Practical Cyber Security for Cyber Security Practitioners

Prof. Sandeep Kumar Shukla

Department of Computer Science and Engineering

Indian Institute of Technology, Kanpur

Lecture 31 : Key Takeaways from the Course

So, tomorrow's exam is 9 to 11, and I have given the chart of sitting in RM 101, KD 101 and KD 102. So anyway, today maybe we will have a shorter class because I just wanted to summarize what we have been doing through the semester.Just to give you an idea about what it is that is expected of you to have learned right. So, first thing is that you know many times we think about cyber security, we think about malware and we also think about intrusion detection or we think about you know specific vulnerabilities right. So, we think about buffer overflow or privilege escalation, we think about web application vulnerabilities such as cross site scripting or we think of CSRF or SQL injection, command injection this kind of stuff right or we think about DDoS, but what I wanted people to understand students to understand is that attackers especially attackers who work in groups supported by often by criminal gangs or nation states etcetera they actually plan much bigger than what you would think that exploiting a you know command injection or exploiting and remote code execution vulnerability or buffer overflow vulnerability. They actually use that as a first step to get their first payload into execution.

Goals of this class (1)

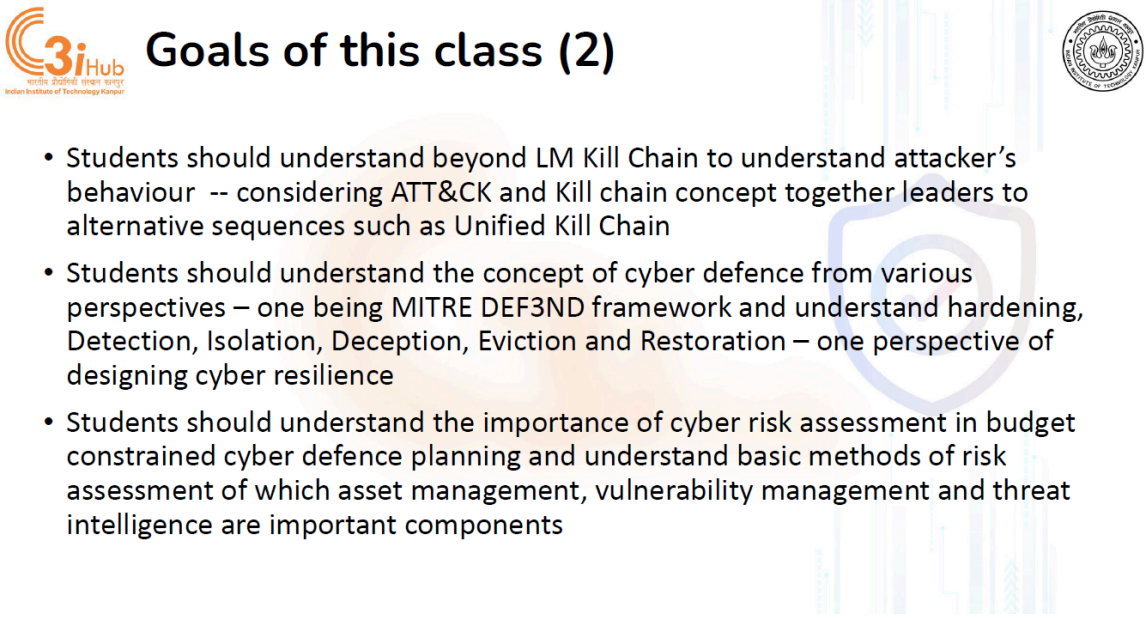
- Students should know about attack patterns and kill chains to comprehend how attackers plan, execute and affect our organizational IT or OT systems
- Students should know attack tactics and techniques through standard terminology and taxonomy such as MITRE ATT&CK
- Students should know planning cyber defence against various techniques employed by attackers
- Students should be able to surmise TTPs used by attackers from incident reports or from raw forensic data collected post attack
- Students should be able to understand that cyber defence is more than protective tools such as firewalls, but also involve people and processes

And then they actually do various things- lateral movements, they do privilege escalation, they do data collection, they do credential harvesting, they do you know final impact for example, like encryption of your data or your files or wiping your files or exfiltrating your files and so on. So, therefore, we have to think in terms of cyber attack cyber attacks more like a you know it is a sequence of activities that starts with the reconnaissance activity as well maybe you know based on reconnaissance some weaponization activities right. So, you weaponize the weaknesses in the target system and you create exploits or you create social engineering collaterals and then you actually get into the system. So, when you do that you remember that either you exploit weakness in the target in the software or maybe also hardware not so common, but also in hardware firmware etcetera or you exploit weakness in the people right.

