Active Directory/Windows and UNIX/Linux Auditing

Baccam Consulting, LLC
www.securityaudits.org
tanya@securityaudits.org
Objectives

- Going to look at the higher risk areas as it relates to Active Directory/Windows and UNIX/Linux Audits

- There are additional areas to address, but we will address the primary controls that should be in place
Overall Agenda

- Background
- Users/Groups
- Permissions
- Passwords
- Patching
- Auditing/Logging
Active Directory Definition

- A registry for the network, info about AD objects
  - Objects include servers, volumes, printers, users, computers, etc.
- Centralized configuration control for management of objects and their relationships on a network
- Active Directory Domain Services (AD DS) stores directory data and manages communication between users and domains

- http://www.microsoft.com/activedirectory/
AD Design and Topology

- Review AD design documentation
- Review AD topology
AD Terms

- **Forest**
  - Set of one or more domains with a shared schema
  - Forest is the security boundary, not the domain
- **Tree**
  - One or more domains in a contiguous namespace
- **Domain**
  - Core logical unit of AD
  - One level below the forest
- **Organizational Unit (OU)**
  - Logical container in the domain environment
- **Objects**
  - A single entity and its attributes
What else can AD do?

- Authentication
- Access Control
- Apply Security Policy
  - Templates can be used to control password policies, account lockout policies, Kerberos policies, auditing policies, user rights, and other policies
- Auditing
- Data protection for data at rest
  - Encrypting File System (EFS)
  - Digital signatures
- Data protection for data in transit
  - IPSec
- PKI
- Trusts
Windows Key Concepts

- Workstation versus Servers
- Workgroups versus Domains
  - Workgroups require accounts on each individual system
  - Does not deal with security
  - Domain specifies the management boundary in AD and all systems share a common database of accounts
- Local versus Domain accounts
  - “Layers” of authentication
  - Ex. Member servers local account policy should be reviewed since there is little need for machine local accounts, workstations may or may not need local accounts
Registry

- Stores information about the system and how the system is configured
- TONS of information is available in the registry
- A “database” of information that can be queried or modified when a user has the appropriate permissions
  - Users should not directly change registry values unless they really know what they are doing!
- Hives of information
  - HKEY_CURRENT_USER: Stores information about the current user’s preferences and configuration.
  - HKEY_LOCAL_MACHINE: Stores information about the hardware, operating system and application settings for the local system.
  - HKEY_USERS, HKEY_CURRENT_CONFIG, HKEY_CLASSES_ROOT
- Tools: regedit, Dumpreg
File Systems

- NTFS
  - Offers many features
    - file-level security, compression, auditing, encryption, etc.
  - Preferred file system on Windows boxes
- FAT
  - Alternative to NTFS
- Other file systems exist
csvde

- csvde
  - -f : specified the import/export file
  - -r : created a search filter
    - ex. objectClass=computer

- csvde –f <filename> -r objectClass=computer
UNIX

UNIX “Philosophies”

- Do one thing and do one thing well
- Originally built with the developer in mind
- Everything is treated as a file
Logical File System (1)

- /etc
  - The “brains”
  - Contains the administrative files, including the configuration files for different services.
  - Users, passwords, messages, and tab files
  - Similar to the Windows registry
- /bin
  - Contains binary files, or executable files
  - At times the bin directory is also linked to other directories such as /usr/bin
  - Today executables are stored in multiple locations
- /sbin
  - Contains binaries including system binaries, daemons, and administrative programs
- /home
  - Usually the location of user home directories
Logical File System (2)

- /root
  - Often the home directory for root’s files
  - Different than the “root directory”

- /usr
  - Contains the files that are used by multiple users of the system, including some administrative tools
  - Home directories can be placed here too

- /var
  - Contains variables or rapidly changing data
    - logfiles
    - spools, such as the mailqueue

- /proc
  - Contains information about processes
Logical File System (3)

- /lib
  - Contains the shared libraries

- /dev
  - Contains the device files
    - monitors, disk drives, CD-ROMs, printers, memory
  - Should only be writable by root

- /mnt
  - Reserved for mounting removable file systems

- /boot
  - Contains most of the files involved in constructing or running the bootstrap

- /tmp
  - Contains temporary files
Prioritization

- You can’t audit everything
  - You need to prioritize systems – DCs, Operations Masters, important servers, etc.

