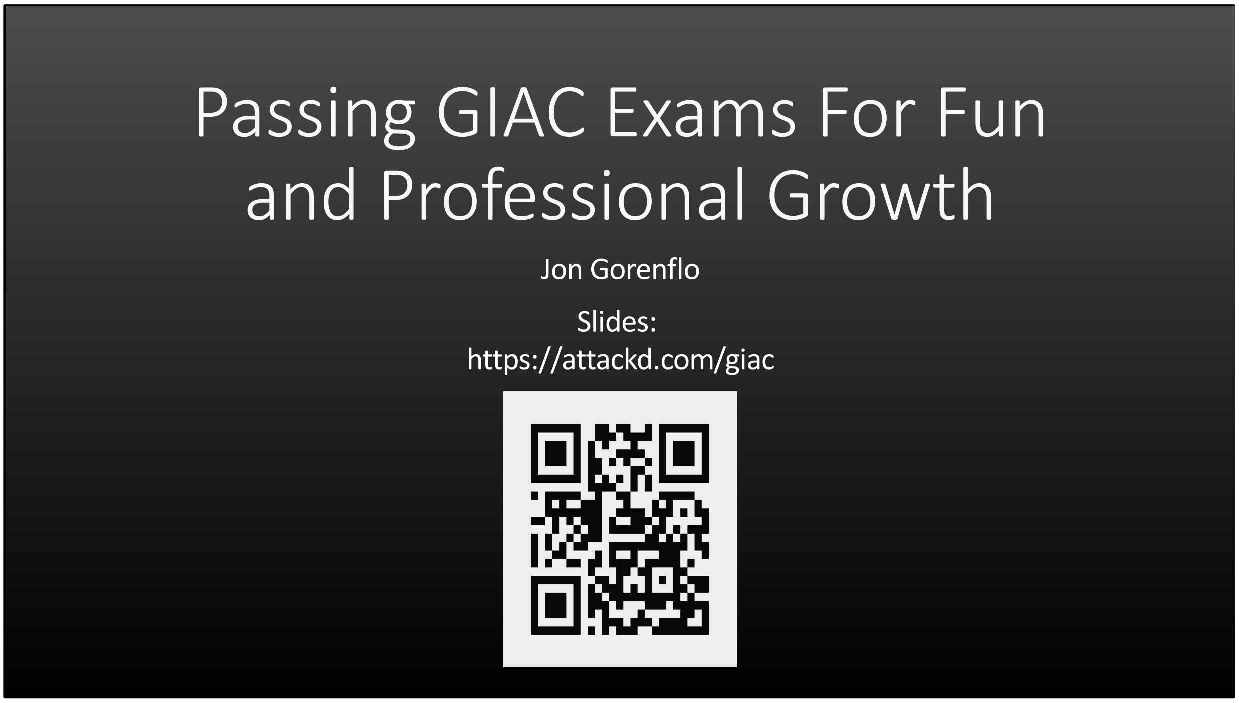
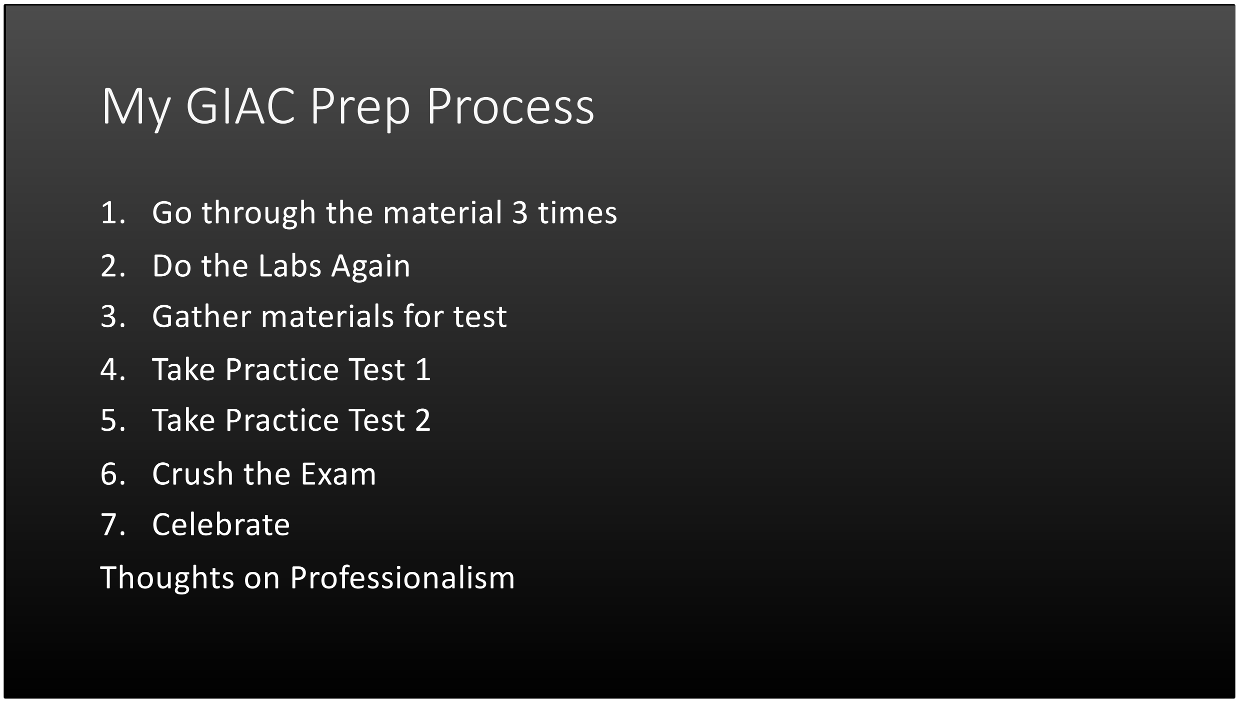


