# Final exam (100 points)

Kenneth Mead, Winter 2021

Due 4/27 @ 11:00am

**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 exam).

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 **BOTH** (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. I will be actively checking for plagiarism. It is far better to lose points on a question than to have your grade withheld and be put on academic probation or suspended.

# Grading strategy

**The questions cover the slides from “7 – Windows Security Model” to “14 – VPN” on Moodle**. Each of the answers can be found in the slides. I have intentionally created this exam with a lot of questions to give you as many extra credit opportunities as possible. I’m really just creating extra grading work for myself in an attempt to help you during this crazy semester.

You can answer as many questions as you want. There are a total of 115 possible points. I’ll only grade out of 100 points, and any questions you answer will go toward extra credit. For example, suppose you answer every question and lose 20 points overall for incorrect responses/lack of detail. Your grade would then be 95.

The strategy is entirely up to you. For example:

1. You can fill out the entire exam and just plan to have as much extra credit as possible.
2. Or, you can figure out which questions get you closest to 100 points and only answer those, leaving all other questions blank.

Good luck!

# Windows Security Model (20 points)

## Question 1 (4 points)

What is the difference between a client-server and a peer-to-peer network structure?

Client-server is a centralized structure. All clients report to the same server.

Peer-to-peer is a decentralized structure. Clients rely off of connecting to each other for receiving services. This also means each client is a server.

## Question 2 (2 points)

What is the difference between a workgroup-joined and a domain-joined network structure?

Workgroup-joined computers are connected locally through a peer-to-peer connection. A domain-joined structure relies off a centralized domain of resources for users to pull data from.

## Question 3 (4 points)

How are DACLs and SACLs used in Windows security?

Windows uses DACL’s to determine what users have access to computer resources. SACL’s are used to determine how access to resources is audited.

## Question 4 (10 points)

Describe in detail the differences between Linux and Windows security designs (6 points). Describe at least one approach for **each** OS to harden the system (4 points).

Linux can harden its system by installing AppArmor. AppArmor applies security at the application level. This means that there are security settings for each application that can run on the system.

Windows can harden its system by making sure these are enabled

* Device Guard
* Credential Guard
* Application Guard
* Exploit Guard

And, if possible, apply a group policy.

# Application Servers (8 points)

## Question 5 (6 points)

Describe the concept of an n-tier architecture in application servers. How is an n-tier structure different compared to a localized and a client/server architecture? Make sure to answer all points.

N-tier architectures divide up the front-end, back-end, and data storage of an application across a network. Localized and client/server architectures differ because they still bundle some components together into one. For example, the client/server architecture splits the front-end and back-end interfaces, to improve security and other properties. This does not separate the database from the data processing. In an N-tier architecture, the data processing and database would have their own dedicated machines/containers N-tier utilizes different machines/containers for each subprocess in the process.

## Question 6 (2 points)

What is the difference between an application server and a monitoring server?

Application servers provide services for users. Examples of this is webservers, ftp servers, and email servers. Monitoring servers provide insight on computer hardware, performance statistics, and network statistics.

# Web Servers (22 points)

## Question 7 (4 points)

Describe the difference between authentication and authorization.

Authentication is being able to prove who we are. Authorization is having high enough privileges to do what we want.

## Question 8 (4 points)

What is a protocol listener? Why would you want additional protocol listeners on a web server?

A protocol listener is a program that continuously listens for incoming data on an open network port. It will only accept incoming data that confines to the specific protocol it was designed for. An example of this is the httpd service on Linux.

## Question 9 (4 points)

What is the purpose of an application pool in IIS? Why would you need more than one?

Application pools define specific back-end functionality for a webserver. The advantages of having multiple pools are

* Websites are isolated from each other
* Websites can run different versions of software
* Websites can have the same applications, but with different settings
* It provides a layer of security between the webservers themselves

## Question 10 (10 points)

What are the five forms of IIS authentication? Briefly describe each one.

* Basic authentication. AKA a username and password. The must provide a correct username and password pair to authenticate
* Digests. A digest still uses a username and password but hashes them before sending the data to the authentication server.
* Form authentication. The user is prompted to submit a web form with his credentials for authentication.
* AD DS authentication using the Kerberos authentication protocol. It works by introducing a Key Distribution Center between the server and the user. The server and user securely communicate by using these keys to encrypt and decrypt their data.
* NTLM authentication (depreciated)

# Group Policy (12 points)

## Question 11 (4 points)

What is a group policy object (GPO)? How would you apply a GPO to a domain?

A group policy object contains all the user and computer enforced policies. Policies can range from things such as disabling the command prompt to whether or not the screensaver is enabled by default.

To apply a GPO to a domain, go to

Administrative Tools -> Group Policy Management -> Group Policy Management Editor

Left click on a domain, and select Action -> Link an Existing GPO -> Select the desired GPO -> OK

## Question 12 (4 points)

How are group policy settings different when applied to User Configuration vs. Computer Configuration? Provide an example of a setting applied to the User Configuration but not the Computer Configuration.