- Other items also have to be looked at in a comprehensive audit
A Note on Tools…

Many of the tools we discuss should only be used with WRITTEN PERMISSION from an authorized individual, and with appropriate experience!
Overall Agenda

- Background
- **Users/Groups**
- Permissions
- Passwords
- Patching
- Auditing/Logging
User Key Principles

- Principle of Least Privilege
- Separation of Duties
- Rotation of Duties
User and Group Concepts

- Users and groups exist at multiple levels
- Types of Groups in an AD environment
  - Universal
    - Used to grant access to users that exist across multiple domain trees or forests
    - Can only contain accounts from the same forest
  - Global
    - Can be used to grant permissions to systems in any domain within the current forest
    - Can only contain members from the current domain
  - Domain Local
    - Can have any members
    - Only applicable at the domain level
  - Local
    - Local groups are specific only to the machine they exist on

Tools for User and Groups

- **Commands:** net group, net localgroup, net users
  - net group “Domain Admins”
  - net group “Enterprise Admins”
  - net group “Domain Users”

- **Dumpsec**
  - ‘LastLogonTime’ may be different from one box to the next since other domain controllers were not actually used to authenticate the logon
    - Dumpsec gives you a warning about this type of activity, and can query all domain controllers.
  - Computer accounts that show up in the users reports end in a “$”.
    - The computer accounts are necessary to join systems to the domain, and this is part of why they exist.

- **Dsquery**
- **Csvde**
Dumpsec
/etc/passwd

- Lists users on the system
- Contains 7 fields separated by a “:”
  - Name – the username
  - Password – password field
    - Should have an “x”
  - UserID – user’s identification
    - Watch out for accounts with a UID of “0”
    - Look for duplicate IDs
  - PrincipleGroup – user’s group ID (GID)
  - Gecos – stores the user’s full name
  - HomeDirectory – user’s home directory
  - Shell – user’s default shell
Sample /etc/passwd

```
linux:/ # cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/bin/bash
daemon:x:2:2:Daemon:/sbin:/bin/bash
lp:x:4:7:Printing daemon:/var/spool/lpd:/bin/bash
mail:x:8:12:Mailer daemon:/var/spool/clientmqueue:/bin/false
news:x:9:13:News system:/etc/news:/bin/bash
uucp:x:10:14:Unix-to-Unix CoPy system:/etc/uucp:/bin/bash
games:x:12:100:Games account:/var/games:/bin/bash
at:x:25:25:Batch jobs daemon:/var/spool/at/jobs:/bin/bash
wwwrun:x:30:8:WWW daemon apache:/var/lib/wwwrun:/bin/false
ftp:x:40:49:FTP account:/srv/ftp:/bin/bash
postfix:x:51:51:Postfix Daemon:/var/spool/postfix:/bin/false
sshd:x:71:65:SSH daemon:/var/lib/sshd:/bin/false
ntp:x:74:65534:NTP daemon:/var/lib/ntp:/bin/false
nobody:x:65534:65533:nobody:/var/lib/nobody:/bin/bash
tanya:x:500:100:tanya:/home/tanya:/bin/bash
linux:/ #
```
/etc/group

- Lists groups on the system
- Each line in the file names a group
- The primary group that a user belongs to is listed in the /etc/passwd file
- Contains 4 fields separated by a “:”
  - Group name – gives the group name
  - Encrypted password – gives the group password
  - Group ID – group identification number
  - List of comma-separated users who are in the group
- Commands: groups, id, chage -l
Sample /etc/group

```
# cat /etc/group
root:x:0:
bin:x:1:daemon
daemon:x:2:
sys:x:3:
tty:x:5:
disk:x:6:
lp:x:7:
ew:x:8:
kmem:x:9:
wheel:x:10:
mail:x:12:
news:x:13:
ucp:x:14:tanya
shadow:x:15:
dialout:x:16:tanya
audio:x:17:tanya
floppy:x:19:
console:x:21:
ucuc:x:22:
at:x:25:
pub:x:32:
video:x:33:tanya
games:x:40:
xok:x:41:
trusted:x:42:
modem:x:43:
ftp:x:49:
postfix:x:51:
maildrop:x:59:
www:x:62:
sshd:x:65:
ntadmin:x:71:
nobody:x:65533:nobody
nogroup:x:65534:nobody
users:x:100:
linux:/ #
```
Overall Agenda

