Win\_7\_base\_gpo\_v3. Here are the old settings:
  + Deny access to this computer from the network: SRDTE\Support\_388945a0, SRDTE\NoGuests, Guests
  + Deny log on as a batch job: SRDTE\Support\_388945a0, Guests
  + Deny logon as a service: (not defined)
  + Deny logon locally: SRDTE\Support\_388945a0, Guests
  + Deny logon terminal services: <not altered> Everyone
* SWANMONITOR is locking the screen again. Making a new set of GPOs to apply to swannet “SWANMONITOR\_Prevent\_Lockout”
* User configuration > policies > admin templates > control panel > personalization
  + Enable screen saver: DISABLED

# 9/11/14 – thursday

* Troubleshooting problems with Display Last Interactive Logon, setting.
* Troubleshooting problems with replication on SSCPAC. SSCPAC-DC3 was turned back on and had replication problems.
* Test .SA separate AD group thing…
* Changed permissions that “Old Town\_Messaging\_Group\_Admin” group had on the OLD Town\Messaging\_Group OU
  + OLD Permissions:
    - Create computer objects
    - Delete computer objects
    - Create group objects
    - Delete group objects
    - Create user objects
    - Delete user objects
  + NEW Permissions:
    - Full control
* Finally adjusted the WMI filtering on SSCPAC GPOs that push LabAdminGroups to machines in Lab OUs.
  + GPOs that push LabAdmin.SA 🡪 WMI Filter 🡪 Workstations Only
  + GPOS that push LabAdmin.MA 🡪 WMI Filter 🡪 Member Servers Only
* After lunch, keep working on SSCPAC-DC4 VM. Get IA SIPR request form from the blog and submit.

FOR FRI: Keep working on SSCPAC-DC4.

# 9/12/14 – friday

* CLO Enforce script on SOUTHBROTHER will only run if an admin is logged in. Make sure that admin acct stays logged in over night so the script can run. STIGS prevent us from saving the password in Task Scheduler and running in without being logged in…
* Taking Snapshots
* Added SSCPAC-DC4 to domain. Applying all the goodies!
* GEMX Needs patches:
  + MS14-051
  + MS14-052
  + MS14-045
  + MS14-046
  + MS14-049
  + MS14-053
  + Upgrade to Firefox 32.0+
    - Previous ver on Gemx: 31.0
  + Upgrade to Adobe flash player 15.0.0.152, or 13.0.0.244 for systems that can’t be upgraded past 15.xx
    - Prev. Activex 13.0.0.241
    - Prev. plugin 13.0.0.241
* SWANMONITOR needs patches
  + Firefox 32.0+
  + MS14-052
* SUCCESSFULLY Updated patches on GEMX/SWANMONITOR. Keeping the TV on now to monitor it’s uptime incase it times out or does odd stuff.

FOR MON: Finish patching workstations. Mark and Nat’s systems need a few things. Montego too if I didn’t finish it on Friday.

Rebuild Jenny a new workstation.

TUESDAY: Touch-base w/ Thuy regarding the PKI request screenshot I emailed her.

* Be on the lookout for a reply from LT. Dailig regarding the Risk Assessment form.
* Build Jenny a workstation for PAC.

# 9/16/14 – tuesday

* Rebuilt workstation Windows 7 Pro for Jenny.
* Building SSCPAC-DC4. Sent

WEDNESDAY: Keep applying updates to Jenny’s new macine. Finish script stuff… the notes I made about improving the arrays.

# 9/17/14 – wednesday

* Building 2 laptop workstations…
* Troubleshooted port connection problem on the workbench.

## Server cert for SSCPAC-DC4 is complete. Cont with instructions on the PKI SOP from page 20. Follow instructions extremely carefully! - Keep doing updates on ThreeMile so it gets completely configured. - Keep working on script.

# 9/18/14 – thursday

* Working on script
  + New-item –path <path> .name <name> -ItemType file
  + $header = “username,fname,lname,comment”
  + $header | Add-Content test3.csv
  + $outputdate = (Get-Date).ToString(‘d’)
  + 9/18/2014
  + $outputdate = (Get-Date).ToString(‘T’)
  + 9:35:28 AM
* FOR MONDAY:
  + Script seems pretty much done. Double-check with Anabel and “arm” the script.
  + Install certificate on SSCPAC-DC4.
  + Install that list of applications on the laptops that Alex mentioned. Refer to the old XP laptop for application list.
  + Check w/ Kyle about DameWare license management so I can install DameWare on PAMATI for Jenny.

# 9/22/14 – monday

* Troubleshoot CPU1 fan error on NAURU in datacenter
* Finished final edits of .csv file logging on CLO Enforcement script, got Anabel’s approval, and armed the script.
  + Ran the script, 31 user accounts auto-enforced. Script will continue to run every Mon-Fri at 18:55.

# 9/24/14 – wednesday

* Sent report to Laura Salazar regarding problems with SSCPAC-DC4 and the DC\_Tools scripts.
* Setting up workstation for Scott
  + –finish installing updates
  + –do a remote SCAP scan from GALAPAGOS to see what it scores. I’d like to use it as a test baseline machine to see what I can possibly do about the local machine settings. Would it be possible to use the Security and Analysis snap-in to export pre-confiugred settings, and them push them via GPO to machines?
* Need to draft a complete end-to-end SOP for building workstations.
* Things to be updated regarding Win7 STIG GPOS:
  + First score: 97.67%
  + 3.063 Anonymous Access to Named Pipes. Our machines have stuff listed. It wants NO STUFF listed :/
  + 4.022 BUILTIN\Administrator hasn’t been renamed. Shouldn’t a GPO do this? Is this because I already created an account called “swanroot”?
    - Renamed to “xAdministrator”
  + 5.260 Unnecessary features installed. Windows Media Center. SimpleTCP Services, Telnet, TFTP Client.
  + WINGE-000200 DenyNetworkAccess doesn’t have local accts that are members of “Administrators”
  + WINUR-000017 DenyNetworkAccess is set for the security policy, yet still doesn’t have proper accts in it
  + WINUR-000021 DenyNetworkAccess is set for remote desktop policy, yet doesn’t have proper accts in it.
  + Second score: 98.84%
* Built JEDI-JENM domain for Ed VanHouten
* Troubleshooting issue that LCDR Trevino was having joining system to domain. Possibly a DNS problem? Machine was imaged w/ PAC. Instructed him to re-image the machine.

# 9/25/14 – thursday

* Found fix to my problem with the DCInfo script. I was running it in a profile signed in with credentials from the parent domain. Once I signed in with child domain credentials the script ran fine. Going to wait until non-peak hours to fire up SSCPAC-DC4 and continue the process. Will need to re-request a cert from Thuy.
* Received request from Henry Serranoh for his OU request. Need to build it. Following SOP I created for making new OUs.
* OU Created. Email sent to Henry including instructions for connecting to our new AD servers.

FOR FRI:

* Call Thuy and see about status of certificate request. SSCPAC-DC3 needs to be demoted as soon as possible. That thing is causing problems. Get SSCPAC-DC4 up and cert’d as soon as possible.
* Start building Nat’s machine. Make a step-by-step checklist of the process. Use high-ish level steps. All the way from requesting an IP address to finishing installing final software.

FOR MONDAY: Look through the gpresult58.html file in the RSOPs folder of the shared drive, and try to find out why Henry Serrano’s machine can’t remote log on to SSCPAC-AD1 or any of the other AD machines.

-Keep working on the box that will be going down to datacenter

-Image a new box for Nat at some point. Be sure to create an SOP for the process as you go along.

# 9/29/14 – monday

* Ed VanHouten is still having problems installing SCM90Meter on his JEDI-JTNT box. I told him to try un-joining it from the domain, and then installing .He was getting some “admin settings do not allow installation” error message when he tried before, even though his pc object was being blocked from receiving GPOs.
* See if Henry sent the error message back so I can further troubleshoot
* Work on installing the new certificate on SSCPAC-DC4
* Take a look at the checklists that Alex and Jenny have and use on new workstation builds.
* Scanned COZUMEL. Results 97.67% Unnecessary features installed (5.260). Built-in admin account status (4.039). GPOs should have this set…
* Need to have the firewall opened up for SSCPAC-DC4 so it can talk to OCSP. Also need to have a good scan completed on it before we open it up to “SIPR” from “SIPRNET – PENDING”
* Mitigate the 4 vulnerabilities that it shows for SSCpAC-DC4

# 9/30/14 – tuesday

* Troublehsooted “no domain trust” error that Woldeyes was having with SWAN.50.74 . Since he could not logon locally to unjoin from the domain and rejoin, I instructed him to just shut down the machine for 15 minutes, unplug the network cable, and then plug it back in. We’ll see how it goes. Here’s hoping…
* Installing updates on SSCPAC-DC4 so that I can have it switched over to full “SIPRNET” connectivity so that it can talk with the PKI OCSP servers. Need to scan it again after updates are applied. Hoping that everything gets cleared up and it’s just a handful of KBs that need installing.
  + Seems to be stuck on update #5, KB2975719, Update for Windows Server 2012 R2.
* Doing a SCAP scan on NAURU to see how it goes. Hopefully it will have most everything covered. Last time I ran a scan on COZUMEL, it showed up that the local administrative account was not disabled, even though the GPOs were set to disable it. It apparently needed to also be set locally via the Security Configuration and Analysis snap-in.
  + 2.021 Software certificate installation files
  + 4.039 Built-in Admin Account Status Why does admin account NOT come up as disabled when GPO is set?
  + 5.260 Unnecessary Features Installed Windows Media Center features…
  + WINGE-000200 DenyNetworkAccess known-issue
  + WINUR-000017 Deny access from the Network DenyNetworkAccess known-issue
  + WINUR-000021 Deny log on through Remote… DenyNetworkAccess known-issue

# 10/1/14 – wednesday

* LCDR Trevino called, turns out that his problem adding that workstation to the domain was due to his .SA account enforced for smartcard login. You cannot adda machine to the domain using smartcard. I unchecked smartcard enforcement, set his password, and instructed him to try adding the machine again. I haven’t heard back from him since.
* Woldeyes could not do anything on WKS5 with administrative credentials. He had not moved the machine object from the transient OU, so I instructed him how to do that, and told him to reboot the machine. Haven’t heard from him since.
* Installed software on Nat’s machine, and now applying updates.

FOR THURSDAY:

-ADMIN MEETING!!!

-FAKARAVA is not on my list of assets in ACAS. Why? Need to scan so we can take it off SIPR – Pending

- install Visual J# 2nd ed so that vsphere can be installed

-install Splunk last. Clear logs fisrst so we don’t bloat splunk.

-install that software on the 2 laptops per the list Alex emailed that I printed out.

-examine Paul Plummer’s script for DenyNetworkAccess.

FOR MONDAY:

-go thorugh my list of stuff for the Windows GPO Copmltete project on One Note and see if I can apply most of that to my machines via Security Templates.

-after that, give Nat his machine finally…

-also look over the script files that Paul sent in.

# 10/6/14 –monday

* Test to make sure that the exception STIG actually works, then test it on the CTB machines to verify that this really is the setting that they need to have disabled. Once we know that it’s the setting that needs to be disabled, then I will turn the setting back on, and have them fill out an IA Special Request on the high-side to send in to IA for exception approval.
* Demoted **SSCPAC-DC3**
* Remotely disable MediaCenter feature on machines via PowerShell by executing CMD line:
  + Invoke-Command –computername <computername> {dism /online /disable-feature /featurename:MediaCenter /norestart

# 10/7/14 – tuesday

* Tried to disable the MediaCenter feature via WinRM in PowerShell, only to find out that the WinRM service isn’t started on a lot of my workstations.
  + Created a GPO on SRDTE called “Create\_WinRM\_Listener” to start the WinRM service, and allow listening from all IPs on it.
  + This will allow me to use “Invoke-Command” via powershell on my workstations to accomplish tasks…
  + I can’t automatically push Gpudate to machines, so I’ll have to wait for the machines to automatically check in. Every workstation should be good to go by about 10:45a.

For WED:

* See OneNote workbook for project notes and To Do regarding DenyNetworkAccess script
* Check and see how Tod Hintz is doing with the 2 workstations he emailed us about yesterday that were having KDC problems and couldn’t log him in using smartcard.

# 10/8/14 – wednesday

* FINISHED DenyNetworkAccess script AND IMPLEMENTED IT! BOOYAH!

# 10/9/14-thursday

* So for some reason my Workstations that are on SSCPAC in the StarkLab OU are coming up at 50% (RED) on SCAP scans…
* Created script to run on SHUTDOWN on workstations to disable MediaCenter feature.
* FOR TUESDAY:
  + Do a SCAP scan on one of the machines in datacenter. TOBAGO is taking waaay too long.
  + It seems like machines aren’t having the admin/guest accounts disabled and renamed properly like they should
  + Test the “enhanced” Windows Feature disable script to make sure it actually works. It seemed like things were failing unexpectedly when I tried running it on NAURU. I’m also afraid that unchecking all of the games won’t actually uncheck the final “Games” box and that it will still show up on the hit list. Take a look at that.

# 10/15/14 – wednesday

* Potential GPO causing problem: “Mapped Drives for SRDTE Staff Users” . This is also suspicious:

|  |  |  |
| --- | --- | --- |
| Group Policy Drive Maps | Pending | 10/14/2014 7:09:53 AM |
| |  | | --- | | Group Policy Drive Maps did not complete policy processing because the user needs to log on again for the settings to be applied. Group Policy will attempt to apply the settings at the user's next logon.  Additional information may have been logged. Review the Policy Events tab in the console or the application event log for events between 10/14/2014 7:09:53 AM and 10/14/2014 7:09:53 AM. | | | |

Group Policy dependency (Network Location Awareness) did not start. As a result, network related features of Group Policy such as bandwidth estimation and response to network changes will not work.

# 10/16/14 – thursday

* Keep working on the big GPO troubleshooting list.
* Block (55-59) may hold one of the offending GPOs. After applying that block, I got flip-flopping time results at logon, consistently switching between times of 1:40 and :07 each try usually after a gpupdate or just a standard reboot, respectively. However it gave me another longer 1:40 logon time after just a standard reboot, so something is wrong there. When I come in on Monday, try to logon using javery.sa on CAICOS, and time the logon. Then do a reboot and time it. Then try it with a gpupdate. Hopefully I’ll notice a pattern, or something that looks promising. Then unlink the entire (55-59) block and do that same reboot/logon process tango again. Hopefully that time the loogns will all remain consistent and short, telling me that one of the gpos in block (55-59) is where my problem is.
* So it looks like Loopback policies were the problem. Now I’ll need to find he GPOs on SRDTE with loopback that are causing problems, and also fix the 2 gpos that had loopback so that they’re still applied correctly.

FOR TUES:

Take one of the SRDTE-AD1 or 2 VMs off of the domain, blow the current OS away, reload windows… do a SCAP scan. See what the score is. Then try to load the security template on the machine, and re-scan with SCAP. If all goes well, the score will be close to 100%, or somewhere around 99.60% , that would be ideal.

THURS: The GPO “Install\_Fixit\_51026” has been created in SRDTE, with WMI filtering to only apply to machines with Microsoft Office installed on them. I’ve linked it so that it’ll touch all NOC workstations. Time to see how it goes. Need to push EMET 5.0 to all NOC workstations as well. SSCPAC, strangely, does not have a GPO that pushes EMET to machines. Is there a reason for this?