User configurations are applied whenever a specific user logs in to any computer on the AD DS network. Computer configurations apply on each computer, regardless of user.

An example of a configuration applied to user and not computer is whether or not a user can access the command prompt or not.

## Question 13 (4 points)

What does it mean to specify a GPO to be enforced? How is this different than a GPO that blocks inheritance?

An enforced GPO applies its policies to all child GPO’s. Blocked inheritance is when a GPO does not inherit additional policies from its parent GPO. The difference is that enforcement will still take precedence over blocked inheritance. If a parent GPO has enforcement, then all children will inherit its policies no matter what.

# Single Sign-On (12 points)

## Question 14 (3 points)

What are the three factors of multi-factor authentication?

* Knowledge
* Possession
* Inheritance

## Question 15 (4 points)

How are tokens used in SSO? Specifically, what type of data is contained in a token, and at what stage of SSO is it used?

Tokens are used to authenticate users between applications. A token contains information about the user. It can contain the user’s email, system info, etc. In addition, the identity provider’s signature is part of a token and is what makes it valid.

SSO tokens are used when the user is requesting access to protected resources. More specifically,

1. The user requests for protected resources in an app
2. A request is sent to the identity server
3. The server authenticates the user, creates a token, signs it, and sends it back
4. The app provides the resources to the user if the signature is valid

## Question 16 (5 points)

Assume I want to log into cit349.ou and I have logged into csi3670.edu (i.e., a different domain). Can I use a cookie or a session to reuse my login from csi3670.edu to cit349.ou (2 points)? Why or why not (3 points)?

Yes, but only if the two domains have a connection through LDAP or AD DS. If so, then the user should be able to authenticate. The domains should be using the same authentication database. The authentication token will simply need to be saved in the browser’s cookies.

# Failover Clustering (18 points)

## Question 17 (2 points)

What is the purpose of failover clustering?

To make sure that servers have the most uptime as possible

## Question 18 (6 points)

What is the purpose of a quorum (4 points)? What is the purpose of having a witness (2 points)?

A quorum is used to decide whether or not cluster members are able to provide service. If the quorum does not return enough votes from the members, then the cluster may not provide the uptime needed. Votes are decided on a majority bases. Therefore in the case that there is an even number of cluster nodes, a witness is needed to break ties.

## Question 19 (10 points)

What are the hardware requirements of failover clustering? What do we need at minimum? This question is worth more points, so make sure to be detailed in your response.

At minimum, to perform failover clustering each server needs hardware that

* Recommended that hardware is “Certified for Windows Server 201X”
* A general rule of thumb to keep each server’s hardware within the same family of each other. For example, try not to use processors with different architecture
* The servers must be able to connect to multiple networks. A single ethernet port isn’t going to cut it.
* Network adapters (ie. CAT5 cables) should be all the same and use the same protocols
* Each node must have the same file system with a master boot record or a GUID partition table

# Penetration Testing (11 points)

## Question 20 (4 points)

Describe two reasons why penetration testing is a necessity.

Penetration testing is critical because if we do not attempt to find the weaknesses in security, then a hacker will. It is not good if a hacker finds a vulnerability first. An additional reason for wanting it is because environments can change overtime, and penetration testing will ensure that an environment is still as secure as it was before.

## Question 21 (3 points)

Describe three ways to perform reconnaissance.

* Social engineering. An example of social engineering is when an outside threat pretends to be on the inside of a company, affiliated with the company, or beneficial to the company in some way. In turn, an employee will think the threat is okay and proceed with whatever nonsense is provided to them. In the end, the employee is scouted for information about system information and security.
* Network scanning. Hackers can use existing methods to “scan” the network of the system their interested in. They can scan an AD DS address book or port scan for open ports that can be exploited.
* Documentation/Social media. Some companies publish their security policies or have media events where they talk about their processes. This information may provide key points to what vulnerabilities their system may have.

## Question 22 (4 points)

Describe the concept of pivoting in penetration testing and provide an example.

Pivoting is gaining a single access point to a network and using that single point to branch off into more access points. For example, as a hacker you successfully gain access to an employee’s computer. You can look at that computers mapped network addresses or email contacts, and then deploy another attack on those locations or people to possibly gain another point of entry.

# VPN (12 points)

## Question 23 (4 points)

Describe how a traditional connection is different from a VPN connection.

A traditional connection simply sends unencrypted data over the network without masking identity. A VPN encrypts and masks the identity of where the data is coming from.

## Question 24 (4 points)

Describe two reasons why you should use a VPN when on a public network.

1. A VPN will hide your ingoing and outgoing data from outside connections (packet sniffers).
2. A VPN will also allow for users to bypass any restrictions set on the public network.

## Question 25 (4 points)

Describe how a VPN server is different from a proxy server.

A proxy simply acts as a middleman between you and your data’s destination. A VPN does the same, but in addition your data is encrypted going to and from the VPN. This provides a much higher level of security. No cleartext is sent over the internet.