- Background
- Users/Groups
- Permissions
- Passwords
- Patching
- Auditing/Logging
Permissions - Ownership

- Every object has an owner including objects in an NTFS volume and objects in Active Directory
- Owner of an object controls who has access to the object
- Default owner is the user who created the object
  - If creator is a member of the Administrators group, the Administrators group is the owner
- Owner can always change permissions – even if deny permissions exist
Changing Ownership

- Ownership can be taken by
  - Users with the “Take ownership” user right
  - Users who have the “Restore files and directories” user right

- Ownership can be transferred by
  - Current owner by giving the “Take ownership” permission to another user
  - An administrator can take ownership
  - Users who have the “Restore files and directories” user right
Permissions - Inheritance

- Permissions flow from parent to child
- Permissions are inherited when an object is created or a parent ACL is changed
- Best not to block inheritance
- Explicit ACEs take priority over inherited ACEs
  - Inherited Deny permissions do not prevent access to an object if the object has an explicit Allow permission entry
  - Explicit permissions take precedence over inherited permissions, even inherited Deny permissions
- Each ACE specifies how inheritance should occur
Permissions Key Concepts

- Denies override allows
- Other than denies, permissions are cumulative
- Default deny exists if no explicit permissions exist
- Permissions are composed of special permissions
- Different permissions exist for different objects
  - File permissions – full control, modify, read and execute, read and write
  - Directory permissions – full control, modify, read and execute, list folder contents, read, write
  - Registry permissions – full control and read
- Tools: Dumpsec, showacls.exe
Combining Share and NTFS Permissions

- **Effective permissions**
  - Calculate final share permissions
    - Explicit Deny overrides Allow
  - Calculate final NTFS permissions
    - Explicit Deny overrides Allow
  - Effective permissions is calculated by examining both results, and the more restrictive is applied to a given user request

- Share DACLs are ignored for local access
- No inheritance of share permissions
Mandatory Integrity Control

- Vista and later
- Also known as Windows Integrity Control
- Labels are assigned for integrity purposes
  - No labels, means a default of medium is applied
  - Label is stored as part of an object’s SACL
- When you run a process, your SAT has an integrity SID that identifies the MIC label
  - Low: for IE or other programs set to low
  - Medium: processes launched as a standard user (the default)
  - High: processes launched with administrative privileges
  - System: for most services
- A process cannot edit or delete a securable object unless that object's MIC label is the same as or lower than the MIC label of the process.
  - Evaluated prior to DACLs
  - Securable objects are basically anything that can have permissions assigned
User Account Control

- Vista and later
- Allows users to install and run programs as low-privileged accounts and temporarily raise privileges as needed
- No log on and log off needed
- No runas or dropmyrights needed
- UAC does not apply to the built in Administrator account by default
- Uses MIC to implement
Privileges or Rights

- Rights versus Admin rights
  - User Rights
    - Assigned rights
    - Can be changed, granted or revoked
  - Admin Rights
    - Automatic based on built-in groups
    - Cannot be granted, removed or changed
    - Granted by assigned users to the built-in groups
- Rights are machine specific
- High risk privileges should only be granted to Local System and Administrators
- Low risk privileges are normally too detailed to audit

- Tools: showpriv.exe, Dumpsec and SCA
Permissions

- **Read**
- **Write**
- **Execute**

Access given to non-owner, non-group users
Access given to the file’s group
Access given to the file’s owner
File type
Directory Permissions

- r = List the contents of the directory
  - List the file names
- w = create, delete, rename files in the directory
- x = can ‘cd’ into the directory, access contents, not list contents
  - List information from the inode – information about the files
  - Need access to the inode to be able to read/write files in the directory
- Permissions do not grant users the right to run certain programs, they grant the right to use certain system calls
  - Ex. ‘cat’/’more’ – written using read() system call, so read permission is necessary
File Resultant Permissions