Passing GIAC Exams For Fun and Professional Growth

Jon Gorenflo

Slides:
https://attackd.com/giac



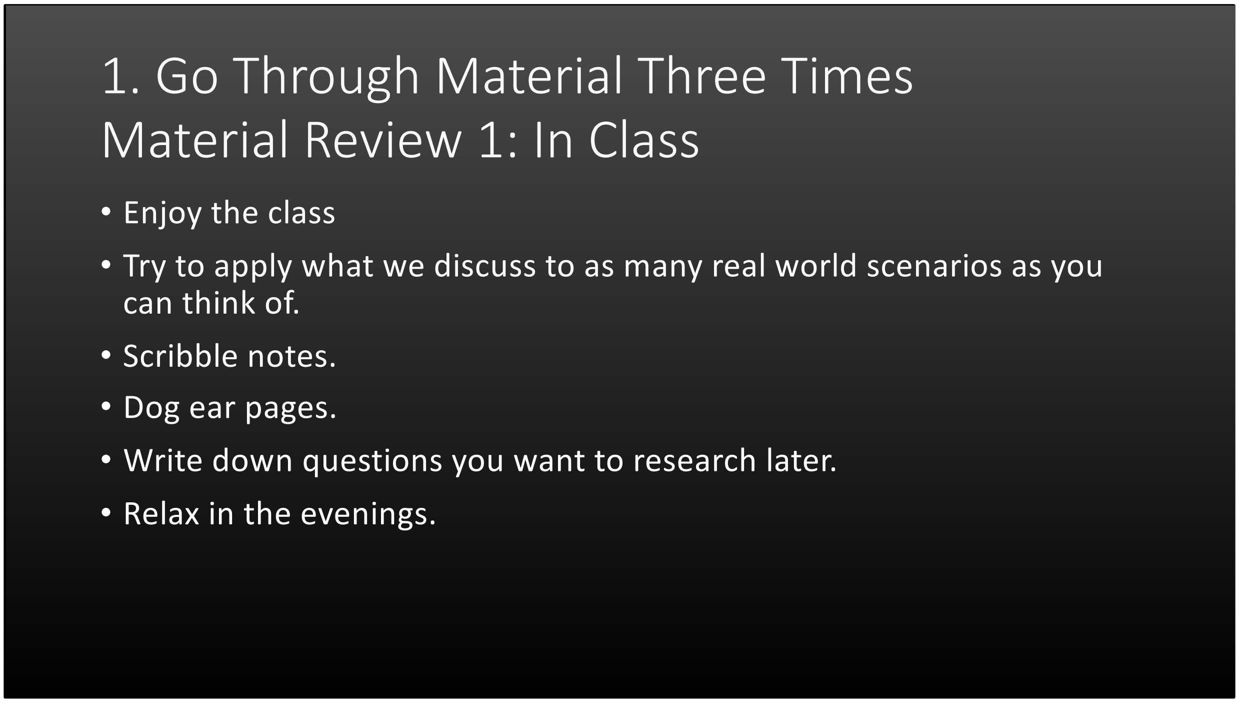
My GIAC Prep Process

1. Go through the material 3 times
2. Do the Labs Again
3. Gather materials for test
4. Take Practice Test 1
5. Take Practice Test 2
6. Crush the Exam
7. Celebrate

Thoughts on Professionalism

This is my process for taking and passing GIAC exams. I have taken and passed the GCIH, GAWN, GMOB, and GPEN. I've never failed a GIAC exam, but I reserve the right to screw that record up in the future.

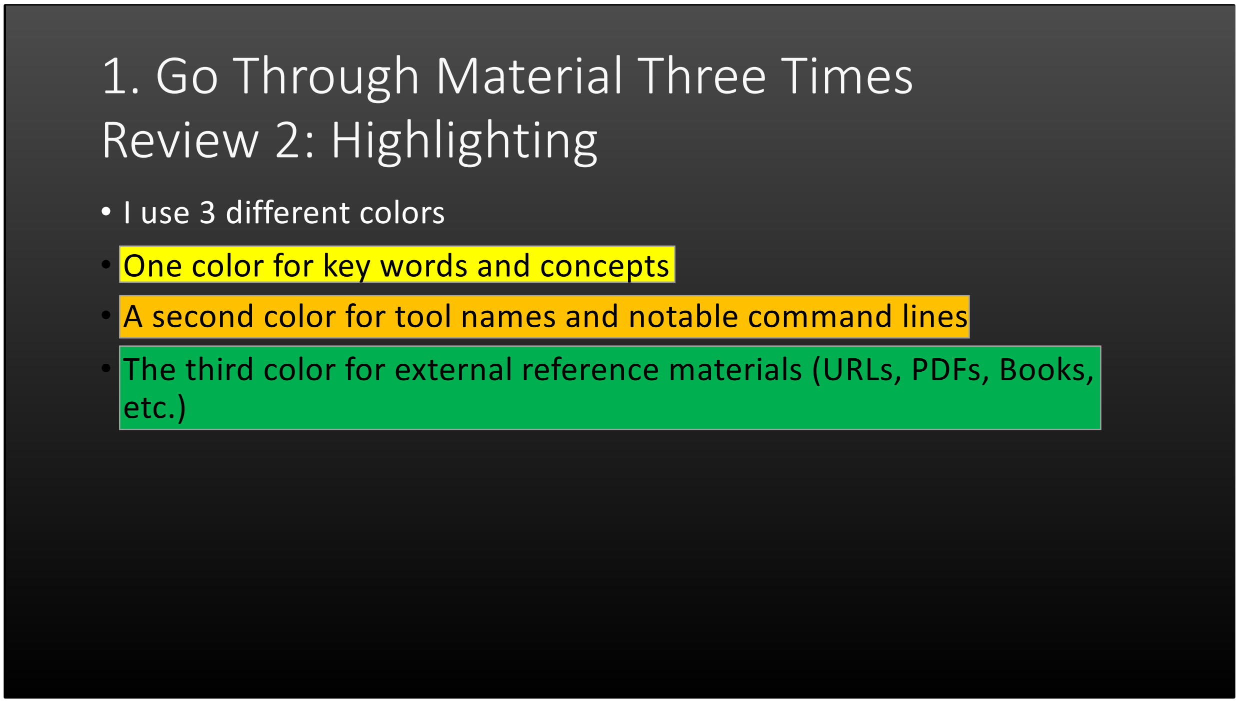
1. Go through the material 3 times - This sounds like a lot, but I'll explain what to do each time you go through the material
2. Do the Labs Again – DON'T SKIP THE LABS. DON'T. "But what if I…" NO! Do the labs. PLEASE!!
3. Gather materials for test – This will cover the items I like to have with me for the exam. SPOILER: #1 on the list is the course books!
4. Take Practice Test 1 – The practice tests assess two things: 1) Your knowledge. 2) Your study/test taking system. I'll explain how to use the practice tests to measure both and make adjustments.
5. Take Practice Test 2 – See #4
6. Crush the Exam – This is an obvious step in preparing for the exam, and couldn't be left off! I also cover a few less common exam tips to help you succeed.
7. Celebrate – This is one of the most important steps!!!!! You'll see why!



1. Go Through Material Three Times
Material Review 1: In Class

- Enjoy the class
- Try to apply what we discuss to as many real world scenarios as you can think of.
- Scribble notes.
- Dog ear pages.
- Write down questions you want to research later.
- Relax in the evenings.

This area intentionally left blank because I didn’t think I needed to say anything more than what’s already on the slide.



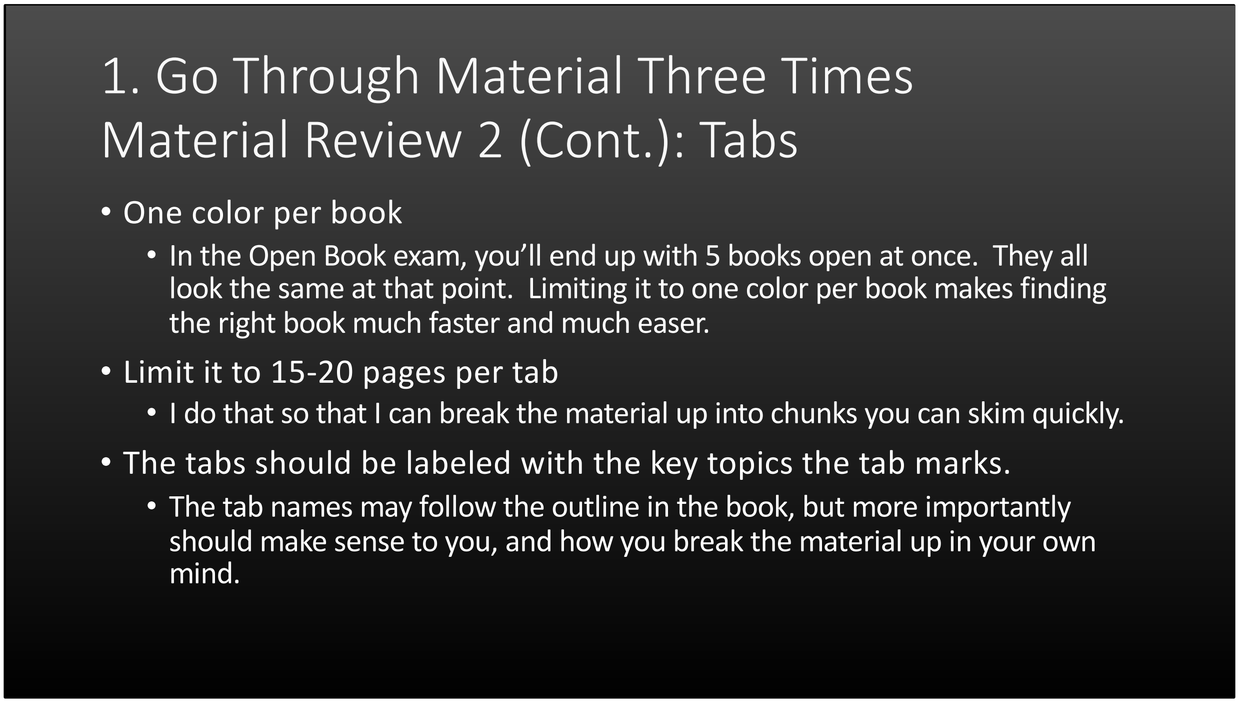
1. Go Through Material Three Times
Review 2: Highlighting

