Chapter 1 – Introduction to Security

This document contains two main sections. The first is an introduction to the course which contains an introduction to the material you'll learn in the course, describes the course goals, explains the relationship between this course and the Security+ certification, and explains how to use the lecture notes. The second section of the document contains material that will help you with this specific section of the course. It explains the material presented in the book, provides tips for completing the assignments for this chapter, and provides ways for checking your comprehension of the material covered in this chapter. I strongly urge you to read the entire document as it will be very helpful in meeting the learning objectives and completing the assignments for this chapter.

Objectives

At the end of this module students will be able to:

1. Describe the learning objectives and goals for the class.
2. Define computer security and cyber security, and explain why they are important for both home and business users.
3. Identify threat actors and their attributes.
4. Describe the different types of vulnerabilities and attacks.
5. Explain the impact of attacks.
6. Setup a Virtual Machine to use for testing.
7. Write a paper using APA format.

Course Introduction

This starts the first section of the Introduction to Computer Security course. In this introduction you'll learn why a course in Computer Security is needed, why 'Introduction to Computer Security' may not be the best name for the course and how computer security is related to cyber security and information assurance, what you'll learn in the course, and the course goals, and how to use the Lecture Notes and other material I've prepared for you.

The first concept to explore is why computer security is needed from a human or sociological point of view. The reason, which is pretty obvious, is that we use computers and networks to store and transmit data and information which has value to individuals and organizations, and this information needs to be protected from unauthorized access or use. If we lived in a fantasy world of puppies, rainbows, and unicorns, where we didn't have to worry about people stealing our data, there wouldn't be any need for computer security. But we live in the "real world" where some humans and some of our social constructs are flawed, and people want to steal data. And since we now store large amounts of sensitive data on computers, we need some way to secure that information.

Securing computer and network systems is a complex job that requires knowledge of many different components, which is sad for computer users but great for you or anyone that wants to pursue a career in computer security.

Course Name and Cyber Security and Information Assurance (CSIA)

The next thing to learn about is some terminology, and why I think a better name for the course would be Information Assurance. Computer security refers to ensuring the confidentiality, integrity and availability of the information processed and/or stored by a computer. This includes everything from providing physical security, to data security, and practicing safe computing. But taken literally, computer security, means protecting computers, which is a major component of cyber security, but not the only component as cyber security also covers protecting things like networks, mobile devices, embedded devices, etc.

And cybersecurity is actually a component of information assurance. Information assurance is a business term which is used to describe all the things that are done to protect a business's assets and its data. In addition to cyber security, information assurance includes things like risk management and planning for business continuity. Don't worry about these terms and what they mean at this point. For now, the point to take away is that even though the course is called Introduction to Computer Security the course provides an introduction and overview of the main concepts of cyber security and information assurance and should be called Introduction to Cyber Security and Information Assurance (CSIA).

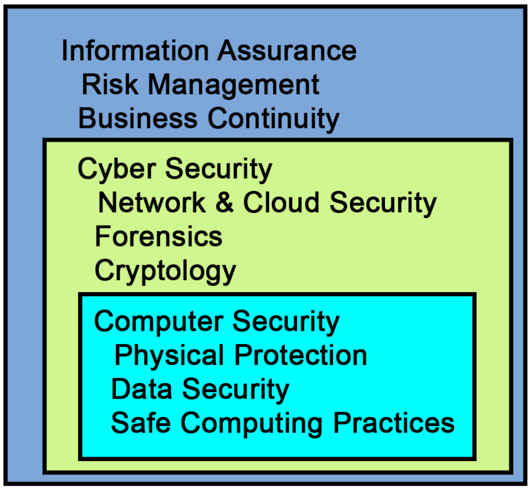


Figure 1.1 – The components of Computer Security, Cyber Security, and Information Assurance.

What You'll Learn in the Course

So, what will you learn in this class? The easy answer is that you will learn about Cyber Security and Information Assurance (CSIA). But as you've just seen Information Assurance encompasses a wide variety of subjects, from protecting systems from different types of attacks like malware or phishing, to encryption and cryptology, to digital forensics where you look for evidence of attacks and crimes, to business continuity and lots more. And even though I've been told that I'm a good teacher, and I'm sure that you're an intelligent individual who is eager to learn, there's way too much in Cyber Security and Information Assurance for you to learn it all in one single class. This is why CBC has several CSIA classes which will provide you with in depth knowledge and hands on experience in several aspects of cyber security. But you have to start somewhere so this class was designed as a “starter” class, and it’s meant to provide you with an overview and an introduction to many of the subjects that you’ll learn about in-depth in later classes. In other words, in this class you’re going to learn a little bit about a lot of “stuff”, while in later classes you will learn a lot about a single subject. As you go through the course try and keep in mind that you aren’t expected to be an expert in any of the course subjects at the end of this class, only to have a general idea of what they are and what you’ll be getting into in the Cyber Security degree program.

Course Outline

Now let’s look at the course outline. But before we do, please take note of two things. The first thing to note is that you may see several new terms during this discussion of the course outline. Don’t worry if any of the terms don’t make sense as we go through the outline as you’ll learn their definitions later in the class.

The second thing to note is the reason or purpose for discussing the course outline. We’re doing this to try to show you how all the course components fit together with the hope that this gives you some perspective or some framework to see that these are all pieces of one large puzzle instead of just a bunch of random separate subjects.

> **Chapter 1: Introduction to Security** – the basic but important concept that attackers can use vulnerabilities to steal data.
>
> **Chapter 2: Threat Management & Cybersecurity Resources** – once you know that attackers take advantage of vulnerabilities, the next thing to learn is how to determine what problems any specific system may have. In this section you will learn about the databases of vulnerabilities used to check systems for security problems and the tools

used to perform these checks.

Chapter 3: Threats & Attacks on Endpoints – Up to this point the main thing you've learned about attacks is that they "happen" without much more explanation. In this section you'll learn about the main categories of threats and attacks and take a closer look at how attacks in some of the categories are performed.

Chapter 4: Endpoint & Application Development Security – All the defense processes you've learned about up to this point have been reactive. That is, they are ways to respond to vulnerabilities and attacks after they occur. In this section you'll learn about the proactive things that are being done to try and find and fix new vulnerabilities before attackers do, how new threats found, solutions discovered, and how this information communicated, and methods that developers and engineers can use when creating new systems to ensure they're secure.

Chapter 5: Mobile, Embedded, and Specialized Device Security – Up to this point we've mainly been looking at securing computers. In this section you'll learn about the special security problems faced by laptops, tablets, phones, industrial controllers, and IoT devices, and some ideas for protecting these types of devices.

Chapter 6: Basic Cryptography – The two main ways of protecting data are physical protection, and scrambling it so only authorized individuals can read it. Cryptography is the science of scrambling data, and this section introduces the two main categories of cryptography, which are hashing and encryption.

Chapter 8: Networking Threats, Assessments, and Defenses – This section introduces security issues associated with networks, mainly the Internet, and how to protect from them.

Chapter 12: Authentication – In this section you'll take a closer look at cryptographic hashing, as well as the different types of password systems and two factor authentication or 2FA.

Chapter 13: Incident Preparation, Response, and Investigation – In this section you'll start to look at some of the business aspects of cyber security including having a plan in case an attack does occur, how to determine what happened, and how to work with law enforcement and the public or customers.

Chapter 14: Cybersecurity Resilience – This section looks at more business aspects of cyber security, focusing on things to do to keep a business running if an attack or other disaster occurs such as having backups and redundant systems.

Chapter 15: Risk Management & Data Privacy – In this section you'll learn about the risk management process, which provides a way to rank risks and allows the most urgent problems to be dealt with first.

You'll also be introduced to two important concepts that don't have their own sections. These are access control and policies and procedures. Access control has been stuck into section 13, and policies and procedures have been combined with the information in section 14.