So, remember this is we have been saying many times that cyber security is about people process and technology and sometimes it may be weaknesses in the process right. So the example we talked about that Sarah Palin's Yahoo email getting hacked, Yahoo account getting hacked or you know somebody's Mac Dogan's Apple account, Amazon account getting hacked and so on. These are basically business processes that were weak, that were not thinking in terms of various possible ways of exploitation or threats. So, you can have these weaknesses in your software hardware firmware etcetera or you can have your weaknesses in your infrastructure. For example, you can have a DNS your DNS local DNS resolver might have been attacked and a SBI's URL may be translated to an IP address which is under control of an attacker right and then somebody goes into SBI website and then the local resolver says that ok I have the 'SBI.' whatever you know com URL translation already in my cache I am going to give it to him.

when he goes there he is actually seeing a website that looks like SBI. So, he types in his

username password and gets his credential compromised and from there things go on. Now in case of Indian banks it is slightly better because we have also two factor issue, but then two factor has been compromised in the recent times like recently duo has been compromised. Okta has been compromised. So, this two factor compromise also is not uncommon, but in any case nobody is claiming that any of the protection mechanisms that you use is going to be 100 percent.



So, it is always about reducing the probability of getting attacked. So, you do two factor you do not give up on two factor just because there has been some attacks on two factor because two factor still reduces the probability of getting you know compromised through your user account right. So, that is so in any case so the idea is that you have to understand this reconnaissance to weaponization to initial access to execution to privilege escalation or persistence you know lateral movement collection exfiltration and all this stuff right. Also you have to understand that how these tactics are implemented. So, there are certain now of course, there are you know almost 200 techniques and so on you cannot be doing all of them, you cannot be knowing all of them, but at least you have some idea that what are these techniques that can be used for implementing a particular tactic.

And then you have to also understand the kill chains right. So, we talked about the Lockett Martin kill chain which is earliest kill chain that was there, but that has only 7 different phases which is rather simplified and then we talked about unified kill chain which is a little more elaborate and which basically is post ATT and CK. So, it talks about these various phases that are related to ATT, CK it also kind of gives you a little more nuanced way of doing these attacks you know repeating certain tactics through the kill chain and so on. So, now we also saw that When we look at an attack forensic, we

look at the forensic information about an attack either by reading a threat report. or by looking at the raw data that is the logs and other things that we see we can kind of guess what TTPs are being used or we can kind of surmise what TTPs are being used and then we can also give defensive recommendation that next time.

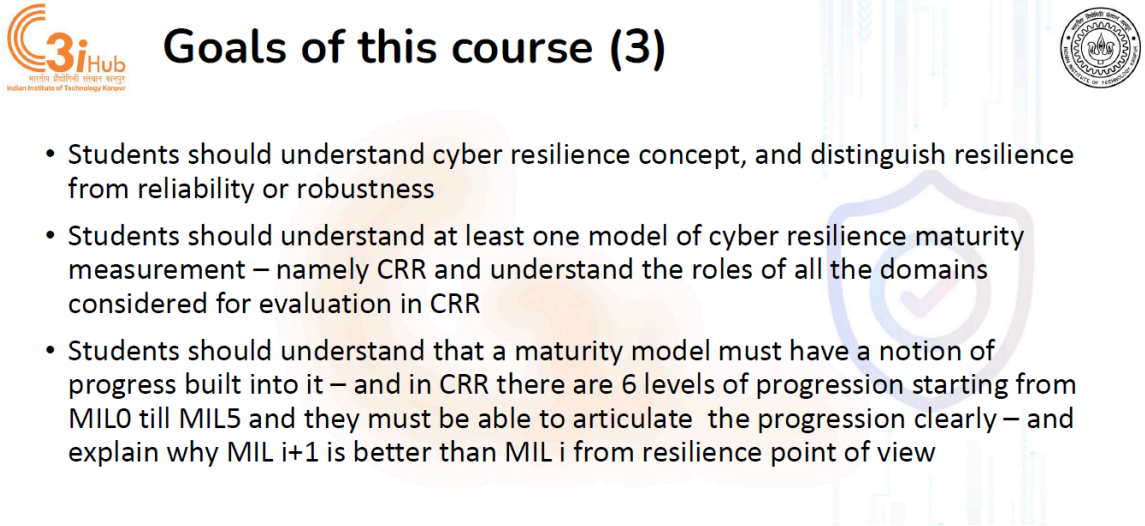
So, that particular technique cannot be successful. if we do this right. So, this kind of defensive recommendation from the TTPs that has been applied to your system by an attacker is one way of thinking in terms of defense right. So, that is how you improve the defense of your system. And also you know defense is one thing that one has to understand is that defense is not always about you know adding a new rule in the firewall or adding you know endpoint security tools or adding network intrusion detection or adding antivirus or just adding stronger authentication access control this kind of stuff these are necessary, but not sufficient.