# 11/03/14 – monday

* Pushed out the Install\_Fixit\_51026 GPO to the SSCPAC domain. WMI filtering should ensure that it is only pushed to machines that have Microsoft Office installed.
* Error when logging on to SSCPAC-AD3 w/ smartcard:
  + The requested key container does not exist on the smart card.
  + Testing this on SSCPAC-AD4. The Smartcard service was disabled. Going to start the service, set to automatic, and reboot to see what happens.
  + The servers need to have .Net 2.0 installed to install
  + Installed via “Manage” installing .NET Framework 3.5 Features (Includes .NET 2.0 and 3.0)
    - Installation failed. Error 0x800ff0907. Rebooting.
  + According to Guy Anderson, the 90Meter software must be installed using an RDP session, NOT a console session, and with an administrator account.
  + Need to install the RootCerts…this requires that JAVA be installed.
  + Installed Java 7\_72.
  + **SUCCESSFUL STEPS:**
    - Mount Server 2012 .iso (not the one that end’s in “dev”)
    - Run the powershell command Install-WindowsFeature –name NET-Framework-Core –source D:\sources\sxs
    - Ensure that .NET 3.5 has been installed
    - Install Java
    - Install DoD Root Certs
    - Re-install Tumbleweed
    - Install 90 meter. ( via RDP!!)

# 11/04/14 – tuesday

* Here’s the useful **WMI Query**: Get-WMIObject –Query “SELECT \* FROM something WHERE this=that” –ComputerName <name>
* FOR WEDNESDAY:
  + Update the blurb about poodle since I had to add the option for “CLIENT”
  + Reboot machines, cause they’re going to need fix applied.
  + Yeah…Keep working on task list in MS OUTLOOK.

# 11/05/14 – wednesday

* Finished the software audit list for Jenny, and emailed it back to her.
* Finished editing write-ups on the IAVA and ACAS Fixes page for POODLE and OLE.
* Sent email to admins regarding vulnerabilities and their fixes.
* Created slides for the admin meeting tomorrow.
* To Do Thursday:
  + MEETING DAY 9:00am!
  + Figure out how to do Firefox STIGS
  + Double-check the file share problem on the DCs. The WINUR-000017-MS stig should be unlinked in the morning. Test if the access to shares still works. If it does, re-link the GPO, wait 90 minutes, and see if it affects access to the shares.

# 11/07/14 – friday

* Time to deploy out the Mozilla.cfg file to all workstations that have Firefox installed.
  + Mozilla.cfg goes in c:\Program Files (x86)\Mozilla Firefox
  + Local-settings.js goes in c:\Program Files (x86)\Mozilla Firefox\defaults\pref
* 2012 DC STIG GPO break up
  + Currently, a lot of the STIG settings being pushed to DCs are all contained within one GPO. This is big and bloated, and makes it difficult to troubleshoot which settings are causing problems, since turning off the one GPO disables multiple settings.
  + I will be working on going through the 2012 DC stig, and creating individual GPOs for each STIG setting, but I not linking them immediately. Again, create the GPO, do not link it. This will be taken care of later.

# 11/10/14 – monday

* Roundtable meeting!
* Created SQLSERVICE.MA and SQLSERVICE.SA accounts for Scott, and added them to the member server admins and workstation admins respectively.
* Filled out IAM Special Request form for javery.ex and klauro.ex accounts. Those accounts will replace stark.sa (shared) account.
  + Need to change the stark.sa account and split it out to two accounts, one each for Kyle and I.
* FOR WED: Keep working on DC checklist, and the to-do checklist written in my journal.

# 11/20/14 – thursday

Get a data call list of all servers on sscpac and their administrators. We need to link the 5 GPO’s that deal with .MA stuff (on my paper) directly at each person’s OU, and set the inheritance above the Win2K8 GPO so that the settings take.

FRID: Keep working on figuring out how to successfully delegate all group policy controls, using the stark.sa account. Need to figure out how to alternatively give sronge.sa permissions to edit his group policy w/o being a member of Group Policy Creator Owners…

# 11/21/14 – friday

* Was able to delegate rights to create GPOs by adding the user to the GPO container, in the delegation tab.
  + Now the user can’t edit the GPO they create, from the server, because the Group Policy Management Editor snap-in is disabled…
  + Going to enable the “Group Policy tab for Active Directory Tools” and “Resultant Set of Policy snap-in” on the GPO-007-WT\_ADServerLockDown gpo
  + Also enabling everything in the Group Policy Snap-in section. Kyle already had “Administrative Templates (Computers)” and “Administrative Templates (Users)” enabled. I’m enabling the rest of them too.
  + Also enabling everything under the Preferences container.
  + None of that worked.
  + Trying to unlink the GPO and see if that does it…
  + Changed the “Restritc user sto the explicityly permitted list of snap-ins” from “Enabled” to “Disabled”. I don’t think we need to be that specific with the restrictions. The user’s aren’t going to have administrative privileges anyway, so even if they can open snap-ins, they have no power.
* Settings to apply to delegate GPO rights on the Lab’s OU container:
  + Create groupPolicyContainerObjects
  + Delete groupPolicyContainer objects
  + Read gPLink
  + Write gPlinnk
  + Read gPOptions
  + Write gPOtions
* Settings to delegate GPO creation rights on GPO container:
  + On the “Delegation” tab, just add the user’s name, or group.

MON: Patch NAURU…and the rest of the machines in datacenter that keep getting failed scans…

# 11/24/14 – monday

* Linked the .MA GPOs on the Sailor domain, STIG-WINUR-000017 – STIG-WINUR-000021 .
* Added EnPasFlt .dll to SRDTE-DC4. Restarting system.
* Spreadsheet created to track checklist files and Kyle and I go through and update every checklist. It’s saved as “2015 Audit Checklist Tracking Sheet” under the STIGs folder on the Windows Admins share.

FOR MONDAY: Finish working on the checklist 100% completion list. Work on getting SSCPAC-DC4 100% stigged. It looks like the default domain controller policy for SSCPAC is just going to need to be updated. Be sure to note everything in change management!!!!

# 12/1/14 – monday

* Working through the checklist checklist and getting the servers up to 100%. Currently editing the Default Domain Controller Policy to fix 2 incorrect settings on SOUTHBROTHER.
* Sscpac\sysvol admin templates freaking out on sscpac DCs when trying to view admin templates in RSOP: srm-fci.adml/admx TerminalServer-Server.adml/admx VolumeEncryption.adml/admx FileRevocation.adml/admx
* TUES: Keep working on the servers left on the checklist list. Only 8 more to go. Then probably start building that server for the SolarWinds demo…

# 12/2/14 – tuesday

* Finished up getting my servers to 100%. Kyle said he’d work on getting all the SSCPAC-AD# servers up to 100%, there are four of them.
* Troubleshooted a call with an admin of system “S-COMPLAB21” where the new patch for Flash 15.x would not install the ActiveX portion. The plug in would install just fine, however it would throw an error message saying that the ActiveX control for flash player could not be registered. I couldn’t figure out exactly what the cause was, so the admin said he would try to go back to version 13.x and install the updated versions for that instead.
* Time to install all the new versions of Flash on my systems since Shavlik isn’t licensed anymore…
* Time to start the manual checklist fun:
  + Scan my workstation
  + Overlay the XCCDF results over the manual checklist
  + Grey out all of the matches, those will be automatically covered by GPOs.
  + Make a list of all the remaining settings that are things that need to actually be SET, not things like “physical security checks” and whatnot.

# 12/3/14 – wednesday

* Setup an exception GPO in the seaside\MDA\Computers\Wi7 OU to apply a different settings to the “Interactive Logon: Number of previous logons to cache”, and set it to 10, just for testing purposes. The STIG says to set to 2. We have all of ours normally set to 0 on every other system.

# 12/5/14 – friday

* Creating a ps script to iterate through the registry keys/values and check that they’re set properly.
* Maybe the values can be stored in a hash table?
  + $RegistryValues = @{“HKLM\Software\CBSTEST” = “CurrentState”; “HKLM\Software\CBSTEST” = “AutoStart”}

# 12/8/14 – monday

* Questions for SolarWinds during demo:
  + Can LEM and Server & Application Monitor coexist on the same server? Are there any special system requirements for this (ram, disk space) to work?
  + How exactly do the price tiers work for LEM? Do the how much of the event logs can 1 “node” record? Are multiple nodes needed for multiple event logs (Application / Security / System), or will they need to be more specific based on machine IDs?
  + Need to also check that it is “Common Criteria” or whatever the Gov/DoD certification for software is, approved.
  + What is “LWE250” is this some license tier package?
  + Is there a standalone executable package to install the trial/demo rather than the VM .ofv template?

# 12/16/14 – tuesday

* Doing .NET Framework stigs. A lot of the STIGs require searching for multiple files and searching through each of those files for a specific string. There are too many files and too many individual systems to do this manually, so I’ll need to script up something to find the files, and then search each of those files automatically for the string text.
  + Dir c:\ include <filename> -recurse | select-string <string>
  + Dir c:\ include \*.exe.config -recurse | select-string EnableFIPS
* **How to translate SIDs back and forth**
  + **Domain User to SID**
    - $objUser = new-object system.security.principal.ntaccount(“DOMAIN\_NAME”,”USER\_NAME”)
    - $strSID=$objUser.translate([system.security.principal.securityidentifier])
    - $strSID.value
  + **SID to Domain User**
    - $objSID=new-object system.security.principal.securityidentifier(“ENTER-SID-HERE”)
    - $objuser=$objSID.translate([system.security.principal.ntaccount])
    - $objuser.value
  + **LOCAL USER to SID**
    - **$objUser = New-Object system.security.principal.ntaccount(“LOCAL\_USER\_NAME”)**
    - **$strSID=objUser.translate([system.security.principal.securityidentifier])**
    - **$strSID.value**
* The next thing I need to script is something that will find all….
* So HKCU only displays users that are currently logged in, or have “switched users”, so it won’t display users that haven’t logged in yet, but that have saved profiles on the machine. I need to ask Guy how they worked through this requirement with the.Net stig. I remember him mentioning something about deleting user profiles, or maybe just registry keys.

Might try this command

Reg add HKEY\_USERS\[enter-SID-here]\software\microsoft\windows\currentversion\wintrust\trust providers\software publishing /f /v State /t REG\_DWORD /d 10000

Greg mani.sa is a member of:

CLO Exempt – Privileged user accounts

Domain Users

Seaside\_TO53223\_admins

Seaside\_TOS3\_Admins

Seaside\_TO\_Users

Adamj.sa was a memberof:

Domain users

Remote desktop users

Srdte workstation admins

Swannocusers

Swansupport

Keep working through the Google\_Chrome GPO that’s been linked.

# 12/19/14 – friday

# 12/22/14 – MONDAY

* Working on LEM queries to satisfy STIG requirement V-43713
  + ( DestinationAccount != "Anonymous Logon" ) AND ( "Event Name" = UserLogon )
  + The following account finds all criteria required except that it doesn’t filter for NON-DOMAIN accounts:
    - {( DestinationAccount != "Anonymous Logon" ) AND ( "Event Name" = UserLogon ) AND (LogonType="Windows: Network")}
  + Did a test local log on to MONTEGO with .\swanroot, here’s the query used to pull a local logon event log:
    - {( "Event Name" = UserLogon ) AND ( "User Name" = swanroot )} montego
    - Looks like I can use LogonType=”Windows: Interactive” to find local ones.
  + This SHOULD do it, but nothing comes up:
  + {( DestinationAccount != "Anonymous Logon" ) AND ( "Event Name" = UserLogon ) AND (LogonType="Windows: Network") AND (LogonType="Windows: Interactive")}
* Writing documentation for all privileged accounts in the domain. This will reference STIGs:
  + V-1140 Windows 7 V1R17 Manual
  + V-36431 Active Directory Domain V2R4 Manual
  + V-36432 Active Directory Domain V2R4 Manual
  + V-36433 Active Directory Domain V2R4 Manual
  + V-36434 Active Directory Domain V2R4 Manual

Use the excel spreadsheets of SA and MA usernames from SSCPAC domain to complete the privileged user account document for the SSCPAC domain. Use the SRDTE domain document that I completed on Monday.

# 12/23/14 – tuesday

* Finished documentation for all privileged accounts on SRDTE and SSCPAC domains. The documents have been created as PDF forms with digital signature fields.
* Next is to alter my CLO script to include a block of script that will auto check the box for “Do not delegate” on privileged accounts (SA, MA, DA, EA).
* Checked the box for “NO DELEGATION” on all privileged accounts in SSCPAC.
* Why is my script suddenly unchecking the “No delegation” box when it toggles the “Smartcard Required” box?
  + FIXED.
* **Things I still need to finish on Active Directory STIG:**

1. **Change the local administrator account password on every machine. They need to be unique passwords.**
2. **Install the proper 90Meter software and drivers on *every* server to enable smart card logon.**
3. **Write up policy document, or find document, and keep list of dates when all passwords that are annual will be changed.**
4. **AD 0190 command not working…**
5. **We don’t have selective authentication setup on our trusts. This will be a CAT II open finding.**
6. **Create a list of accounts that have delegated OU ownership throughout the domain.**
7. **Setup event ID logging and alerts on LEM**
8. **Create an SOP for Active Directory backups.**

* Send the pdf documents for the SRDTE and SSCPAC privileged account letters to Jenny and then Anabel for signatures. Put them in the SOP binder after that.

# 1/5/15 – monday

* My next project is studying Peter Thung’s “clo\_Account\_status” script to figure out why there is such a big difference between CLO Enabled accounts and CLO Enforced accounts. Right now, the report that it generates spits out SAMAccountName values
* With the exception of “lumbrera.sa” every account that is CLO Enforced has a UserPrincipalName that includes their EDIPI and PCC.
* Excel wasn’t doing what I wanted it to with duplicate deletion because it was keeping the value that had a duplicate, and deleting it’s twin instead of deleting both. I want it to delete both, and only leave the remaining unique values.

# 12/29/14 – monday

* Building a new workstation replacement for Alex to get rid of SNOOP.
* Need to change the email address that the CLO SCRIPT sends from. Currently it’s using [swanscan@spawar.navy.smil.mil](mailto:swanscan@spawar.navy.smil.mil) on line 1482 of the script. I’ll have Dave create another account or something to send those script report emails from.

# 12/31/14 – wednesday

* Use this command to find large files on Windows:
  + Dir c:\ -recurse –ErrorAction silentlyContinue | sort length –descending | select –first 20
  + Adjust the “select –first ##” bit accordingly depending on the amount of results you desire.

# 1/6/15 – tuesday

* SORNA got a clean ACAS scan! Sent an email to Jenny and cc’d Nat to get it out of quarantine and into production.
* TOBAGO is still too full on C:\ to accept patches. Going to run Disk Cleanup utility and see if that helps.
* Deleting double entries in excel by using the following system on this webpage: [www.mrexcel.com/archive/Data/13428.html](http://www.mrexcel.com/archive/Data/13428.html)
* Finish CLO report on why there is such a large difference in the numbers. I put all the totals from 1/6/15 report into **CLO\_Status 20150106**, so use that as a quick reference. Go through and get a detailed list for each domain that I have privileges in AD to search, and list which accounts are different, and why if possible – this may only be possible on SSCPAC. From there, figure something out, and make sure the report looks somewhat nice and legible at quick glance.

# 1/8/15 – thursday

* Keywords in my script:
  + PIN RESET
  + SERVICE ACCOUNT
  + FAILED TOKEN
  + TOKEN FAILURE
  + NEW TOKEN
  + SECONDARY
  + GROUP
* Got the CLO account status script to list the status of every windows account. Now I need to use the data dump that Dave gave me of all SWAN LDAP accounts, and compare to that. He said that he noticed quite a few AD accounts that did not have a corresponding LDAP account, meaning that the accounts are unregistered, which is much more important to fix than CLO. Once those are discovered and listed, then I can start taking care of CLO discrepancies.
* Take a look at the list of accounts that I went throught that were unregistered in LDAP, the “compare ad and ldap dump” spreadsheet, and take action on those accounts. STANG is one that I’ll need to work with servicedesk to notify the user and admin, because that account is currently not SWAN registered.

