# Midterm exam (100 points)

Kenneth Mead, Winter 2021

Due 2/21 @ 11:59pm

**NO LATE SUBMISSIONS ACCEPTED**

Replace your name at the top where mine is in red font. For each of the questions below, type your responses in red font. Because this is a take-home exam where you have over a week to work on it, make your responses as detailed as possible (within reason, no need to submit a 50-page report). Several questions are intentionally open-ended and may require time to think about. For the questions with the script, you can just copy directly from your VM into this document. Again, due to the take-home nature of this exam, I expect that your script will work, and any errors in your script will result in you receiving 0 points for that question. **Make sure you copy/paste correctly.**

Plagiarism policy

Please note that you must complete this exam on your own (do not copy from a classmate) and each response must be in your own words. Even if you use the slides from class as a reference, you still must rephrase (think about how you would explain it to a fellow student). If you use online resources, you must (1) cite your source, and (2) rephrase in your own words.

Direct copy/paste from any online sources or the class slides will not be tolerated. You have over a week to consider your responses and rewrite them accordingly. Any instances of copy/paste will not only lose points but will also be reported to the Dean of Students. Please email me if you need any questions/clarifications.

## Question 1 (8 points)

Describe in detail the differences between the Lightweight Directory Access Protocol (LDAP) and Active Directory (AD).

LDAP is the industry standard protocol used to manage directory information services. To elaborate, LDAP provides the details on the technique that should be used but does not provide an actual directory service.

Active Directory is an actual directory service provided by Microsoft. It manages user authentication, directory access per user, assigns and enforces security policies, and can manage installation/updating of software.

Their difference is that LDAP does not actually provide a directory service, it simply provides the tools to get the job done. On the other hand, Active Directory puts LDAP to use and provides the actual directory service.

## Question 2 (4 points)

Given the following LDAP tree, provide the *distinguished name* (starting with the uid, as we may have multiple instances of Bob Ross, a uid may be preferable in this case).

dc=local

dc=csi3670

ou=Users

uid=bross

objectClass=posixAccount,inetOrgPerson

cn=Bob Ross

[mail=bross@csi3670.local](mailto:mail=bross@csi3670.local)

uid=bross,ou=Users,dc=csi3670,dc=local

## Question 3 (2 points)

As a follow-up, what is the purpose of a *distinguished name*?

Distinguished names provide a reference to the containers and organizational groups an object is part of. This information is used during authentication and access control processes. For example, it can determine whether or not a user has the right authority to access a directory by comparing its relative distinguished names to the LDAP directory database.

## Question 4 (8 points)

In an AD environment, what is the purpose of the *domain controller* and why would we want more than one?

The domain controller is the system that LDAP is actually implemented on. We would want more than one because it gives us the advantages of a decentralized environment. The biggest advantage of decentralizing a directory service is lower risk of system failure. If one domain controller becomes inaccessible, then users can still access the other one and continue working.

## Question 5 (6 points)

Two-way transitive trust is one of the benefits of domain controllers. Describe this concept.

Two way transitive trust is the ability to authenticate users from one domain in a separate domain, and vise versa. For example, business A trusts business B, and business B says it trusts business C. This tells business A that it can also trust business C, through the transitive property. Although, in the real world this trust has to be manually setup in the AD DC. To me, this *kind of* sounds like HTTP Cross-origin resource sharing (CORS).

## Question 6 (8 points)

Assume you are a sysadmin setting up a server environment for the first time. What are **two** considerations that you have when selecting a version of Windows?

Will this server need to support virtualization?

How scalable will this server need to be. In more detail, how much data will be coming in and out? Will it need to be an optimized datacenter?

## Question 7 (4 points)

After buying your servers and setting up an AD, you realize you need to set a *functional level*. What is a functional level and to what level **should** it be set?

The functional level of an AD DC determines what services it can support (ie. Kerberos auth, FTP, IIS). They should be set to the highest level that the system can support.

## Question 8 (12 points)

You realize that you’re out of money, but you still have several servers to provide. Either using open-source software such as Xen or using a pre-existing agreement with VMware, describe **two types** of servers you would virtualize and **why**. State any assumptions you’re making about the equipment used to provide virtualization as well.

