Nox (00:00):

I'm going to be talking about my career, my journey into cybersecurity, how I got into technology in general, because I have some interesting things around that that I have not really spoken about in the past. So that's going to be quite interesting to talk about. But for those of you who don't know me, my, pseudonym is nox or nox cyber. However, you may know me as on LinkedIn, as JJ. I've been in security for roughly around four years now, but I've been in technology for much longer. So my journey into technology was quite an interesting one. So I wasn't actually educated. I was homeschooled for quite a lot. So I messed around with computers quite a lot because my dad was actually a Unix engineer. Which is quite interesting because he taught me most things, most things I know about computers now. However, when I was at the age of about seven, Yahoo was the prevalent search engine then and when you're a kid, you're very curious. I searched out about how to,

Nox (01:11):

How to use my dial

Nox (01:13):

Up modem to hack. That's how basically I'm showing my age there. But, I learned how to kind of mess around with my dial-up modem and make international calls, which would charge the other caller. I was sat there just doing it as a, as a prank all the time. And I got a big slap on the wrist of my parents when they found out when I was doing it.

Nox (01:33):

So, my passion

Nox (01:36):

for technology grew from then, at the age of about 13, I am quite curious again, and I got tied up with some of the wrong kind of people and I was doing some very naughty things on internet. I was doing stuff like, defacing websites and DDoSsing, again, I, you know, very much regretted that, however, it did kind of lead me on to my next, phase, which, for me, it kind of pushed me towards joining the forces. So around 2011, I decided, I'm going to join the forces and I managed to get into the Royal signals. This was actually the first time I actually went to anything called a school. So I went to the Royal school of signals and there, I learned about technology or learn about network communications. So I like communications all the good stuff. And then I unfortunately got discharged because of an injury and I then moved on to, I was in a quite boring role, moved into being a first-line, support analysts, Lockheed Martin. It was a very weird environment. It's one of those environments where everyone's really, really military and that's coming from a guy that was in the military, but they were too military for me.

Nox (02:55):

It was quite an interesting place to work. Didn't enjoy it.

Nox (03:00):

So I left and this is where my kind of journey to cyber security began because while I was working in Lockheed Martin and don't know if anyone recalls, but in 2017, there was the big WannaCry attack. And when the WannaCry attack took place, they needed somebody from the support desk to pick up the Slack and then make sure all the machines are patched because there's lots of machines that will be had like remote users back then. They need to come in and out to make sure that the machines were patched. And as I was, as I was searching for the relevant patches for these machines, I was coming across cyber security blogs. I was starting to learn that actually, this is actually a real kind of tangible career. I didn't know about it then that hacking was a career. So I dived into it and I started to learn more about it.

Nox (03:50):

And I started to get quite a friendly local recruiters. When I left Lockheed Martin, I, I had kind of done it quite hastily. I kind of just said, well, I'm leaving, but I didn't have anything. I didn't have any backup. I was like, Oh, okay. What do I do next? So I talked to my local recruiter and he said, Oh, I have a graduate, role. But it's a SOC analyst graduate role. You don't have a degree. So for me, I was just like, can I at least try, could you put me forward? He said, look, do you know what? We'll, I'll, I'll put you forward. But, I don't think you're going to get it basis on the basis that you don't have a degree. I was hanging onto my phone. Like I really want that call. I really want that call.

Nox (04:33):

I still remember I was sitting on the beach, with my phone in my hand. Cause I was expecting a call from the recruiter and recruiter called and said, look, they want to bring you in, but you're going to have extra stages. At your interview stage, I said, okay. So I went to my first interview and they sat me down and they gave me a computer and he said, can you write an email to this executive? Who's not technical to try and resolve his problem. So what they're trying to test for is your soft skills. So I written the email and I said, Oh, that was very, very good. They didn't give you too much feedback. Three or four days later, I got another phone call and they said it went really well, but we want to bring you in for another two interviews.

Nox (05:21):

So they brought me in for this interview and the CTO sat in the chair and he started grilling me. He was throwing all these questions at me and all these technical questions I was doing really good. Then I remember at one stage I messed up on the question and I was thinking, I've not got the job now. They were quite blunt about everything and I felt, you know, I've done really bad here. I don't think they're going to hire me, but that same day they called me and offered me the job. Now, at this point, I didn't really have any certifications. I didn't have security plus I didn't have anything. The only certification I did have was a BTech in technology. So just sat there at a desk. They went is a SIM tool entree, and I was just like, Oh God, what do I do?