Sometimes, you have to also think in terms of people and people and processes. For example, in one of the committees I was listening to this particular financial organization who had an attack in the following way. So, I might have said this to a class in class before that one employee who left 2 years ago his account was still there and in his account in the recycle bin he had left a malware and then that malware was activated through another channel and that is how the attack happened right. So, this is a process problem right. So, when an employee is terminated or an employee leaves you need to immediately recycle you know reclaim the account and you know delete all the account files and everything and cleans this disk space and all that stuff.

If you leave it around then many things can happen. So, in the Maruchi Shire sewage plant the attack that happened in 1919 Australia. So, there you know the there was a disgruntled contractor who actually was let go in the company, but his account was not terminated and this is 1990. So, there was no two factor authentication and you probably use dial up modem to contact the system and so he dialed up and then he did the setting such that there was a huge spillage of sewage right. So that is not a well that in one sense it is a failure of the process and because in the in the this is an HR process problem right.

So, security can actually happen from the HR process weaknesses right. So, therefore, you have to understand that it is not only about you know cleaning up malware or cleaning up or blocking you know connection requests and so on it is also have to have the right set of processes and so on. So, beyond Lockheed Martin kill chain we talked about unified kill chain and you have to also understand that you know how these things interact like ATT and CK and the kill chain concept because ATT CK does not imply any sequence ATT CK is about the various tactics. There are 14 tactics within each tactics there are many techniques and procedures, but they do not imply a particular sequencing

of the tactics kill chains do imply sequencing ok. and then you have to understand the different framework right.



So, the question is that if I am a cyber security professional and I have been called in as a consultant to an organization how am I going to I mean I have to start somewhere right. So, what do I do right. So, these all these frameworks and standards are actually way of actually wrapping your head around the problem, problem of organizing cyber security of a of an organization. So, you can go ahead in many different ways right. So, you can use NIST CSF framework to frame your activities or you can go by MITRE different framework or you can go by other things like standards like ISO 27001 etcetera.

But what the NIST different framework tells you is that you have to be able to do hardening right. So, understanding hardening how do you harden applications, how do you harden the network, how do you harden the credentials and so on. These are very important part of understanding how the cyber security is you know has to be thought about right say what should I do if I am gone into a consultant. gone as a consultant what should I do like you know I should ask them about first thing I will ask them about is how much hardening they have done right and I will tell them that ok. So, have you done this and have you done that and have you done this other thing and then they will say we have done this, but we have not done that then I can tell them that you know this is something you have to do.

I also have to tell them how to go about detection right. So, many organizations do not do much about detection right. So, they do not have a SIEM or SOC or they do not have an endpoint security solution in place. So, detection is actually often only done post facto right. So, when logs are looked at when something happened and then you look at the log and you detect that oh at this point in time there was some error.

you know some malicious payload was sent to so and so and so IP address and so on so forth, but that is not good enough right. So, you have to be able to detect before it hits the target right. So, detection for detection will talk about like ok. So, do you do network intuition detection, do you do endpoint detection, are you actually trying to detect you know what is happening in your DNS traffic and what is happening in your routing traffic and so on. So, detection is important.

Then isolation like how do you isolate critical applications right. So, applications like if you are running the non-critical and critical applications on the same machine. If the non-critical application gets attacked then critical application will suffer right. So, you have to do isolation. So, what are the different isolation techniques? What is the use of deception techniques right? So, honey pots and honey credentials and so on.