- I use 3 different colors
- One color for key words and concepts
- A second color for tool names and notable command lines
- The third color for external reference materials (URLs, PDFs, Books, etc.)

Using 3 different colors forces me to categorize the material as I read it. It helps me with a couple different things.

First, it helps me stay engaged while I'm reading. Sometimes, especially when I'm reading something dry, my mind will wonder, and I'll read an entire page, but actually I was thinking about how much laundry I have to do. Then I must re-read. By trying to categorize it all as I go, it keeps me more engaged.

Second, it helps me recall more, as well. As I read through the material and specifically look for key words and concepts, tools, command line examples, and external references, I'm amazed at how much more there is in the material that I didn't initially pull out. It helps me process the material at a much deeper level.



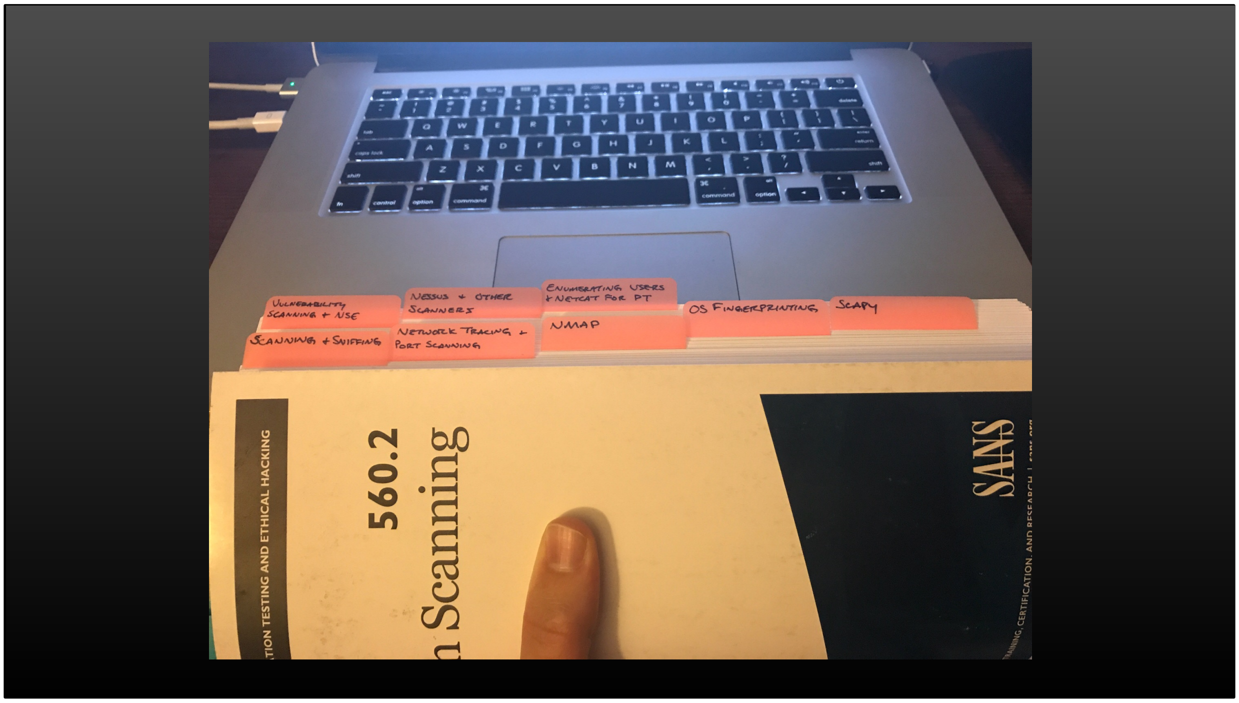
1. Go Through Material Three Times
Material Review 2 (Cont.): Tabs

- One color per book
  - In the Open Book exam, you'll end up with 5 books open at once. They all look the same at that point. Limiting it to one color per book makes finding the right book much faster and much easer.
- Limit it to 15-20 pages per tab
  - I do that so that I can break the material up into chunks you can skim quickly.
- The tabs should be labeled with the key topics the tab marks.
  - The tab names may follow the outline in the book, but more importantly should make sense to you, and how you break the material up in your own mind.

I can't stress how much I like having one color of tab per book.

I developed this approach after taking my first practice test for SEC504 with yellow sticky notes marking the sections. 30 minutes into my practice test, I had a stack of open books, and no idea which book was which from question to question.

The goal is to know as much as possible and only use your books when you MUST, but you want those times to be quick and frictionless.


VULNERABILITY SCANNING + NSE
NESSUS + OTHER SCANNERS
ENUMERATING USERS + NETCAT FOR PT
OS FINGERPRINTING
SCAPY
SCANNING + SNIFFING
NETWORK TRACING + PORT SCANNING
NMAP
ATION TESTING AND ETHICAL HACKING
560.2
n Scanning
SANS

Once tabbed, I can hold my closed book in my left hand, roll it slightly, and see every topic in the book.

When I find the section I'm looking for, I reach up with my right hand, place my thumb on the tab, and then flip open the book.

Now, I only have 15-20 pages to sift through to find the answer I'm looking for.

1. Go Through Material Three Times
Material Review 3: Index

- SUPER IMPORTANT: The power of the index is ***not*** having an index. The power of the index is ***the process of indexing***. DON'T use someone else's index.