1st server would be a datacenter server. The server would utilize Ubuntu Linux, LDAP, OpenSSH, DNS, OpenSSL, and MySQL. This server’s purpose would be to securely house and provide data to the network.

2nd server would be our webserver/application/runtime server. The server would utilize Ubuntu Linux, LDAP, Gnome Desktop, and Apache. This server’s purpose would be to house runnable code and user interactable services such as the Apache webserver. Having this server separate from our datacenter server maximizes security.

## Question 9 (6 points)

Describe the differences between an AD domain, an AD tree, and an AD forest.

An AD domain is where a domain controller resides. An AD tree is a collection of AD domains, and an AD forest is a collection of AD trees.

## Question 10 (10 points)

How would you share files in a Windows-only environment? In a mixed Windows-Linux environment? State any assumptions you’re making about the environment.

Sharing files over a windows environment can be as easy as setting up a shared directory with the correct permissions assigned, and then saving the files into the shared directory.

Sharing files across different OS’s is similar but could possibly run into problems. As long as the directory is visible on networks (ie firewall is setup properly) the only other process should be setting up each users permissions on each system. This could mean having to create users on the Windows system and Linux system. After that, all the user needs to know the location of the file being shared, and his credentials.

Depending on the file manager in the Linux distribution, additional packages may need to be installed.

## Question 11 (8 points)

Describe the differences between bare-metal virtualization, paravirtualization, and containers.

Bare metal virtualization is when each OS being virtualized operates as if it had full control of the computer.

Paravirtualization is when each OS knows it’s being virtualized and acts accordingly.

Containers are something similar, but completely different. They operate above the OS, and on the application layer. They are environments with set libraries, settings, and applications.

Explained simply, virtual machines are virtualized operating system environments, and containers are virtualized application environments.

## Question 12 (4 points)

What is the Principle of Least Privilege and why is it important?

The principle of Least Privilege states that every component of a computing environment needs to be able to access see the bare minimum it needs to operate. For example, a program does not need to know the technical parts of accessing memory, it only needs to know what data is stored in the memory. The OS will handle the memory accessing and provide its data to the program. Therefore, the program is less privileged since it needs to rely on the OS to do its job.

It is important because with it, it is easier to facilitate security and understand faults in a system. For example, if reading memory fails, then we know it is either because of the OS or the hardware, not our program.

## Question 13 (6 points)

Describe in detail the difference between an enlightened guest and a non-enlightened guest in Hyper-V. How does this affect communication between other VMs?

## An enlightened guest is one that knows its being virtualized by Hyper-V, and a non-enlightened guest does not. In addition to knowing their being virtualized, enlightened guests can access the VM bus directly. This allows for optimization and better communication between other VM’s, since each VM can manage itself based on the activity of other VM’s. Non-enlightened guests do not get this information and must act simply based on what Hyper-V allocates for it.

## Question 14 (14 points)

Write a PowerShell script that accepts three command-line string parameters, in any order (i.e., do not rely on the order that the parameters are given). You may assume that 3 or less parameters will be entered. Define default values for each parameter. Print each parameter name and its associated value to the screen. Furthermore, write to the screen whether any parameters are duplicates (make sure the comparison is case-sensitive), and if so, which ones.

# Midterm - Question 14

# Name: Kenny Mead

# Date: 2021-02-21

param (

[string]$param1 = "Wheres",

[string]$param2 = "my",

[string]$param3 = "supersuit"

)

Write-Host "Param1`tParam2`tParam3"

Write-Host $param1 "`t" $param2 "`t" $param3

if($param1 -ceq $param2){Write-Host "Param2 is a duplicate of Param1"}

if($param1 -ceq $param3){Write-Host "Param3 is a duplicate of Param1"}

if($param2 -ceq $param3){Write-Host "Param3 is a duplicate of Param2"}

## Extra credit (10 points)

A lot of you are currently or have been in jobs involving system administration. Even if you haven’t, it’s still a good opportunity to start exploring in this field. This is your opportunity to teach me something that also interests you. Write at least two paragraphs describing a new technology/concept that relates to system administration that we have not yet gone over in class. Make sure to cite any supplementary sources and to rephrase in your own words (even though this is extra credit, don’t copy/paste).