Course Goals

Personal and Professional Security

This class is an overview of computer security, and it has two main goals. The first is to provide a first step into a degree and career in cyber security by introducing you to the main concepts and terminology you'll encounter in information assurance, and the second is to help you on a more personal level by using what you learn to help you improve the security on your personal devices and your home network. In this section we'll delve a little deeper into these two goals as well as look at the relationship between this course and the Security+ certification.

Course Goals – Introduction and Overview of Career in Security

There are a couple things you should note about the course goals as they pertain to a career in cyber security or computer science. The first is to remember that this class is an *introduction* to computer security, and you'll be presented with basic information about several different subjects, which means you'll learn a little bit about a lot of things, but you won't go into detail on any specific subject. That is, you'll be introduced to things like threats from malware or attackers, encryption, cracking passwords, checking systems for security issues with vulnerability and penetration testing, and finding evidence of attacks using forensics, but you won't be expected to know the details of any of these items or become an expert in any subject. If you pursue a cyber security degree at CBC, you will find that there are separate courses that do a much deeper dive into each of these subjects and since each course is dedicated to a single subject, they will provide you with more in-depth knowledge and hands-on experience regarding that single subject. But this class only provides an introduction to each of these subjects, which will hopefully leave you wanting more. It can feel like going to a restaurant for an overview of their meals. The chef brings out small bites of different salads, breads, vegetable dishes, main courses, desserts, etc. You get a single bite of each delicious item, but only a single bite then you must move on to the next item.

As you progress through the class, please keep in mind that there is no expectation that you will have mastered these subjects by the end of the class. You're just being introduced to the concepts, and starting to learn the terminology that you'll build on in later classes. It's a good sign if you find the subject introduced in each section of the class leaves you wanting to know more.

Course Goals – Increase Personal Security

My second goal for you is to help you increase your personal security. Hopefully you're already doing the essential security basics on your home devices, like making backups and installing updates. But if not, you'll learn why and how you should be protecting your devices, plus you'll gain experience with ways to perform advanced tasks such as locating missing or stolen devices, securing your home router, etc. When you're done with the class, even if you don't go into a career in Cyber Security, your personal security should be more robust.

(Not) Certification

The last thing that I think is important for you to understand is the relationship between this class and the Security+ Certification. In the past the official class description said that this class would help prepare you for the CompTIA Security+ Certification Test, which is a good basic certification. I changed the course description when I started teaching the class because it's more than a little deceptive. I hold several industry certifications and I know how hard the exams are to pass and what it takes to pass one. While the material in the class will help you begin to prep for the Security+ exam there is a lot, lot more you will need to know to pass the exam. Unless you already have a few years' experience with Cyber Security and Information Assurance, just taking this class isn't going to be near enough to pass the certification exam. The course will help with preparation for the certification exam, but it's only a beginning of what you'll need to know and do to pass the exam.

Hopefully you understand that certification exams are meant to be used by individuals who already have a few years' experience with a product or in a particular area. Once you have that experience, using a book like the one we're using in this class can help you prepare for the certification exam by identifying and filling any holes you may have in your knowledge and experience. But it would be very difficult, maybe even impossible, to just read this book and then pass the Security+ test. You'll be ready to take the certification test when you can read the book and say "I completely understand what the book is saying and I already know about each subject in the book", and you can easily answer every review question. In other words, you'll be ready to take the test when you don't need the book.

Another possible point of confusion is the book. During the class you'll be using a book that is designed to help individuals with the Security+ Certification test. However, we're just using the book as an additional learning resource, and only a portion of the book. The book was chosen because it is well written, has relevant hands-on exercises, and is a decent resource … but regardless of the title you are not expected to pass the Security+ test. Even though the book says Security+ in the title you don't have to pass the certification exam. You aren't even expected to take it.

I'm going to repeat myself just to be clear. You do not have to pass or even take the Security+ exam for this class. If you do choose to try the Security+ exam, please note that passing any certification test requires additional study and work on the student's part. In other words, this class will be a good starting point for you if you want to take the Security+ test, but it's not the only thing you should do if you want to pass the test.

On the other hand, if you already have your Security+ Certification, make sure and get in touch with the instructor as soon as possible as you may be eligible to receive Non-Traditional Credit for the class without having to take it. You should do this right away; because if you qualify for the credit, you can get your tuition $$$ back and hopefully still have enough time to sign up for another class.

The last thing I'd like to say about certification is that even though passing the Security+ exam isn't a requirement for this class it is a good long-term goal as most employers give much more consideration to certifications than they would to your grade in this class. I've never seen a job description that says you need at least a 3.0 in Mr. Sako's class; but I've seen plenty of job descriptions that list Security+ or other certifications as a requirement.

Using the Lecture Notes

While the book mainly concentrates on cyber security in a corporate setting, which is where the jobs are, I've created a bunch of material to help you see where you can apply what you're learning to your personal devices and networks and help you put the course material in perspective by relating it to your personal security. The extra material I've prepared for you includes lectures, videos to provide extra background as well as help you complete some of the assignments, and some optional assignments to help you improve your personal security posture.

If we're in class together then I'll be lecturing a good portion of the time. I'm not the kind of instructor whose lectures consist of reading power point slides, because I assume that you already know how to read. And I'm not going to make you watch me read slides because I personally hate taking classes where this occurs. Instead, I try to provide you with any extra background information I feel may help you understand the class material or lead the class in a discussion regarding the material being covered. We would also spend quite a bit of time learning how to do some related hands-on work, which will either help you complete the assigned exercises, or help you improve your own home security. For example, if we're learning about password security, I'd provide some background on how passwords are scrambled using hashing before they're stored, and then we'd do some exercises on cracking passwords using tools that crack the specific password hash.

But we may not be in class together. Maybe this is an online section of the class, or maybe there's a pandemic. And if we're not in class together then you might think you're going to miss hearing the lectures. However, I've spent hundreds of hours documenting what I'd be telling you in the classroom to make sure that you don't miss anything by taking the class online. If you read the lecture notes for each section of the class, you'll have access to pretty much the same lecture information you'd get if we were together in the classroom.

You’ll find a set of lecture notes in each Module/Chapter/Section of the class. I strongly suggest that you read the lecture notes as they should make the class more interesting by making the material more applicable to your own life. They will definitely help you complete some of the assignments as someone keeps changing that darn Internet and some of the instructions in the book no longer work, and the only way to complete these assignments is to use the tips in the Lecture Notes. The Lecture Notes also contain a few extra questions that you’ll need to answer for some assignments, plus extra credit opportunities. Note that the additional questions and extra credit aren’t in every section. The only way to find out which sections is to use the Lecture Notes.

What this section is about – what you should learn

Now let’s talk about what you should learn about CSIA in this section of the course. In this introduction section the main things you’ll learn about are the Buy-In, some of the challenges in cyber security, about attackers and vulnerabilities, and about the impacts of attacks.

Buy-In

One of the first concepts presented in the book is something I call the “Buy-In”. The buy-in is something that should happen in any class, or any section of training, and as the name implies, Buy-In is where you decide that you want to learn the material, as opposed to sitting through a class because someone told you that have to take it. Or in psych talk this is where the motivation to succeed is internalized, instead of relying on external motivators. Translated to plain English this means that you will be way more successful if you make the conscious decision to do something because you can see the value that you will gain for your efforts. Or the flip side of this concept is that you won’t put in much effort at all if you feel this is just another chore that you are being forced to do.

Even though it may seem obvious, and a little silly, the Buy-In is very important. Just think about your experience in real life. Outside of school and college I'm sure you put much more time and effort into your hobbies and things that you *want to do* and choose to do, than you do into things you feel that you *have to do*. Simply adopting an attitude that you want to do something is a proven key to success in any endeavor.

With that in mind, one of the first things the book does in this section is to try to convince you that Computer Security is important and learning about Computer Security is worth your time and effort. The book does this by discussing a few actual cases where security was breached and the impacts of those incidents. Unless you live under a rock, I'm sure you're bombarded with these types of stories on a daily/hourly basis. I'm also guessing that beyond reading about the break-ins and data theft, there's a chance you may have personally been a victim of some cybercrime. Have you ever been notified by some company, or group of lawyers suing a company, that your personal data has been compromised? Do you think your personal data would have been stolen if the organization that lost it was practicing good cyber security? If you haven't had your data compromised, you should consider yourself lucky as this happens all too frequently.

