

## An American Hacker in London: Course Review of CSTA by 7Safe

As most of you know, I do not have a college degree. I'm not alone&hellip; Bill Gates, Mark Zuckerberg, Richard Branson and countless others have had great success without this particular piece of paper. A common question in The Ethical Hacker Network Community Forums is if someone should get a degree, gain experience or achieve certifications to which I quickly respond by saying, &ldquo;Yes!&rdquo; All make for a better resume. Unfortunately, I only have 2 out of 3. In addition to sounding hypocritical, there are plenty of other reasons why I get that nagging feeling that I should get my degree: what if this online magazine thing goes caput, what if I ever want to teach, or, the most pressing item at this point in my life, am I setting a good example for my kids? But even if I do want to pursue a degree, how do I find the time? An undergrad degree is no longer good enough, and that adds even more time and effort to reach for a masters. So as always, I&rsquo;ll put it on the back burner and let those voices continue in my head&hellip;

&ldquo;You&rsquo;ve got to kill yourself, Don, before it&rsquo;s too late.&rdquo;

&ldquo;Why are you doing this to me?&rdquo;

&ldquo;I&rsquo;m cursed to walk the Earth as the undead until the bloodline is severed. You have to get a degree, Don, or you&rsquo;ll make others like me.&rdquo;

This American hacker recently had the opportunity to travel to the UK to attend the launch of the latest update (version 5) of the Certified Security Testing Associate (CSTA) ethical hacking certification course by 7Safe. When looking at their website, every page of every course shows the MSc logo and the credits to be earned towards a Master&rsquo;s Degree in Computer Security & Forensics&hellip; that nagging corpse of an idea kept reappearing telling me, &ldquo;Don&hellip; get your degree or people will die!&rdquo; OK, so I&rsquo;m not a werewolf from the classic horror film that inspired Thriller, and I&rsquo;m not spawning a group of undead. It just seems as though every time someone asks me about a college degree, I feel like a new undead idea roams the netherworld of my brain. Will I forever be cursed with these visions?

So what&rsquo;s the deal with this course, the certification and why should I consider this one over what seems to be a never ending choice of new security training providers? How does it compare with similar courses in areas of content, price, availability and acceptance in the industry? And what&rsquo;s all the talk of college degrees? Get all the details after the break.

Discuss in Forums {mos\_smf\_discuss:Editor-In-Chief}

Argh!!!! I fat fingered it AGAIN!

I started my trip by spending a couple days in London to play tourist&hellip; uh, I mean&hellip; adjust to the time difference. Like a true hacker, even my choice of entertainment seems to be dictated by my desire to learn. And so it was that I found myself at the Shaftesbury Theatre the night before class seeing Svengali, the latest live stage show by the ultimate social engineer, Derren Brown. Of course the rest of the world sees him as a magician, mentalist and wildly charismatic television personality sharing airtime on the same channel that brought you The IT Crowd. It is my perception that he is the best hacker of the human mind, and thus, in my world, a reality. As it turns out, the reality of the evening was truly better than fiction. It was fun to use the powers of observation and a little social engineering to not only crash the after party but also have a conversation with the one and only conjurer himself. With the help of some new friends in the UK, we had a night that, in a word, was brilliant.

With thoughts of the previous evening running through my head, I boarded the train from London Liverpool Street Station and headed for Cambridge with a huge smile on my face. The enjoyment of a new culture continued, as it felt as though I had just left Platform 9  $\frac{3}{4}$  as the car was filled with uniformed students on their way to institutions so unknown to me that they might as well have been Hogwarts. This sense of wonder persisted throughout the trip including the course itself and not just because of the location or the destination lunches at pubs like The Slaughtered Lamb...

&ldquo;Wait! You just can&rsquo;t let them go,&rdquo; pleads the innkeeper.

&ldquo;Go!&rdquo; yell the locals. &ldquo;Stay on the road. Keep clear of the moors. Beware the moon.&rdquo;

&ldquo;What the hell was that all about?&rdquo;

Soon after arriving at the 7Safe training facility, I see those slick posters for MSc wretchedly staring at me. Clearing my

head with some coffee with the other students and reliving my night in the West End seems to do the trick. Before long, our instructor, Jerome Smith, called the class to order. Introductions were the obvious starting point for this 4-day course, and I must say that I was highly interested in getting to know more about Mr. Smith. Another common question in EH-Net's Forums is how good a class will be, and the best answer is always that it depends on the instructor. I was informed of the instructor's name and short bio before attending the course, but did not know of him personally. After my time with him, I'm glad I got to know him. He not only was a kind family man, experienced pen tester and a very good instructor but also developed the course and designed all of the hands-on exercises and intricate labs as well. All in all, a lovely chap.