<table>
<thead>
<tr>
<th>File Permissions</th>
<th>Directory Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>-</td>
<td>- r x wx</td>
</tr>
<tr>
<td>-</td>
<td>None None None Delete file</td>
</tr>
<tr>
<td>r</td>
<td>None None Read data Delete file Read data</td>
</tr>
<tr>
<td>w</td>
<td>None None Add/Delete data Delete file Add/Delete data</td>
</tr>
<tr>
<td>rw</td>
<td>None None Update data Delete file Update data</td>
</tr>
<tr>
<td>x</td>
<td>Can’t execute Can’t execute Execute Delete file Execute</td>
</tr>
</tbody>
</table>

Baccam Consulting, LLC © 2005-2014
Permissions – Octal Equivalents

- Permissions can also be specified in 3 or 4 digit octal values
  - Read (r) = 4
  - Write (w) = 2
  - Exec (x) = 1

- Examples
  - -rwxrw-r-- = 764
  - -r-xr------ = 540
“Special” Permissions Illustration

Examples
- drwxrwxrwt = 1777
- -rwsr-xr-x = 4755
Querying for Files

- `find / \( -perm -004000 -o -perm -002000 \) -exec ls -ld {} \; >> suid_sgid.txt`

- `find / -type f -perm -2 -exec ls -l {} \; >> world_write.txt`

- `ls -laR / >> allfiles.txt`
Overall Agenda

- Background
- Users/Groups
- Permissions
- **Passwords**
- Patching
- Auditing/Logging
Passwords

- Verify how passwords and sent
  - Data in transit

- Verify how passwords are stored
  - Data at rest
Password Policy

```
C:\Windows\system32>net accounts
Force user logoff how long after time expires?: Never
Minimum password age (days): 0
Maximum password age (days): 42
Minimum password length: 0
Length of password history maintained: None
Lockout threshold: Never
Lockout duration (minutes): 30
Lockout observation window (minutes): 30
Computer role: WORKSTATION
The command completed successfully.
```

Account/Password Policy Tools

- `dsquery user -limit 0 -o rdn -stalepwd 90` = finds users with passwords older than 90 days
- `dsquery user -limit 0 | dsget user -dn -pwdneverexpires` = returns User Accounts with Yes/No for Pwdneverexpires
- `dsquery user -inactive 4 -limit 0 -o rdn` = user accounts inactive for over four weeks
- `dsquery user -disabled -limit 0 -o rdn` = disabled accounts

- Commands: net accounts, SCA and Dumpsec
Passphrase Policy Recommendations

- Maximum Password Age: 60 days
- Minimum Password Age: 1 day
- Minimum Password Length: 15 characters
- Password History Length: 24 prior passwords or 365 days
- Password Complexity
- Lockout Duration: 5 minutes
- Lockout Threshold: 5 failed attempts
/etc/shadow

- Stores the encrypted passwords, as well as other information about passwords
  - Don’t use /etc/passwd to store encrypted passwords!

- Permissions on the /etc/shadow file should not allow normal users to read the file
  - 640 should apply to the file where the owner is root and the group is shadow, or similar
/etc/shadow Fields

- Contains 9 fields separated by a “:”
- Username or User ID
- Password in its encrypted format
  - All accounts should have a password, be locked out or removed
  - Fields starting with “!” or “*” means account is locked out
- Number of days since Jan 1, 1970 that the password was last changed.
  - “=DATE(1970,1,1)-DATE(2005,6,30)” = 12,964
  - “=DATE(1970,1,1)+12964” = 6/30/2005
- Minimum number of required days between password changes
- Maximum number of days that a password is valid for
- Number of days before expiring that the user starts to receive a warning message
- Number of inactive days allowed for the user
- Date after which the account can no longer be used
  - Number of days since January 1, 1970
- Flag – not currently used
Sample /etc/shadow

```
linux:~ # cat /etc/shadow
at:!:12743:0:99999:?:
bin:*:8902:0:10000:
daemon:*:8902:0:10000:
ftp:*:8902:0:10000:
games:*:8902:0:10000:
lp:*:8902:0:10000:
mail:*:8902:0:10000:
man:*:8902:0:10000:
news:*:8902:0:10000:
nobody:*:8902:0:10000:
ntp:!:12743:0:99999:?:
postfix:!:12743:0:99999:?:
root:$$2a$05$yGmbIzuq.gh7guJtXHcYuN/cSQd.jfDA7CcBLinotMSKQG3ny97CK:12859:0:10000:
sshd:!:12743:0:99999:?:
wucc:*:8902:0:10000:
wwwrun:*:8902:0:10000:
tanya:$$2a$05$oJNfA2_jA4CGD6j06JCYW.e2hqyhUaUT7m3q8494GBZUqo4JUp1Znm:12859:0:99999:?:
```
PAM