Nox (06:12):

So it was like trial by fire, learn security quick as you can on the job. It was a very interesting scenario. That's when I started, spending all my evenings learning network plus I still remember, I still remember sitting there with a note pad and pen doing sub-net and by hand, hours and hours, hours, just to get used to it, just to find out that I didn't actually really need it because we have some calculators, it was just more for a test. And then I moved to, carnival. So carnival cruise lines. That was really interesting, because it was very unusual for somebody to move, from a T1 sock to T2 kind of sock work in less than a year. So to speak, it was less than a year and with no certifications. And, that role at carnival was possibly the hardest role because I had the responsibility of taking charge of a lot of the patching taking charge of a lot of the implementation of new processes.

Nox (07:22):

I was on the change control board, so there was a lot more responsibility and I will admit I've winged a lot of it. And, I'm safe to say that I've winged quite a lot of my career insecurity, but it's not without, doing my research without studying. So it does play a part too, if you think you can do something, just go ahead and just do it because you know, the worst that can happen is you just get a little bit embarrassed, but the end of the day, you've got a nice warm bed to go home, to wake up. Tomorrow's a new day and just crack on. And that's the kind of attitude that I had for out my career. And so I went from T1 to T2, within the space of a year and unfortunately COVID came along as we all know.

Nox (08:06):

And it said, you know, you said no to a job said, you know, job gone. So I was made redundant. That's when I found very quickly, I found a new kind of role, as a cyber security engineer that was more around pen testing. So I've done about six months of pen testing there. I think I done six pen, six impenetrable, pen tests, and a couple of web apps. That was very interesting. That was very trial by fire as well. Cause I wasn't actually a pen tester until that point. I was just a SOC analyst. So I moved into pen testing pretty rapidly. So that was good fun, but again, I didn't know, I didn't like the work environment. It was one of those work environments where I, if you've worked in security, you assume find out that if security is in the way of the business, security becomes Blass and it's very difficult to make a change into the business if you're too abrasive.

Nox (09:05):

And today I am now working for, a company called Cyberclan, which I'm now a T2 SOC analyst there at the moment, but I'm doing more malware analysis of malware reversal. So a very interesting role, that's quite challenging, because we we're completely remote SOC. So it's quite a new work environment. And so a lot of our EDR and our SIM tool was all remote or deployments or remote relying, quite a lot of, cloud. That's quite difficult. There are a lot of client calls as well. So your soft skills are very much challenged. If anybody is looking to getting to security, I would say that soft skills has played possibly the biggest part of my career and to this day and then when he's help anyone with it and I want it to make this talk more about community and more about helping people, more about kind of helping people get in and break into the industry.

Nox (10:10):

So I've kind of put together, Nox's top 10, top 10 tips to break into the industry. So if you've got like a notepad, you know, maybe take this down, but if you want me to send you, send you this at the end, just let me know, and I will drop it to you guys. Maybe we could probably pin it in the channel, but number one, networking is important. So growing your network and cyber security is very important because this allows your efforts to reach more people. More often not the hiring manager and with this, you can bypass any like ATS filters that it may have and so if the company is using like, an automatic, applicant tracking system, you can use networking to pass this and get yourself seen by the hiring manager, number two, study hard, but let people know.

Nox (11:08):

So producing write-ups blogs videos that can help draw the right attention to your networking platform. And over time, you're going to build an audience. And this audience is going to allow you to be seen by the right people, again, helping to build that network, get yourself seen by the studying manager, tip number three is study, right. Just because somebody else is doing it doesn't mean it's going to be right for you. This requires you to really assess what current level you're at. What, what kind of knowledge do you have and understand that the kind of next step in terms of your study. Number four, Foundations make the professional, So every three months I tend to go back over my network studies over my security fundamental studies, just to keep everything fresh, just to make sure that my knowledge is up to scratch because believe it or not, and you will find yourself.

Nox (12:05):

If you look back at your more advanced knowledge is built upon your foundation so, keep that fresh and it's really going to help you go far in your career. Five is always pick your first step correctly. You know, sometimes you may not be able to get to that perfect role, that pen testing role right away, and you might need to take a different alternative path to get there to your dream role. Lots of people do this and it may get you into the industry quicker. So that may be something to look at. So if you want to be a pen tester, maybe look at being as junior SOC analyst first, and just get yourself into security and build your network up.

Nox (12:40):

Number six

Nox (12:41):

Is to plan your studies. And I found this is really, really good, especially if you're aiming for a role so basis on your first step or that role, you'd like to go into make sure that you plan your studies around them and complete any certifications that is required for that role. So I find that looking at job descriptions really does help

Nox (13:02):

Identify

Nox (13:02):

Any requirements to get into that role. So you may look at pen testing in your country and you may need OSCP, CRET, whatever it may be. You may need that. So this can help you kind of align your studies to that perfect role.