In any case, I don't know if what the book provides is enough to convince you that pursuing a career in Cyber Security is a goal worthy of your time and effort. Don't get me wrong as I'm not saying that this isn't a good career path, I think Cyber Security is a great degree and career. It's a high demand, well-paying field, the work is super interesting, and your efforts can actually make an impact and help your fellow man on an individual basis and help society as a whole. I'm just saying I don't know if the few paragraphs in the book are enough to convince anyone that cyber security is a good career choice. But since you're taking this class, I'm going to assume that you have already internalized the desire to increase your knowledge in this field.

Cyber Security Challenges

After convincing you that cyber security is important, the book describes some of the challenges in providing this security. There are several challenges, which is good news for anyone who wants to pursue a career in Cyber Security. If providing security were easy then there probably wouldn't be as many jobs, and the pay scale would be a lot less. Just as a side note, I think that it's a little funny that they list a lot of technical issues as being the main challenges, but they don't really come out and say what the biggest challenge is, at least in my opinion. And what is the biggest security challenge? I think the biggest challenge I've faced is with the users I support. You can make systems perfectly secure, but as soon as you let users on the systems you can still have problems. Your users will choose weak passwords, they'll give away sensitive information on social media, they'll fall for phishing attacks, and they'll find all sorts of ways to make your life really interesting. Yes, really darn interesting.

After this the chapter starts to introduce terms that have special meaning in security. Things like the CIA triad which stands for Confidentiality, Integrity, and Availability, and risks, vulnerabilities, and threats. Most of the terms defined in this chapter are important, but there are a few that I've only seen on certification exams. In any case, using the correct terms is important in any career field, especially as you start your career. You don't want to be the n00b that doesn't know the difference between a saw and a drill, or in this case a vulnerability assessment and a risk analysis. But don't worry about memorizing all the terms and definitions at this point. You'll gain experience with many of these later in this class, and in other classes as you finish your degree. Remember this class is an overview of everything you're going to learn in later classes, so you'll be exposed to hundreds of terms and phrases, way too many to try and memorize at this point. Once you start working with the various tools and programs on a daily basis the terms and terminology will all fall into place. And soon you'll be geeking out and speaking like a cyber security pro.

Oh … and the tests for the class are open book and open note, which is another reason you don't need to memorize any of the terminology. You want to try and understand the new terms, and start using the new terms, but don't get so wrapped in trying to memorize things that you fail to see the bigger picture.

Attackers

The next subject that's introduced are some of the groups that may perform attacks. As we discussed earlier, we don't live in a perfect world and there are people out there that want to steal your information. This includes lone individuals, criminal gangs, state actors, etc. They can be categorized in different ways such as hackers with different hat colors, or as script kiddies, hacktivists, state actors, and insiders. These are more terms you should start to become familiar with.

One thing to note here is how many attacks are attributed to insiders, somewhere between 30% and 50% depending on the source[1,2]. If you're surprised by how high this number is think of how much harder it is to protect systems from someone who already has access. It's like protecting items in your home. It's one thing to protect them from people outside your home where you can use walls and doors to provide physical protection. But how much harder is it to protect yourself from people who've you let in and are already inside the house? So, while we need to be concerned about all the various people that may attack our systems, in my mind the most dangerous ones and the ones you need to worry about the most are your fellow employees.

Vulnerabilities

Another subject introduced in this section are vulnerabilities or weaknesses in a system. That is, if someone wants to attack your system how do they get in? For an attacker to accomplish this

[1] https://techreport.com/statistics/cybersecurity/insider-threat-statistics/#:~:text=Last%20year%2C%20approximately%2031%25%20of%20all%20data%20breaches,from%20an%20insider%2C%20a%20contractor%2C%20or%20an%20employee.

[2] https://securityboulevard.com/2023/04/insider-threat-statistics-for-2023-reports-facts-actors-and-costs/

your system must have some type of weakness or weak point which is called a vulnerability. The vulnerability can be some problem with the programming code used by the system, or it can be a mistake made by a user such using weak passwords.

Vulnerabilities are an important concept to understand and while we only touch on them briefly here, you'll learn quite a bit more about them in the next chapter. At this point you're really just being introduced to the concept that a vulnerability is a weakness that an attacker can leverage to gain unauthorized access to a system or disrupt the system, so it won't be available for authorized users.

You'll also be introduced to the concept that vulnerabilities are associated with a platform which means your phone will have different vulnerabilities than a Windows based computer, which will have different vulnerabilities than a Linux computer or Mac, or cloud platform or smart appliance, etc. And you might think that patching all the vulnerabilities on a platform will make it safe. But in reality, almost all platforms rely on old legacy code or outside systems, which you don't control, which is turning out to be one of the current ways attackers are getting into systems. There are many examples of this such as the 2013 attack on Target Stores[3], where the attackers first attacked the company that supplied the Point of Sale (cash registers) used by Target.

The different categories of attack vectors such as via USB, wireless, over the network, etc. are then discussed. It's likely that you're already familiar with many of the different attack vectors and attack types, but it's also quite possible that there will some terms and terminology that you haven't heard of before. Once again, it's not super critical that you understand or memorize the details of every single attack type. That is, unless you're taking a certification exam. You'll learn more about the main attacks in other classes as you progress through the other classes in your degree program. In these later classes you'll learn how to protect devices

[3] https://www.cardconnect.com/launchpointe/payment-trends/target-data-breach/

from all kinds of attacks, and even learn how to perform some of the attacks yourself as you test the security of systems you're responsible for protecting.

Impacts of Attacks

The last concept introduced in this section is the potential impacts of attacks. If somebody does gains unauthorized access to data, what does that mean? The impact obviously depends on a lot of factors, but it can range from having no effect to putting a company out of business or leaving a country vulnerable to attack. For example, if someone breaks into my computer they won't find much, maybe my Netflix password. But on the other end of the spectrum you've probably seen the movies where criminals take over computers or networks and have the ability to hold the world at ransom, or take down all the satellites we use for GPS and communications, rendering us blind to physical attacks.

The simple, but important concept, is that being the victim of an attack is a bad thing. This brings us back around to the buy-in concept, which is that learning about computer security is a good thing.

Summary

We can summarize this section by saying that data and information have value, so attackers will try and take advantage of vulnerabilities to steal it, and if an attack is successful, it can be harmful to the data owner. The main concepts from this section might seem obvious and simple, but they provide the framework for the rest of the course, and for cyber security and information assurance. That is, if data had no value, or if there were no vulnerabilities, or if attackers didn't exist, then there'd be no need to cyber security.

Personal Security

As you learn about all the attacks, attackers, and vulnerabilities I think that there are a few things you should be thinking about and that you take away from this section. The first can be summed up with the phrase “stranger danger”. That is, while computers and the Internet are great resources and can help build connections between friends and family, provide entertainment, and help us learn, they also present plenty of dangers that can ruin lives and destroy businesses. When you have young children, you want them to experience the world and see its joys and wonders, but you also need to remind them that nature and humans can be cruel, and they need to have some sense of wariness around strangers and new situations. Hopefully you are aware that there are scammers and fraudsters, and worse, on the Internet, that are constantly trying to entice you with free movies, fake contests, work from home offers, etc. in the hopes that you’ll fall into their trap. If you think that animals in the wild are like characters in Disney movies, or go to a bar with someone you just met and leave your drink unattended while you go to the bathroom, or if you think that the sites that offer free copies of Windows or other software are safe to use, then I’m worried about you being too naïve to survive long in the real world, and I certainly wouldn’t hire you to protect me or my systems.

The second thing I believe you should think about is how you protect yourself and your own computer from these types of attacks[4,5,6,7]. That is, are you running your antivirus and malware scanners? Do you stay away from sketchy websites and avoid opening email attachments from people you don't know? Do you use strong passwords and 2FA, change your passwords regularly, and avoid using the same password for multiple sites? Are you doing your backups in case some ransomware encrypts your entire disk? And are you downloading and installing all the updates for all the software on your computer on a regular basis? Are you careful about the information you post on social media? These are the basic tasks that if performed, will protect you, or help protect your devices from malware.

