Name: Matthew Young

**Take Home FINAL Exam**

1. (5 pts) For this question, answer just ONE of the following: 1.1, 1.2, or 1.3
   1. Suggest one new lab for the next offering of this class. Specify how this lab benefits students’ understanding or mastery of course concepts? *150-250 words, or*
   2. Suggest one new hands-on exam question for the next offering of this class. How does this activity reflect/measure students’ understanding or mastery of concepts? *150-250 words, or*
   3. Suggest one new take-home exam question for the next offering of this class. How does this activity reflect/measure students’ understanding or mastery of concepts? *150-250 words*

**Answer:**

My new lab idea is an ethernet port security lab that has a dual focus: enterprise network protection and home-based network protection. The lab would require the participant to be able to exclude an attackers device from accessing the network over a direct ethernet connection using a common tool like whitelisting[[1]](#footnote-1), and a potentially more complex tool that is more applicable to enterprise grade networking technology, the overall key being that the connection is wired and is often neglected in terms of security when building a network both at home and in a business (NOTE: I don’t actually have metrics on how overlooked ethernet port security is, but I have talked with a couple of professors and friends about it in the past). This helps students with grasping physical ways around security in more intricate detail than doing something broader like a passive recon. Additionally, the lab could be further amended by requiring the participant to find a way around the security used on the ethernet port e.g. MAC address spoofing.

1. (5 pts) There have been several instances of schools & school districts getting hit by ransomware in 2020, the most recent being reported in late November 2020[[2]](#footnote-2). Provide a list of cybersecurity recommendations for school principals & school district leaders to enhance their ability to deal with ransomware (both prevent it & recover faster from it). *200-300 words*

**Answer:**

Let me preface this answer by saying that my mom has worked for a school district for about a decade now, and I tend have conversations about security all the time with both of my parents regarding what goes on in the world. That said, some of the big security flaws in a school district come from lack of awareness, but most of them come from lack of understanding. In short, they need to understand the weight of a ransomware attack and how it can affect an organization, not just be aware of it and then push it to the back of their minds later. The following are my recommendations for principals and leaders in schools and school districts:

* Keep up with security news
* Backup everything **essential** to running the organization frequently
* Evaluate your risk as a cost/effect scenario (time systems are down, cost of replacing hardware, etc.)
* Raise awareness and understanding among staff regarding cybersecurity
* Run scenarios on possible attacks and test your prevention and preparation measures
* Just because something is easy doesn’t mean it is secure
* During an attack, don’t let pride dictate decisions regarding security (Would you rather look bad, or make things worse **AND** look bad?)

1. (5 pts) The CFO of your organization just heard that a competitor recently suffered a ransomware work stoppage after an executive’s laptop was compromised inside their home Wi-Fi network (due to another device in the executive’s home network being compromised). The CFO has asked for the best security person (you) to come up with a short list (3-5) of recommendations that the IT department could deploy remotely to all of its 12 executives currently working from home. *200-300 words*

**Answer:**

Fair warning, I’m not sure that all of these can be done remotely.

With the remote nature of the working environment of the year in mind, I have quite a few recommendations. Firstly, for the exact scenario presented, keep business and personal systems on separate networks, be those VLANs, LANs, WiFi SSIDs, or switches (if hardwired), keep important systems separate from other systems (hard to enforce remotely). Next, don’t let just anyone on to your network, use security like WPA to keep your network secure and don’t give out the passcode to just anyone who asks (can be done remotely). Third, conduct regular security scans on your systems - while not the best, even windows defender has this capability and will alert you if it detects a security threat (can be done remotely: require a system scan before remoting in to work or connecting to business networks). Lastly, make restrictions to usability on business computers given to any employee – yes, I do mean any: from custodians all the way up to executives (i.e. restrict users to only using the remote work software and files on their business computer, which means NO BROWSING THE WEB OR USING IT FOR PERSONAL USE).

1. (5 pts) Write a short summary of the key points of this Trustwave report about the GoldenSpy[[3]](#footnote-3) malware. GoldenSpy appears “embedded in tax payment software that a Chinese bank requires corporations to install to conduct business operations in China.” *200-400 words*

**Answer:**

Trustwave SpiderLabs conducted a threat hunt in April 2020. The client they worked with on the threat hunt was found to have a type of software on their systems that was later classified as malware. This malware, later named “GoldenSpy”3, was downloaded through an executable file tacked onto a legitimate local Chinese tax payment software. The malware itself does not download until two hours after the initial tax software download, makes duplicates of itself that coordinate to always keep it running, and staggers its information broadcasting variably in order to avoid detection and deletion by system security software3. GoldenSpy allows a remote actor to interface with the system it is installed on with system level privileges which makes it highly dangerous due to the ability to run any program available on the system3. As far as has been noted, the GoldenSpy campaign began in April 2020, but there are several software variations that exist from all the way back in December of 20163. The scope of the campaign has not yet been determined, but as of the publishing of Trustwave’s report they theorize that it could be as small as a single business or as large as every corporation in China that is affected.