# 1/14/15 – wednesday

* Installed .NET 2.0 framework on SSCPAC-DC4 and SRDTE-DC4 so that 90Meter could be installed, so that smartcard logon would work properly.
* Called Guy Anderson to ask about the .NET STIG “nibbles” problem, and he said to look through Paul Plummer’s STIG Assist script documents and find the solution in there.
* CLO Exempt Group Accounts
  + Currently the groups are:
    - CLO Exempt Tracking
      * Only members are “CLO Exempt – Administrators” and “CLO Exempt – Group Accounts”
    - CLO Exempt – SWAN PKI List
      * About 20 user accounts. Lots of disabled accounts. The group hasn’t been modified since September of 2014, so it’s not an actively managed account and probably isn’t referenced anywhere functionally in AD.
    - CLO Exempt – Privileged user accounts
      * Looks like every admin account (SA MA DA) in SSCPAC. This is a useful group and makes business sense to keep.
    - CLO Exempt – Administrators
      * The only member is Russ Fujikawa’s SA <fujikawa.sa>. I’m going to get rid of this group, since it doesn’t seem to be used for anything.
  + I decided to change the order of the IF/THEN logic in my clo\_enforce script, and found that I was missing a significant number of accounts before.
  + Also decided to enforce disabled accounts. Ran the script without skipping disabled accounts, and 82 were enforced.

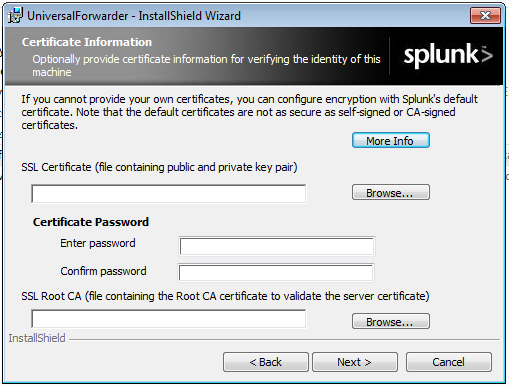
# 1/15/15 – thursday

* Installing LEM on all workstations and removing SPLUNK.
  + Manager name: lem.spawar.navy.smil.mil
  + Install comm prt: 37890
  + Legacy: 37891
  + Secure: 37892
  + MIDWAY

# 1/20/15 – tuesday

* Get a list of all user profiles on Windows. Go into the registry and find the:
  + HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList
  + Expand the profile list, and it will show you all of the SIDs for profiles.
  + I’m did a SCAP scan on Borneo (new machine in A223), and will try to get a list of all user profiles on that workstation – which should be very small since it’s new – and then go into each profile and edit the nibble value. Finally I will scan the machine to verify that the fix worked.
  + For WED: I was able to clear BORNEO on the .NET ACAS scan. Everything worked. Keep doing that on the rest of the machines. Look at the HTML outputs for details as to which accounts it’s finindg in the registry.

# 1/21/15 – wednesday

* Looks like every workstation has authentication scan failures on ACAS. Rescanning on MIDWAY to check it out…
* The script Peter wrote the spits out numbers for CLO in other domains is showing very different numbers for the SSCPAC domain than my script is. I’ll need to take a look into his and see what it’s looking for, because I can’t have discrepancies *that* large in the numbers.
* Going to use MIDWAY as my test machine for SPLUNK SSL issue.
* 
* The SSL settings are more advanced than I remembered. You need to provide certificate files for SPLUNK to use. Apparently you can configure encryption with Splunk’s default certificate, however I believe that would still flag the vulnerability in ACAS.

The ESX Server IP addresses are 140.199.57.10 – 140.199.57.14 . There are 4 of them.

# 1/26/15 – monday

**CLO MEETING NOTES:**

Everything needs to be centralized around Thuy’s CLO Exception List. We will need to start by adopting a policy of having ONLY THE SERVICE DESK uncheck CLO enforcement on users’ accounts. When a user needs a PIN reset or has a failed token, they will contact the service desk to have their account un-enforced and setup for username/password…but then do they also send an email to [swantoken@spawar.navy.mil](mailto:swantoken@spawar.navy.mil), or should the service desk then forward the request over to the SWAN Token team? That seems to be 7798

Once the user contacts Service Desk, service desk will unenforced CLO on the account, and set them up for username/password logon, AND use a new tool that Thuy will create that will add that user’s account to the CLO Exceptions List. That way, the user’s account will be skipped by the nightly enforcement script and they will be able to use their username/password until they get the new PIN. When the user gets their new PIN, they will be downstairs with Jarie, and she will use Thuy’s tool to remove the user from the CLO Exception List. Then, when the nightly enforcement script runs that night at 6pm, that users account will be enforced back for CLO logon since they will no longer be on the CLO Exception List.

This same process will be followed for token failures, however with those there is a 2 week grace period, as opposed to a two day grace period.

It was decided that Jared would be looking at the exception list regularly, or at least weekly, to record the dates that accounts were added to the CLO Exception List in order to track how long an account had been there. PIN resets are only allowed two days, and failed token replacements and new users are only allowed two weeks.

I will need to send a list of the service/secondary/group accounts to Jarie and LT Dailig for re-vetting, since a lot of those accounts have been on that list since the beginning, and that was over 2 years ago.

# 1/27/15 – tuesday

* Starting to dive into the “nibbles” automatic script registry edit project.
* The location in the registry where you can find a list of all user profiles is:

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\[list of users…]

* I’ve found that you can tell regedit to load in a profile into HK\_Users to then do work inside that hive. Refer to this website for the how-to:

Scilnet.fortlewis.edu/tech/Users/load\_HKEY\_USERS.htm

* + Highlight HKEY\_USERS and select “load hive” from registry menu
  + Browse to profile in the directory c:\Users\[username]
  + You might need to change the folder options to “Show hidden files, folders, and drives” and uncheck “Hide protected operating system files (Recommended)”
  + …or just have it automatically look for a file called “NTUSER.DAT” in the user’s root directory, even though it’s “hidden”
  + Regedit will then ask what you want to name the hive, I just tell it to use the SID since that’s what it would be referred to as
  + You can then drill down to the “Software Publishing” key and change the “State” value accordingly.

# 1/29/15 – wednesday

## Slow Logon Troubleshooting

Host: CAICOS

Referring to gpsvc.log.

GPO: Configuration-Tumbleweed-Standard-4.10-conf \srdte.spawar.navy.smil.mil\policies\{1DDF335E-A957-42CF-A262-86BF33960C54}

WMI Filter ID: {58f6f4f1-ef73-48f9-9e0f-3d6b9bb3c65d}

Processing starts 12:51:38, ends 12:52:08

Duration: 30 seconds

GPO: Configuration-90Meter\_1.22s-Baseline

Processing starts 12:52:08, ends 12:52:38

Duration: 30 seconds

GPO: Configuration-Tumbleweed-Standard-4.11-conf {e6951ddd-62e9-4dd8-a650-a41056043959}

Processing starts 12:52:38, ends 12:53:08

Duration: 30 seconds

GPO: Configuration-Tubmleweed-Standard-4.10-conf \policies\{1DDF335E-A957-42CF-A262-86BF33960C54}

WMI Filter ID:

Processing starts 12:53:08, ends 12:53:38

Duration: 30 seconds

…

GPO: Configuration-90Meter\_1.22s-Baseline {128519fd-1387-47e2-82f5-3cf0ff3af908}

WMI

Processing starts 12:53:40, ends 12:54:10

Duration: 30 seconds

It looks like the WMI filtering may be screwing up the process somewhat. The logs show that a WMI Filter is found, and then it spews out many lines of calls with failures, finally saying “Evaluate returned error. Hr=0x80041069” and then “The GPO does not pass the filter check and so will not be applied”. Check the WMI filters and make sure that they’re written efficiently. Or possibly set GPOs to only set ONCE on systems, then never again?

GPO:

WMI: {

Processing starts 12:54:10, ends

RESTART CAICOS 2:14:10 pm.

Moving CAICOS to the \_Testing\_Logon OU since I need to completely remove the tumbleweed and 90Meter GPOs, instead of just unlinking them. I’d rather not do that in the SSCPAC OU since that would potentially affect users.

# 1/30/15 - friday

So after re-linking those 3 GPOs in the testing OU, I still can’t recreate the delayed logon. My logons with javery.sa are only taking :07 seconds or less. I should try setting up my sscpac\javery account to my smartcard, and place that account object in the same container as the ServiceDesk folks just to recreate their logon scenarios perfectly.

WMI Filter: one problem could be that the filter searches using “SELECT \* FROM **Win32\_Product**…” whereas a lot of the WMI filters I created use “SELECT \* FROM **Win32\_Service**…”. It’s possible that the product filter takes more time / processing than the service filter. I should google around and see if filters are still applied to the machines even when GPOs aren’t linked.

So I need to change the current WMI filters. I found this query string that seems to do exactly what I need:

SELECT \* FROM CIM\_Datafile WHERE Name = ‘c:\\program files\\microsoft office\\office12\\winword.exe’ AND Version = ‘x.x.x’ “ just change it up to fit whatever program installation is needed.

The old WMI Query for “Tumbleweed Desktop Validator 4.11” was “SELECT \* FROM Win32\_Product WHERE (IdentifyingNumber = ‘{0768D7D7-0D13-4740-9684-A42DDF095BA4}’ AND Version = ‘4.11’)”

Going to change that to “SELECT \* FROM CIM\_Datafile WHERE Name = ‘c:\\program files\\tumbleweed\\desktop validator\\dvservice.exe’ AND Version = ‘4.11.0.594’ “

The old WMI Query for “Tumbleweed desktop validator 4.10” was “SELECT \* FROM Win32\_Product WHER (IdentifyingNumber = ‘{0768D7D7-0D13-4740-9684-A42CCF0-5BA4}’ AND version = ‘4.10’)

I’m changing that to “SELECT \* FROM CIM\_Datafile where (Name=’c:\\program files\\tumbleweed\\desktop validator\\dvservice.exe’ and version = ‘4.10.0.344’ )”

The old WMI query for “90Meter version 1.2.22” was “SELECT \* FROM Win32\_Product WHERE (Vendor=’90Meter’ AND Version =’1.2.22’)

I’m going to change that to “SELECT \* FROM CIM\_Datafile WHERE (Name=’c:\\program files\\90meter\\cacpivmd\\carddetector.exe’ AND version=’1.2.22.0’ )”

TO DO MONDAY:

* Finish updating Windows 7 STIG v1r18 for SRDTE and SSCPAC domains.
* Keep working on any other stigs that need to be completed.
* Take a look at the first page list in notebook and see what CCRI tasks can be completed.
* Remind Chris Holt from SolarWinds to send us another renewal license. He said his guy was out of the office last time.
* There’s a Windows DNS STIG…

# 2/2/15 – monday

**Notes from phone conversation w/ Laura Salazar, PKI Team, regarding request of new DC certificates:**

Run GrabDCinfo\_v2.0.1\_SIPR

Spits out folders for some of the domain controllers into the directory above it. Need to copy those directories into the C:\ drive on each of those DCs in question.

Now, go back to the main DC, open the certificates MMC.

Run the DCcertReqSRDTE-DC1.bat script administratively. This should create a cert in the Certificates MMC > Certificates Enrollment Requests > Certificates (thing here)

Now go to that file on the c: drive, into the certs directory, and into the DC\_CERT directory within that. There will be 3 files. One is a .req file. If you edit this file, you will see the certificate hash between the lines “\_\_\_\_BEGIN NEW CERTIFICATE REQUEST\_\_\_\_” and “-----END NEW CERTIFICATE REQUEST----“ . This will go to that website.

Go to the website (kyle emailed URL) use firefox.

Click on the 3rd link for NSS Domain Controller….

Make sure the drop down says PKCS#10, and paste that text blurb of the certificate request into the big text box below the drop down.

Fill out your personal information in the 3 text boxes below that.

Now, for the DNS Name and GUID fields, go back to

Send request iD screenshot to local certificate authority.

**>>End Phone conversation notes<<**

* So the DoD SIPRNet CA-21 expired 2/1/2015, and caused most of our servers to stop servicing PKI requests because their certificates were now expired and invalid. We had to contact Laura to help with requesting the new certificates. Now the certificates are back, but I’d like to wait for her to return my phone call so she can walk me through how exactly to replace the old certificate. I imagine that it’s a simple enough matter of importing the new and deleting the old, but just in case, I want to speak with her first.
* I’ve imported the certificates into SSCPAC-DC1 and SSCPAC-DC2, and also backed up and deleted the old certificates out of their certificate stores. We need to check in the morning to see if there is a Tumbleweed event ID of 16 in the logs. That would show that the certs are checking in w/ OCSP correctly.
* FOR TOMRROW:
  + Install new JAVA on ANTIGUA so Jarie can test out the token software and see if that was the problem that it broke last time.
  + keep working on the swanroot password change project for each workstation.

# 2/3/15 – tuesday

* spoke with Laura Salazar (619-767-4479) and verified that Kyle and I followed the correct process when importing our renewed certificates on the DCs.
* DCs appear to be working properly and serving smartcard logon requests properly.
* Uninstalled Java 7.76 on ANTIGUA and installed Java 8.31. Rebooted the machine. Jarie will be trying to do her token stuff today and let me know if the application breaks again.
* Logged into srdte-dc4 to test the DSRM – directory services recovery mode – password, and it worked with the “swanroot” account.
* Can’t seem to get any of the SSCPAC DCs to actually start in “safe mode” or “dsrm” mode as it would otherwise be called.
* Working on setting up LEM reports
  + So far the only query I have to work off of is: ( ProviderSID = \*4624\* ) AND ( InsertionIP = galapagos.srdte.spawar.navy.smil.mil )
  + Got a list of event IDs
    - 4608 STARTUP
    - 4609 SHUTDOWN
    - 4624 LOGON
    - 4634 LOGOFF
    - 4647 BEGIN LOGOFF
    - 4778 SESSION RECONNECTED
    - 4779 SESSION DISCONNECTED
    - 4800 WORKSTATION LOCKED
    - 4801 WORKSTATION UNLOCKED
    - 4802 SCREENSAVER INVOKED
    - 4803 SCREENSAVER DISMISSED

# 2/4/15 – wednesday

* Section 4.2.4 in the red CCRI readiness binder says we should:
  + “Enable auditing/logging features for all NIIPRNet and SIPRNet systems. At a minimum, include in the log/audit record the following information: successful and unsuccessful login attempts; file system modifications; and privilege changes. Perform weekly log reviews for evidence of abnormal or malicious activity. “
* Had conference call with Omar from SolarWinds to troubleshoot the connector issue we were having with LEM in the browser. Omar suggested downloading and installing the LEM client application on my PC, and that worked great! It’s real time too.

# 2/5/15 – thursday

* HOW TO SET **DSRM PASSWORD** ON A DOMAIN CONTROLLER
  + Run ntdsutil.exe
  + At the ntdsutil prompt, type **set dsrm password**
  + At the following ntdsutil prompt, type **reset password on server null**
    - Note: entering **null** will set the dsrm password on the current DC that the command is being run on. Otherwise, you can enter the host name of a server you want to set the dsrm password on.
  + You will be prompted to enter the password twice
* HOW TO BOOT A DOMAIN CONTROLLER IN DSRM MODE
  + Open the charm bar, click the cog icon representing **settings**, then left-click on **power** and hold down the **shift** key while you click **Restart**.
  + Select one of the two **Operating System: Recovery** options. Click **Continue**.
  + On the next screen, choose **Troubleshooting – Refresh or reset your PC, or use advanced tools**.
  + The **Advanced Options** screen will appear.
  + Choose **Startup Settings – Change Windows startup behavior**.
  + The **Startup Settings** screen will appear.
  + Click **Restart.**
  + The server will restart a second time, but this time will display the **Advanced Boot Option** screen.
  + On this screen, select **Directory Services Repair Mode**.
  + The server will boot into DSRM Mode.
* TO DO MONDAY:
  + Respond to Microsoft concerting the DSRM incident ticket I submitted. See paper for details.
  + Continue STIGs.
  + IAVM STIGs need getting done.
  + Hash out CLO ServiceDesk processes.
  + Talk to JREES about access to the spreadsheet and it’s format.

