Introduction to Auditing Active Directory

Prepared and presented by: Tanya Baccam
CPA, CITP, CISSP, CISA, CISM, GPPA, GCIH, GSEC, OCP DBA
Baccam Consulting LLC
tanya@securityaudits.org

Objectives

- Understand the AD Architecture
- Identify key audit steps for AD
- Look at available tools for auditing

What is Active Directory?

- Active Directory (AD) is a centrally managed database with information about AD objects
  - Servers, workstations, people, printers, etc.
  - Authentication, authorization
- First released with Windows 2000 server
- LDAP

Active Directory Objects

- Resources – printers, shared directories, etc.
- Security principals – computers, servers, user accounts, groups, etc.
  - Security principals are assigned a SID

Directory Information Examples

- For a computer
  - NetBIOS name, operating system version, service pack level, the last time the computer logged into the domain, etc.
- For a user account
  - Person's name, phone number, group memberships, etc.

Obtaining an Inventory

- Obtain a listing of servers and workstations
- Review the operating system, version, and service pack in use for any outdated versions

- A listing can be obtained with:
  - csvde -f %COMPUTERNAME%-domainComputerObjs.csv -r objectClass=computer -l dNSHostName,operatingSystem,operatingSystemVersion,operatingSystemServicePack,lastLogon,LastLogonTimestamp

What Else can AD Do?

- Access Control
- Apply Security Policy
- Auditing
- Data protection for data at rest
- Data protection for data in transit
- PKI
- Trusts

AD Terms

- Forest
  - Set of one or more domains with a shared schema
- 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

Objects

- Hierarchical arrangement of objects
- AD objects represent entities that make up a domain
- Each object is uniquely identified by a Globally Unique Identifier (GUID)
- Each security principal object is assigned a security identifier (SID)
  - Used for security-enabled objects

Organizational Units

- Organizational Units (OUs) are containers within the domain environment
- OUs can exist at multiple levels within the organization
- OUs can contain OUs within OUs
- Get a list of organizational units
  - `dsquery ou dc=mydom,dc=com`
  - `dsquery ou domainroot`