[4] https://www.howtogeek.com/173478/10-important-computer-security-practices-you-should-follow/

[5] https://www.pcmag.com/how-to/12-simple-things-you-can-do-to-be-more-secure-online

[6] https://www.msn.com/en-us/news/technology/10-simple-security-actions-that-keep-you-much-safer-online/ar-BB1qOr9a?ocid=entnewsntp&pc=W089&cvid=0d7b5a6ac51842f4b2fb846c36abb98a&ei=57

[7] https://www.pcworld.com/article/2304346/5-outdated-security-practices-you-shouldnt-use-anymore.html

And then there's protection from phishing attacks. Are you aware enough to not respond to phishing emails or texts or phone calls? Have you gotten the calls about your social security number or bank account being locked, or emails from the attorney representing your Rich Nigerian uncle? Do you know how to respond to these types of calls or texts and how to differentiate between valid communication and phishing? Recognizing and knowing how to (not) respond to phishing attacks might seem simple, but some attackers do a great job of impersonation and it can be hard to distinguish between a valid phone call or valid email, and fake calls or emails. And apparently AI is going to make it even easier for the attackers to create real looking forgeries which will make identifying the fakes even harder.

As you read this information the first thing you should think about is protecting yourself and your home systems. The reason I say you should think about this first is that this is a great way to put what you're learning into context, as you should be fairly intimate with your own computer, your home network, and any other personal devices you might need to protect like phones, gaming consoles, etc.

The last thing is that you need to begin to switch your thinking from taking care of your own computer to what you will do if you get a job as a system or network administrator, or as the cyber security expert at a company; some type of job where you have to secure computers for an entire company instead of just your own computer. Is there anything that you'll do differently to protect an organization's systems from malware? That is do you think you should still run antivirus and malware scanners, perform backups, and install updates? (Nod your head yes. 😊)

But now for the tricky part, which is what would you do to protect the company from phishing attacks? I think that is a super tricky one, as you have to get all employees to be aware that they should not respond to suspicious emails, texts, or phone calls. Do you have any ideas how you would accomplish that? It might seem like there should be a simple solution, but just the fact that I'm even mentioning this should be a clue that it's not easy and that you'll learn more about this later in the class.

In my opinion, a big part of the problem with social engineering attacks is the way we go about trying to fix the problem. That is, in general terms we have attackers who are trying to steal the information, and defenders who are trying to protect it. With phishing we put all of the responsibility on defenders, while giving several key advantages to the attackers. The defense against these attacks is training everyone so they don't fall for the attacks. This might not be too difficult if you're just training yourself, and you have some technical skills, plus a healthy level of distrust of your fellow human beings. But it's really hard to train groups that include people who aren't technically inclined or aren't Internet savvy. And, as the book describes, the attackers take advantage of human nature and the fact that most people want to provide help when they can and training people to fight against some of their basic instincts is very difficult.

The attackers on the other hand, get almost free rein. The email companies don't check or verify accounts before handing them out, and some phone companies don't check or verify someone's identity before they assign a phone number. This allows the attackers to impersonate anyone they want and hide behind a cloak of anonymity. The attackers can constantly change their identity, which makes tracking them down very difficult.

As an analogy, think about how you protect your home. You don't let anyone and everyone into your house, only the people you recognize. The pressure is on you to screen people before letting them access, which probably isn't a problem if you're the only person living in the house. But now, imagine if you were in charge of physical security for a large apartment building. You need to train everyone living in the building to keep it secure, which would be a big job. But to make things even more fun, there are burglars who can impersonate anyone they want just by touching a button. Pressing the button allows them to change their appearance, their clothing, and gives them valid identification. Now how hard will it be to protect the building?

My solution would be to disrupt the attacker's ability to remain anonymous. That is, if you want to get an email account, or any type of Internet account, you would have to provide proof of your identity. Or if you want to get a phone number, you have to provide proof of your identity. This way, if you get a spam email, or a phone call telling you that the IRS is coming for you, you'll know exactly who is behind the attack. The argument against stripping away anonymity is that it would put political dissidents in danger in some countries. This is a valid point, but there's a fix for this too. It's completely possible to have two Internets. Why not build a new Internet, parallel to the existing Internet, that's secure and where it's much more difficult to be anonymous? There could be interchange between the two Internets, but any traffic coming from the unsecure side could automatically be flagged, so that you would know to proceed with extra caution when dealing with the unsecure information.

And just to be clear … the idea that anonymity on the Internet is a cause of many of the Internet's problems is just my opinion. Just something for you to think about, and something we'd discuss in class if we were actually meeting in class.

The Activities for This Section

There are two activities or assignments for this section, your first hands-on assignment and a writing assignment.

1. Required Hands-On Projects Homework

As the book states, running or testing software on your own computer may not be desirable as the programs may have unexpected consequences, not to mention adding unnecessary programs that you will only use once or twice. To help you with this, you have the option to use a virtual machine (VM) to do your installs and testing, and to do the hands-on assignments for this class.

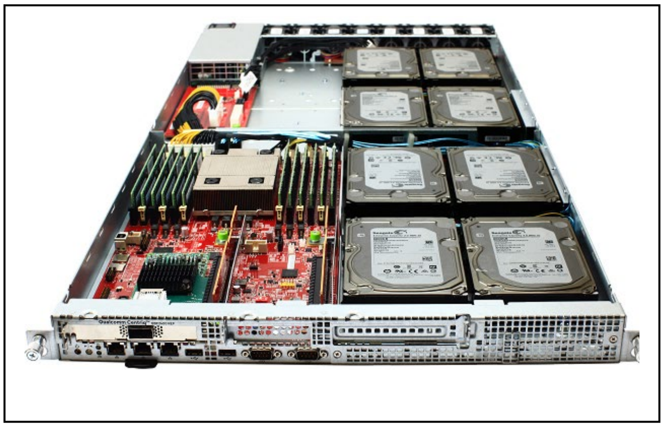
If you don’t know what a virtual machine is, you should watch the following videos, or do your own Internet research. You won’t be tested on this material, but I know how confusing it can be to if you’ve never worked with VMs before, so I put this material together to help bring you up to speed.

https://tonysako.com/home/virtual-machines-vm-introduction-and-overview/ - Virtual Machine Overview Intro and Definition
https://tonysako.com/home/virtual-machine-benefits/ - Virtual Machine Benefits
https://tonysako.com/home/virtual-machine-costs/ - Virtual Machine Costs

In the past we had each student create their own virtual machine using a product called Oracle Virtual Box. But this process is a little complicated, so I have created a Windows 10 virtual machine for you instead. (You’ll learn how to create your own VMs in later classes including CS430 Linux Administration.) The virtual machine I’ve made for you is already setup and running in the CBC Cloud; all you need to do is connect to the CBC Cloud and start the machine. You can do this with any browser, and once it's running, you'll have what looks like a Windows 10 computer running in your browser window!

The first hands-on assignment is to access the cloud based Virtual Machine (VM) that’s been created just for you. This machine resides in the CBC Cloud and can be accessed from anywhere you can get an Internet connection. While you’re not required to use the VM for your assignments (except for this assignment), we’ve built it for you just in case you want to use it and don’t want to use your personal machine for the remaining hands-on assignments. It’s also there in case you can’t use your personal machine because of technical constraints. For example, some of the assignments won’t work with the Home version of Windows. If your personal computer is running Windows Home, then you will have to use the VM to complete the assignment.

In this assignment you will connect to the CBC Cloud, which is technically called the vWorkspace Farm. vWorkspace Farm is too long and cumbersome, so I'm going to refer to it as the CBC Cloud. And in case you're curious, the CBC Cloud is really just a group of high-powered CPUs running in a rack in the CBC data center.