# 2/9/15 – monday

* The patch that I had to have emailed to me from a TechNet link (KB2937044) x64, appears to work on Server 2012, and fixes the issues I was having.
* Microsoft refunded our 1/5 call since I was able to fix the issue without their assistance.
* I went through and changed all “swanroot” account passwords on Member Servers. All “swanroot” account passwords on workstations were changed last week.
* **SID FILTERING**
  + I’ve setup SID filtering on Groomlake.
  + URL to a helpful TechNet page about SID Filtering:
    - <https://technet.microsoft.com/en-us/library/cc755321(v=ws.10).aspx>

SUMMARY of FRIDAY: What I’ve been working on is collecting all STIG settings across all of our required STIGs that make any mention of documentation or policies. From there, I’m highlighting the items that actually apply directly to our situation, and will require documentation to be either created, updated, or found. In my mind, this is the first step in tackling this big requirement – that is identifying all the problems (lack of documentation) that will need to be resolved. Once I’m confident that we’ve identified all the necessary requirements for documentation, the next step would be to pool those together and take a look at the various types of things/policies that need to be documented. Some things can probably be put together in one document, while others will need separate documentation. My biggest concern with all this documentation is how we are going to organize it in a way that makes sense, and is scalable. We don’t have any true knowledge base solution on the high-side. Maybe when there’s a pocket of free time we can look into getting something for KB. Going hand-in-hand with that is how to handle version control and numbering of these forms, plus their layout and appearance. I’d like to have some sort of standardized form for all of this that would make it instantly recognizable. **Keep in mind that a lot of this is supposed to be all IA’s job, according to Chris.**

# 2/17/15 – tuesday

USBSTOR issue that Scott sent me a list of offending workstations that have items listed in their “USBSTOR”.

Under C:\Windows\inf there are a few files that you can search against the hash string associated with each hit finding. Those files are:

-setupapi.app.log

-setupapi.dev.log

-setupapi.offline.log

The file that I found entries listed in was setupapi.dev.log .

According to Scott, entries that have hashes that include ampersands “&” in the first few characters such as “7&3151c88b&0&1” as opposed to “abcdef012314e7b6&0” are false entries. Supposedly Windows creates these false entries in this USBSTOR for USB devices or just other devices that it doesn’t recognize? However this is very strange because one of the “false entries” is very distinctly named “flip cc”, which is a real device.

Here’s what I’m going to do: use CAICOS as a test machine.

Make copies of all three of those .log files. Edit out the bits that make reference to the offending USB devices. Reboot machine. Check files for any residual references. Ask Scott for a rescan.

# 2/18/15 – wednesday

* MS15-011
  + Hardened UNC Paths GPO
  + Computer Configuration / Administrative Templates/ Network /Network Provider

|  |  |
| --- | --- |
| **Value Name** | **Value** |
| [\\\*\NETLOGON](file:///\\*\NETLOGON) | RequireMutualAuthentication=1, RequireIntegrity=1 |
| [\\\*\SYSVOL](file:///\\*\SYSVOL) | RequireMutualAuthentication=1, RequireIntegrity=1 |

Configured GPO “MS15-011” on SRDTE domain. Restarting SRDTE-DC1. Going to check ACAS afterwards to see if the MS15-011 vulnerability still shows up for SRDTE-DC1 after the reboot. I’m also noticing most of the workstations no longer show MS15-011. Perhaps they just need to install all the WSUS patches and reboot now? I saw that at least half of my workstations were clear of MS15-011 even before I applied the GPO fix steps.

According to the technet page for support.microsoft.com/kb/300483 there is a known error that might affect some clients causing Security event log error ID 1108 to be generated instead of the usual 4688 audit event. To fix this, KB3004375 should also be installed. This patch is already installed silently alongside 3000483 for Server 2012.

~~Apparently the GPO might not be necessary. I already applied the GPO to SRDTE domain, however all my systems that are still being flagged in ACAS are in the SSCPAC domain. Actually no, there are still some in SRDTE, such as BORABORA.~~

Never mind, definitely need to have the GPO in place. If it breaks some workstations and causes intermittent logon issues, then, oh well. The users and admins can just restart their machines.

FOR MONDAY:

Keep working on usb registry stuff on MIDWAY and trying to find that junk out…

Also be ready for the 9am meeting. Review the notes you took from Thuy’s meeting on Thursday.

Expect phone calls from those people, it’s in your calendar. To setup their trusts…

Also need to pickup SPAWAR badge. Eva said that she resent my visit requests.

# 2/24/15 – Tuesday

* Windows Last Logon
  + Computer Configuration > Policies > AdministrativeTemplates > Windows Components/ Windows Logon Options > Display information about previous logons during user logon ENABLED.
  + I apparently had a GPO called “Display\_Last\_Logon”, but it was on the SSCPAC side. I don’t see anything currently in SRDTE.
* Window pops up after dmain join:
  + Window came up prompting for credentials to change domain dns name of computer in the domain.

# 2/26/15 – wednesday

* Kyle phone call. All member servers, application, outlook, internet explorer should be done. When dave gets back, go through the Windows DNS STIG w/ Dave and make srue that open finding s are taken care of or noted/documented.
* Should run the peter account script on SRDTE to take care of the accounts in our domain.
* Working with Pablo Lopez to fix NCTSI domain trust. When he tried SRDTE credentials on his workstations, he received the following error:
  + “The name or security iD of the domain specified is inconsistent with the trust information for that domain.”
  + When I try to create the trust I get this error:
    - The local security authority is unable to obtain an RPC connection to the Active Directory Domain Controller DC3. Please check that the name can be resolved and that the server is available.
  + I had IT1 Pablo Lopez create the outgoing trust from his domain controller, and that was successful. However, he was still not able to authenticate on his machine with SRDTE credentials.
  + I might try updating the name suffix routing for the trust, and see how that goes. That option comes up every time you validate the trust.
    - Trying to update the suffix routing does not seem to have worked.
  + One odd thing is that his domain FQDN is NCTSI.NAVY.SMIL.MIL, he does not have “SPAWAR” in the domain, however when I ping “NCTSI” it returns “NCTSI.SPAWAR.NAVY.SMIL.MIL”. I should talk with Dave about that and see if that could be causing problems. It would be strange that it just now started causing problems, even though it’s been configured that way for a while now.

# 2/27/15 – thursday

# 3/3/15 – Tuesday

* Talked to Fransisca Smith numerous times regarding JEDI’s lack of the SWANSCANNER(.sa/ma/da) accounts. Nothing was accomplished since she insisted that she didn’t currently have the time to setup the accounts in her domain, however she said she would eventually take care of it.
* Need to try integrating the automatic account disable feature into my nightly script. I should first test this with a “disarmed” script that won’t do anything besides spit out a list of users to disable.
* Step through the script, see what happens… use that to figure out how the fuck it works.
* Analyzing Peter’s Script
  + Line 235, $numDaysSinceLastLoggedInOrCreated is the list where the number of days is dumped, regardless of wether it’s since created or logged in.
  + Stepping through, after the prompt comes up, if you enter “1” to do the normal functions that we usually tell it to execute, then it calls what looks like a custom function called “DetectDormanAccounts” (no ‘t’ ?)
  + $listUsers is the list that all the users get dumpted into during the data call collection.

# 3/4/15 – wednesday

* Trying again to setup **Last Interactive Logon** for systems.
* See TechNet for details on unclass:
  + <https://technet.microsoft.com/en-us/library/dd446680(v=ws.10).aspx>
* Comp Config > Administrative Temlates > Windows Components > Windows Logon Options > Display information about previous logons during user logons = Enabled

# 3/11/15 – Wednesday

* Changed settings on the w2k8\_base\_gpo. So why the FUCK does ISNSWEB1 score LOWER after the change? Suddenly it went from 88.21% 🡪 87.83% and findings for “The built-in guest account will be disabled” and “ The built-in guest account will be renamed” came up…. I don’t remember changing that in the 2k8 base gpo… fuck.!!!

# 3/12/15 – thursday

* The Windows 2008, and Windows 2008 R2 stigs are different. This is problematic since I’ve been updating the w2k8\_base\_gpo on SSCPAC using 2008R2 stig settings. I’ve copied that STIG and renamed it w2k8\_R2\_base\_gpo. What I need to do is replace every linked instance of W2k8\_base\_gpo with w2k8\_R2\_base\_gpo.
* Setting the Server 2008 Standard GPO
  + 5.038 – don’t see the “Terminal Server” contiainer listed under Administrative Templates. Just “Windows Components”

# 3/23/15 – monday

The registry delete script now seems to work, now that I added the –Recurse switch. Now to delete those setup log files and whatnot.

>Push-Location

>Set-Location c:\windows

>Test-Path (filename) ex; Test-Path comsetup.log

>Remove-Item to delete the item. Ex: IF((Test-Path comsetup.log) –eq $true){do the deleteion}

# 3/27/15 – friday

Working on CLO\_enforce\_script.ps1, again…

Moving **[int]$flags = $Properties.useraccountcontrol[0]** from line387 to 366

Moving **$Flag\_Results = UserAccountControlFlags –Flag $flags** from line 388 to 367

Commented out line 543

The “CLO User Cleanup.xlsx” spreadsheet has the list of accounts that I’ve been working on. There are 4 accounts that were listed with FAILED TOKEN, but not in the exceptions lits. Check if those actually have failed token.

Also see if Thuy responded back to email that I sent out on Friday afternoon. Would like to have all these extra accounts added to the exceptions List.

Remove CROBERTS from the exceptions list, he only had an exception for Friday 3/27/15.

Don’t forget to start DTA’ing the clo exceptions list over each day.

IT1 Lopez getting those systems

# 4/10/15 – friday

**Project - Mass Reboot of Systems Remotely**

Adam is going to give me a list of IP addresses of all the workstations and member sever on the network that will need to be remotely rebooted before our preliminary ACAS scan for the inspection. Here’s the options I’ve found to accomplish this task

**# 1 “shutdown /i”**

This is the built-in windows UI way of executing remote shutdowns. I can enter in a list of machine host names, and the CMD line will tell me when machines did not accept my command and give me an error message. The problem is that this UI will require host names, and if I have a list of IP addresses, then it will be a manual labor process.

**#2 “shutdown –r –m** [**\\serverIP**](file:///\\serverIP) **–f –t 0”**

This is the same command in CMD, but it does not bring up the UI, and could be more scriptable.

-r reboot

-m machineIP

-f force

-t countdown timer – 0 for immediate.

This is the error message presented if CMD cannot remotely shutdown a system:

“140.199.56.83: The entered computer name is not valid or remote shutdown is not

supported on the target computer. Check the name and then try again or contact y

our system administrator.(53)”

I think I could script up this line of code and just do something like a FOREACH $IP in $IP\_List {shutdown –r –m [\\$IP](file:///\\$IP) –f –t 0}

I just have to make sure that I’m separating workstations and member servers.

# 4/13/15 – Monday

**Import-Csv** *-Path* "\\140.199.56.11\pki\_share$\clo\_exemption\_list\_from\_pki\_token\clo\_exempt\_list.csv" | **ForEach-Object** { $uid += $\_.uid; $edipi += $\_.edipi}

# 4/16/15 – thursday

Building array tables for use with CSVs.

$array =@()

$obj = New-Object PSObject

$obj | Add-Member –MemberType NoteProperty –Name “First” –Value “Justin”

$obj | Add-Member –MemberType NoteProperty –Name “Last” –Value “Avery”

$obj | Add-Member –MemberType NoteProperty –Name “Domain” –Value “SRDTE”

$array += $obj

$array

First Last Domain

----- ---- ------

Justin Avery SRDTE

$obj = $null

#//// REPEAT AS NEEDED ////

a

Was able to add email functionality to the clo\_enforce\_script.ps1 so we can email the list of admin accounts to IA on the High-Side.

Just need to change the $emailTo variable on line #704 to include IA. Also need to modify the $emailSubject and $emailBody variables accordingly with meaningful stuff.

# 4/21/15 – tuesday

Need to query a list of services on all member servers, so will use this query:

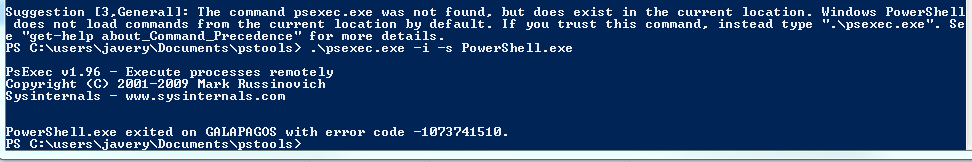
Get-Service | Select-Object displayname, name, status | Export-Csv -Path C:\users\javery.ma\Deskt

op\ServicesList\_srdte-ops001.csv –NoTypeInformation

# 4/22/15 – wednesday

* Edited permission in ADUC for each project lab’s OU. Resticted the ability to change CLO enforcement on user accounts.
* Found out how to lock down OUs so that lab admin groups cannot create user objects. Will need to announce this at next forum, possibly. Definitely need to formally document all Service Desk processes before this time, so that the Service Desk is ready before the switch.
* Keep working on downloading and figuring out which file for 15-033 applies to my two affected systems (BORNEO, and NIKOA). There was a user that sent an email in complaining that he was also having issues with this patch.
* Admins cannot drag user objects into their OU’s if I restrict the ability for them to create child objects. We may need to figure out some sort of chart method where by the Service Desk can figure out which lab the user should go into based on the Building and Room numbers entered on the SWAN User Account form.

# 4/23/15 – thursday



Here’s how I used psexec.exe to open PowerShell with System level permissions.

# 4/29/15 – wednesday

**Remote Query Installed Programs:**

PS C:\Windows\system32> Invoke-Command -ComputerName zanzibar {Get-ItemProperty HKLM:\Software\Microsoft\Windows\CurrentVersion\Uninstall\\* | Select-Object DisplayName, DisplayVersion | Format-Table -AutoSize}

# 5/6/15 – wednesday

**repadmin /replsummary**

**repadmin /showrepl**

**repadmin /syncall**

# 5/20/15 – wednesday

## SHAVLIK PROCESS INSTRUCTIONS

1. Log onto [\\san-shav](file:///\\san-shav) (128.49.5.55) using PAC\userid.MA account credentials. Move data files from \\128.49.5.55\console$ to somewhere so it can be zipped (zipping optional, saves time during scan)
2. Go to the \\128.49.5.55\patches$ share, sort by “Date created” and look for the most recent files since the last time you moved things over
3. Move the patch items from \patches$ to the DVD
4. Once the \console$ is finished zipping, move that to the DVD
5. DTA the DVD from UNCLASS to SIPR
6. Go to \console$ on MRPATCH and DELETE the data files that are there
7. Copy the data files from the DVD to the “SHAVLIK” folder on your desktop. Extract the data files from the zipped folder.
8. Copy the data files folder over to MRPATCH in the “C:\ProgramData\LANDESK\Shavlik Protect\Console” directory
9. Start Shavlik?
   1. Select machine group from the “2. Select/Confirm targets:” list.
   2. Make sure that the path for the patches is looking in the E:\ drive
   3. Go to step 4. And check “Auto-deploy patches after scan”
   4. Make sure the drop-down is selected for “No Restart”
   5. GO!