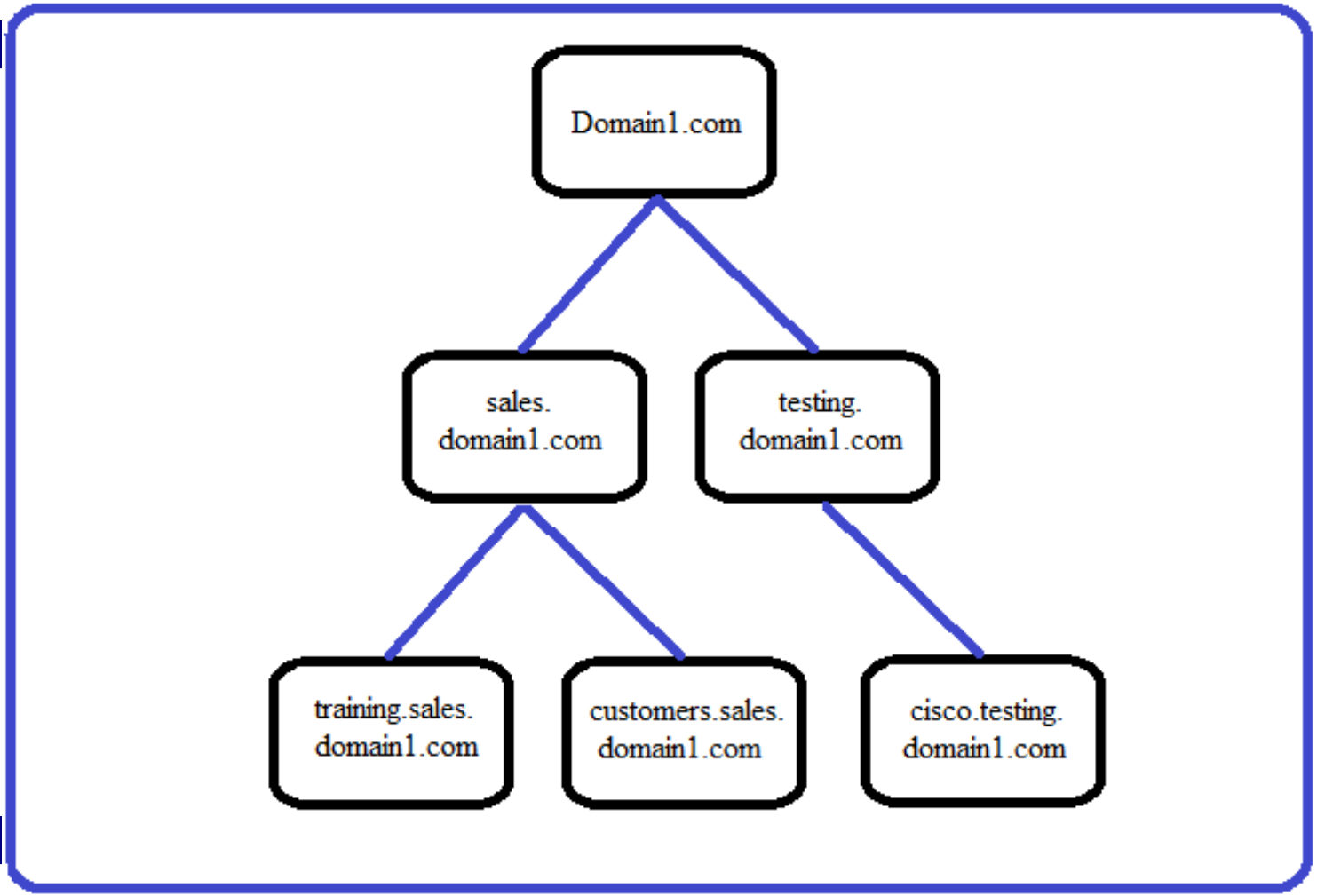
Domain

- Can be a partition within an AD forest
- Default administrative owner of a domain is the Domain Admins group
- Domain is authoritative for the identity and credentials of the users, computers, and groups that reside in that domain
- Multiple domain controllers should exist for redundancy

Tree

- Trees and Forests are used within Windows 2000 and later environments to logically connect domains
- Tree: a set of domains that have a common network configuration and catalog of information
  - Each tree has a unique name – ex. tree1.com
    - Systems can be a part of the tree – ex. servera.tree1.com, serverb.tree1.com
  - Two or more domains where the DNS names of the domains are in a hierarchical, parent-child relationship
  - A tree shares a single Schema, Configuration Naming Context and Global Catalog

Example Tree

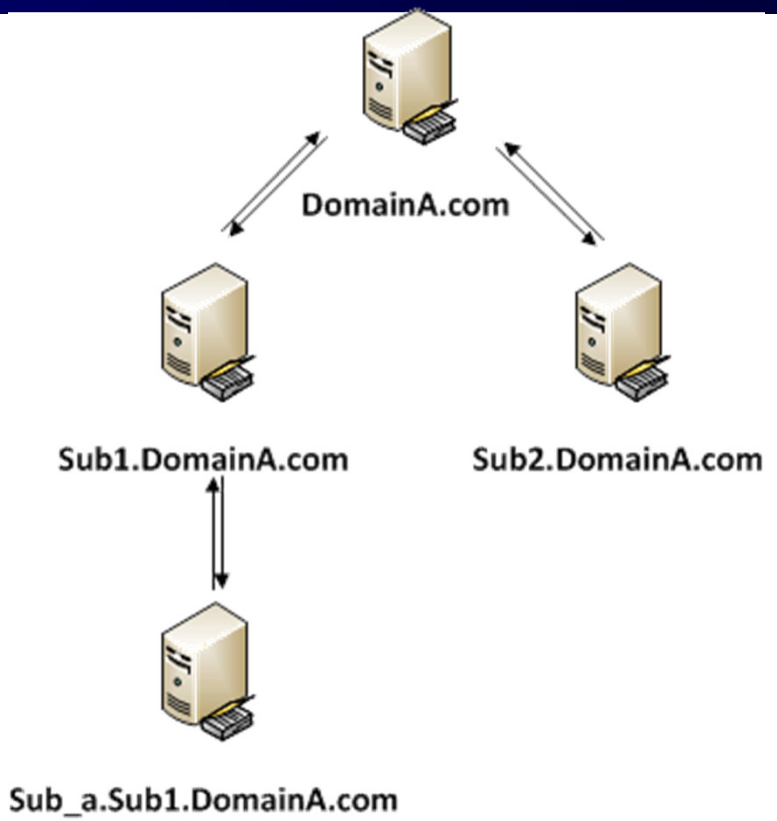


Forests (1)