Then it was straight into the courseware with Section 1: Introduction. This started with a quick look at what hacking is, what it is not, a little history... common items for a course with this focus. The time dedicated to this task was timed perfectly as to not be too long to bore the old guard but enough to get all of the students into the mindset of a hacking class. This was followed by a quick mention of the hacking methodology used in the course. Although it was a common set of bullet points, I thought it was odd to not even mention other methodologies like OSSTMM. It's a small point, but I thought it was worth mentioning as many in the course were not pen testers, and it would be nice for them to know that there are accepted methodologies already out there and accepted by the industry. I think he did bring it around by making very clear that there is a big difference between the methodology that a real attack might have and one that is used by an authorized penetration tester. The Introduction Section came to a close after a quick overview of the lab environment and how the exercises utilized it.

Section 2: Networking Refresher was also a good choice, as this course was not meant to be on the basics of security or networking, yet his audience would consist not of advanced hackers but those with different levels of experience. This short, 11-slide section was just enough to make sure that students of varying backgrounds were now focused in a common direction. It covered the obligatory OSI Model followed by a quick progression down from covering the TCP/IP protocol suite to TCP/UDP to ports. This led right into the first of many well designed lab exercises. The Sniffing Traffic Exercise was a great toe-in-the-water type of lab for two reasons. First reason is that the students we introduced to a technical exercise very early on in the very first day, and, secondly, it also gave a good indication of how the labs, quizzes and reviews would work throughout the course. This particular lab presented packet capture using Wireshark and Ettercap. The XP host machine had a copy of Outlook Express already setup to send and receive email with Wireshark used for the capture. We also used the XP host to run VMware with a customized version of Backtrack running Ettercap. This combination allowed us to quickly get used to the lab setup, run both Windows and Linux tools, see common packets like those associated with the 3-way handshake, find the username and password of the email account as well as get used to common Linux commands. Notice that I did not mention the inclusion of a Linux primer. Intermixed in the exercise itself were enough steps to get those unfamiliar with Linux to learn as they went. There are also questions asked in the labs where the students are required to write the answers, since the information gathered even at this early stage are utilized in later labs. This cumulative concept also keeps the students focused on the fact that everything you do needs to be recorded and can be used later just as in a real-world penetration test. Being an ethical hacking course, this section, as all of the others, ends with a summary as well as a discussion of countermeasures.

Now would be a good time to make a few general observations about the exercises and lab environment as well as the choices made by Jerome in designing the class, because the following statements apply to the course as a whole. The most important thing to mention right off the bat is that the course is held in a classroom containing computers already setup including fully licensed copies of Windows. Many other courses require the students to bring their own laptops leading not only to wasted time in setting up the environment but also hampered learning due to the lack of a real corporate Windows environment in which to hack. Therefore, the entire custom lab environment was ready to go from the first keystroke with XP client machines containing common apps, a fully functioning domain controller with varying user accounts, a customized copy of Metasploitable serving up email, web apps, etc. and an updated, slightly modified version of Backtrack. With each of OSs being customized to maximize interactivity during the exercises, it was obvious that a lot of work, forethought and testing went into creating this course. Extra kudos go to Jerome and the crew, because all of the exercises worked flawlessly. For a first time run of a course, this was mightily impressive. And it went right along with their philosophy that the students would be learning by doing instead of listening to boring lectures. I can't speak highly enough on how the design of the lab environment not only maximized time but also learning. And remember, this is only a 4-day course, and thus efficiency would be vastly important. In the end, the labs are what truly separate CSTA from other courses.

As it would in the methodology, the next section of the course was Section 3: Information Gathering. Nothing too complex was discussed in this section. All of the normal big picture ideas one would expect to find were discussed such as technical vs. non-technical methods as well as active vs. passive information gathering. Specific tasks were also covered such as google dorking, website crawling, metadata discovery, DNS enumeration and more. But the more important facets to mention are the way in which these methods are taught. First of all, the students will find that they are not overloaded with every tool under the sun, yet will concentrate on utilizing best-of-breed tools that are readily available and used by professionals every day. This is true for the entire course and not just this section. The second facet harkens back to my previous paragraph on the virtues of the lab environment. During the first exercise, the students use wget to copy the contents of the labs web server. While perusing the metadata, a username is found in the creator field of a document. Take a wild guess where that username will appear again? You got it&hellip; in a lab further down the course. The same thing happens during the second lab on DNS enumeration using both dig and fierce, where the students discover DNS records, IP addresses, email addresses and more from the live lab network surely to be utilized later. In following the idea of exploring best-of-breed tools instead of every single one, I found that the extra time spent in the labs on fierce was very effective, especially using the built-in dictionary list and playing with the reverse lookups of neighboring IP addresses of found hosts. Good stuff.