"We can have no access to concepts except through study of linguistic language and, hence, the use of those words through which these concepts are expressed."
– Anthony Flew

- There are many indexing techniques out there, these two are pretty popular:
  - The Pancakes Method: https://tisiphone.net/2015/08/18/giac-testing/
  - http://digitalforensicstips.com/2012/11/sans-index-how-to-guide-with-pictures/

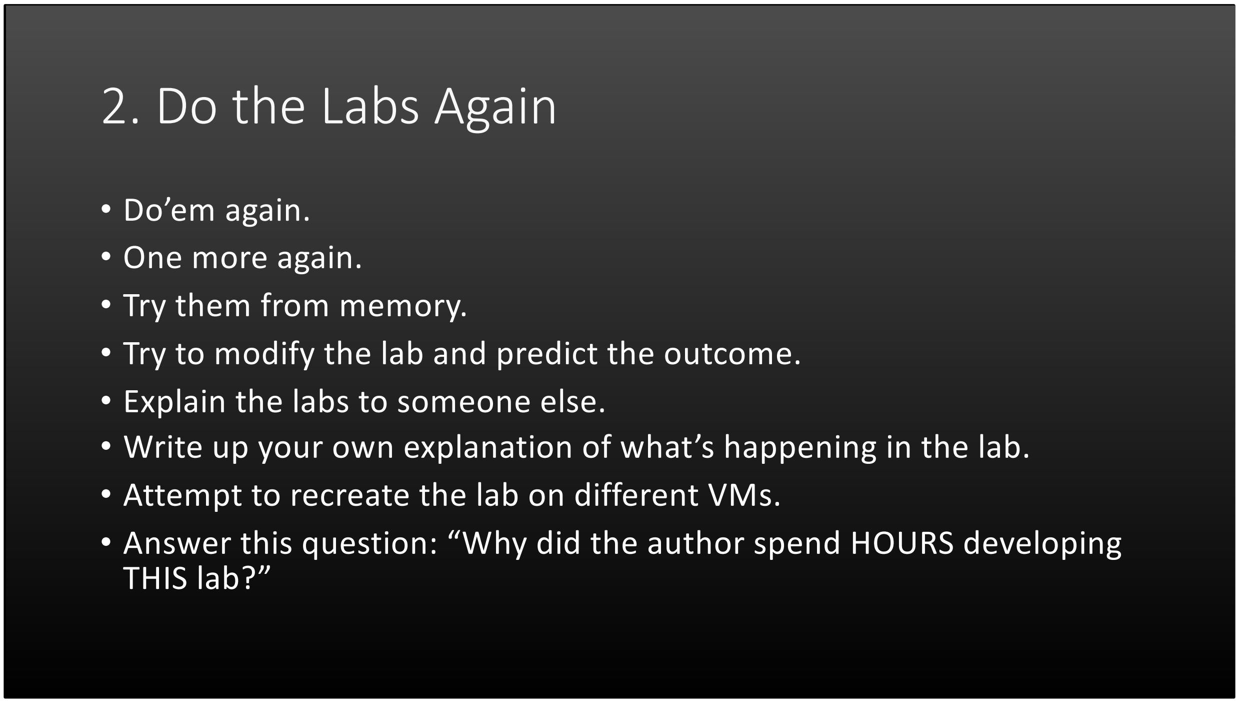
This is word for word what is on the slide above, but it's SUPER IMPORTANT: The power of the index is ***not*** having an index. The power of the index is ***the process of indexing***. DON'T use someone else's index.

The better your index, the less you'll use it! I know, you're sitting there thinking, "Jon is off his rocker. Why on earth would I invest hours upon hours to create an index that he says I won't use much if I put enough time into it?" BECAUSE!!! The reason you create the index is so that YOU DON'T HAVE TO USE IT!!!!!!

Ok… That is a slight exaggeration, but I hope you get the point. Indexing is a fantastic study technique. Some other general tips:

1. Don't copy word for word from the book and put it into your index. Take the time to rephrase what it is saying into your own words. Magic happens in our heads when we force abstract concepts into our own language. It helps us learn. And that's the power of the index.
2. I like to set my index up like I high light the material. Once high lighted, it makes it very easy for me to go back and index later.
3. I have seen some GREAT cheat sheets that were simply JUST the command

entered in the various labs. Even without the additional context of the lab, they are very helpful.



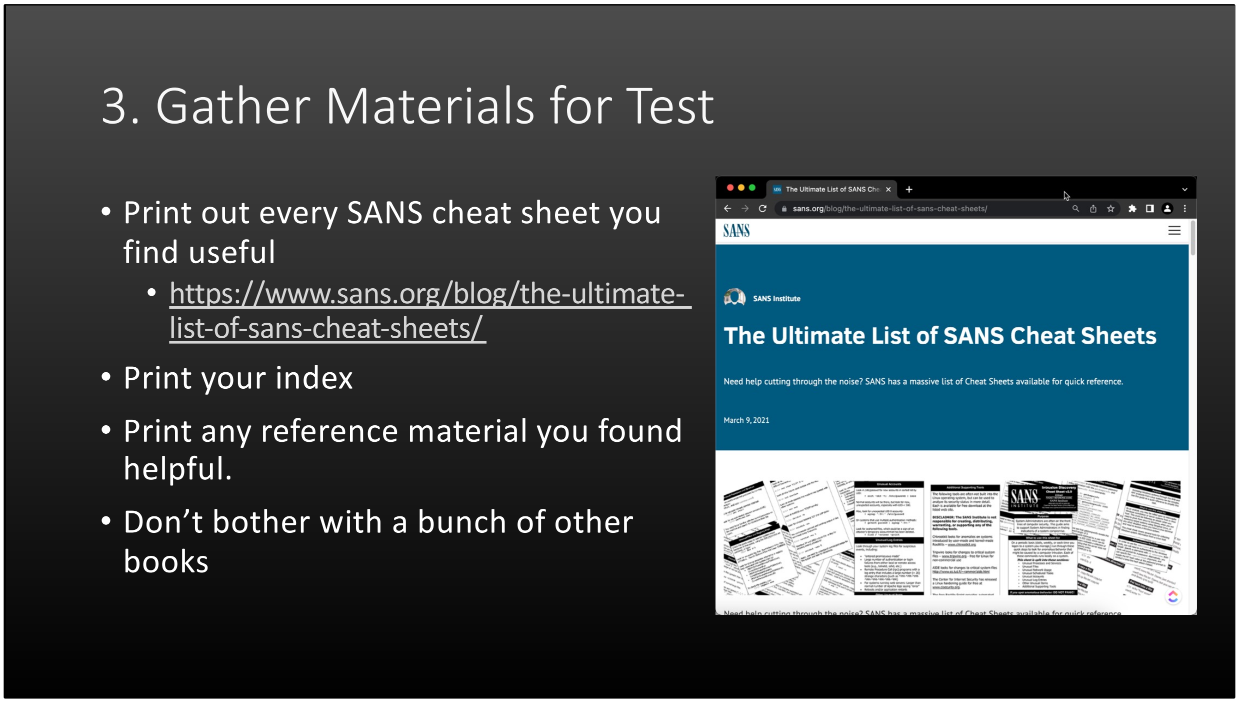
2. Do the Labs Again

- Do’em again.
- One more again.
- Try them from memory.
- Try to modify the lab and predict the outcome.
- Explain the labs to someone else.
- Write up your own explanation of what’s happening in the lab.
- Attempt to recreate the lab on different VMs.
- Answer this question: “Why did the author spend HOURS developing THIS lab?”

The labs reinforce the concepts in the material. The labs are a little bit like Fight Club. The first rule of labs is DON’T SKIP THE LABS. Srsly. Plz.

The more times you do the labs, experiment with the labs, rebuild the labs, explain the labs, the better off you’re going to be. Beyond doing the labs, try to answer the question, “Of all the things in all the world that this course covers, why did the author spend HOURS developing THIS lab?” How could you use it at work?

Again, just like indexing, there’s ***magic*** in explaining the labs in your own words. MAGIC!