1. (5 pts) Based on the previous question (about GoldenSpy), outline 2-3 methods to help reduce the security risks for organizations operating in the country (and thus must install that software). *200-300 words*

**Answer:**

Due to the requirement by local banks to use the software, the only foreseeable way to help secure the systems that need to use the legitimate software are to try to outwit, isolate, or outright remove the hazardous malware. In terms of outwitting it, it may be possible to modify the executable file or another file used by it to change the overall function and have it either transmit fake data, transmit data to a company-owned system, or completely disable the transmission of data altogether. Another option would be to isolate the software or the system running the software by using a dummy machine not connected to the rest of the network or, alternatively, by installing the software on a virtual machine so it cannot grab data from the host machine but is still operable for the intended use of the legitimate software. The only other option would be to forcibly remove, engineer out, or quarantine the original executable file from the legitimate tax software download, sadly this option is not as likely to be successful due to the legitimate software potentially having a hidden piece of code or a clear piece of code that is entirely dependent on the existence of the malicious program which would force the download and installation of the malicious software.

1. (5 pts) Write a short summary of this Europol[[4]](#footnote-4) report (w/ TrendMicro & UNICRI) about how cybercriminals misuse and abuse AI and ML. *200-400 words*

**Answer:**

Substitute for Question 8 || SIDE NOTE: you really want us to read 80 pages of a Europol Report… no way man, not happening.

1. (10 pts) Create a detailed, plausible, professional development plan, for yourself, with a 3-year timeline (post-graduation) in 3-6 month increments or sprints. In your plan, include a brief analysis[[5]](#footnote-5) of your own strengths and weaknesses, and how those impact the areas you chose to include for further professional development. Your plan should address continued development of your technical skills (25-40%) and your non-technical skills (60-75%) and contain a master plan of activities and/or events/workshops/education that you could follow. Make reasonable assumptions from a budget/monetary perspective. Must be at least 1 page.

**Answer:**

I can’t think of a way to start this so this is how I’m starting it. First, a recap, this is my final semester at mnsu before graduation with a bachelor’s in Computer Information Technology with a minor in technical communication. Sadly, I’m at a slight disadvantage compared to some of my peers in that I was a lazy POS as a freshman and killed by overall GPA pretty early, so it has been a little more difficult for me to find opportunities to get some real-life experience. That said, I had quite a few internship interviews going in to 2020 that all canceled on account of COVID-19, so I had to get a course waver and still don’t have experience in my field.

What I’m shooting for right now is to get an entry level position in IT either as a junior/level 1 software/network/security/database guy (Yes I have applied for all of these types of positions, and a few have already gotten back to me). Once I get that entry level job I plan on expanding my education a little bit depending on how I like the work I do. I plan on getting my CCNA at some point in the first year during that first entry level job. I haven’t looked at a whole lot of other certifications yet, but I have a goal of doing one certification course per year to help keep me up with the changing state of technology and what new systems have been implemented. Additionally, these certifications will help me to become more valuable to employers and should lead to further career advancement.

After the second year of working the entry level job described earlier I plan on either being promoted or finding higher level work elsewhere (I don’t know how realistic this is due to my lack of experience). By the time I have that second year of experience under my belt I should also have two certifications that should allow me easier entry into a more specialized job of my choice (as evident by my choice of starting certification, I plan on learning more about networking, though that may change in the future). With any luck, at this point I will be making enough money to be financially stable and should have approximately half or more of my student loans paid off (current value of student loans: $22,000 || Not bad I know).

As of my third year after college, I should be in a well-paid position ($60,000+) with three additional certifications and approximately 80% of my student loans paid off. As of right now, I plan to stay in Minnesota for these first few years, but nobody knows what the future holds, and I could just as easily get a lucrative job offer in another state which I would be inclined to take.

Strengths/weaknesses:

* I’m told I’m good at database work, but I don’t like that kind of work
* If the class is anything to go by, I am good at networking and I love doing it (Future job field?)
* I travel light, so I’m willing to go where opportunity takes me
* I know how to budget myself (but there is always room to improve)
* I am prone to making expensive decisions sooner rather than later

Here’s a summary of my sprints:

**SPRINT 1 (3 Months)**

* Learn everything I need to know about my entry level job
* Move out of my parents’ place
* Use my free time for hobbies to try and keep stress to a minimum during the learning phase

**SPRINT 2 (6 Months)**

* WORK, WORK, WORK
* Start preliminary studying for CCNA
* Get a new car (Maybe? Depending on expenses)
* Use my free time for: 50% expand my knowledge and better myself ||| 50% hobbies

**SPRINT 3 (3 Months)**

* Get my CCNA
* Do a year end evaluation on my finances
* Look for job advancement opportunities
* Pay off some (20% +) of my student loans
* Pay taxes (even though they are theft)