# 5/22/15 – FRIDAY

# 5/26/15 – tuesday

May need to import the root certificate for an application to run for Jessie Atalig. Windows Eyes is an application that assists vision impaired users. It will not run properly on his systems, and the vendor told him that the application would have to be white-listed in the domain. Some Googling landed me on this page: <https://technet.microsoft.com/en-us/library/cc754841.aspx> , particularly the section that explains “Adding certificates to the trusted root certificate authorities store for a domain”.

**90Meter**

Finally found it on the high-side: <http://iase.rel.disa.smil.mil/pki-pke/function_pages/tools.html>

For Monday:

* 90Meter is pretty much finished up. Might look into solutions for pushing it, but it’s challenging since the older versions would first need to be uninstalled.
* Will need to do monthly MSR report, and send that to Russell.
* Find something.
* Also check LEM to see if croberts.sa has locked his account/ had failed logon attempts. Still trying to figure out what’s causing his repeated lockouts.

Created a new croberts.sa account for Chris Roberts after deleting his old account multiple times. He couldn’t change the password, and kept getting an error message. It turns out that the problem was due to the account minimum password policy. I was trying to change the password multiple times in the same day, and that was preventing the password from being changed, and causing the error message.

# 6/19/2015

SolarWinds Orion SAM Server and Accounts Manager webpage (view w/ Firefox): <http://srdte-mon/Orion/SummaryView.aspx?ViewID=1>

Brought up old Dell chassis from B159 to remove main CPU fan and use it as a replacement for the faulty CPU fan that is making too much noise in LANAI (John Harmon’s machine).

Started Windows 7 IAVM Checklist

Assisted Sarah in setting up her new user accounts and email.

# 6/22/2015

Finished Windows 7 IAVM checklist

Started Windows 2008 IAVM checklist

# 6/23/2015

Took old Dell tower chassis down to B159 for storage and future DRMO.

Finished Windows 2008 IAVM checklist

|  |  |
| --- | --- |
| **Remedy on SIPR** | **Remedy on UNCLASS** |
| Would need to work with Devin Rankle to assist with setup on SIPR remedy. Unsure of ETA for completion. | Could have accounts and groups setup in about 1 week |
| Internal to SWAN office only | Service Desk could field some calls and submit tickets to SWAN |
| Service Desk could not put in tickets | Could not include sensitive or classified information. Would need to scrub IPs |
| Could keep detailed notes on each ticket if sensitive or classified information is involved |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# 6/25/2015

## WSUS PROCESS

**Removing Unnecessary Updates**

1. Open WSUS utility, expand left, open “Updates”
2. Click “Search…” on right-hand side and enter KB number
3. Right-click on search result and choose “Decline”
4. Go to “Options” on the left-hand side
5. Click on “Server Cleanup Wizard”
6. Leave all boxes checked and click “Next” to run wizard.
7. The next time “Check for Updates” is ran on a workstation or server, the KBs that were removed should no longer appear.

**Potential Future WSUS rebuild**

1. Re-build the WSUS server
2. Point the database for WSUS to SRDTE-DB01.
3. Put the repository bit on the E:\ drive, so that it’s not on the C:\ drive. STIGs mandate that it shouldn’t be on C:\ as it is now.

Troubleshooting WSUS issue

1. Working on SRDTE-ops001
2. Uninstalled KB3058515 so I can have an update to use. Restarted the server.
3. Windows Update utility showed that KB3058515 was available for install from WSUS. Tried installing and it failed.
4. Checking the C:\Windows\WindowsUpdate.log shows errors regarding the CAB file for that update similar to the CAB file error that Microsoft Support mentions: Failed job file: URL = <http://140.199.56.55/Content/5C/4C78B3FC8FE98D97C7FB973348EE5FB30EE89F5C.cab>
5. Checking C:\Repository\WsusContent\5C for the CAB file shows that it is missing. MS said in the email that this could be due to incomplete metadata sync.
6. Followed instructions to open admin cmd prompt and run c:\Program Files\Update Services\Tools\WsusUtil.exe reset.
7. Reset the utility at 1:10pm. Microsoft said to wait for a few hours…
8. Continuing on 6/30/15: Still cannot find the .CAB file located in the windows directory in WSUS as seen above.
9. Restarting WSUS server, then will check if .CAB file has populated afer.

Shavlik Missing files from recent scan:

Lyncmso2013-kb3039779-fullfile-x86-glb.exe \*\* have this one BTS-DLGW-2

Npp.6.7.9.2.Installer.exe

(MS15-046) Powerpoint2013-kb2975816-fullfile-x86-glb.exe \*\*Need to get off patch repo -BTS-DLGW-2

# 6/30/2015 – Tuesday

KEYLARGO was having problems installing 9 updates – it would instantly fail each time. I installe

If we need to contact Microsoft for support issues, contact:

Rino Ortega

SPAWAR Command Information Office

Software Benefits Manager

Echelon II FAM Support Team

4301 Pacific Highway

San Diego, CA 92110-3127

[Rino.ortega.ctr@navy.mil](mailto:Rino.ortega.ctr@navy.mil)

858-537-0573

Declined KB2670838 on WSUS because it was hanging up and causing issues on KEYLARGO (Platform Update for Windows 7 x64-Edition

# 7/2/2015

SIPR Kiosk in Topside A33 rm. 3018

**Export PuTTY Settings**

Do this logged in from the account in question. Open registry and export HKEY\_CURRENT\_USER\Software\Simontatham. This is where the PuTTY settings are stored in the registry. Then, merge those exported registry settings on the destination computer, logged in as that user.

**Export Tectia SSH Client Settings**

Copy this directory C:\Users\<username>\AppData\Roaming\SSH” to the user profile on the destination machine.

# 7/9/2015

**90Meter GPO WMI filter fix**

I didn’t have the WMI filter updated to accomidate the recent version update to 90Meter 1.2.27s. So that’s what I’ll do now.

**OLD WMI QUERY:** SELECT \* FROM CIM\_Datafile WHERE (Name=’c:\\program files\\90meter\\cacpivmd\\carddetector.exe’ AND version=’1.2.22.0’)

**NEW WMI QUERY:** SELECT \* FROM CIM\_Datafile WHERE (Name=’c:\\program files\\90meter\\cacpivmd\\carddetector.exe’ AND version LIKE ’1.2.2%’)

# 7/13/15 – monday

Turning on KERBEROS logging:

Enable logging by creating the following registry entry on the system desired:

**HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos|Parameters**

Registry value:  **LogLevel**

Value Type: **REG\_DWORD**

Value Data: **0x1**

# 7/16/15 – THURSDAY

**PowerShell Command to Set ChangePassword At Next Logon**

Run from SSCPAC-DC4 – for SSCPAC domain

$userid = @()

Import-Csv –Path “C:\sscpacadmins.csv” | ForEach-Object {$userid += $\_.userid}

$userid

ForEach($uid in $userid){ Set-ADUser –Identity $uid –ChangePasswordAtLogon $true}

Run from SRDTE-DC1 – for SRDTE domain

$userid = @()

Import-Csv –Path “C:\srdteadmins.csv” | ForEach-Object {$userid += $\_.userid}

$userid

ForEach($uid in $userid){ Set-ADUser –Identity $uid –ChangePasswordAtLogon $true}

Here’s a good query I can use to WMI query the GPO that will look for older versions of the software.

gwmi -Query "SELECT \* FROM CIM\_Datafile WHERE (Name='c:\\program files\\90meter\\cacpivmd\\cardd

etector.exe' AND version < '1.2.27%')"

**UNINSTALL COMMANDS AND LOGIC**

$app = gwmi win32\_product –filter “(Name LIKE ‘%90Meter%’) AND (Version < ‘1.2.27%’)”

IF($app.version –lt ‘1.2.27’

{

$app.uninstall()

}

# 07/21/15 – tuesday

**Microsoft Malicious Software Removal Tool**

1. Run KB…. As administrator
2. Click Next
3. Choose Quick Scan and click Next
4. Scan will run
5. Scan should complete saying “No malicious software detected.
6. Click Finish
7. Restart system

# 09/02/15 – wednesday

WSUS2 1,342.76 MB / 149,403.50 MB downloaded as of 9/2/15 at 08:30am.

WSUS2 ran “wsusutil reset” 9/2/15 at 10:01am. Let the server sit there and resync for a long time.

# 09/08/15 – tuesday

WSUS2 ran “wsusutil reset” 9/8/15 at 3:20pm.

298.80 MB / 43,436.57 MB downloaded…

# 09/09/15 – wednesday

4,656.39 MB / 43,438.45 MB as of 9/9/15 at 7:25am.

4,679.69

# 09/10/15 – thursday

8,633.79 MB / 46,985.37 MB

# 09/11/15 – friday

11,648.73 / 56,026.80

# 09/14/15 – monday

32,262.57 / 58,587.98

# 09/15/15 – Tuesday

36,161.02 / 58,587.98

# 09/16/16 – Wednesday

40,821.86 / 58,587.98

# 09/17/15

44,406.83 / 68,157.77

# 09/23/15 – wednesday

107.25 MB / 17,981.23 MB as of 09:51am

# 09/24/15 – Thursday

1. MB / 18,383.74 MB

# 10/15/15 – thursday

101.41 MB / 6,714.47 MB Updates needing files: 250

# 10/19/15 – monday

4,944.83 MB / 6,714.47 MB updates needing files 91, as of 07:23am.

5,051.06 MB / 6,714.47 MB updates needing files 86, as of 09:24am.

5,296.55 MB / 6.714.47 MB updates needing files 47 as of 14:21pm.

# 10/20/15 – Tuesday

User ocnfiguruations > admin templates > Microsoft word [ver ####] > word options > security > Trust Center > VBA Macro Notification Settings > Enabled (Disable all ecept digitally signed macros)

# 10/23/15 – friday

**Notes from Laptop PostIT:**

10/20/15

Still waiting for Darvin Glen to fix the plant acct. # associated to this laptop before Anabel willl release it over to Aaron Valencia

S/N: MXL5252N28

66001-12117

USSCPAC 1047LW7

HP Z BOOK 17 G2

1785 408759 – 0

30 8D 99 21 33 D0

# 11/2/15 – monday

**HBSS Show McAfee shield in Task Bar**

Open CMD as Administrator

Run: C:\Program Files (x86)\McAfee\Common Framework\**cmdagent.exe** with switch **/s**

Shield should now be available

**For Monday:**

Finish going through new STIG changes for Win 7. Maybe write up an explanation of the changes that have been made, such as the removed requirement for an “Auditors” group, and the fact that admins supposedly are allowed to RDP into workstations so long ans it’s ISSO documented, and a specific patch hass been installed from Microsoft that allows configuration of some “Restricted Administrator” mode. Be sure to document any changes in the Excel change management sheet.

Figure out how to fix the SWAN-VCTR certificate vulnerability. Possibly troubleshoot that issue Aaron Gould emailed about.

Already sent an email to Jackie from DLT Solutions and told her to contact Allison Dray about the maintenance contract renewal purchase.

Read up on KMS so we can figure out how we’re going to deal with OS keys in regards to our future .ISO project.

# 11/9/15 – Monday

## V-1074 “An approved DoD virus scan program is not used and/or updated”

Symantec Antivirus was previously listed as an approved virus scan program, but has now been removed. McAfee VirusScan Enterprise 8.8 remains on the list.

## V-1077 “Permissions for event logs must conform to minimum requirements

The permission for the Application, Security, and System event logs were previously mandated to be set as:

Administrators – Read and Execute

“Auditors” group – Full

SYSTEM – Full

Eventlog – Full

The updated STIG now allows the default permission settings on these logs to be allowed. These default permissions give the Administrators group Full access, while the other group permissions remain as they were. This updated STIG also removes the requirement for there to be an “Auditors” group, however allows for this group to remain on the permissions list with Full access. Current settings now look like this:

Administrators – Full

SYSTEM – Full

Eventlog – Full

GPOs in the SRDTE and SSCPAC domains for these settings have been changed to allow Full permissions for the Administrators group. No changes have been made to any “Auditors” groups or GPOs at this time.

## V-1091 “System halts once an event log has reached its maximum size”

In the past, the following Security Option setting was required:

“Audit: Shut down system immediately if unable to log security audits” 🡪 “Disabled”

The reason for this was that a shut-down system would cause a denial of service situation. The updated STIG removed this requirement entirely, leaving it up to the administrator to set is as either “Disabled” or “Enabled” or “Not Configured”. It seems that DISA doesn’t care about this setting anymore.

No action has been taken in either domain.

## V-1137 “An Auditors group has not been created to restrict acces to the Windows Event Logs”

This setting was previously required to create an “Auditors group for controlling the Windows Event Logs…” This requirement has been removed. Instead, the BUILTIN\Administrators group on system is now allowed to have full access to Windows Event Logs and manage them.

GPO STIG-1.010-WS is still enabled on the SSCPAC domain, and adds a group called “EventLogAuditors” to the group workstations. It will not be removed or changed at this time, because there is a chance that administrators are using it on their systems.

## V-14248 “Terminal Services / Remote Desktoop Services – Prevent users from connecting using Terminal Services or Remote Desktop”

The older STIG denied the use of terminal services to remote in to workstations, unless it was used for system administration, in which case it had to be documented with the ISSO. We decided to deny terminal services on workstations entirely to reduce the amount of documentable exceptions.

The new STIG still denies the use of terminal services to remote in to workstations unless it is used for system administrations, but now requires that system administration via terminal services be done using a new “Restricted Admin mode”. This mode can be installed using Microsoft patch detailed in KB2871997. We will not be making any changes to the current SSCPAC or SRDTE policy.

No changes will be made at this time, we still deny the use of terminal services to remote into workstations.

## V-14250 “Automatic updates must not be used (unless configured to point to a DoD server)

Previous STIG setting did not allow automatic updates to be configured, unless those updates came from a DoD server.

New STIG settings have removed this STIG entry, which would seem to indirectly allow automatic updates regardless of the source of those updates.

No changes are being made at this time in either domain.

## V-26473 “Unauthorized accounts must not have the Allow log on through Remote Desktop Services user right”

Previous STIG settings mandated that “Allow log on through Remote Desktop Services” be defined, but contain no entries (blank), and gave to exceptions to this rule.

New STIG settings, in conjunction with V-14250, allow Administrators to be granted this user right as long as it is documented with the ISSO, and that the “Restricted Admin mode” be used.

At this time, no changes are being made. Though, it could be argued that we could allow system admins to use terminal services to remotely administer their systems, but there would need to be strict documentation with the ISSOs.

## V-26496 “Unauthorized accounts must not have the Manage auditing and security log user right”

Previous STIG settings required “Manage auditing and security log” to only include the “Auditors” group.

New STIG settings now allows “Manage auditing and security log” to include “Administrators” and may include the “Auditors” group as well, since it was previously required.

## V-57637 “The operating system must employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs”

# 11/16/15 – Monday

## Upgrading LEM Appliance

I’ve burned the upgrade files to the CD currently sitting in the cd drive on Galapagos. What I need to do is paste the “TriGeo” and “Upgrade” folders that are on that CD into the root of the [\\srdte-fs01\swan\_install$](file:///\\srdte-fs01\swan_install$) share.

At the moment, following the prompt for **upgrade** and choosing the **(n)**etwork option doesn’t work, and yields an “Access Denied” error when I tried to connect to the share. The problem is that my LEM server doesn’t have access to the file server. Opening the console for LEM, entering **appliance** at the cmc prompt to enter the appliance sub menu, and then trying to use the **ping** option to ping the file server results in [NO] ping failures.