My thoughts on Section 4: Target Scanning will follow the same pattern as the last section. It was efficient in its presentation, long on lab work and integrated into the entire course nicely. As you would expect, not every tool ever created is discussed, which allowed the students lots of time to get hands-on work with nmap, netdiscover and tcpdump. Also covered in this section was banner grabbing which included exercises with amap and netcat. Don&rsquo;t let the length of this paragraph fool you. There was plenty of depth in this section not only on the tools but also the hows and whys of port scanning, leading us naturally to our next section.

Section 5: Vulnerability Assessment started with some short lectures on the nature of vulnerabilities, the difference between an assessment and a full penetration test, as well as some additional discussions on design flaws. Most impressive was Jerome&rsquo;s discussion of buffer overflows. Having heard a number of instructors&rsquo; attempts to reach their students, this was perhaps one of the most effective. The chosen words, style of speaking and helpful animations made even some of the less technical students understand programming speak on the stack, remote code execution and return pointers. Although not necessary information to know for novice ethical hackers, it made it easier for them to understand what they were doing when it came time to play with Nikto and Nessus in the labs.

It is here that it becomes important to mention a fact about the CSTA course as stated by 7Safe themselves. &ldquo;This 4-day ethical hacking training course is a hands-on journey into the hacking mindset, examining and practically applying the tools and techniques that hackers use to launch &lsquo;infrastructure&rsquo; attacks.&rdquo; So this is not a course on web application security, wireless security or reverse engineering. 7Safe has other courses dealing with these topics, and therefore barely touch on these topics in this course. In interviewing Jerome Smith as well as Alan Phillips, CEO of 7Safe, it was a conscious decision for 2 main reasons. In the first place, the last version of CSTA was only 3 days, and, in the current economy, every extra day means more expense for the student and/or their company. So they had to make important decisions about what can be included and what can&rsquo;t in their compromise of deciding on a 4-day course. That naturally led to the second point. They wanted to make sure that the focus was on being an infrastructure course, which would allow them to include more lab time on the core ideas of network pen testing and leave the other topics for their other courses.

&hellip;Other courses? That would mean more credits towards MSc. Their glossy brochures shine with the possibilities. Hmm&hellip; according to their site, an MSc is worth 180 credits broken down into 12 modules of 15 credits each. Each 7Safe course (& exam, where applicable) and associated written assignment constitutes a module. The independent study is a further module, and the MSc project is worth 60 credits (the remaining 4 modules). 7 security courses all with credit towards a masters, very interesting&hellip;

The focus of the course becomes more important as we move forward through the rest of the sections, as it makes clear what is and is not covered. But without getting into the details of everything in the course, let's just say that the meat is contained in the next 4 sections on hacking Windows and Linux.

Although Section 6: Attacking Windows and Section 7: Privilege Escalation &dash; Windows covers the obvious topics of Windows hacking, what stands out in these sections are the use of new technology and a lab that contains a working domain controller. For the sake of brevity, let me cover both of these sections in just a few sentences. Together these 2 sections have 15 labs allowing for hours of hands-on work with the latest and greatest tools and techniques. Just a few of the highlights include Windows enumeration with lots of command line time, extensive use of Metasploit with Meterpreter including using one of the vulnerabilities used by the infamous Stuxnet malware, and thorough coverage of password attacks including Ophcrack, John the Ripper, Cain, rainbow tables and even learned about Windows workstations that use salts when storing cached domain credentials. There was also a great exercise on token stealing and the use of the Meterpreter module, incognito, in addition to working with the latest technique for the 'pass the hash' attack. Oh, and that domain controller... it wasn't just there to fill in a bullet point. It was actually utilized to show how a network looks and reacts when one is present. There was no single exercise dedicated to hacking domain controllers. Better yet, it was simply put as another integral part of the lab network with which the students had to deal.

The Linux portion of the course includes Section 8: Attacking Linux and Section 9: Privilege Escalation &dash; Linux. As was done with the Windows sections, I'll cover the Linux sections in a brief manner. Sections 8 and 9 included nine more labs for your hacking pleasure. More work was done with Metasploit including pivoting, the differences in password attacks including salts, OpenSSH/OpenSSL attacks, and exercises on exploiting sudo, suid and flawed scripts. There was some great work on shell script flaws including command injection and path exploits that were a lot of fun.