3. Gather Materials for Test

- Print out every SANS cheat sheet you find useful
    - https://www.sans.org/blog/the-ultimate-list-of-sans-cheat-sheets/
- Print your index
- Print any reference material you found helpful.
- Don't bother with a bunch of other books

The Ultimate List of SANS Che
sans.org/blog/the-ultimate-list-of-sans-cheat-sheets/
SANS
SANS Institute

The Ultimate List of SANS Cheat Sheets

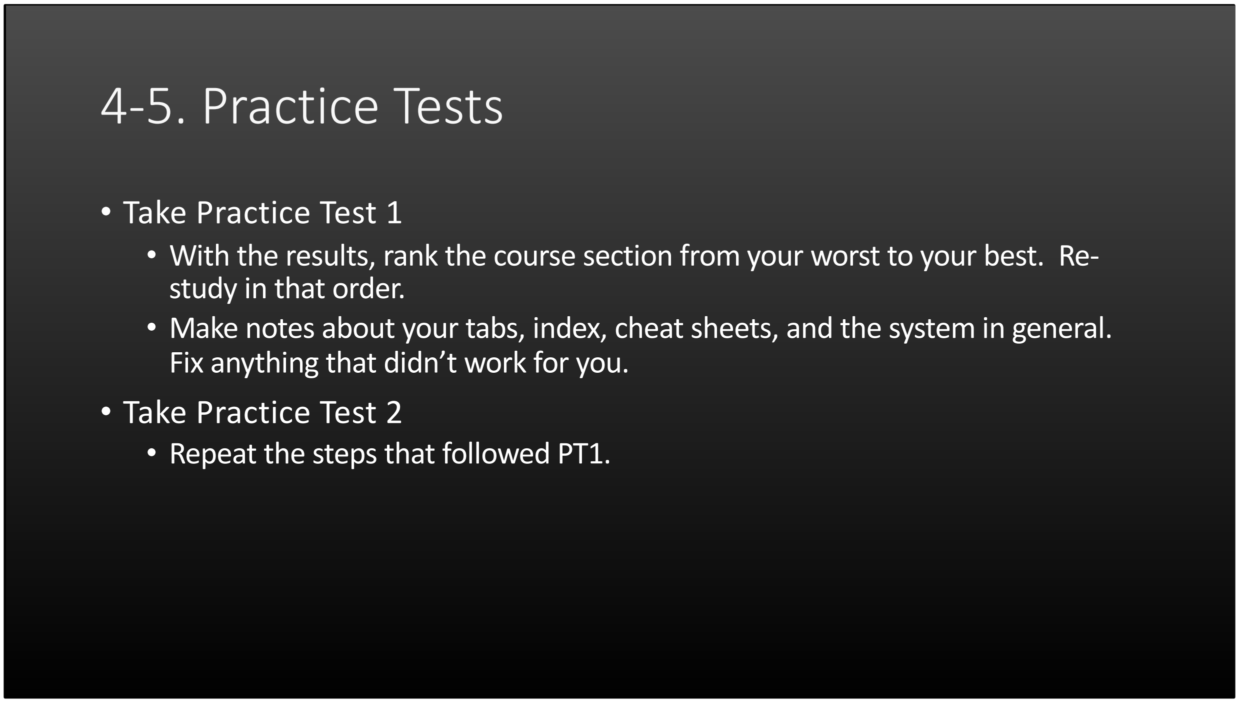
Need help cutting through the noise? SANS has a massive list of Cheat Sheets available for quick reference.

March 9, 2021

The test is open book, open notes, open library…if you can carry it in there. ANY paper-based material is acceptable.

Let me stress one thing: Focus on the material you received from SANS to take the class. While you can take any paper-based items to the exam, there are only a couple things I recommend beyond what you were given with the course material.

1. Go to The Ultimate List of SANS Cheat Sheets. Print everything that you remember being discussed in the class.
2. Print your index
3. Any other material you found helpful



4-5. Practice Tests

- Take Practice Test 1
  - With the results, rank the course section from your worst to your best. Re-study in that order.
  - Make notes about your tabs, index, cheat sheets, and the system in general. Fix anything that didn't work for you.
- Take Practice Test 2
  - Repeat the steps that followed PT1.

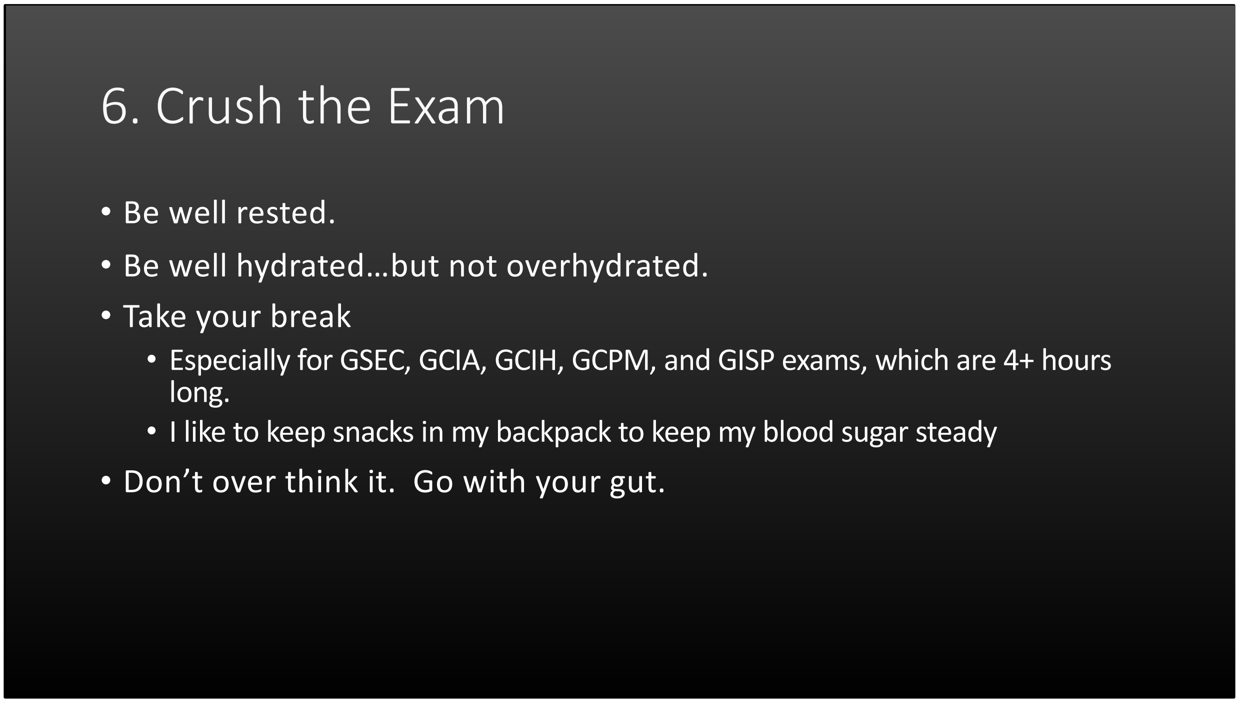
As I mentioned at the beginning, the practice tests test 2 things.

1. It tests your knowledge.
2. It tests your test taking system.

After your first practice test, make notes about where you felt weak in your knowledge and go study those areas. MOOOOAAAARRRR INDEXING!!!!

You should also have a feel for where your system failed you. Make tweaks to the system, as necessary. After my first practice test is when I decided I needed color coded books.