**Need to talk to John Harmon to make sure that the firewall rules allow traffic to the file server.**

**Dave took a look at the end of the day and found out that the problem had something to do with the type of packet that the LEM server sends out on a PING – it was being blocked by swan-watcher (the firewall?). By that logic, the other traffic that we’re trying to use in order to connect to the file server must also be blocked.**

# 11/23/15 – Monday

**Establishing domain trust with TBMCS – JAOC.RAPTOR / JAOC.RHINO**

We’re once again trying to establish a trust between SRDTE and the two TBMCS domains ran by Thomas Dang: JAOC.RAPTOR and JAOC.RHINO. According to him, there are credentials available to us that we can use to set up the trust from our end. According to my notes from OVER a year ago, those credentials are:

JAOC.RHINO

Thomas Dang sent an email with the new DC IP addresses, and DOM GUID. We will be using the same administrative account for his domain that we used previously: domadmin, pswd: Abcd\_123Abcd\_123. He is still going over the pre-scan checklists with his systems and will email us once they’re online so we can establish the trust.

If those credentials do still exist the password is long past expired and would need to be changed.

I do need to figure out – again, which type of trust it is that we need specifically: outgoing or incoming?

**ANSER: Need at least an INCOMING trust**

SRDTE

OTHER

**Trusted Domain**

**Trusting Domain**

**Trust Direction**

**INCOMING**

**OUTGOING**

**This allows machines in the “OTHER” domain (the Trusting Domain) to authenticate SRDTE credentials. This allows SWAN to use SRDTE\scanner.sa credentials in ACAS to scan systems in the “OTHER” domain.**

It turns out that the two TBMCS domains are at a Windows Server 2003 Domain Functional Level. According to Guy Anderson,

# 11/30/15 – Monday

**Dormant 335+ days account cleanup**

This Excel function allows you to search through a column of values and return “TRUE” or “FALSE” for another value

Tags: Excel lookup, vlookup, excel find

=IF(ISNA(VLOOKUP( <single cell value to look for> , <entire column range to search> ,1,FALSE)),FALSE,TRUE)

# 12/4/15 – Friday

**Troubleshooting SPLUNK and CRIME vulnerability**

Program files\SplunkUniversalForwarder\etc\system\local\README

This directory contains local settings that override all other settings, including the fault settings, and specific configuration file settings. For details on configuration files, see $SPLUNK\_HOME/etc/system/README directory for specific examples.

**Configuration file Stanza structure**

[stanza1\_header]

<attribute1> = <val1>

# comment

<attribute2> = <val2>

…

[stanza2\_header]

<attribute1> = <val1>

<attribute2> = <val2>

…

Configuration files are merged and layered from all of the different conf file locations. They are given precedence is this order:

* 1. System directory – highest priority
  2. App directory
  3. User directory – lowest priority

# 12/7/15 – Monday

**User Configuration >> Administrative Templates >> Microsoft Excel 2013 >> Excel Options >> Security >> Trust Center >> “VBA Macro Notification Settings” to “Enabled: Disable all macros except digitally signed macros”**

# 12/10/15 – Thursday

WSUS Updates 07:45 – Updates Needing Files: 272, Downloaded 312.66 MB of 6,584.42 MB

14:30 – Updates Needing Files: 127, Downloaded 1,363.02 MB of 6,584.42 MB

**Using CHARGER script to check accounts against LDAP**

1. Copy simple list of user accounts
2. Log on to charger.spawar.navy.smil.mil with standard account
3. create a text account to paste that list into
   1. vi somelist.txt
   2. right-click and choose “paste”
   3. make sure there are no extra spaces left over at the end
   4. enter :x to exit vi and save the changes
   5. run the check ldap script on that text document you just saved by entering
   6. check\_ldap\_user.sh somelist.txt
   7. .

# 12/31/15 – Thursday

**Attempting to troubleshoot DNS issue w/ SSCPAC-DC4**

Repadmin /replsummary ran as 14:41:05 on 12/31/15 showd that SSCPAC-DC4 failed with error of (1726) The remote procedure call failed. According to <https://support.microsoft.com/en-us/kb/2102154> a DNS issue can cause this, and sure enough I see DNS errrors in the event log on SSCPAC-DC4 constantly – it’s time to fix this bullshit.

The Microsoft page above lists a DCDIAG test that I performed:

Dcdiag /test:dns /v /e /f:dcdiagfile.log

That dcdiagfile.log should be in the C:\Windows\system32 directory. According to that, there are no HOST A or AAA records for my SRDTE domain controllers, and those SRDTE domain controllers are failing the BASIC tests that are run during that diagnostic.

I need to find out how to fix the HOST record problem and the BASIC test failures.

I also was able to successfully uninstall LEM and JAVA from SSCPAC-DC4, so it should hopefully STOP restarting mysteriously.

# 01/07/16 – Thursday

To Do on Monday:

* Look back over the PPT slides from the admin forum meeting and try to put as much of that info on the SWAN blog or somewhere where people can access it. We needs as much concise, effective communication about this re-imaging as possible.
* Work out a solution for the Service Desk to track the people that email back or not regarding their inactive SWAN accounts. Also make sure that they’re aware that this is about to come down to the pipe, and it’s going to add some work to their load. Talk with Pat.
* Review the i3lab domain trust problem. The last I remember, we were waiting to get some script command from Dave. I had previously sent that to Thomas Dang, but my computer crashed at some ppoint and I lost those emails. Maybe I can contact Thomas Dang to get that email from him that I sent with the command in it.
  + **HAVE DAVE CHECK HIS HIGH-SIDE EMAIL**. I would have emailed him the command results from TDANG, and that might have the command script text line in it that we need to sue.

# 01/12/16 – tuesday

**Post Meeting Details – External Domains**

The idea that we talked about in the hallway following our meeting in A411, related to how to keep track of whether or not a user was actually using the SSCPAC account that is created when they request access to SWAN. There are a few problems that we’ve realized:

1. We realized that users who send a request into the Service Desk to get SWAN access may not need an SSCPAC domain account. The only thing they require is approval to be on the SWAN network, and usually to get a SWAN email/ldap account. Some of these users are on other project domains, and never log on to the SSCPAC domain account that gets created for them.
2. The really big deal was thee idea to create additional “hosts” categories that go into LDAP. We currently have the (S) attribute, also known as the “Swan” attribute. If we could add subcategories below this that tell us exactly which domain a user is logging into, then we could better track the accounts that a user has. Ex: (S) – (ITF) or (S) – (JEDI) or possibly (S)-(ITF)-(JEDI)-(TBMCS) if they have multiple accounts in multiple domains. Regardless, this all needs to come back to a centralized tracking in LDAP from the registrar. Anabel said that she would speak with Taryn to figure out how feasible this is.
3. Other thing we talked abotut was following the naming convention that unclass uses for service accounts: **username.svc.sa** for example, for a service accounts of the .SA type – do similarly for MA or DA accounts. I suppose standard service accounts would just end with the SVC and that would be it. We need to start using this convention on our domain, then get in contact with the external domain admins and asks that they do the same in order to make account auditing easier, so we can identify their service accounts.

Kerberos protocol encountered an error while validating the kdc certificate during smartcard logon.

In an attempt to fix the HTTPS 88099 vuln, using SRDTE-MON as the test amchine, I adjusted the URL Rewrite to actually include a test message in the action value field. Hopefully this makes the header vuln go away.I kicked off a scan before I left. (as of 02/16/2016 this vuln has disappeared from ACAS on my member servers)

# 02/16/16 – Tuesday

Going through the IE11 STIG. The new V-64717 “Prevent ignoring certificate errors option must be enabled” cannot be implemented otherwise it would brick people from being able to access a lot of DoD websites on SIPRNet.

# 02/18/16 – Thursday

A couple of issues with patches/servers that have occurred today:

**SWANSADR** – attempting to apply Windows updates to this server, but it seems to get hung up on the 2 of 10 of the updates. “Security Update for Microsoft .NET Framework 4.5.2 on Windows 7…” is the one specifically. The first time this happened, I clicked the “Stop Installation” button, and rebooted the system. This is now the second time I’m attempting to install updates, and it seems to be hung again.

**SRDTE-DC1 | SRDTE-DC3 | SRDTE-DC4** – all of our SRDTE DCs are very slow to startup after a reboot, and especially slow to log in since about 12:00 noon today. I suspect that Windows Updates are to blame. All of the srdte DCs started acting slow after their post-update reboots. I’ve uninstalled the 11 offending updates from SRDTE-DC3, but it still seems to be taking a long time to restart – however this long restart was the one directly after I uninstalled all of those updates. I just restarted the system again around 15:25, and it seemed to take a normal amount of time to finish booting. It still took forever to log in.

**SRDTE-DC3** – I configured Winlogon logging by setting HKEY\_LOCLA\_MACHINE\Software\Microsoft\Windows NT\Current Version\winlogon\GPExtensions\{827D319E-6EAC-11D2-A4EA-00C04F79F83A}\ExtensionDebugLevel to 2, when it used to be set to 1. This will generate a log file at %systemroot%\Security\Logs\Winlogon.log . That should hopefully shed some light into what’s causing the extreme log on delays.

# 02/22/16 – monday

The SRDTE-DC servers are still being slow. I’ve tried taking SRDTE-DC3 out of the “Domain Controllers” OU and putting it into the “Blocking” OU, but that appears to critically break the functionality of a DC. Don’t do that. So I’ve moved it back into the DCs OU.

Meanwhile, my javery.ea account has been moved out of the “Enterprise Admins” OU and into that “blocking” OU to troubleshoot if maybe these issues are being caused by a User Configuration GPO setting. So far, it doesn’t seem like this has had any effect. The SRDTE-DC3 server is still being ridiculously slow to log in.

When I ran an IP reset “ **netsh int ip reset c:\resetlog.txt** “ and a WINSOCK reset “ **netsh winsock reset** “ the IP reset cleared all IP configurations on both SRDTE-DC1 and SRDTE-DC3. However, SRDTE-DC1 seemed to finally allow normal user logins, while SRDTE-DC3 remained slow.

I was also able to fix the “Group Policy was not able to apply TCPIP settings…” error messages by turning on the “IP Helper” service on a DC. I might try to do that on all my other systems that are persistently getting that error message, ONCE I figure out this problem with the SRDTE DCs.

# 02/26/16 – Friday

Another way to **Query Logged in User**

wmic /node:*hostname* computersystem get username

I’ve found that the only way to query who’s logged in to an SSCPAC system is to run it from another SSCPAC system with Administrative credentials that work on the system that is being queried. As I’ve also found out, the **RPC server is unavailable** error can still happen with this one too.

**How to see when the last unexpected shutdown occurred:**

Check the System Event Log for an Error Event ID **6008**. It should display the time of the previous system shutdown and tell if it was unexpected, like so:



# 03/15/16 – Tuesday

Here is the domain query to get the results necessary for the external dns in order to setup a domain trust:

**nltest /dsgetdc:<FQDN>.spawar.navy.smil.mil**

# 06/03/16 - Friday

Trying to test SmartCard logon on SRDTE DCs that I’ve updated the server certs for. They have new SHA256 certs from CA4.

SRDTE-DC4

Logon with SmartCard immediately after replacing old certs with new certs worked fine.

Logon after a reboot gave this error message:

**Signing in with a smart card isn’t supported for your account. For more info, contact your administrator.**

Removing the self-signed RDP cert gives the same error message and doesn’t seem to have any effect:

**Signing in with a smart card isn’t supported for your account. For more info, contact your administrator.**

SRDTE-DC1

Tried logging on with SmartCard after replacing old certs with new certs and it worked fine.

Logon after a reboot fails, gives error:

**Signing in with a smart card isn’t supported for your account. For more info, contact your administrator.**

**SRDTE-DC4**

Replaced new certs with the old certs again. Trying to log on with SmartCard immediately after fails with error:

**Signing in with a smart card isn’t supported for your account. For more info, contact your administrator.**

Trying to log on after a reboot works successfully.

Entered in CA4 cert chain info to Tumbleweed DV on SRDTE-DC4. The info stays even after a gpupdate and reboot, without having to export data and create new GPO.

Installed new SHA256 cert again and removed the old server certs from SRDTE-DC4.

Log off, and logging back in immediately after works.

Rebooting system, and logon FAILED with SmartCard with error:

**Signing in with a smart card isn’t supported for your account. For more info, contact your administrator.**

# 06/06/16 – Monday

* path equals 'C:\Program Files (x86)\SolarWinds\DameWare Remote Support'
* filename equals 'SolarWinds.DRS.Licensor.exe.config'
* xpath equals 'count(/configuration/runtime/enforceFIPSPolicy/@enabled) = 0 or /configuration/runtime/enforceFIPSPolicy/@enabled = "true"'

value\_of equals 'false'

Set <enforceFIPSPolicy enabled= to “true”

Also set this one:

* path equals 'C:\Program Files\keepass-2.23'
* filename equals 'KeePass.exe.config'
* xpath equals 'count(/configuration/runtime/enforceFIPSPolicy/@enabled) = 0 or /configuration/runtime/enforceFIPSPolicy/@enabled = "true"'

value\_of equals 'false'

Also this:

* path equals 'C:\Windows\dwrcs'
* filename equals 'SolarwindsDiagnostics.exe.config'
* xpath equals 'count(/configuration/runtime/enforceFIPSPolicy/@enabled) = 0 or /configuration/runtime/enforceFIPSPolicy/@enabled = "true"'

value\_of equals 'false'

Also these two:

|  |
| --- |
| * filepath equals 'C:\Users\javery\Documents\keepass-2.23\KeePass.exe.config' * path equals 'C:\Users\javery\Documents\keepass-2.23' * filename equals 'KeePass.exe.config' * xpath equals 'count(/configuration/runtime/enforceFIPSPolicy/@enabled) = 0 or /configuration/runtime/enforceFIPSPolicy/@enabled = "true"' * value\_of equals 'false' * windows\_view equals '64\_bit' |
| Collected Item Properties: | * filepath equals 'C:\Program Files (x86)\SolarWinds\DameWare Remote Support\SolarwindsDiagnostics.exe.config' * path equals 'C:\Program Files (x86)\SolarWinds\DameWare Remote Support' * filename equals 'SolarwindsDiagnostics.exe.config' * xpath equals 'count(/configuration/runtime/enforceFIPSPolicy/@enabled) = 0 or /configuration/runtime/enforceFIPSPolicy/@enabled = "true"' * value\_of equals 'false' * windows\_view equals '64\_bit' |

Finally this:

* filepath equals 'C:\Program Files (x86)\SolarWinds\DameWare Remote Support\SolarWinds.MRC.Licensor.exe.config'
* path equals 'C:\Program Files (x86)\SolarWinds\DameWare Remote Support'
* filename equals 'SolarWinds.MRC.Licensor.exe.config'
* xpath equals 'count(/configuration/runtime/enforceFIPSPolicy/@enabled) = 0 or /configuration/runtime/enforceFIPSPolicy/@enabled = "true"'

value\_of equals 'false'

# 06/27/16 – Monday

**ACAS Plugin 35450 fix for SDREN-DC1**

Here’s the fix directions I found and tried out:

1. Open DNS management snap-in
2. Right-click DNS server and select properties
3. Select the advanced tab
4. Check the box for disable recursion
5. Select the forwarders tab
6. Click the edit button and remove each forwarder listed and click OK
7. Uncheck the box for use root hints if no forwarders are available
8. Select the Root hints tab
9. Right select each entry and click the remove button
10. Click Ok

# 06/30/16 – Wednesday

**ACAS Plugin 91603 MS-16-075: Security Update for Windows SMB Server (3164038) \*\*\*BSoD Issue\*\*\***

**Actual KB3161561 – Causes BSoD when Shavlik pushes to systems**

Microsoft notes on their KB article (<https://support.microsoft.com/en-us/kb/3161561>) that there is a known issue when attempting to access DFS namespaces (such as [\\contoso.com\SYSVOL](file:///\\contoso.com\SYSVOL)) on systems configured to require mutual authentication that have this patch applied. Microsoft’s workaround is to set the **SmbServerNameHardeningLevel** registry entry to **0**. However, **SmbServerNameHardeningLevel** is the corresponding registry key to the Group Policy Setting **Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> “Microsoft network server: Server SPN target name validation level”** which is required to be set to **“Accept if provided by client”** which sets that registry entry to **1** by Windows 7 V1R22 STIG **V-21950 The service principal name (SPN) target name validation level must be configured to Accept if provided by client**, which is a **CAT 2** finding

**\*\*\*UPDATE 8/22/2016\*\***

**KB3179573** was listed on that Microsoft support page (above) as a potential fix for the problems caused by KB3161561. I’ve installed it on Galapagos, and verified that it does update the **C:\Windows\system32\drivers\srvnet.sys** file to version **6.1.7601.23491**, while ACAS only requires for plugin 91603 that the version be at least 6.1.7601.23452. Currently scanning Galapagos to see if that will clear plugin 91603 in ACAS. Still need to test a Shavlik scan on it to make sure it doesn’t BSoD.