There are actually two ways to connect to the CBC Cloud, using something called HTML5 or using something called the VMware Horizon Client. In the past the easiest way was to use HTML5, but I've been told that they've fixed the problem with the VMware client and that it is now more efficient. In any case, it doesn't matter which method you choose, and directions for both methods will be provided.

Regardless of which method you use to connect, you will need a username and password to login to the CBC Cloud and see your VM(s). Your username will be the user portion of your CBC student email address. For example, if your CBC email address is DuncanIdaho@columbiabasin.edu, your username will be DuncanIdaho.

Your password will be the same as your CBC student email password. But note that you *may* have to reset your password to get the CBC Cloud system to sync your username and password. Try logging in with your current password and if you're successful don't worry about changing it. But if you can't get in, or get in and can't see the CS150 VM, then reset your password and try again. You can find the instructions for resetting your student password at: https://columbiabasin.edu/resetpassword

Connecting to Your CBC VM Using HTML5

Here are the instructions for connecting to your VM using HTML5. You can either follow along with these instructions, or watch the videos.

https://tonysako.com/home/cs150-introduction-to-computer-security/connecting-to-your-cbc-cloud-vm-using-html5/ - Connecting Using HTML5 (Video Instructions)

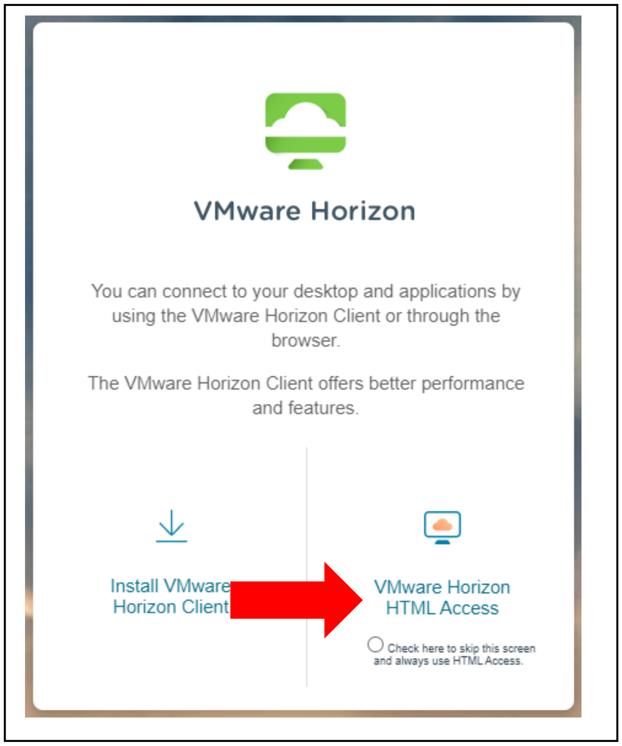
Connecting with HTML5

A. Start your web browser and connect to:

   https://vlabsc.columbiabasin.edu

   This opens a web page that provides access to the CBC Cloud, and allows you to choose one of two ways to connect to the cloud VMs that have been built just for you. You should see something that looks like the figure to the right.

B. Click the button or section that says **VMware Horizon HTML Access**.

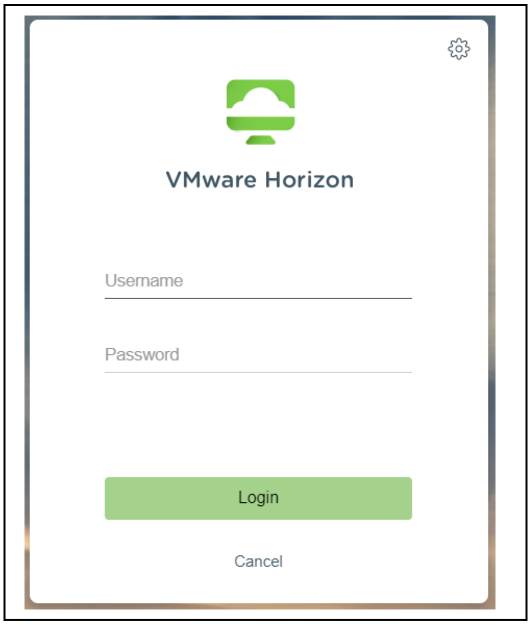


You can connect to your desktop and applications by using the VMware Horizon Client or through the browser.

The VMware Horizon Client offers better performance and features.

○ Check here to skip this screen and always use HTML Access.

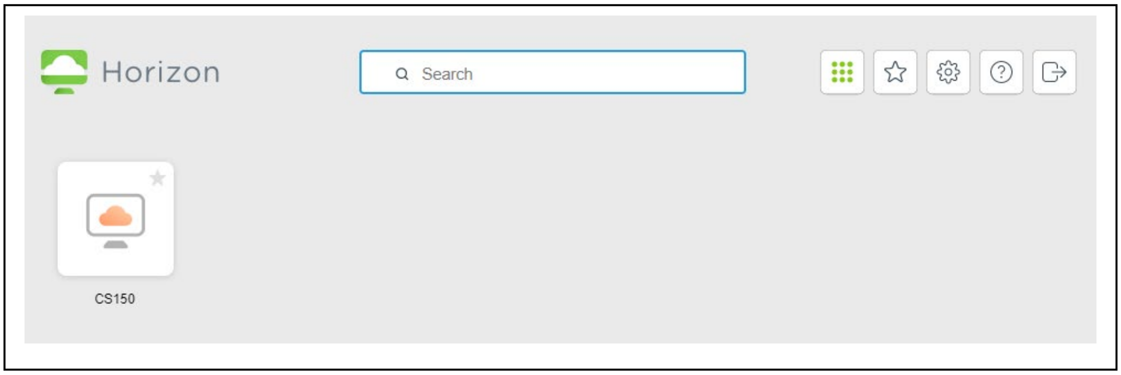
C. You should now see the VMware Horizon login box. Enter your **Username** and **Password** and click **Login**. This will be the same username and password that you use to log into Canvas.



Remember your username will be the user portion of your CBC student email address and your password will be the same as your CBC student email password. For example, if your CBC email address is DuncanIdaho@columbiabasin.edu, your username will be DuncanIdaho.

Also remember that you *may* have to reset your password to get the CBC Cloud system to sync your username and password. Try logging in with your current password and if you're successful don't worry about changing it. But if you can't get in, or get in and can't see the CS150 VM, then reset your password and try again. You can find the instructions for resetting your student password at: https://columbiabasin.edu/resetpassword

D. That will bring you to the web page that displays your Virtual Machines. It will look similar to the following figure, but you may have different VMs available, so what you see may be different. But you should at least see one named **CS150**. If you don't see the CS150 VM you may need to force the CBC Cloud system to sync with your account by changing your CBC Student password, and reconnecting to the CBC Cloud. You can find the instructions for resetting your student password at: https://columbiabasin.edu/resetpassword



E. Click the **CS150** VM to start your Virtual Machine. This will start what looks a computer running Windows, except it will be running in your browser.

F. If you see the following error message, refresh the browser window.

Failed to resolve proxying route for request

G. Once the Windows Virtual Machine is booted and running, you'll see a Windows login screen. Login using the following preset username and password:

Username: Administrator

Password: **T548cstt**

H. At this point you will be logged in, and ready to start using your VM. If you've never done this before, stop and take a minute to think about what has just happened. You've just started a computer, and it's running in your web browser. I hope you appropriately impressed at how cool this is!

I. If you want to use this method to connect to your VM in the future I suggest you bookmark the page, so you don’t have to type the URL again.