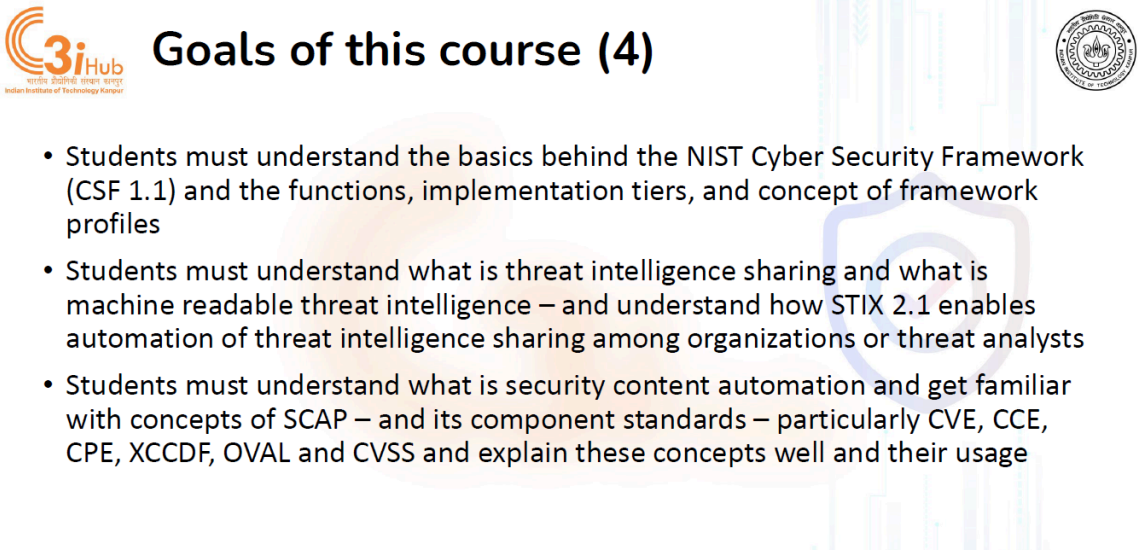
And, then eviction how do you evict and you know a compromised when a system is found to be compromised or a particular credential has been compromised. And, restoration like you know if you are wiped or if you are encrypted you know how to use a backup for restoration so on. So, this is one way of thinking you know how to go about giving a minimal cyber security for an organization it is not necessarily 100 percent also remember that this is not necessarily based on things like risk assessment right. So, we said ok. So, I can I do not have infinite budget.

So, I have to be able to use my budget to do cyber security to maximize the utility maximize the effectiveness. So, I have to be able to do risk assessment and then based on the risk I may have to do higher security level at some particular asset or some network segment and lower security in certain segments and so on. So, and then make sure that the lower security segment is cannot access the higher security segment without going through proper access control and so on. So that part is not there in the defend framework. Defend framework basically kind of gives you a list of things that you should do.

So if I am a cybersecurity consultant going to an organization I will certainly use defend to tell them a laundry list of things that they have they should do and if they have not done then I will tell them to do it, but that is not enough because now they cannot do this uniformly across their entire infrastructure because their entire infrastructure may be too large. So, you need to do risk assessment to figure out which part of the infrastructure requires better security and which part does not. So, so risk assessment is basically about budget constraint cyber defense planning whereas MITRE DEFEND is a unconstrained cyber defense planning and then risk assessment has important part like asset management, vulnerability management and threat intelligence which are also not exactly

you know focused in the different framework. So, this is these components have to be understood. The next thing is about resilience right.

So, resilience is different from robustness or reliability right. So, you know in a reliability is about how what is the mean time to failure gives you a sense of reliability right. So, if your system fails you know does not fail 99.999 percent time then you say it is you know 4 reliability up to 4 nines right. So, robustness is about you know withstanding attacks without failing right.



So, for example, if you have a robust to DDoS attacks then you can handle probably you know giga bps or even higher tens of or hundreds of giga bps traffic and you will not shut down or will not collapse. Resilience on the other hand is different from robustness and reliability and resilience is about you know accepting that when the attack is too much or attack is too virulent, you can actually degrade your performance, you can degrade your service level agreement, but then you will recover and you will recover fast right. So, this elasticity is about resilience. So, understanding that resilience is important and why In cyber security people are talking about resilience is because nobody can guarantee 100 percent security, nobody can guarantee a full robustness right, 100 percent robustness. But what they can do is that plan for this kind of extreme events where they have to degrade their performance or degrade their service level agreement and then come back up as soon as possible as soon as the attack kind of ceases to be applied.