Even while fun was had by all, the theme remained true. Everything we had found during the first few steps of the methodology and attacked in the last four sections were all interconnected. Designing this into the course was not an easy task, yet it was done very well. Knowing the importance of each individual step was also not lost during the course itself, as Jerome was very quick to help someone who had difficulty in an exercise. He was always sure to stress the importance of paying attention and completing every step of every exercise, all while being polite and courteous, another feat for a tech guy.

Speaking of feats, I haven't even accomplished the goal of a bachelor's degree. How in the world could I even consider a master's degree? Wait a minute... Was it another vision or did Mr. Phillips tell me that the University of Bedfordshire would apply all of my experience towards the bachelor's degree and be allowed to enter to MSc program straight away? It's true. It's not a dream. Maybe breaking this curse is closer than I...

Now that the hacking was done, it now became time for the rest of the methodology. Section 10: Retaining Access covered some nice discussions on the topic and then went into some additional exercises of its own including some more fun with netcat as a backdoor and Bandoor RAT. For those of you not familiar with the latter tool, it is a backdoor from NWC, and it was recommended that you visit their site at your own risk. Although this is something that would never be done during a real pen test, it was nonetheless nice to replicate such an attack. And it was done so thoroughly that we even re-enacted the entire client-side attack by configuring the backdoor tool, then we started a bandoor listener, created a bad PDF with a meterpreter payload, sent it to the victim via an email attachment, opened the attachment and then watched the fun from the other VM. Simply put, this could not be done with a run of the mill lab running metasploitable and backtrack. This is yet another testament to the exceptional lab environment in the CSTA course.

It was time for some additional playing in the lab during Section 11: Covering Tracks. A little obfuscation, some rootkit time, a touch of log manipulation with a topping of TOR action, and this was a fun way to end our time in the lab. So the only thing left to do was to wrap things up in Section 12: Conclusion. The conclusion, like most of the lectures, was quick

and to the point. Jerome wrapped things up with a reminder of the methodology, a quick overview of what we had accomplished during our 4 days, some trends for the future, additional reading recommendations and then finally a discussion of the certification exam to commence soon after the conclusion.

Let's not forget that in addition to everything we learned and all the sleep we lost, there was still a very important task left to end the week. The CSTA exam is a 1 hour online exam of 50 multiple choice questions. It only takes 50% to pass, which I was told was a requirement for them to be able to utilize this certification towards the attainment of a master's degree. But because of this, they also have additional 'grades' of Merit at 66% and 'Distinction' at 80%. The exam was pretty straight forward, with the ability to mark questions and return to them later. I felt as though the questions were not difficult, and paying attention in class was enough to make the grade. I'm not sure how much this had to do with my prior knowledge, the class or the exam. Either way, I felt pretty confident when the exam was over. Unfortunately, it is 7Safe's policy not to reveal the results immediately. So I had to wait until after I returned to the States to get my results from Jerome personally through email.

## Final Thoughts

An argument could be made that an attack is an attack, and, as long as one knows the method of an attack, the age, effectiveness and current use of the attack is irrelevant. I think this is a bunch of BS and an excuse for not updating courseware. In the real world of real people spending real money to learn ethical hacking and advance their careers, learning in an environment with the latest OSs with the most recent types of attacks is the only way to show real value. I also feel that it indicates a vested interest by the training company in their students when it cares enough to make the investment in creating new courseware and labs to keep up with the times. 7Safe has accomplished this task in spades.

Each carefully plotted exercise in the well-designed lab not only had clearly marked starting points for what VMs had to be on and when, but also provided was the exact step-by-step commands needed to accomplish a given task. Now I know what you're thinking. This is simply spoon feeding the students. This is true to a certain extent. But for almost every exercise, there were 'Extra Time' portions for those who were more advanced and/or finished the exercises ahead of the class. So Jerome even thought of that. In a post course interview, he was also quick to point out that this strict structure of the course made it easier to offer the course anywhere in the world and eventually online with a very similar outcome regardless of instructor. Either way, with Jerome's forethought, his creation of the CSTA v5 felt more like a novel than a collection of short stories.

Although the course is clearly up-to-date with hands-on exercises second to none, I must mention another CSTA fact as I had done earlier in this review. 7Safe states, 'The course is therefore suited to system administrators, IT security officers and budding penetration testers.' Therefore, it must be made clear that this is not an advanced pen testing course. The amount of coding presented in Section 5 is about all you'll get. It's not necessarily a good or a bad thing. It just helps determine the proper audience. But if you do fit into their descriptions as to the expected student, then you can't do much better than 7Safe's CSTA.