J. Note – When you are done make sure that all your work is saved, and then end your session by closing the browser window containing the VM or logging off the VM. Do **NOT** shutdown the VM by selecting the Windows Shutdown. If you do this it will take a lot longer to access your VM the next time you want to use it. If your VM is powered off, the software that controls all of the VMs has to restart it, which may take several minutes. This process doesn’t start until you try and access the VM, and you don’t see a message that says you’re waiting for the VM to power up, you just see error messages. If this happens don’t panic, your VM should restart and be available in a few minutes. Just take a deep breath and count backward from 1 million …

Connecting with VMware Horizon Client Program

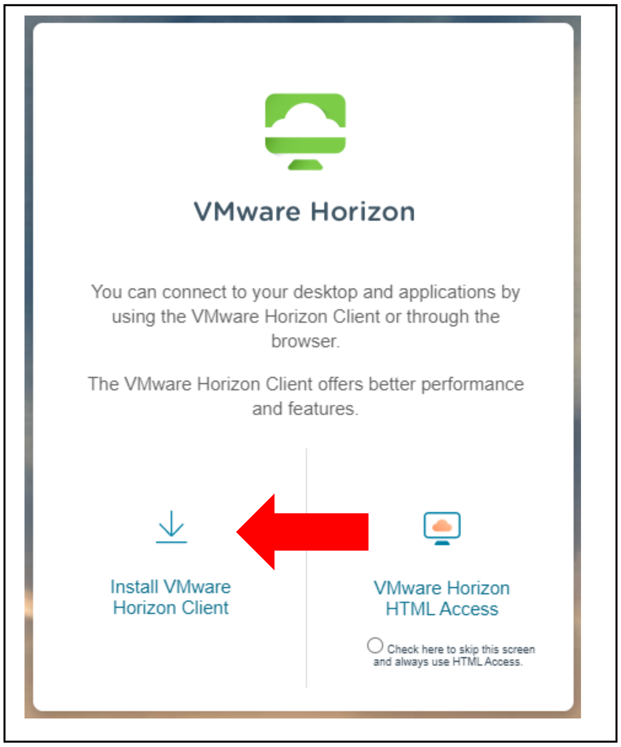
Here are the instructions for connecting to your VM using the VMware Horizon Client. You can either follow along with these instructions, or watch the videos.

https://tonysako.com/home/cs150-introduction-to-computer-security/connecting-to-your-cbc-cloud-vm-using-vconnector/ - Connecting Using vConnector (Video Instructions)

Note – if you connected to your VM using HTML5, you don’t need to do this step. It accomplishes the same thing, except you download a client application to make the connection instead of going through your web browser.

A. Start your web browser and connect to: **https://vlabsc.columbiabasin.edu**

This opens a web page that provides access to the CBC Cloud, and allows you to choose one of two ways to connect to the cloud VMs that have been built just for you. You should see something that looks like the figure to the right.



VMware Horizon

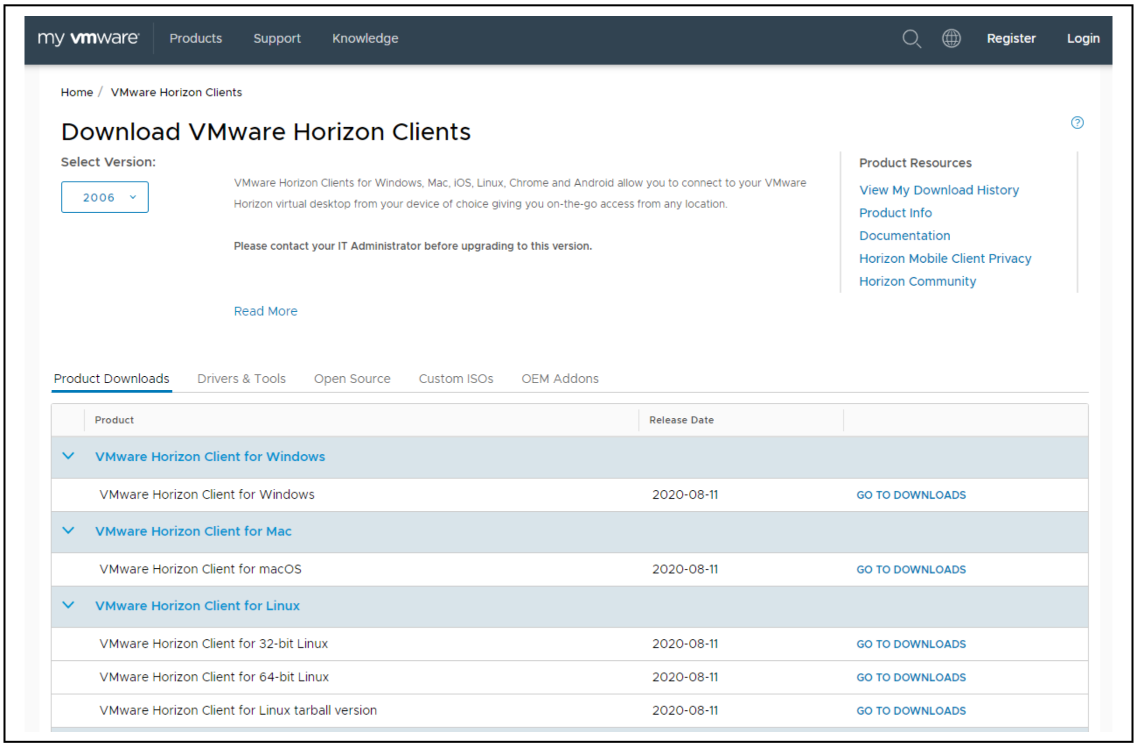
You can connect to your desktop and applications by using the VMware Horizon Client or through the browser.

The VMware Horizon Client offers better performance and features.

Install VMware Horizon Client
VMware Horizon HTML Access
○ Check here to skip this screen and always use HTML Access.

B. Click the button or section that says **Install VMware Horizon Client**.

C. This will display the Download VMware Horizon Clients page. Locate the correct client for your operating system and click **GO TO DOWNLOADS**



Download VMware Horizon Clients

Select Version:

VMware Horizon Clients for Windows, Mac, iOS, Linux, Chrome and Android allow you to connect to your VMware Horizon virtual desktop from your device of choice giving you on-the-go access from any location.

Please contact your IT Administrator before upgrading to this version.

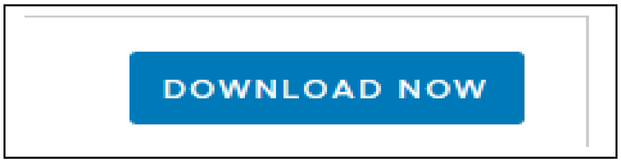
Read More

Product Resources

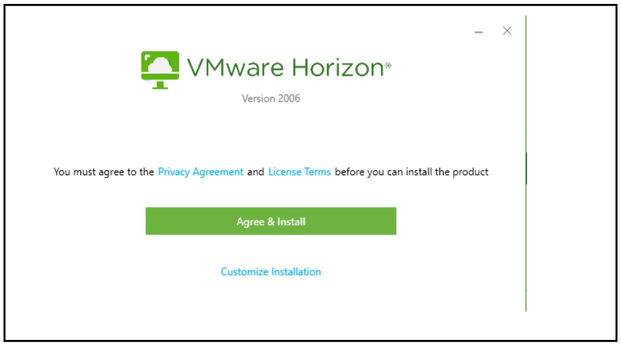
- View My Download History
- Product Info
- Documentation
- Horizon Mobile Client Privacy
- Horizon Community

Product	Release Date	
VMware Horizon Client for Windows		
VMware Horizon Client for Windows	2020-08-11	GO TO DOWNLOADS
VMware Horizon Client for Mac		
VMware Horizon Client for macOS	2020-08-11	GO TO DOWNLOADS
VMware Horizon Client for Linux		
VMware Horizon Client for 32-bit Linux	2020-08-11	GO TO DOWNLOADS
VMware Horizon Client for 64-bit Linux	2020-08-11	GO TO DOWNLOADS
VMware Horizon Client for Linux tarball version	2020-08-11	GO TO DOWNLOADS

D. Click DOWNLOAD NOW

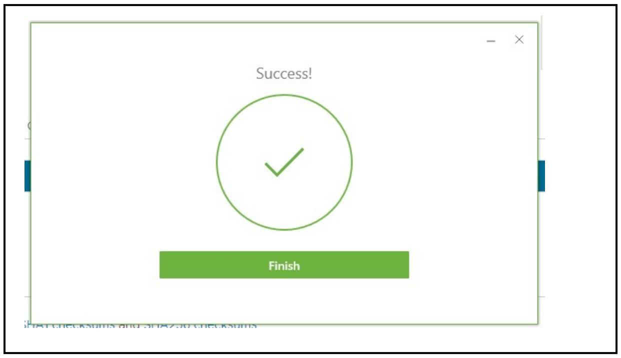


E. Click Agree & Install



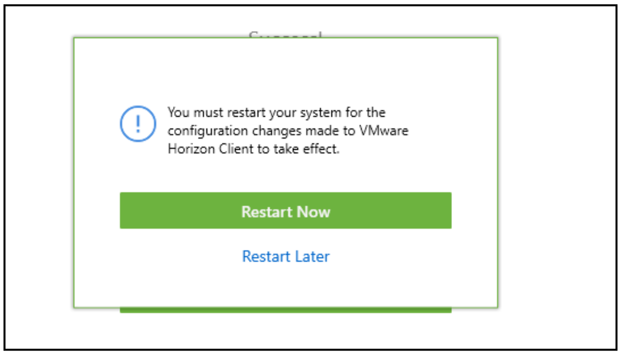
You must agree to the Privacy Agreement and License Terms before you can install the product

F. Click **Finish**



Success!