- Pluggable Authentication Modules
  - Many modules exist
- Library and API that applications can use to authenticate users
- Can be used by many authentication systems
  - /etc/passwd, /etc/shadow, NIS, NIS+, LDAP, Kerberos, etc.
- Important files
  - PAM applications configured in /etc/pam.d or in /etc/pam.conf
  - Library modules normally stored in the directory /lib/security or /usr/lib/security
  - Configuration files are located in the directory /etc/security
Overall Agenda

- Background
- Users/Groups
- Permissions
- Passwords
- Patching
- Auditing/Logging
Centralized Patch Management

• Patches can be “pushed” out after they’ve been tested
  • Multiple groups can exist

• Patches should be prioritized
Windows Update
Wmic qfe list
Patching UNIX

- Easy way for admin to manage source
  - Keep app source code on system and recompile when needed
  - Located at /usr/src or /usr/local/src
- Automated patch management tools do exist
  - autorpm, yast on-line update, apt-get, pkginfo, cron
- RCS, CVS, SCCS
  - Revision control systems
  - CVS allows anonymous client connections so user can “check out” the latest revisions
- You need to know what’s installed in order to keep a system patched!
Auditor Patching Tips

- Who submits changes?
- Who approves changes?
- Is there a patch management system?
- How are changes backed out if necessary?
- How are changes assigned to be completed?
- How is change integrity verified?
- How are changes tested?
- How are changes moved to the production environment?
- What’s the emergency process?

*** Sample a few changes, as well as recent vulnerabilities.
Overall Agenda

- Background
- Users/Groups
- Permissions
- Passwords
- Patching
- Auditing/Logging
Windows Logs

- Logs must be reviewed on a regular basis by administrators in order to identify anomalous or suspicious activity

- Three primary logs for any Windows NT and later systems
  - Application log: provides information about the applications or programs being used
  - Security log: records security events including logon attempts and resource usage such as creating, opening or deleting objects
  - System log: contains information about the system components such as device failures or components being loaded during startup

- For domain controllers
  - Directory service log
  - File Replication service log

- Additional logs may exist depending on the role of the system
Event Viewer
Log Options

- Log File Path
  - Check location and look at permissions
    - Application.evtx - Administrators, Read and Execute
    - Security.evtx - Auditor's, Full Control
    - System.evtx - SYSTEM and Eventlog, Full Control

- Log Access
- Retain logs based on retention policy
- Tool: auditpol /get /category:*
# Recommended Settings

<table>
<thead>
<tr>
<th>Policy</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit account logon events</td>
<td>Success and Failure</td>
</tr>
<tr>
<td>Audit account management</td>
<td>Success and Failure</td>
</tr>
<tr>
<td>Audit directory service access</td>
<td>Success and Failure</td>
</tr>
<tr>
<td>Audit logon events</td>
<td>Success and Failure</td>
</tr>
<tr>
<td>Audit object access</td>
<td>None, Failure or Success and Failure depending on the objects and the risk level desired</td>
</tr>
<tr>
<td>Audit policy change</td>
<td>Success and Failure</td>
</tr>
<tr>
<td>Audit privilege use</td>
<td>Success and Failure</td>
</tr>
<tr>
<td>Audit process tracking</td>
<td>None</td>
</tr>
<tr>
<td>Audit system events</td>
<td>Success and Failure</td>
</tr>
</tbody>
</table>
## Subcategory Audit Settings