Everything isn't rainbows and ponies, though. So here are some places where I feel that the CSTA v5 course can improve:

### 1. Making a Business Case for Ethical Hacking &ndash; I felt the class could have done a better job with emphasizing the

business aspects of pen testing. This wouldn't take much more than the editing of a few slides and a bookending of the course with the discussion and reiteration of the business side of things at mixed intervals during the course, but it doesn't do that currently. Jerome makes a few comments here and there, but I felt it wasn't a big enough commitment. We preach time and again how IT needs to embrace the business side to justify the expenses, and I feel strongly that this must also be true for security in general and ethical hacking more specifically.

2. CTF &ndash; Another addition that would have been nice in order to wrap up all of the newly learned skills would be to have a Capture-the-Flag exercise. I understand the time constraints in a four-day course, but a few extra hours could have been easily made up by maybe starting a little earlier and ending a little later each day.

3. Exam &ndash; The exam wasn't too difficult, and the grading scale leaves room for criticism. Again, I understand the reasoning behind it, but it still leaves that room. At the time I took the course, there was no practical portion of the exam. This will be addressed with a new level of certification called CSTA+ which is currently in the works. I'm not sure when this will come to fruition, but this is definitely a step in the right direction not only for the credential itself, but also for the student looking for a degree. Aaaaaoooooooooooouuuuu! I hear the werewolf crying out my name!

4. Not on the US DoD 8570 List &ndash; This is not a game changer, but if this credential is to really make inroads in the United States, this is a must. It still has the added benefit of being eligible for college credit. Editor's Note: In a post course interview, I understand that qualifying for the 8570 is in the works. Good choice 7Safe.

5. Expanding (Good & Bad) &ndash; 7Safe is following the Microsoft model with the licensing of their courseware. So in addition to it also being available currently in England, Ireland, Scotland, Cyprus and the US, ATPs from more countries are sure to join their growing family of training providers. This will be great as the number of certified professionals will increase making the credential more known and thus more valuable. The downside is that you're going to run into an all too familiar situation, where you're not sure who the instructor will be. As mentioned earlier, the core of the course, the lab and exercises, won't vary between accredited training providers. Also, in the post course interview, 7Safe shared with me their selection and training process of new trainers, so it looks promising. But this is a question that only time can answer.

So I assume the question that most of you want to ask is how does it stack up against other courses? There are numerous courses out there of varying popularity utilizing different delivery mechanisms, so I'll stick to comparing the CSTA course to 2 live, in-person, instructor-led courses offering a certification. CEH by EC-Council is the most widely known ethical hacking certification. I feel like the CEH course, even including the latest version 7 released earlier this year, is now behind the curve. Although they now have information on newer OSs and techniques, the course, by their own design, is meant to be encyclopedic. That's all well and good if it is an actual encyclopedia you want, but the best-of-breed approach taken by pretty much all other training providers offers the best utilization of your time and thus your money. Hands down, CSTA is a far better course than the CEH. How about SANS GPEN? I'd say this is a tossup. Here's how I see it. GPEN by Ed Skoudis is a very well done course. It deals more with the business aspects of pen testing and covers more of the overlapping topics of wireless and web app security. It also has a pretty cool CTF on the last day. On the other hand, it is 2 days longer, costs more and the exam is not included in the price nor is it taken during the 6 days of course time. With the CSTA at approximately \$3000 per course, exam included and fewer days of travel and expenses, CSTA wins out on price. Using a boxing analogy, I think pound for pound CSTA is just as strong as GPEN, but with the 2 more days of the course, GPEN is in a heavier weight class. So if you're looking for a more focused, inexpensive, shorter course, CSTA is for you.

And what about me and the corpses of ideas about college degrees come and gone? The trip was exciting, the course was memorable and the dreams will have to remain just that, dreams. But dreams can become reality, and one never knows what the future holds. Having a degree has not held back numerous successful people around the globe, and neither does it affect my ability to pass CSTA with Distinction, write this review or become the creator and editor of an online magazine not to mention husband and father. All I can say is that I'm glad it's not a life or death situation, and I'm happy it's just a story. I've offered up mine. Now the rest is up to you.

Then again&hellip; maybe it's best to stay off the road, remain in the warm confines of your neighborhood pub with a firm eye on the candle-lit pentangle, and pray. Aaaaaoooooooooooouuuuuuuu!!!!

Donald C. Donzal

Editor-In-Chief

The Ethical Hacker Network