G. You will have to restart your computer before using the new program. Ensure you have all your files closed and your work saved before restarting. Click **Restart Now**



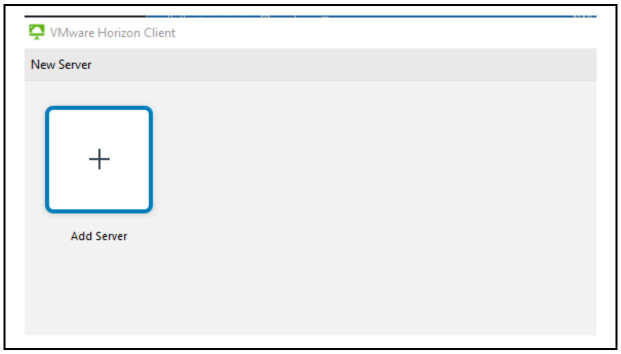
You must restart your system for the configuration changes made to VMware Horizon Client to take effect.

Configuring VMware Horizon Client

Once you have installed the client you will need to configure it to connect to the CBC Cloud.

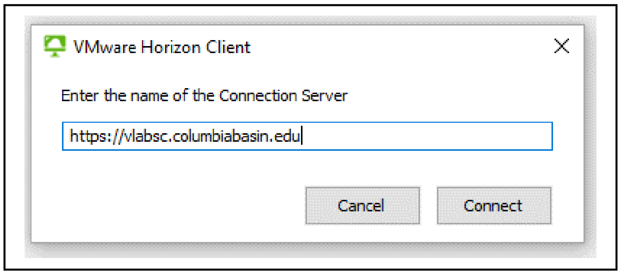
A. Open the **VMware Horizon Client**. The install program put a shortcut on your desktop, or you can find it by going to the Windows Start button and navigating to the **VMware Horizon Client** folder.

B. **Double click** the **+** button to create a new server connection.



C. Enter the name (URL) of the CBC Cloud Server: https://vlabsc.columbiabasin.edu

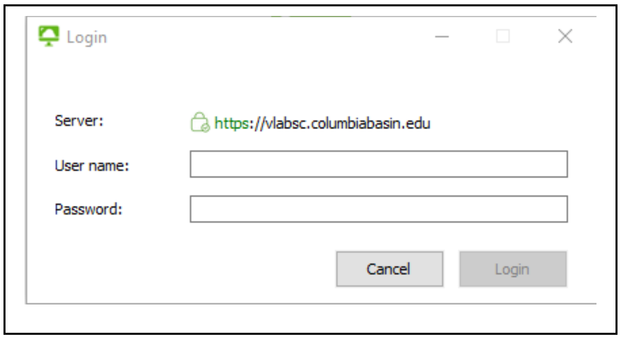
Click **Connect**



Enter the name of the Connection Server

https://vlabsc.columbiabasin.edu

D. Enter your **Username** and **Password** and click **Login**. This will be the same username and password that you use to log into Canvas.



Server: https://vlabsc.columbiabasin.edu

User name:

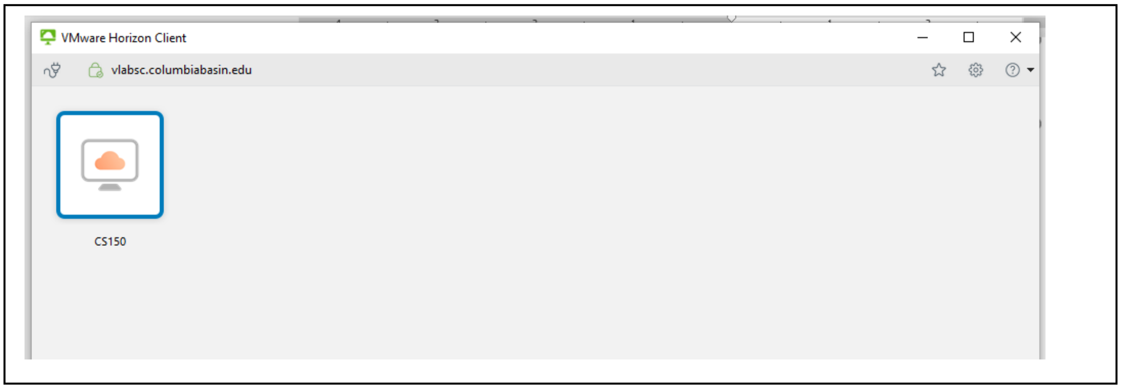
Password:

Remember your username will be the user portion of your CBC student email address and your password will be the same as your CBC student email password. For example, if your CBC email address is DuncanIdaho@columbiabasin.edu, your username will be DuncanIdaho.

Also remember that you *may* have to reset your password to get the CBC Cloud system to sync your username and password. Try logging in with your current password and if you're successful don't worry about changing it. But if you can't get in, or get in and can't see the CS150 VM, then reset your password and try again. You can find the

instructions for resetting your student password at:
https://columbiabasin.edu/resetpassword

E. That will bring you to the web page that displays your Virtual Machines. It will look similar to the following figure, but you may have different VMs available, so what you see may be different. But you should at least see one named **CS150**. If you don't see the CS150 VM you may need to force the CBC Cloud system to sync with your account by changing your CBC Student password, and reconnecting to the CBC Cloud. You can find the instructions for resetting your student password at:
https://columbiabasin.edu/resetpassword



F. Click the **CS150** VM to start your Virtual Machine. This will start what looks a computer running Windows, except it will be running in the VMware Horizon Client window!

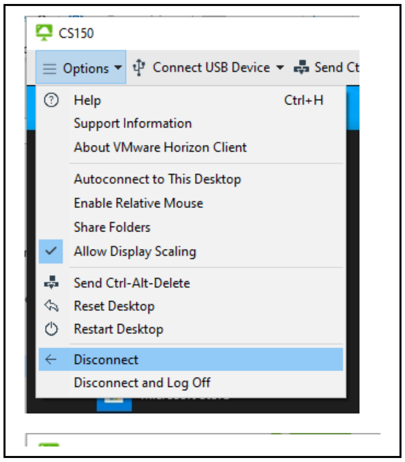
G. Once the Windows Virtual Machine is booted and running, you'll see a Windows login screen. Login using the following preset username and password:

Username: Administrator

Password: **T548cstt**

H. At this point you will be logged in, and ready to start using your VM. If you've never done this before, stop and take a minute to think about what has just happened. You've just started a computer, and it's running in your web browser. I hope you appropriately impressed at how cool this is!