<table>
<thead>
<tr>
<th>System</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Security System Extension</td>
<td>Success and Failure</td>
</tr>
<tr>
<td>System Integrity</td>
<td>Success and Failure</td>
</tr>
<tr>
<td>IPSec Driver</td>
<td>Success and Failure</td>
</tr>
<tr>
<td>Other System Events</td>
<td>No Auditing</td>
</tr>
<tr>
<td>Change</td>
<td>Success and Failure</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Logon/Logoff</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Logon</td>
<td>Success and Failure</td>
</tr>
<tr>
<td>Logoff</td>
<td>Success</td>
</tr>
<tr>
<td>Account Lockout</td>
<td>No Auditing</td>
</tr>
<tr>
<td>IPsec Main Mode</td>
<td>No Auditing</td>
</tr>
<tr>
<td>IPsec Quick Mode</td>
<td>No Auditing</td>
</tr>
<tr>
<td>IPsec Extended Mode</td>
<td>No Auditing</td>
</tr>
<tr>
<td>Special Logon</td>
<td>Success</td>
</tr>
<tr>
<td>Other Logon/Logoff Events</td>
<td>No Auditing</td>
</tr>
<tr>
<td>Network Policy Server</td>
<td>No Auditing</td>
</tr>
</tbody>
</table>
# Subcategory Audit Settings

<table>
<thead>
<tr>
<th><strong>Object Access</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>File System</td>
<td>Failure</td>
</tr>
<tr>
<td>Registry</td>
<td>Failure</td>
</tr>
<tr>
<td>Kernel Object</td>
<td>No Auditing</td>
</tr>
<tr>
<td>SAM</td>
<td>No Auditing</td>
</tr>
<tr>
<td>Certification Services</td>
<td>No Auditing</td>
</tr>
<tr>
<td>Application Generated</td>
<td>No Auditing</td>
</tr>
<tr>
<td>Handle Manipulation</td>
<td>No Auditing</td>
</tr>
<tr>
<td>File Share</td>
<td>No Auditing</td>
</tr>
<tr>
<td>Filtering Platform Packet Drop</td>
<td>No Auditing</td>
</tr>
<tr>
<td>Filtering Platform Connection</td>
<td>No Auditing</td>
</tr>
<tr>
<td>Other Object Access Events</td>
<td>No Auditing</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Privilege Use</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensitive Privilege Use</td>
<td>Success and Failure</td>
</tr>
<tr>
<td>Non Sensitive Privilege Use</td>
<td>No Auditing</td>
</tr>
<tr>
<td>Other Privilege Use Events</td>
<td>No Auditing</td>
</tr>
</tbody>
</table>
# Subcategory Audit Settings

<table>
<thead>
<tr>
<th>Detailed Tracking</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Process Termination</td>
<td>No Auditing</td>
</tr>
<tr>
<td>DPAPI Activity</td>
<td>No Auditing</td>
</tr>
<tr>
<td>RPC Events</td>
<td>No Auditing</td>
</tr>
<tr>
<td>Process Creation</td>
<td>Success</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Policy Change</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit Policy Change</td>
<td>Success and Failure</td>
</tr>
<tr>
<td>Authentication Policy Change</td>
<td>Success</td>
</tr>
<tr>
<td>Authorization Policy Change</td>
<td>No Auditing</td>
</tr>
<tr>
<td>MPSSVC Rule-Level Policy Change</td>
<td>No Auditing</td>
</tr>
<tr>
<td>Filtering Platform Policy Change</td>
<td>No Auditing</td>
</tr>
<tr>
<td>Other Policy Change Events</td>
<td>No Auditing</td>
</tr>
</tbody>
</table>
Subcategory Audit Settings