Rinse and repeat.

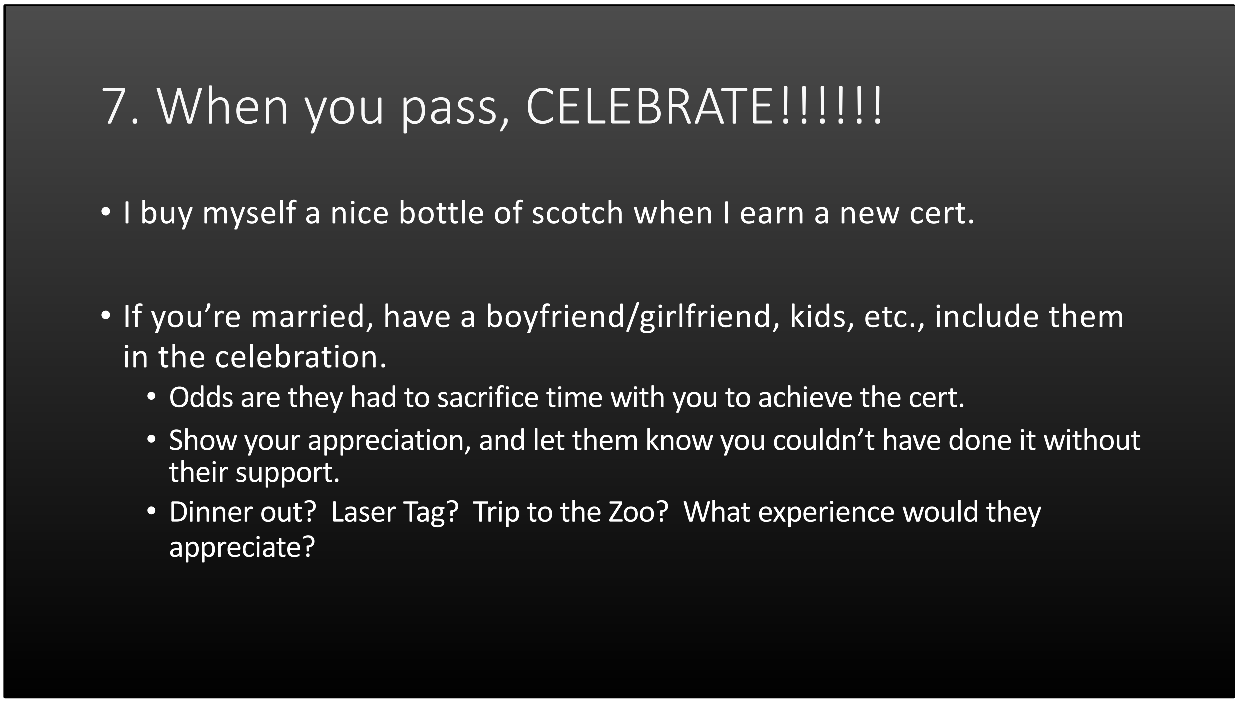


6. Crush the Exam

- Be well rested.
- Be well hydrated…but not overhydrated.
- Take your break
  - Especially for GSEC, GCIA, GCIH, GCPM, and GISP exams, which are 4+ hours long.
  - I like to keep snacks in my backpack to keep my blood sugar steady
- Don’t over think it. Go with your gut.

MUST DO:

1. Get a good night of sleep the night before. NO CRAMMING. Science says it doesn’t help, anyway.
2. And cried. Hydrate the day before…but not RIGHT before…your exam. Be the little piggy that passed his GIAC test, and NOT the little piggy that went WEE WEE WEE all the way home. You don’t want to be 15 minutes into a 4 hour exam and have to burn your break! If you have a medical condition, talk to the testing facility about what accommodations they may be able to make, but plan ahead.
3. Use your break to relax for a few minutes. I like to take a power snack like a cliff bar, trail mix, or the like. You don’t want something sugary that will cause you to crash before the end of the exam.
4. Listen to your gut. It knows more than you. In fact, the reason it’s SOOOO important to put things into your own words is because it helps map what your gut knows to language. If you haven’t done that mapping ahead of time for a topic, your gut might still know. Pay attention to its subtle grunts.



7. When you pass, CELEBRATE!!!!!!

- I buy myself a nice bottle of scotch when I earn a new cert.
- If you’re married, have a boyfriend/girlfriend, kids, etc., include them in the celebration.
  - Odds are they had to sacrifice time with you to achieve the cert.
  - Show your appreciation, and let them know you couldn’t have done it without their support.
  - Dinner out? Laser Tag? Trip to the Zoo? What experience would they appreciate?

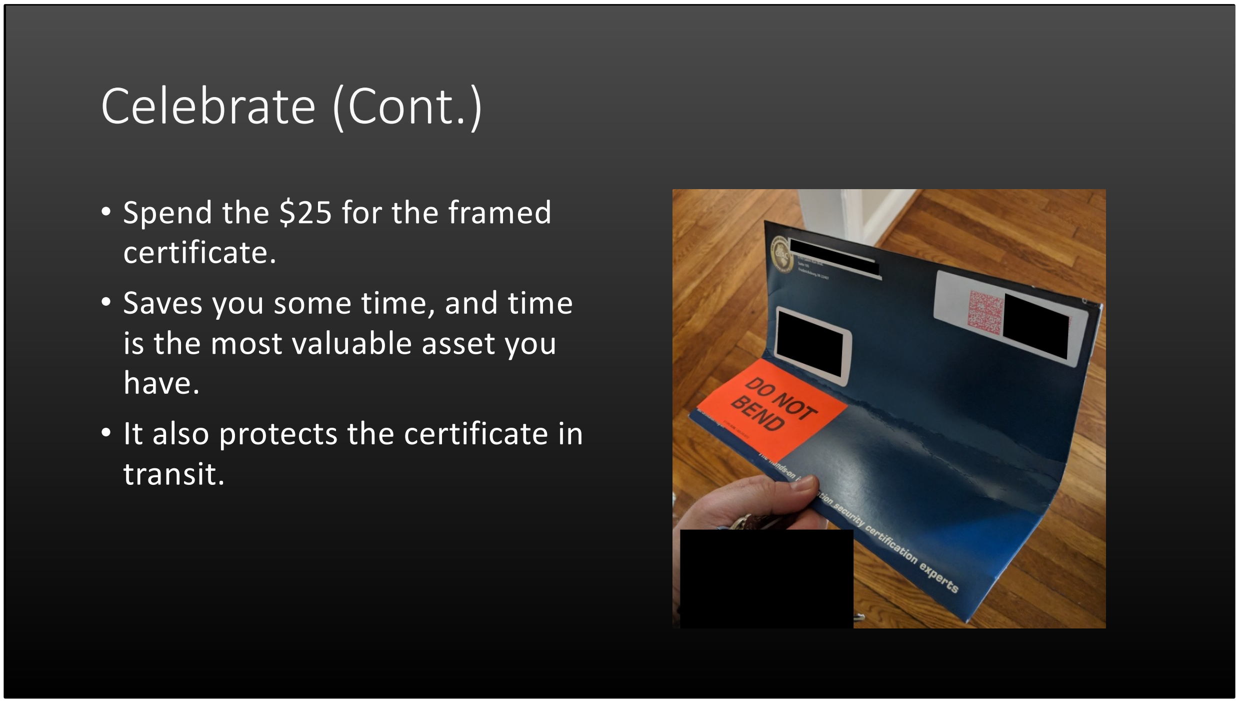
Seriously. Celebrate! This is a big deal! You earned it!