I. Note – When you are done make sure that all your work is saved, and then end your session by selecting **Options > Disconnect** or simply close the browser window containing the VM. Do **NOT** shutdown the VM by selecting the Windows Shutdown. If you do this it will take a lot longer to access your VM the next time you want to use it. If your VM is powered off, the software that controls all of the VMs has to restart it, which may take several minutes. This process doesn't start until you try and access the VM, and you don't see a message that says you're waiting for the VM to power up, you just see error messages. If this happens don't panic, your VM should restart and be available in a few minutes. Just take a deep breath and count backward from 1 million …



Create a New User, and Configure the Account

In the next steps you'll create a new Windows user, add them to the Remote Users Group so they can login across the network, and then test the new account by logging in as that user. You can either follow the written directions below, or watch the video which shows a slightly different way to accomplish the same thing.

https://tonysako.com/home/cs150-introduction-to-computer-security/creating-a-new-windows-user-on-the-cbc-cloud-virtual-machine/ - Creating a New Windows User On Your CBC Cloud Virtual Machine

1. Log into your CS150 Workstation machine if you are not already logged into your virtual machine as **Administrator**. (The password is **T548cstt**)
2. Right click Start and then type **Computer Management**
3. Select Computer Management App
4. Double click Local Users and Groups
5. Right click the **Users** folder and select **New User**
6. Create a user with the name of sUser (or use a username that you can remember).
7. Enter the password. I suggest using **Password.01**, but you can choose any password that meets the Windows security requirements. If you think you may have trouble remembering the username and password, I suggest you write down them down someplace.
8. Uncheck the User must change password at next login
9. Check Password never expires
10. Click **Create**
11. Click **Close**

Next, you will add the user to the **Administrators** group. The user must be in this group to be able to do things like installing software.

1. If necessary, open the **Computer Management** tool again.
2. Double click the **Users** folder
3. Right click the user you just created
4. Click Properties
5. Select the **Member of** tab
6. Click **Add**

7. Type Administrators
8. Click **Check Names** to the right to make sure the group is found. If it click OK. If not, check your typing and try again. Capture a screenshot showing that the user belongs to the Adminstrators group.
9. Click OK
10. Click OK

Now run an acceptance test to check to see if you're able to login to the account you just created.

1. Right click the Start menu.
2. Select Sign Out (under the User button). This will cause the VM windows to close. Note – Do NOT power off the VM. It won't hurt anything, but it will take a lot longer to start the next time you connect to the VM.
3. Reconnect to your CS150 Windows Workstation machine and log in as the user you just created. If you receive an error message regarding the requirement for the user to be in the Remote Desktop Users group go through the procedure detailed below for a fix.
4. Open Task Manager. There are several ways to do this, but if you don't know how right click on the Windows **Taskbar** and choose **Task Manager**.
5. This will display Task Manager. You want to see the **Users** tab. If it's displayed go ahead and click it. If it's not displayed, click the **More Details** button in the lower left of Task Manager.
6. This will display the name of all currently logged in users, although there should only be one. (Yes, just like the Highlander.) Capture a screenshot showing that you were able to login as the user you created.

In the past it's only been possible for a user to login across the network if they're part of the Remote Desktop Users group. The alternative is to be physically sitting at the computer. So, logging in across the network is pretty much the only way to login to your VM. We've tried to correct this, but if you received an error message regarding this when you tried to login it may mean you need to add your new user to this group. (If you were able to login with your new user you can skip this.) To add a user to the **Remote Desktop Users** group follow these steps:

1. Login to the VM with **Administrator** account. The password, unless you changed it, is **T548cstt**
2. If necessary, open the **Computer Management** tool again.
3. Double click the **Users** folder
4. Right click the user you just created
5. Click Properties
6. Select the **Member of** tab
7. Click **Add**
8. Type Remote Desktop Users
9. Click **Check Names** to the right to make sure the group is found. If it click **OK**. If not, check your typing and try again.
10. Click **OK**
11. Click **OK**

Note – When you are done, sign out of your account or simply close the browser window containing the VM. Do NOT shutdown the VM by selecting the Windows Shutdown. As noted above shutting down the VM won't hurt anything, but it will take a lot, lot longer to start the next time you connect to the VM.

You now have two accounts on your cloud VM, the Administrator account and the account you just created. You can use either of these accounts if you choose to use the VM for any of the remaining class assignments. As you'll learn a little later in class, in a real world situation you'd want to use the non-admin account for all of your daily work, and only use the Administrator account when you were doing things that required administrative privileges. But in this class, and probably on your home system, it doesn't really matter since you're the only person using the computer.

What to submit for This Hands-On Project:

- Make screenshots after the specified steps. . If you need help creating a screen shot there are many videos on YouTube that will provide further instruction and details. Do NOT take a picture of your screen with your camera/phone. If you do you will have to redo the assignment and get the screenshots in the correct format.

- Add the screenshots to a document, along with a header that contains your name and the date. The document you submit can be a word doc, a PDF, or in .odt format.

- Go to the Assignment in Canvas and upload your document as your submission.

Required Case Project Homework (Writing Assignment)

For the writing assignment for this section, you need to do the following **Case Project** which is located at the end of the chapter. Note that your book makes a distinction between *"Projects"* and *"Case Projects".* For this assignment you want to be working on the *Case Projects*.

Case Project 1-2 Security Podcasts or Video Series

I'm including the text from the book for this Case Project, just in case you have any delay in ordering your book. Note that I'm only doing this for the Case Project for this chapter, so make sure you've ordered your book.

Case Project 1-2. Security Podcasts or Video Series

Many security vendors and security researchers now post weekly audio podcasts or video series on YouTube on security topics. Locate two different podcasts and two different video series about computer security. Listen and view one episode of each. Then write a summary of what was discussed and a critique of the podcasts and videos. Were they beneficial to you? Were they accurate? Would you recommend them to someone else? Write a one-page paper on your research.

What to submit for This Case Project:

If you haven't already read the Guidelines for Writing Assignments, now would be a good time. The document explains what you'll need to do for the paper and provides details on how your paper/report will be graded. Also, remember if you need help creating your references the Citation Machine web site will be your new best friend.

When your project is complete, turn it in by opening the Assignment in Canvas, and clicking the **Submit Assignment** button.

Also, remember to check your TurnItIn score. If the score is higher than 30% your submission will NOT be graded. You will need to either edit your material and put more of it in your own words or add more original material. Once you have made your changes, you can resubmit your work. There is no way to check your TurnItIn score before submitting your work. But don't worry about making multiple submissions, everyone does it and it has no impact on your grade.

https://tonysako.com/home/cs150-introduction-to-computer-security/cs150-checking-your-turnitin-score/ - How to check your TurnItIn score

Ways to Check Your Comprehension

In my mind, one of the main things that differentiates learning in the real world versus the model used in education is how feedback is applied and used. Say for example you want to learn how to format a thumb drive to use NTFS so you can copy files larger than 2GB. In the real world you'll probably watch some online videos to learn how to do the formatting, and then get immediate feedback on your comprehension when you try and do the formatting. The key point is that the feedback is immediate, if you understand something then you can move on, but if the feedback indicates that you didn't learn the item, then you can spend a little more time learning. In education the feedback is typically provided by tests or quizzes. In this case the feedback isn't immediate, it's usually delayed by several days, if not several weeks, at which point it's almost worthless. For example, say you're taking a class with a mid-term and a final exam. If you take the mid-term exam and do poorly it's feedback that tells you that you didn't comprehend the material covered by the exam. But by the time you get the exam results it will be too late to do much about it. You could have used that feedback weeks earlier, and spent more time studying, but getting feedback with this long of a delay won't help you at all.

This is really a long, roundabout way for me to suggest that you use the review questions at the end of each chapter to check your comprehension. The test over this chapter won't be for a few weeks, but you can do the review questions any time. I don't have the questions loaded in Canvas, so you'll have to just read them and figure out your answers on your own. Or you could try and connect with some other students in the class and drill each other using these questions.

As I just mentioned, the test over this section isn't due for a few weeks. If you look in the Canvas Modules you'll see a Module for Test 1. This Module contains a link to the actual test, which will actually cover a few chapters in the book. The Test 1 Module also contains a link to a Practice Test which has been provided to help prepare you for the real test. You can take the Practice Test as few or as many times as you want. You're not required to take this test, but I strongly suggest that you use it as part of your test preparation.