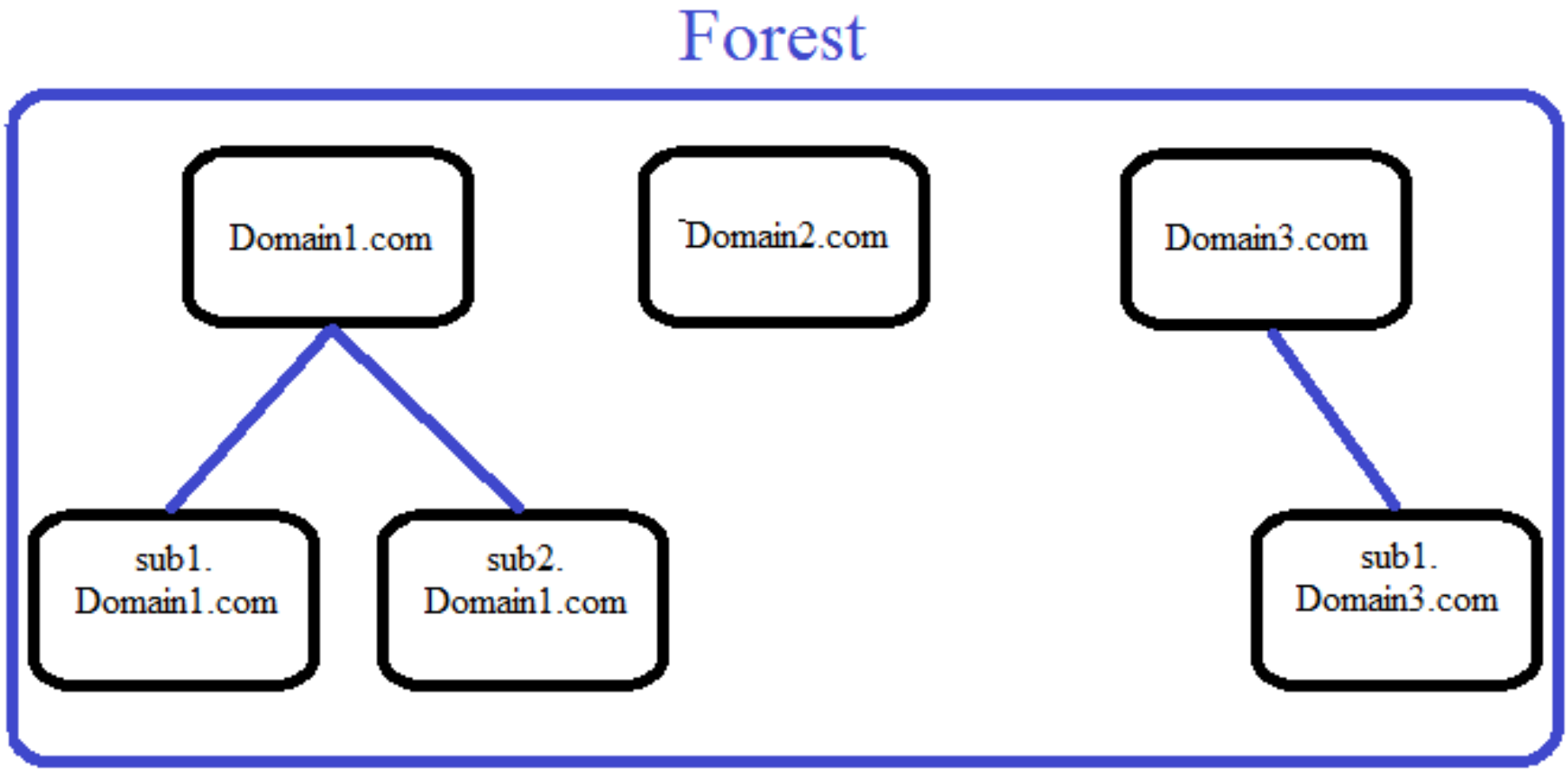
- A collection of domains with a shared naming context
- A forest consists of all trees that also contain two-way (transitive) trusts to other trees
- The “root” domain is the first domain created in the forest
  - Schema and Enterprise Admins are in the root domain
- Forest is the replication boundary