# 07/29/16 – Friday

**16-044 Recurring vulnerability on CAYMAN and LANAI (SDREN)**

This patch vulnerability keeps coming back. As of today, I’ve applied KB3146706 x64 on both the workstations, and verified that the file C:\Windows\System32\ole32.dll version is updated to 6.1.7601.23392 from old version 6.1.7601.19131. The version stayed after a reboot. But, something keeps causing the file version to revert back.

**SDREN OCSP** –Mark sent an email on unclass 7/29/16 at 11:45am w/ an attachment. Read that.

**POP3s** – The original plan was to block POP3 from the switches on Monday, 8/1/16, however not enough users know about the requirement to use POP3s instead of POP3, so we’re waiting. We’re going to send out emails on UNCLASS and SIPR to every user w/ instrucitons for Outlook and Tumbleweed on how to set that in their client. Then we’ll have dave watch on the server and see who’s still accessing w/ port 110 (POP3) near the end of the month. We’ll call/email those people and have them set their email up properly. I wasn’t able to find a GPO setting or registry entry that could be pushed from the domain to quickly set this for everyone.

**Kim Trieu and Edge** – She was trying to access a site from her system and noticed that the “Developer Tools / Document Emulation Mode” was set to “Edge” by default. She tried to set it back to 7 and restart IE, but restarting IE caused it to default back to Edge again. She called me asking for assistance, but I couldn’t find any STIGs or GPOs that are set to control that, so I told her to check UNCLASS for instructions on fixing that, and said that I’d be available to talk on Monday if she still needed assistance.

**SCCM Certificate Vulns** – check that those are the only ones still showing up on ACAS. Everything else regarding Microsoft patches should be taken care of. Need to take snapshots of each SCCM server, and then fix those cert vulnerabilities. Be sure to export all the certs in the cert MMC before doing anything just in case you screw something up. Don won’t be able to do any SCCM stuff for at least half a day.

# 08/12/16 – Friday

**Trying to get GemX Service to start**

Event viewer Application log showed event 10005 saying DCOM attempted to start the service netprofm, but couldn’t because dependencies wouldn’t work.

I looked at the dependencies for netprofm, and DHCP was included, which was disabled as a service. I enabled the DHCP service, set it to automatic, and started it. After that, netprofm started.

Tried starting the GemX service, but it still woudlnt go.

**FIX =** Update JAVA\_HOME environment variable to the updated path to the JRE directory each time Java is updated. Otherwise the GemX service won’t start properly.

# 08/24/16 – Wednesday

**VMWare vCenter Upgraded**

DTA’d over the necessary update installation files, and updated from vCenter version 5.0.0.45571 to version 5.0.0.47492. Had to temporarily turn off HBSS, and extend the disk drives since they were running out of space. During the installation process a “VC” password is asked for, and I was able to get that from Dave.

# 09/01/16 – Thursday

**Certificate Thumbprint Registry Entry**

After replacing the old SHA1 server certificate on SRDTE-DB01 with a new SHA-256 cert, the SNETREG.SPAWAR.NAVY.SMIL.MIL website stopped working. Scott found out that the problem was because the registry key:

**HKEY\_Local\_Machine\SOFTWARE\Microsoft\Microsoft SQL Server\MSSQL.X\MSSQLServer\SupserSocketNetLi\Certificate**

Needed to have the **Thumbprint** value set to the same thumbprint as the new SHA-256 certificate. Once that was set on SRDTE-DB01 registry, then the web application could once again communicate with the database server.

We will need to do the same thing with SRDTE-DB03 when those certs get updated so that it doesn’t break SNETREG-DEV.SPAWAR.NAVY.SMIL.MIL.

# 09/22/16 – Thusday

**(35450) DNS Server Spoofed Request Amplification**

It looks like I had already set a few settings on SRDTE-DC4 to clear this vulnerability, since it is not flagging in ACAS like the other SRDTE DCs. The DNS properties had been set to check the box for “Disable recursion (also disables forwarders)” on the Advanced tab. The Root Hints tab was also empty since I had deleted all those root hints that were listed there. I also had edited the C:\Windows\System32\DNS\CACHE.DNS file by commenting out all the root hints entries. This prevented the root hints from popping back up in the Root Hints tab in the DNS properties after a reboot. I had made a copy of the CACHE.DNS file called “CACHE – Copy.DNS” in that same folder in the event that I needed to revert back to previous settings.

On SOUTHBROTHER, I’ll do the same thing. I’ve checked the box in the Advanced tab to “Disable recurions (also disables forwarders)”. I’ve made a copy of the CACHE.DNS file, and edited the original by commenting out all the root hints entries. Next I’ll delete all root hints listed in the root hints tab. Rebooting SOUTHBROTHER to make sure the root hints don’t come back.

Same action taken on SRDTE-DC1.

Issue appears to be **SOLVED** at least on SRDTE DCs. The vulnerability isn’t coming back up in scans, and unless some sort of network problem occurs from the changes that have been made, I’ll let everything stay as it is.

Will need to implement on SSCPAC DCs at the end of the day when I reboot them for Windows Updates.

**UPDATE:** Checking the box to “Disable recursion (also disables forwarders)” was a bad idea, since it broke DNS resolution on any systems that were pointing to my DCs for DNS – the DC DNS couldn’t then forward requests to Dave’s external DNS for final resolution. So, I’ve gone in and unchecked that box, rebooted DCs, and verified that the root hints tab remains empty after the server starts back up. So far, a vulnerability scan of SOUTHBROTHER shows that everything is fine, so that vuln. Hasn’t popped back up.

# 09/23/16 – Friday

**SRDTE-WEB1 Mysterious Network Connection Failure**

After shutting down SRDTE-WEB1 to take a snapshot, and then booting the system back up, I was unable to log in using my domain credentials because there was no network connectivity to the server. I verified that it was not pingable from my workstation either. I logged in to SRDTE-WEB1 using the local swanroot administrative account, and opened up the Network Properties. The top portion of that window where is says “View your active networks” wasn’t displaying, but showed an error message saying that Service or dependencies failed to start. I rebooted the system a few times, and even tried booting into Safe Mode, but it still wasn’t working. Next I opened Services, and enabled the DHCP service which had been disabled. This supposedly shouldn’t cause any problems on the server since it is set to use Static IP address. After I enabled DHCP, and started the Network Level Assistance (something like that?) service, the normal Network Connections window popped up, but there was still no network connectivity. If I opened the Network Adapter Properties, I could see that there were packets being sent AND received, but I couldn’t even ping the Gateway. I rebooted the system one more time, and it suddenly worked. I have no idea why… I decided to stop touching SRDTE-WEB1 for the rest of the day.

# 09/28/16 – Wednesday

**SRDTE-WEB1 Self signed cert issue**

The old SHA1 cert was removed yesterday afternoon. The new SHA256 cert has been on the server for a while now. The PowerShell fix for 57582 still needs to be ran. All older certs were exported out of the certificate store onto the \PKI directory, and the current cert hash that is set in the WMI variable for Terminal Services has been saved to the SRDTE-Web1 desktop.

# 10/4/16 – Tuesday

**Windows 10 IP address 10.10.10.10 problem**

1. Open IP settings, and set IP address / Subnet Mask / Default Gateway / DNS correctly.
2. Open administrative command prompt
3. Enter: netsh winsock reset catalog
4. Enter: netsh int ip reset reset.log
5. Restart system

# 10/11/16 – Tuesday

**Activate Windows 10 Installed from CD**

We ran into a problem where a system with Windows 10 installed from our CD was not able to have the product key manually typed in through normal means. The fix was to search on the workstation for “**slui 3**” and run that as an administrator. That would bring up the window where you could enter in the product key. From there, you would choose the option to activate Windows over the phone. As with the normal Windows 10 phone activation process, skip the first prompt where you are asked if you are activating Windows 10, and wait until it asks what type of product you are activating – say “Windows”. After that, follow along with the standard phone activation prompts to active the key.

# 10/27/16 – thusday

TCP 6129 Dameware Ports

TCP 5985 PowerShell Remoting (Enter-Pssession) (HTTP)

TCP 5986 PowerShell Remoting (Enter-Pssession) (HTTPS)

**How to See Firewall Deny Logs**

SSH Into inmon.spawar.navy.smil.mil and log in with user ID and password

Dave has setup an alias so all you need to type is **watchnoc**

Alternatively, you can type **sudo /usr/local/bin/watchnoc**

# 11/04/16 – Friday

**“SSL 64-bit Block Size Cipher Suites Supported (SWEET32) (94437)”**

Servers are using 64-bit block ciphers, (3DES / “triple DES”) and should be configured to use AES instead.

3DES BAD AES GOOD

# 11/30/16 – Wednesday

**SHA 256 Schedule**

Server admins encouraged to request and test **SHA-256 certs on servers prior to 12-16-2016**. If problems are identified prior to this, a new SHA1 certificate can be issued, giving additional time to develop a solution. If the problem is not identified until after 12-16-2016, there will be no ability to roll back to a newly issued SHA1 cert.

**SHA items on ACAS**

* **ACAS detected 49 IPs with SHA1. Set to CAT 1 and put on 3 week block list.**
* **RESOVLED: Exceptions for self-signed SHA1 should go to IA Special Request Form.**
* **RESOLVED: Exceptions for external webservers that can’t go to SHA2 DoD need IA Special Request Form.**
* **Some self-signed certs can be upgraded to SHA2.**

**PKI Risk Assessment Pages**

IA PKI Risk Assessment wiki page:

<https://wiki.spawar.navy.mil/confluence/display/SSCPACIA/Risk+Assessment+Review>

SSC PAC PKI Office wiki page:

<https://wiki.spawar.navy.mil/confluence/display/pki/SIPRNet+PKI>

# 12/12/16 – Monday

**Installing Server Certificates**

Save the shorter block of certificate hash text to a text file, and save that file with a .cer extension

Certreq –accept <file>.cer

**Server 2012 Hour Long Startup Problem “Applying Audit Policy Configuration settings…”**

Via process of elimination I found out that the **DenyNetworkAccess\_Logon\_Script** was the GPO that was causing the long log on problem. Don had added his WindowsAppXRemove.ps1 startup script to my existing DenyNetworkAccess startup script, and I think Don’s script was causing errors on the Windows Server 2012 systems, creating the 60 minute hang up problem we witnessed.

# 12/13/16 – Tuesday

**SSL 64-bit Block Size Cipher Suites Supported (SWEET32) (94437)**

I’m still getting this vulnerability on all my servers. I’ve looked at the “Non-64-bit Cipher Suites SWEET32” GPO that was setup to fix this problem, and noticed that one DES cipher “SSL\_CK\_DES\_192\_EDE3\_CBC\_WITH\_MD5” was still included in the list. I’m going to remove that and see if it makes a difference in clearing this plugin.

**SSL Self-Signed Certificate (57582) (35291)**

Southbrother (should be fixed?)

SRDTE-WEB1

SRDTE-SCCM-SQL1

# 12/14/16 – Wednesday

**Tumbleweed Desktop Validator updates – re: John Harmon**

Changed Tumbleweed 4.12 on GALAPAGOS, exported those settings, then uploaded that to SYSVOL as **dv-standard-gpo\_4.12\_swan\_ocsp.txt** and that is linked to the **Configuration-Tumbleweed-Standard-4.12-conf\_SWAN\_OCSP** GPO.

-restarting GALAPAGOS to ensure settings will stick in 4.12

-appears to work successfully

Changed Tumbleweed 4.11 on MIDWAY, exported those settings, then uploaded that to SYSVOL as **dv-standard-gpo\_4.11\_swan\_ocsp.txt** and that is linked to the **Configuration-Tumbleweed-Standard-4.11-conf\_SWAN\_OCSP** GPO.

-will restart MIDWAY to test and ensure 4.11 settings stick.

-MIDWAY appears to have successfully received the configuration settings too.

Currently two GPOs are still linked in the SRDTE directly under the **SRDTE Users and Computers** OU, **Configuration-Tumbleweed-Standard-4.10-conf** and **Configuration-Tumbleweed-Standard-4.11.conf**. I’m going to unlink the 4.11 GPO, and then link my two SWAN OCSP GPOs: **Configuration-Tumbleweed-Standard-4.11-conf\_SWAN\_OCSP** and **Configuration-Tumbleweed-Standard-4.12-conf\_SWAN\_OCSP**.

# 12/15/16 – Thursday

**SWANSADR Patching**

MS16-144 still showing up. Waiting for [December 2016 Security Monthly Quality Rollup for Windows Server 2008 R2 for x64-based Systems (KB3207752)](https://patches.csd.disa.smil.mil/SecureDownload.aspx?sfs=asset&fGuid=188236) to download so I can try installing it on SWANSADR. Was still downloading when I left.

16-146, 16-155, and 16-153 are still showing up as well…

# 01/04/17 – Wednesday

**Problems connecting via RDP into Server 2008 systems**

Going to try unlinking “Remediation\_PID\_Enforce\_NLA\_for\_Terminal\_Services” GPO from the Domain Controllers GPO. That should un-grey the option to NOT require Network Level Authentication for RDP connections. Going to see if that makes a difference.

* Restart SOUTHBROTHER
* Check the box to NOT require Network Level Authentication
* Test RDP connection into SOUTHBROTHER

UPDATE (01/05/2017) I’ve re-linked “Remediation\_PID\_Enforce\_NLA\_for\_Terminal\_Services” GPO in the Domain Controllers OU on SRDTE.

ROOT CAUSE: The requirement to use FIPS-compliant encryption settings that were configured on client workstations was conflicting with the recent configuration changes made to the domain that turned off 3DES encryption ciphers (SWEET32 vulnerability). This was a conflicting problem because FIPS requires the use of 3DES specifically. The problem only affected Windows 2008 servers because that is an older operating system that used older encryption protocols – specifically 3DES (I think).

FIX: I turned off the FIPS requirement configuration setting in both the SRDTE and SSCPAC domains by disabling that setting in each domains’ Windows 7 GPO package. I also had turned off the SWEET32 vulnerability fix GPO in both domains, just to ensure that all possible root causes had been eliminated while I was troubleshooitng**. I’ve since turned the SWEET32 GPO back on in SRDTE**. Since FIPS has been turned off, this should not cause any problems, though I want to wait at least a week or two before I decide that we can turn SWEET32 GPO back on in the SSCPAC domain.

UPDATE (01/10/2017) **I had to turn off the SWEET32 GPO in the SRDTE domain again.** It looks like turning the SWEET32 vulnerability fix GPO back on broke the ability to RDP from workstations into Server 2008 systems again. Even with the FIPS requirement setting turned off on these workstations, the SWEET32 fix, which removes all instances of 3DES encryption, breaks RDP functionality into those Server 2008 systems. Is that because Server 2008 boxes only use 3DES to encrypt their RDP connections?