<table>
<thead>
<tr>
<th>Account Management</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>User Account Management</td>
<td>Success and Failure</td>
</tr>
<tr>
<td>Computer Account Management</td>
<td>Success and Failure</td>
</tr>
<tr>
<td>Security Group Management</td>
<td>Success and Failure</td>
</tr>
<tr>
<td>Distribution Group Management</td>
<td>No Auditing</td>
</tr>
<tr>
<td>Application Group Management</td>
<td>No Auditing</td>
</tr>
<tr>
<td>Other Account Management Events</td>
<td>Success and Failure</td>
</tr>
<tr>
<td><strong>DS Access – Domain Controller Only</strong></td>
<td>(Can be set to no auditing for 2014 member servers)</td>
</tr>
<tr>
<td>Directory Service Changes</td>
<td>Success and Failure</td>
</tr>
<tr>
<td>Directory Service Replication</td>
<td>No Auditing</td>
</tr>
<tr>
<td>Detailed Directory Service Replication</td>
<td>No Auditing</td>
</tr>
<tr>
<td>Directory Service Access</td>
<td>Success and Failure</td>
</tr>
<tr>
<td><strong>Account Logon</strong></td>
<td></td>
</tr>
<tr>
<td>Kerberos Service Ticket Operations</td>
<td>No Auditing</td>
</tr>
<tr>
<td>Other Account Logon Events</td>
<td>No Auditing</td>
</tr>
<tr>
<td>Kerberos Authentication Service</td>
<td>No Auditing</td>
</tr>
</tbody>
</table>
Typical UNIX Logs

- /var/log – typical log directory
- /var/run/utmp
  - Currently logged in users
  - Ephemeral in nature
  - Binary file
  - Log must be created
  - Contains: Username, terminal, login time, remote host
  - Commands: finger, who, w, users

- wtmp
  - Login-logout history
  - Binary file
  - Contains: Username, terminal, login time, logout time, remote host
  - Commands: finger, who, last
Typical UNIX Logs (2)

- btmp
  - Bad login attempts
  - Binary file
  - Log must be created
  - Commands: lastb
- messages
  - Messages from the syslog facility
- secure
  - Access and authentication
- /var/adm/sulog
  - Logs use of the su command
  - /etc/default/su identifies the location of the log
- aculog
  - Dial-out modem log
Typical UNIX Logs (3)

- **lastlog**
  - Logs each user’s most recent login and possibly the last unsuccessful login
  - Command: lastlog

- **loginlog**
  - Bad login attempts

- **/var/account/acct**
  - Process-level accounting
  - Command: sa

- **Extended audit capabilities are available**
  - Can be specific to each Vendor and/or version of UNIX
Syslog.conf

- Syslog provides for log centralization
- Main configuration file for syslog
  - # lines are ignored
  - Each entry has the following
    - Facility
      - auth, authpriv, cron, daemon, kern, lpr, mail, mark, news, syslog, user, uucp, local0 through local7
      - Specifies the subsystem that produced the message
    - Priority
      - debug, info, notice, warning/warn, err/error, crit, alert, emerg/panic (same as emerg)
      - Defines the severity of the message
    - Action
      - Lists the log file location
Example syslog.conf

#; Critical system failures that management needs to see
*.err;*.crit;*.emerg /var/log/critical.log

#; Do not log auth/authpriv messages here; rather log them to
#; a separate file for processing by security staff.
auth,authpriv.none /var/log/messages
auth,authpriv.debug /var/log/auth.log
cron.info /var/log/cron.log
news,kern,lpr,daemon,ftp,mail.info /var/log/daemon.log

#; For more critical errors tell root. Ignore user messages.
*.err;user.none root
Logrotate

- Logs need to be managed
- Allows automatic rotation, compression, removal, and mailing of log files
- Each log file may be handled daily, weekly, monthly, or when it grows too large
- Normally, logrotate runs as a cron job
Auditor Log Tips

- Logs should be reviewed on a daily basis or according to policy
  - Unsuccessful user login attempts
  - Superuser access
  - System modifications

- Review what is being logged
- Centralized logging should be occurring
- Integrity checking tools should be used
Conclusion

- Looked at the higher risk areas as it relates to Active Directory/Windows and UNIX Audits

- Other areas to consider
  - Services
  - Software
  - Ports
  - Encryption
Thank you!

Tanya Baccam, CPA, CISA, CISM, GPPA, GCIH, CITP, CISSP, Oracle DBA
Baccam Consulting, LLC
tanya@securityaudits.org
Training Opportunities – www.securityaudits.org/events.html
972.294.4193