Forests (2)

- Forest is the security boundary
  - Not the domain



Example Forest



Reasons to Create a Forest

- Testing/training labs
- Applications that require schema modifications
- Legal requirements
- Acquisitions/mergers of other forests
- Requirement for fault tolerance overrides everything else
- Inadequate bandwidth or requirements to be disconnected for long periods
- Isolate critical business resources
- Isolate dangerous users and computers

Forest Audit Step Considerations

- Review the administrative controls to prevent unauthorized granting of trusts between forests
- Ensure that users from another forest are not members of the groups which
  - Administer computers that store critical data
  - Provide access to critical data
  - Responsible for service management
  - Administer server administrator groups

Trusts (1)

- One-way

- Two-way

Trusts (2)

- Transitivity
  - Transitive trusts
  - Intransitive (nontransitive) trusts
- Can facilitate “single sign-on” capability across domains
- Tool: netdom query trust

Domain Controllers

- AD database is stored and managed by DCs
- Servers can be member servers or domain controllers (DCs)
- Responsible for allowing hosts to access domain resources
- DCs are the foundation to the AD directory services
- Stores user accounts
- Authenticated users
- Enforce security requirements

Active Directory Replication

- One or more domain controllers can exist in a domain
  - A single DC is a single point of failure.
  - Multi-master replication
- Ensure that replication traffic is being encrypted as necessary
- AD Replication is organized around sites
- A site is a collection of one or more subnet objects
  - Physical concept

RODC

- Used primarily when physical security risks exist
- The RODC must be 2008 (or later)
  - Can have other DCs that are not 2008
  - PDC Emulator must also be 2008 (or later)
- Gets a full copy of the AD database w/o certain password hashes
  - By default, no password hashes are sent to the RODC – Default Deny
    - Deny overrides Allow if conflicts exist
  - Can select which ones you want to send
  - Two groups can be leveraged for enforcing RODC password replication policy – other groups can be leveraged
    - Allowed RODC Password Replication Group
    - Denied RODC Password Replication Group

DC Audit Steps

- Verify that there are enough domain controllers for fault-tolerance and performance
  - How many DCs are there and where are they located?
- Verify where the DCs are physically located
  - Are there any RODCs/sites that lend themselves to RODCs?
- Verify whether DCs built are transported and placed in a physically secure and/or controlled location
- Review how traffic is sent for replication
  - Encrypted?
  - Signed?
- Review the DC build procedures for reasonableness

Group Policy (1)

- Group Policy can be used to control security settings
  - Apply and/or configure policy settings
- Group Policy Object (GPO)
  - Group of information that specifies how objects within a particular group of users will act and be configured
    - Contains the Group Policy (GP) settings
  - Settings stored in multiple locations
    - GP container
    - GP template

Group Policy (2)

- GPOs can be applied at multiple levels
  - Site, domain, OU
- GPOs are inherited and cumulative
  - Processed in order of local, site, domain, organizational unit
- GPO override options exist
  - Block Inheritance
  - No Override
- Tool: `gpresult`

Global Catalog Servers

- Global Catalog (GC) is a distributed data repository
  - Portion of the database that's replicated throughout the forest
- GC is stored on DCs that have been designated as Global Catalog Servers
- DCs that replicate across domain boundaries are called Global Catalog Servers
- Some AD data is marked as part of the Global Catalog, while other data is not
  - A subset of the AD database
  - Not a separate database from the AD database
  - GC is distributed via multi-master replication