Turning off SWEET32 and restarting NIKOA doesn’t immediately fix the problem of it not being able to RDP into SWAN-VCTR. I think I’ll leave the systems as they are until lunch time and then try again.

# 01/11/17 – Wednesday

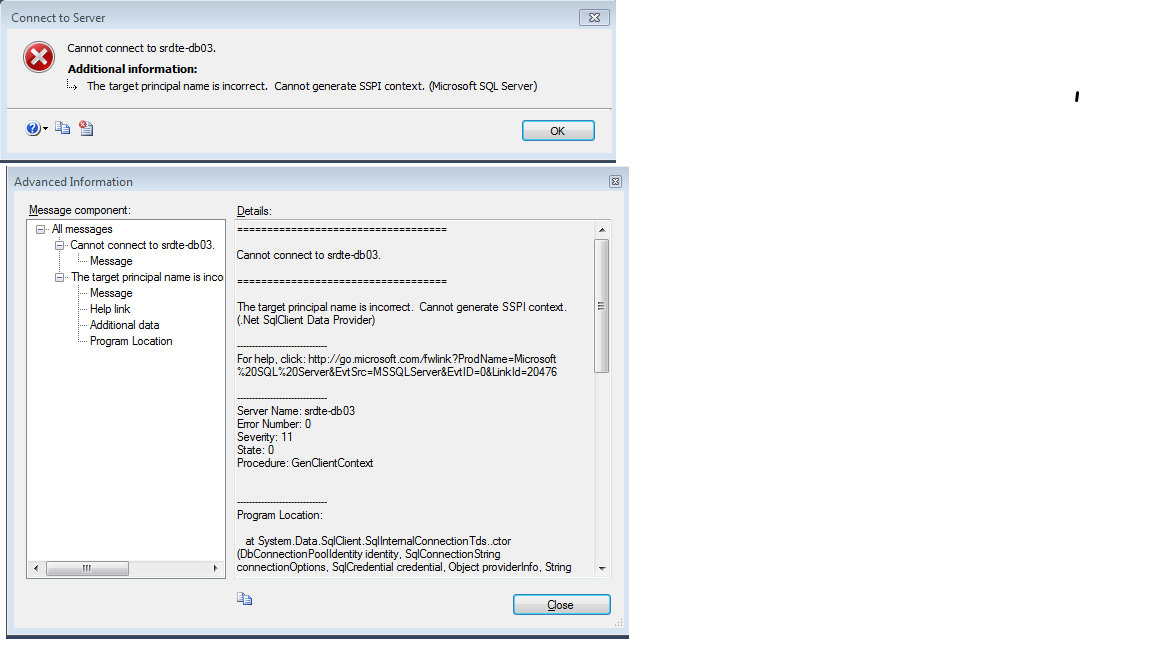
**December .NET Patch installation problems**

Pamati and other systems still had plugin **MS16-155: Security Update for .NET Framework (3205640) (95772)**

Successfully installed **“.NET Framework 3.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2 on Windows 7 and Windows Server 2008 R2 for x64 (KB3205402)”** specifically the **ndp45-kb3210139-x64.exe** patch.

The old version of c:\windows\microsoft.net\framework\v4.0.30319\system.data.dll was 4.0.30319.34297 and the new should be 4.0.30319.36373

# 01/19/17 – Thursday

**SQL SRDTE-DB03 Connection problem**

Scott got this error message when attempting to connect to SRDTE-DB03 through the SQL management application from his workstation. The fix was to go on SRDTE-DB03, edit the “SQL Service” service, and change the credentials that it was running under. It was set to run with SQLService.ma.svc . Scott changed it to run under local SYSTEM credentials, and that fixed the problem.

**Firefox STIGs work**

Firefox locations:

C;\Program Files (x86)\Mozilla Firefox\firefox.exe 🡨 x86 directory

C:\Program Files\Mozilla Firefox\firefox.exe 🡨 64-bit directory

WMI Syntax: SELECT \* FROM CIM\_Datafile where (Name=’c:\\program files (x86)[\\mozilla](file:///\\mozilla) firefox\\firefox.exe’)

Local-settings.js goes in C:\Program Files (x86)\Mozilla Firefox\defaults\pref directory, or the other 64-bit Mozilla install directory.

# 01/24/17 – Tuesday

Working with Derek Fox on possibly corrupt profile error/ issue. His profile object exists at **SSCPAC Users and Computers \ San Diego \ Seaside \ MGF \ Users \ Derek A. Fox**. I’m going to put him temporarily in the blocking OU to see if that makes a difference.

# 01/25/17 – Wednesday

## Tumbleweed Enterprise Domain Controllers task:

I’m going to split up the Tumbleweed Enterprise config GPO so that the SRDTE domain controllers and SSCPAC domain controllers are receiving different GPOs. This will allow us to change configs if necessary, especially in the case of troubleshooting like we had to do this last Monday when SmartCard authentication stopped.

The old GPO that both domains were receiving was named **Configuration-Tumbeweed-Enterprise-4.11-conf**. That GPO points to a config file on SRDTE\SYSVOL called **dv-enterprise-gpo\_4.11.txt**.

The new GPO for SRDTE is called **Configuration-Tumbleweed-Enterprise-4.11\_SRDTE-conf**. I have already linked it in the SRDTE Domain Controllers OU, and unlinked the old GPO. I’ve also adjusted this new GPO to point to a newly named configuration file: **dv-enterprise-gpo\_4.11\_SRDTE.txt**.

**Update 01/30/2017: dv-enterprise-gpo\_4.11\_SRDTE.txt** is a good working configuration. I’m going to make a master copy of that first. Next I’ll rename the other GPO (tumbleweed\_4.11\_012517\_logon\_authentication\_ON.txt) so that IT is named Configuration-Tumbleweed-Enterprise-4.11\_SRDTE-conf. That will allow me to test switching Tumbleweed back over to verifying certs so we can see if it breaks CLO again.

That did not fix the CLO logon problem. Right after I switched the DCs over to the “regular” Tumbleweed Enterprise config that validates each cert, the logon process broke with an error message saying “The domain specified is not available.”

## Derek Fox <dafox> corrupted profile

Spoke with Jack McNabb on the phone and Damewared into the box that Derek was logging in to. Saved a copy of the error message to my Pictures folder. Look in the event log after I logged in with SA credentials and saw around 10 errors citing roaming profile issues copying the ntuser.ini file. Told Jack about this. He will research some on his own to see if its something that can be fixed from his profile server side. Otherwise, the last step effort will be to completely delete Derek’s existing user account and profile directories, and create from scratch on Friday. Jack will let me know how it goes first before we need to resort to that last ditch effort, though.

# 01/26/17 – Thursday

## Shavlik & External Certs Issue

Adam thinks that my GPO that applies the external certs may be overwriting the certs every time, and prompting the system for a reboot somehow? That doesn’t make sense to me. BUT, in the interest of troubleshooting I’ve temporarily turned off the “DoD Approved External Certs” GPO linked under SRDTE Users and Computers.

## SWEET 32

Going to try linking the **Non-64 bit Cipher Suites SWEET32** GPO under the “Domain Controllers” OU in SRDTE to clear the vulnerabilities I’m seeing affect

# 01/27/17 – Friday

Nexscan3w Turned on **Application Layer Gateway Service.**

# 01/30/17 – Monday

Going to start trying to clear the remaining

**42873 SSL Medium Strength Cipher Suites Supported** and the

**94437 SSL 64-bit Block Size Cipher Suites Supported (SWEET32)** 73 machines affected – 11 are mine

I’ve linked the **Non-64-bit Cipher Suites SWEET32** GPO under the SCCPAC SWAN > Member Servers OU so that I can test the 94437 vuln that is affecting SSCPAC-AD1 through SSCPAC-AD4. It seems like it cleared the vulnerabilities.

I think that I can apply the GPO fix directly to the affected servers, but not any workstations (except maye the few affected) and have everything be ok. I’m going to try with applying it to SWAN-VCTR and leaving it for a while. Then I’ll try to RDP into the server from some workstations to make sure that RDP still works, since that was what broke in the past.

Applied to SRDTE-SCCM, SSCPAC-DC1, SSCPAC-DC2.

**SSCPAC-DC1 works with RDP after applying SWEET32. SSCPAC-DC2 does NOT work after applying SWEET32.**

**Problem is still FIPS.** Most machines are still having the FIPS setting applied locally, via the either gpedit.msc or hard-set registry settings at HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\Lsa\FIPSAlgorithmPolicy\ value:ENABLED value should be set to “0” in order to turn FIPS off. I’ve gone into all the GPO settings I could find, and have set the local registry settings to set that value to “0”, whereas many of them were setting it to “1” before.

**Turned Non-64 bit Cipher Suites SWEET32** **GPO back on in SRDTE and SSCPAC domains**.

I got a list of all Windows Server 2008 systems in SSCPAC, remotely adjusted the FIPS settings in the registry (on those I could connect to) and then saw them change back 90 minutes later. Had to go back in and adjust the **w2kk8\_ms\_base\_gpo** and **w2k8\_R2\_ms\_base\_gpo** settings to turn FIPS to “disabled”.

# 01/31/17 – Tuesday

Linked the **STIG-Firefox 32-bit** and **STIG-Firefox 64-bit**

**Token Reliability Testing w/ Gary Delgado**

* SafeNet SC650 v1
* SafeNet AT SC650 v3.3c

Phone call notes:

4.0 SafeNet or GD token’s being used, they want to track. Gary said he’ll talkl to Linda to get the tokens we need to help to help them test this.

D.O.T. & E. doesn’t like the failure rate. Newr tokens should work better, and this needs to be proven by tracking in service tokens.

PowerShell script. Output was being possibly put up on IntelShare. Maybe. Gary’s not sure. Gary said he’ll get the info when he talks to Linda, and get us the details on the script, what’s outputted, and how often the NSA wants us to upload this result data, and where to upload it.

Testing phase is being called “TRT” should be going on for another 6 months.

**Made a change** to Microsoft\_Office\_2013\_User GPO for Set the policy value for User Configuration -> Administrative Templates -> Microsoft Word 2013 -> Word Options -> Security -> Trust Center -> Trusted Locations "Disable all trusted locations" to "Enabled".. Set it from “Disabled” to “Enabled” STIG ID: DTOO133 Rule ID: SV-53571r1\_rule Vuln ID: V-17471

**Maybe make a change**

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKCU\Software\Policies\Microsoft\Office\15.0\word\security

Criteria: If the value VBAWarnings is REG\_DWORD = 2, this is not a finding.

Fix Text:

Set the policy value for User Configuration -> Administrative Templates -> Microsoft Word 2013 -> Word Options -> Security -> Trust Center "VBA Macro Notification Settings" to "Enabled (Disable all with notification)".

**Made change**

**Group ID (Vulid):** V-17520 **Rule ID:** SV-53572r1\_rule **Rule Version (STIG-ID):** DTOO134

Changed from “Enabled” to “Disabled”

Verify the policy value for User Configuration -> Administrative Templates -> Microsoft Word 2013 -> Word Options -> Security -> Trust Center -> Trusted Locations "Allow Trusted Locations on the network" is set to "Disabled".   
  
Procedure: Use the Windows Registry Editor to navigate to the following key:   
  
HKCU\Software\Policies\Microsoft\Office\15.0\word\security\trusted locations   
  
Criteria: If the value AllowNetworkLocations is REG\_DWORD = 0, this is not a finding.

**Enter-PSSession** setup

I was able to get into SWAN-VCTR by running **Enable-PSRemoting** from an administrative PowerShell window on SWAN-VCTR. It presented 4 prompts, responded [Y] Yes to all, and then it worked.

# 02/01/17 – Wednesday

First thing when I get in tomorrow I want to test out CLO issues w/ John. Re-enable logon authentication in the DCs Tumbleweed policy. Get a good sampling of errors from that. Next, John will turn off BORACAY and MACTAN so that we can test if Tumbleweed still fails relying on DISA.OCSP alone. If DISA.OCSP still fails, then that’s a good indication that the problem isn’t our OCSP servers in SWAN. Not really sure where to go from there, but it’s more information.

# 02/02/17 – Thursday

**Re: SWEET32 (94437)** – 4 of my servers were still flagged with the SWEET32 vuln. All of them have the GPO being applied, but these servers have not been restarted. I’m guessing that restarts will be required to actually apply the non-3DES settings and clear this vulnerability.

# 02/06/17 – Monday

## Server Message Block (SMB) Protocol Version 1 Unspecified RCE (uncredentialed check) (96982)

Windows 8 and Server 2012 have new PowerShell cmdlet **Set-SMBServerConfiguration**. You do not have to restart the computer after you run the **Set-SMBServerConfiguration** cmdlet.

To obtain the current state of the SMB server protocol configuration, run: **Get-SMBServerConfiguration | Select Enable SMB1Protocol, EnableSMB2Protocol**

To disable SMBv1 on the SMB **server 2012**, run: **Set-SmbServerConfiguration –EnableSMB1Protocol $false**

To disable SMBv1 in **Windows 7**, set registry value: **Set-ItemProperty –path “HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters” SMB1 –Type DWORD –value 0 –force**

The registry entry you’re modifying is **SMB1.** REG\_DWORD: 0 = Disabled. REG\_DWORD: 1 = Enabled. Default: 1 = Enabled.

When applying to SSCPAC, look for OUs that block inheritance and apply to them as well.

“Failed to run task sequence” An error occurred while trying to receive policy 0x80004005 .

# 02/08/17 – Wednesday

**SSL RC4 Cipher Suites Supported (Bar Mitzvah) (65821)**

Problem popping up on SSCPAC-DC2. What I’ve tried is editing local GPEDIT.MSC, and taken out the 3 RC4 entries:

TLS\_RSA\_WITH\_RC4\_128\_SHA

TLS\_RSA\_WITH\_RC4\_128\_MD5

SSL\_CK\_RC4\_128\_WITH\_MD5

**MTC2-SOA system moves**

At Paul Camarata’s request, I moved C2RPCSIPRWKST2 / 3 / 10 / 14 from the C2RPC\Computers\Win7 OU, into the MTC2-SOA\Computers OU.

KEYLAGO GoogleChromeStandaloneEnterprise560292487.msi “File validation failed”

KEYLARGO Firefox Setup 51.0.1.exe “File validation failed”

Reboot, and try Shavlik again. If it fails again, try installing the certs located at every step of the chain on those install files.

After a reboot, Shavlik successfully installed those 2 patches on KEYLARGO…

BAHAMAS lync2013-kb2881013-fullfile-x64-glb.exe

BAHAMAS excel2013-kb2920753-fullfile-x64-glb.exe

CAICOS rrlync2013-kb2881013-fullfile-x64-glb.exe

CAICOS excel2013-kb2920753-fullfile-x64-glb.exe

# 02/14/17 – Tuesday

**Phone conference w/ NAOC2 and SWAN**

Sounds like nothing will happen until they talk with the Joint Community before they can remove the firewall/shutdown the firewall. Sounds like nothing else is going to happen until that occurs.

**SMB1 Additional Fix**

**HKLM\SYSTEM\CurrentControlSet\services\LanmanWorkstation\**

**DependOnService REG\_MULTI\_SZ bowser mrxsmb20 nsi**

**HKLM\SYSTEM\CurrentControlSet\Services\mrxsmb10\**

**Start REG\_DWORD 4**

Systems had DependOnService set to “bowser MRxSmb10 MRxSmb20 NSI” and had Start set to “3”

**Papergirl - HP LaserJet Pro 400 color MFP m475dw**

Has vulnerabilities that can’t be fixed with any additional configurations. Problems exist at the firmware level. The current firmware is 20150126 which is the same version that is listed on HPs website. I don’t think this model is getting updated anymore. Probably EOL.