So, then in cyber resilience you have various maturity levels right. So, we discussed about various maturity levels of some MIL 0 to MIL 5 and we said that you know if you are MIL 3 this is what it means and if you are MIL 5 this is what it means and what we have to understand is that why is it that MIL 5 is better than MIL 4. is it just you know in what way is it better why do I have to target mil 5 rather than mil 4 or mil 3 right. So, this

kind of understanding is required and also the 10 domains that we talked about in the CRR model like asset management to vulnerability management to you know third party or you know what we call the external dependency management and so on. All these different domains we have to understand what they are, what functions we expect from them and then what kind of maturity we expect from them.

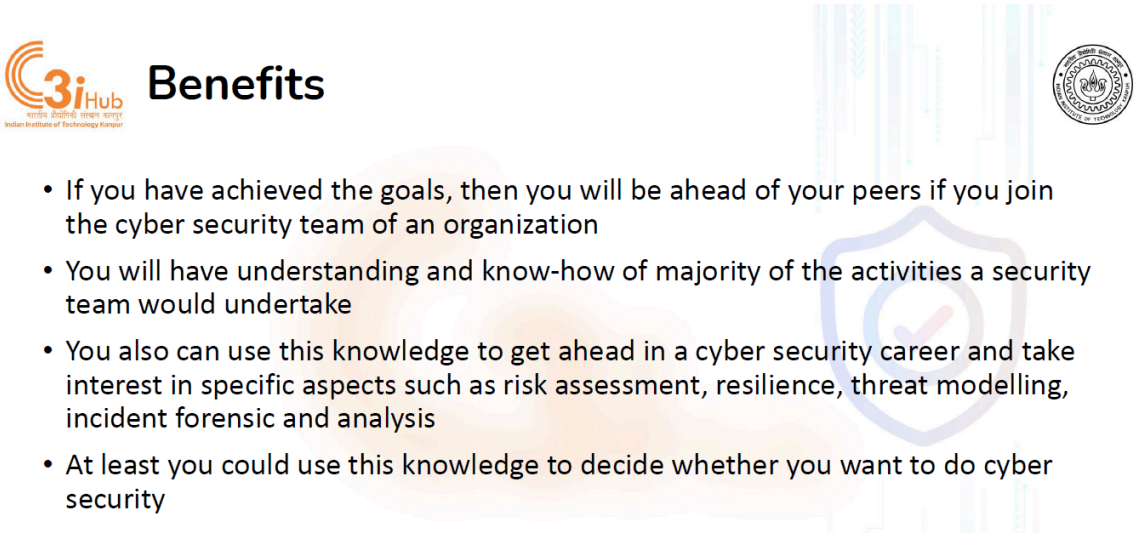
So that is the resilience thing. We also discussed a little bit about NIST CSF 1.1. and we talked about 5 functions. This 2 point CSF 2.0 has 6 functions, but we talk about 5 functions that is identify, protect, detect, respond and recover and then we talked about this implementation tiers right.

you know risk risk aware and you know ad hoc and so on so forth. So, what are these implementation tiers why would I want to be in a certain implementation tier versus another implementation tier and then there are framework profiles right what are these framework profiles. So, NIST CSF is another way of you know if I go to consult an organization I might say ok. So, what is your identify function? Do you identify risks right? Do you identify your assets? Do you identify your threats right and how do you do that what I what is it that you are doing show me you know how you did their last risk assessment right. So, this is what I will do right then I will I will say ok.

So, here is so, your identify function has this problems then I will say your let me see what you do for protection right. So, do you have strong access control, do you have strong authentication, do you have network segmentation, do you have firewalls, show me your firewall rules and so on. So, I will check what are they doing for protection, then I will say ok. So, protection has this problems, but you should fix it. Now, let us see what you what do you how do you detect and what is your detection rate and you know how you are what are your detection rules do you use AI ML for detection and all kinds of stuff and then I will go back you know from detection I will go to respond.

I want to understand their incident response mechanism do you have a SOC in the SOC what is the what kind of use cases do you have or how do you escalate incidents to higher level and so on so forth. So, I will I will ask them all these questions then I will go into their recovery how they recover do they do proper backup and so on. So, so these frameworks give you a good idea on how to go about you know understanding an organizational security posture or to advise them about their security posture and for implementer how to implement what to implement rather right what to implement and so on. They also can also talk to tool vendors when they talk to tool vendors tool vendors will try to sell you whatever they want to sell right. So, they you may not need it you may already have that function already in some other tool right.