**SPRINT 4 (6 Months)**

* Establish a good reputation within the company I work for
* Start pushing for advancement within my job
* Look into which certification I will get this year and begin studying
* Keep paying off student loans (should be 30% + paid off)
* Again 50/50 mix for my free time being studying and hobbies

**SPRINT 5 (6 Months)**

* Get this year’s certification
* Year end evaluation of my finances
* Pay taxes
* By now, should have 50% + of my student loans paid off
* Take a much-needed vacation (Oktoberfest anyone?)
* Get a promotion or find a higher-level job elsewhere

**SPRINT 6 (6 Months)**

* Settle into new workload
* Start looking at hobbies that I can earn money doing
* Cozy up to the new boss
* Never stop learning on the job
* Should have 70% + of my student loans paid off
* Don’t buy a house or other permanent residence until I’m certain I like where I am
* Start Investing

**SPRINT 7 (6 Months)**

* Become an expert at my job
* Get this year’s certification
* Take some more time off (I always wanted to go to Hawaii)
* HARD DECISION: do I want to stay in the state I’m in or move?
* Yearend evaluation of finances
* Pay taxes
* Invest more
* Should have loans 85% + paid off
* Start teaching my craft on the side
* Start investing in retirement (not a lot at first, but will be more later)

**CONGRATULATIONS YOU’RE STILL ALIVE!!!**

**QUESTIONS BELOW ARE FOR GRADUATE STUDENTS ONLY** although undergrads can substitute 1-2 questions from above with 1-2 questions from below (for 5 pts a piece).

1. (5 pts) Based on unusual behavior, your organization suspects that one of the Windows servers in the   
   New Orleans location had been infected by malware. You confirmed the infection, removed it, and restored from backups. Two weeks later, you realize that a different computer at that same location, a fully patched Mac desktop in service just under a week, is now showing signs of being under the control of the same attacker. As you are certain that you eradicated the initial infection, come up with THREE plausible scenarios that would allow the same attacker to have exerted control over this new machine.   
   *200-300 words, external sources are optional for this question.*

**Answer:**

While I’m not very familiar with the resurgence of malware on a corporate system, there are a few ways I can think of that would allow an attacker access after already being removed from affected systems. One of the methods that could result in this kind of scenario would be having the malware lay dormant for an extended period of time in order to keep a backup restoration from successfully getting rid of the infection by having the infection be on the most recent or the last several backups, thus effectively keeping the malware in play by respawning it on the system. Another method would be to have a seemingly legitimate background program install the actual malware during the systems inactive hours, thus successfully reinstalling the malware using a program that is not as suspicious to security teams and may fly under their radar. The final method that would allow for this scenario would be a combination of malware that lies in wait and replicates itself onto multiple different types of systems (i.e. Windows, Mac, Linux, etc.) so that the malware which seemingly only affects one type of system would be eradicated on those systems without the security team realizing that it is on other systems lying dormant and waiting for the opportunity to duplicate itself back onto the originally infected and new systems.

1. (5 pts) You are employed at a multinational company which depends heavily on GPS for transport and logistics. Create a summary of the risks associated with this reliance on GPS, based, in part, on this   
   7-min CBS Sunday Morning video[[6]](#footnote-6) and accompanying text[[7]](#footnote-7). *200-300 words*

**Answer:**

Answer text

1. How do I authenticate wired connections over my router’s ethernet port? <https://superuser.com/questions/1554828/how-do-i-authenticate-wired-connections-over-my-routers-ethernet-port> [↑](#footnote-ref-1)
2. Ransomware halts classes for 115,000 Baltimore pupils <https://www.bbc.co.uk/news/technology-55129564> [↑](#footnote-ref-2)
3. The Golden Tax Department and the Emergence of GoldenSpy Malware | Trustwave

   <https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/the-golden-tax-department-and-the-emergence-of-goldenspy-malware/> [↑](#footnote-ref-3)
4. Europol + TrendMicro + UNICRI - Exploiting AI - How Cybercriminals Misuse and Abuse AI and ML

   <https://documents.trendmicro.com/assets/white_papers/wp-malicious-uses-and-abuses-of-artificial-intelligence.pdf> [↑](#footnote-ref-4)
5. See HBR: Your Strategy Won’t Work If You Don’t Identify the New Capabilities You Need <https://hbr.org/2017/11/your-strategy-wont-work-if-you-dont-identify-the-new-capabilities-you-need> [↑](#footnote-ref-5)
6. CBS News | Preparing the next generation of GPS - YouTube <https://www.youtube.com/watch?v=uhVj77vJKYQ> [↑](#footnote-ref-6)
7. CBS News | GPS III: How the Global Positioning System's next generation of satellites are being developed <https://www.cbsnews.com/news/global-positioning-system-preparing-the-next-generation-of-gps/> [↑](#footnote-ref-7)