And don’t forget to include your spouse, boyfriend/girlfriend, kids, etc. Do something experiential that is ALL ABOUT THEM. THANK them for their support.

When I travel, I try to take my family out for a nice when I get home. They have to sacrifice to I can do what I love. Right now, we go to Senior Antonio’s. It’s a local Mexican restaurant that is like most Mexican restaurants. My oldest LOVES mixing the queso cheese with the salsa. My youngest gets the worst frozen pizza on the planet earth. Seriously, it’s terrible. But she LOVES it, and that’s what it’s all about. Me giving them something they love for letting me take the time to do what I love.

Oh, they know when it’s time to celebrate! I make sure of it.

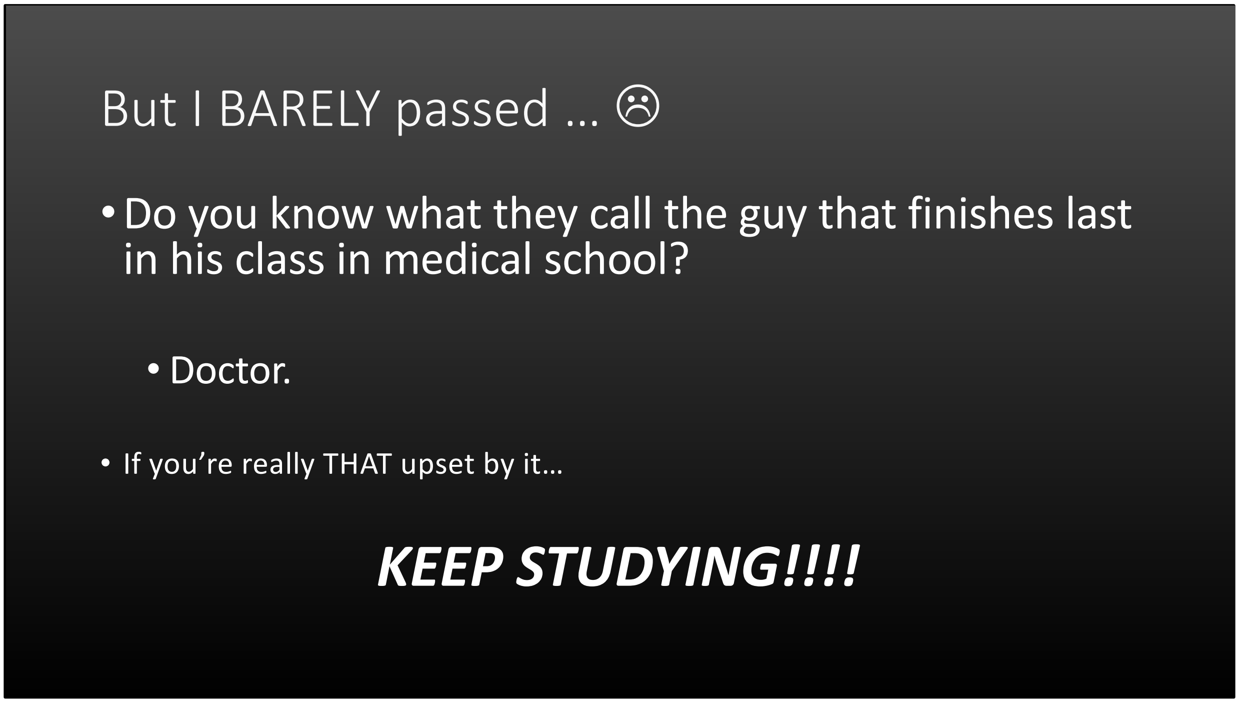
More importantly, I make sure they know that I couldn’t have done it without them!!



Celebrate (Cont.)

- Spend the $25 for the framed certificate.
- Saves you some time, and time is the most valuable asset you have.
- It also protects the certificate in transit.

This is a real picture sent to me by someone I mentored through one of the SANS academies. I guess they didn’t bend the sticker… This is why A.I. is hard.



But I BARELY passed … ☹

- Do you know what they call the guy that finishes last in his class in medical school?
  - Doctor.
- If you're really THAT upset by it…

KEEP STUDYING!!!!

I get this one from time to time. Boo freakin' hoo. YOU STILL PASSED, YO!

No one will see your score but you. Your framed certificate will look the same as MY framed certificate!!

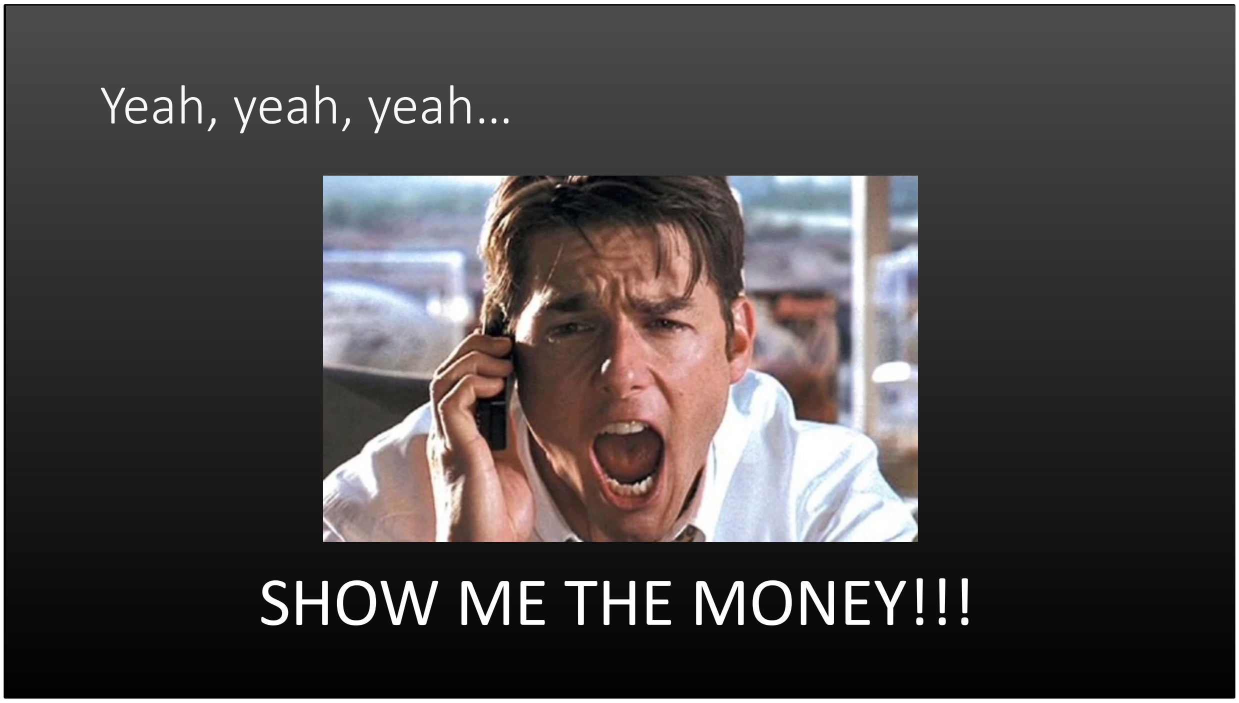
But here's the thing, if you *still* aren't satisfied with your score…

* * * ***<u>KEEP STUDYING</u>*** * * *

This is where PROFESSIONALISM comes into play.