So, this kind of clarity is required and this clarity will come from understanding this frameworks and so on. The next one that we also discussed is the threat intelligence sharing and then machine readable threat intelligence or MRTI and in that STIX 2.1 as the one of the standard data model for you know for capturing threat intelligence and sharing threat intelligence. So this is something that is we have to understand because this is now very common even the regulators like SARTIN and NCIPC etcetera they share sticks threat intelligence with the regulated organizations and those are consumed by their various tools. And then finally, we discussed about this CAP the security content automation protocol and its component standards like CVE, CCE, XCCDF, Oval and CVSS and then how what these things are what is their use you know when you encountered them in real life in various reports and so on you understand what they are and then you can get some ideas.



So, with this topics. I am hoping that you are in a good shape to be ahead of your peers if you join cybersecurity team of an organization. You will have understanding and know-how of majority of the activities a cybersecurity team would undertake. and you can use this knowledge to get ahead in a cybersecurity career and take interest in specific aspects eventually you will become specialized in something and normally nobody will remain specialized all their life 30 year 40 year career on one thing right. So, they might start with risk assessment may move on to resilience they might move to threat intelligence and things like that. So, it does not have to be like a lifelong commitment to any of these, but you excel in one then you go to the next one and then you eventually get promoted and eventually you will become CISO right.

So your goal would be to eventually if you choose a industry career in cybersecurity you want to be CISO right. Or at least you could use this knowledge to decide whether even

you want to do this, right. You may not want to do this, right. So, this is hopefully this will give you an idea about whether this is something you will like or not. So, that is it and from what I just told you, you know, you should get an idea about what will be in your final exam.

And any questions? What is that? Oh, what I missed in the class? Well, I compared to the last time I offered this class, this time I did not miss anything. In fact, I did more I could do SCAP you know I could not do last time for some reason I forgot why. But I think that I could have probably done a slightly more if I could cover like a standard at least 27001 you know some or 62446 standard. that would have been nice because I we have not we talked about a lot of standards, but we have not looked at a standard. So, you know how to look at a standard and understand how to implement it or what an auditor like if I claim to be a 27001 compliant then what an auditor will come and check this kind of thing may be also useful knowledge in this, but we have not had the chance to cover that.

There are several reasons one is of course I got sick quite a bit in this semester, but bigger issue is that nobody comes to class you do not feel enthused to do something you know and this is something that actually the class before me is a math class actually ordinary differential equations right it is a required class for first year students I believe and I saw 7, 8 students and I assume that there should be 200 students in such a class right. So, I think that there is a problem post covid students do not know how to attend classes because I have never had so few students in class throughout the semester right. So, this class has had the on an average I think we had about 20 students out of 83 students right and that is obviously a problem because First of all you know if the students do not come to class you do not you are always worried that the your message is not going through right. So, in this class at least we had a recording of the classes. So, some students might be actually watching them before exam or for something I do not know, but most classes will not even have that right.

So, I do not know how the situation is in other classes, but from the math class I saw it was it was quite scary because I stood there several days and the teacher was teaching very well. So, I do not understand if it is not like the teacher was not teaching well. So, or maybe the students all know how to solve such differential equations I do not know what was going on, but it was situation is pretty bad and as you know that we have big debate around the country about the number of unplaced people in from IITs. So, I do not know if you know that even the top 5 IITs have 30 to 40 percent unplaced this year right. And what that also means is that there is also an issue about AI co-pilot and all that stuff easing the job of programming and so on.

So, one major problem in IIT system now is that 90 percent of the students go into IT

irrespective of what subject they are studying right. Now that means that a country cannot proceed just you know a country cannot progress just by IT people right. there has to be core engineering right and core engineers are not there because everybody go is going into IT. I think that thing will reverse soon and then these students who actually did not learn their core engineering chasing data structure course and machine learning courses will be actually under qualified for their core engineering. I think there is a huge problem that is going to come up in the next few years.

But in any case I think the I have a hypothesis and I do not know the truth of that I do not have enough data to prove it, but I have a hypothesis that the students we are seeing now in the in the undergraduate or even graduate they spend majority of their high school etcetera online education because of covid. So, they do not know what it means to sit in a classroom and listen and study try to understand and ask questions and interact and so on. So, this is going to be maybe a problem for the next several years, maybe it will affect generation of students. Anyway, so I think I am done with this class. So, good luck tomorrow for your exam and then have a good summer and we will see you maybe in the another class.