GC Best Practices to be Covered in Audit Steps

- Each site should have at least one GC server, preferably two or more
- If a remote site can't have a GC server, then set the registry to allow logons without a GC (KB241789)
  - Deny permissions should not be specified for universal groups, when possible
- Infrastructure Master should not be assigned to a DC hosting the GC server
  - Updates may not occur
  - Of course, an exception exists if there is only 1 domain
  - Should be in the same site as at least one GC server though
- Domain Naming Master should be a GC server
  - Otherwise creation of grandchild domains may fail if your forest is not in 2003 mode

Operation Masters

- Some services don't operate well in multi-master replication mode
  - Flexible Single Master Operation (FSMO) mode is used instead
  - FSMO Master– a DC running one or more of the five FSMO services
- FSMO Master now shortened to "Operations Master"
- Tool: `netdom query fsmo`
  - Provides a list of the current Operation Masters

Five Operation Master Roles

- Forest-wide roles
  - Schema Master
  - Domain Naming Master
- Domain-wide roles
  - PDC Emulator Master
  - RID Master
  - Infrastructure Master

- http://technet.microsoft.com/en-us/library/cc773108(WS.10).aspx

AD Audit Steps (1)

- Determine where the Operation Masters are located
- Determine how many domains/trees/forests exist
  - Identify the DNS/NetBIOS names for the domains
- Determine any trust relationships among the domains/forests
  - Identify what kind of trusts exist
- Determine if there are any stand-alone systems
  - Why are they stand-alone?
  - How are they managed?

AD Audit Steps (2)

- Determine what the domain and OU strategy is
- Determine whether OUs being used to delegate administrative authority
- Determine whether OUs are being used to control the security policy for users and computers
- Determine the strategy for GPOs
  - Get a listing of the GPOs that exist

CSVDE

- csvde
  - comma separated value data exchange utility
- Some common switches
  - -f : specifies the import/export file name
  - -r : create a search filter based upon an attribute
    - ex. `objectClass=computer`
  - -l : allows you to specify list of attributes to return
- Note that some output, such as timestamps, may need to have a formula applied to get a human-readable date
  - =IF(CE3>0,CE3/(8.64*10^11) - 109205,"")
  - http://myserverstuff.blogspot.com/2009/03/csvde-to-excel-human-readable-lastlogon.html.

Tools for User and Groups (2)

- csvde
  - csvde -f <<filename>> -r (sAMAccountName="Domain Admins") -l member
  - csvde -f <<filename>> -r (sAMAccountName="Enterprise Admins") -l member
  - csvde -f <<filename>> -r objectClass=user
    - -r objectCategory=person
  - csvde –s 10.10.10.10 –b administrator domain password -f allDomainObjs.csv

DSQuery Summary of Commands

- dsquery server –forest
  - List all DCs
- dsquery server –forest –isgc
  - List all Global Catalog Servers
- dsquery server –hasfsmo [rid|pdc|name|schema|infr]”
  - List Operation Masters
- dsquery ou domainroot or dsquery ou dc=mydom,dc=com
  - List all OUs in the domain
- dsquery group, dsquery user, dsget user –memberof –expand
  - List all groups and members of groups
- dsquery * domainroot -scope subtree -filter objectcategory=computer -attr name
  - List all computers
- “dsquery * domainroot –filter “(&(objectclass=user)(objectcategory=person))” –attr sAMAccountName”
  - List all domain users

Summary

- Discussed the AD Architecture
- Looked at key audit steps for AD
- Looked at available tools for auditing

Auditing Courses Available

- Auditing Network Security in Dallas, TX
  - April 27-29, 2015
- Auditing Active Directory and Windows in Dallas, TX
  - May 18-20, 2015
- Foundations of IT Auditing in Dallas, TX
  - June 23-25, 2015
- Auditing UNIX/Linux in Dallas, TX
  - July 9-10, 2015
- Auditing Oracle in Dallas, TX
  - September 21-23, 2015
- SANS Sec502: Perimeter Protection In-Depth
  - June 15-June 20, 2015
  - http://www.sans.org/event/sansfire-2015/course/perimeter-protection-in-depth

- See www.securityaudits.org/events.html for more information and to register

Thank you!

Prepared and presented by: Tanya Baccam
CPA, CITP, CISSP, CISA, CISM, GPPA, GCIH, GSEC, OCP DBA
Baccam Consulting LLC
tanya@securityaudits.org