The point of the certification is ***<u>NOT</u>*** more money! The point of the certification is to demonstrate your knowledge and abilities! Don't stop just because you took the test! Keep going!

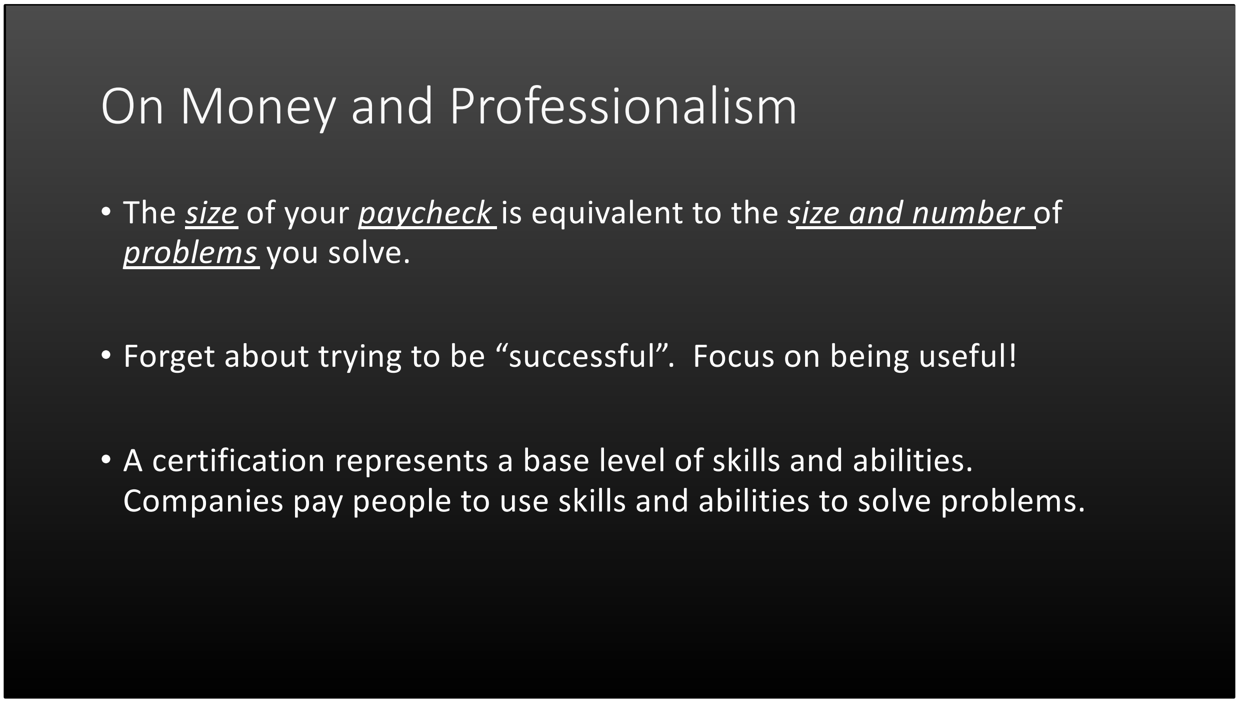
Study enough, and you can join us in as an instructor. Teaching for SANS has changed me profoundly, and all in good ways.



Yeah, yeah, yeah…

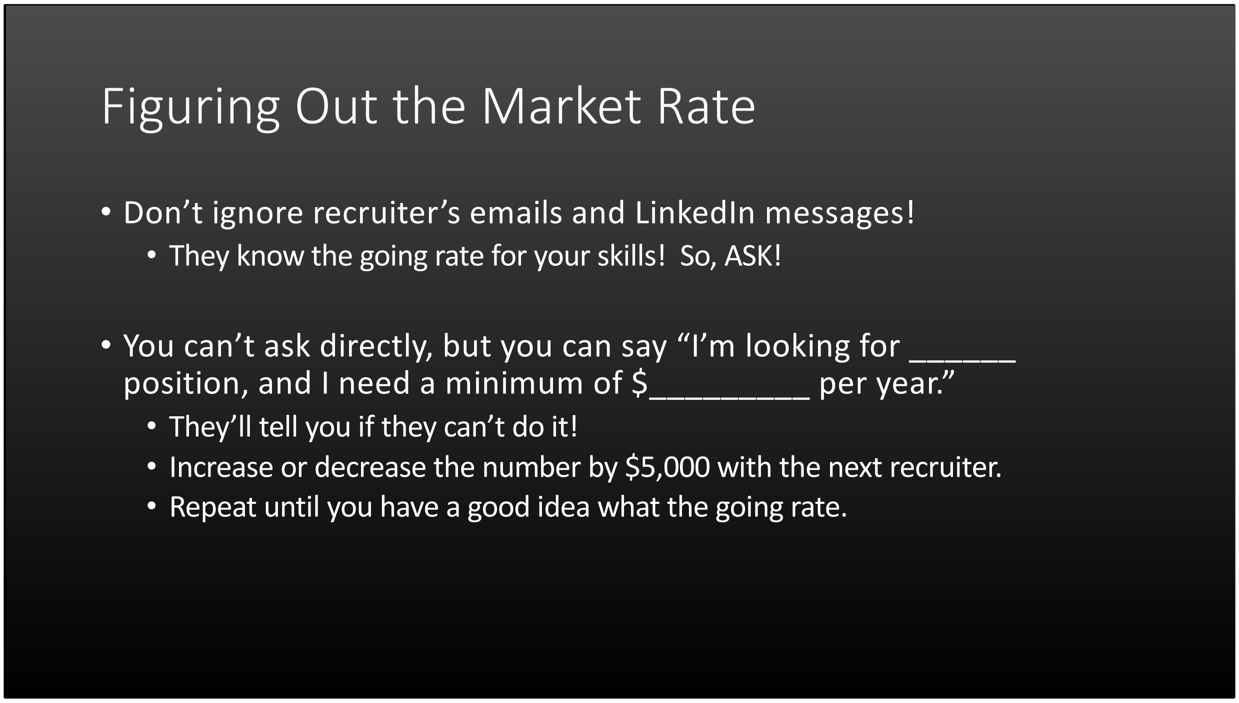
SHOW ME THE MONEY!!!

Ok. I hear you.



On Money and Professionalism

- The *size* of your *paycheck* is equivalent to the *size and number* of *problems* you solve.
- Forget about trying to be “successful”. Focus on being useful!
- A certification represents a base level of skills and abilities. Companies pay people to use skills and abilities to solve problems.



Figuring Out the Market Rate

- Don’t ignore recruiter’s emails and LinkedIn messages!
  - They know the going rate for your skills! So, ASK!
- You can’t ask directly, but you can say “I’m looking for ______ position, and I need a minimum of $_________ per year.”
  - They’ll tell you if they can’t do it!
  - Increase or decrease the number by $5,000 with the next recruiter.
  - Repeat until you have a good idea what the going rate.

Questions?

Slides: https://attackd.com/giac

Jon Gorenflo

Email: jon@attackd.com

Twitter: @flakpaket

That's it. That's all I've got. Go forth and do great things. If you have questions, feel free to hit me on Twitter or Email.

Jon Gorenflo
Email: Jon[at]funsec.net
Twitter: @flakpaket

If we haven't met, hopefully I'll meet you in class sometime. You can see my teaching schedule here:

https://bit.ly/2hHNXIV