Nox (13:17):

Tip number seven, make friends

Nox (13:19):

With recruiters. A lot of companies don't actually advertise their roles on job boards. They don't advertise their roles on LinkedIn. Normally they pass them to recruiters to go do the hard work for them. I think I saw, I saw a blog before, about 80% of jobs are not actually advertised on the boards, but are pass through recruiters.

Nox (13:39):

So if you see a recruiter, introduce yourself to them

Nox (13:44):

You know, send them that friend request on LinkedIn and just get to know them and introduce stuff. Because if you get a bit friendly with them, you may be able to get yourself pushed forward. That's, you know, getting yourself

Nox (13:56):

Seen

Nox (13:58):

Tip number eight, and this is a very important step.

Nox (14:02):

Just applying

Nox (14:03):

For jobs, is not enough, jobs are very competitive and you've may have the same certification as most of the applicants is the ones that stand out, they get that get hired most of the time. So using your network and your content in your post hiring managers do snoop around and they may see your profile and see your content above everyone else's, and that can get you into the role. A lot of the roles that I'm applying for now are quite competitive. So a lot of them mentioned my website. They mentioned my LinkedIn content and that helps generate conversation so we can help them understand and know you better.

Nox (14:42):

Number nine is also really important. So most of these are really important, but this one's very important as well, but soft skills are very important just because you can root a box does not mean you can tell a client how to, how you did it and how to produce a report as a pen tester, especially your report is your product. It's not your testing. It's the product that you produce, which is the report. And your reputation can rest on the quality of your reports. The soft skills are something that not, not just pen testers, but all aspiring security professionals should invest in as well as their technical skills. So place an emphasis on soft skills. Number 10, you know, you are going to fail. There's going to be times where you fail, but just make sure that you're comfortable with failing and you can learn from it.

Nox (15:33):

You know, it may not be easy at the start, but when you do start to get comfortable with it, you can learn a lot from failure. There's at one point I applied for so many jobs and I just kept failing and failing and failing. And sometimes it's important to ask for feedback just so you can understand, like where did you fail? Where do you need to improve? And that can really, really bulks your chances of breaking into cybersecurity. Cause I didn't actually break into cybersecurity. As I didn't have a degree, I didn't have formal educational, higher education. So for me, I took quite an unorthodox route. I was, going forward and put myself out there asking the questions, just talking to the people that I could have been working with or I could be working with and just make themselves known to me.

Nox (16:27):

So that's just something that I found was being, being quite upfront really helped me get that kind of visibility that I needed to get into the industry. Once you're in the industry. That's when that's, when doors start to open, after about your first year in security, you're there for life. You start to learn a lot more. You start to learn that there's a lot more roles open to you. I'll just seem to be really comfortable in SOC work. So I always stay there. But I do pen testing as well. So what I do like to do is like to do lots of TryHackMe just to keep my pen test skills up to scratch. And I'm really, really glad to see that TryHackMe are bringing in lots of more blue team stuff in there as well.

Nox (17:17):

So, lots of good that I'm mentoring, I'm following towards the, TryHackMe. I'm like go on TryHackMe. The cyber-defense path is brilliant. So yeah, you guys my tips, I'm going to probably write them up and if you want me to send them to you, I will give you, kind of a sheet that I've done, but if you've got any questions I'm going to start kind of taking them now. Just so I can, you know, if people need to know anything I can and help you with that. Yes, I am British. So yeah, go ahead. Give me some questions. I'm watching the channel.

Nox (18:01):

Okay. Where do you see yourself five years from now? Probably still a SOC analyst. I don't actually know lots of you have gone on, you know, one day you're probably going to be a CSO, but I, you know, I don't really want to be in that kind of like high-level position of leadership. So probably kind of a SOC analyst T3 kind of lead role. That's kind of where I see myself. So making a blog where I post walkthroughs would help get me a job? Yes, and no. So the block where you write your walkthroughs try and make them quite verbose and try and make sure that or explaining the points very well. So they can see your writing ability that will help you, that will help you kind of portray your soft skills to the potential hiring manager.

Nox (18:56):

Well, what was it like going with your friends to take the ring back to mordor? Well, I didn't actually go there, but the hobbits did so sorry if there's any spoilers for Lord of the rings, but you should have watched it by now, but should you focus on cybersecurity as a first role, is it more logical to move to an admin role first then move career? Yes. So if you can't get into cyber security and you find it quite difficult, it's not that uncommon to take a different route, maybe go for junior networking kind of route or sysadmin kind of route that will allow you to gain some relevant experience that can help you move into cybersecurity.

Nox (19:33):

Are you into binary exploitation? Not particularly, more malware, analysis of malware reversal. How important are certs if the job in my country don't really look for them? If you want to work abroad again, that comes to studying where you want to go, because let's just say, for example, you want to move to otherwise, let's say you want to move to, India, CEH in India is absolutely massive. CEH in the UK is not as massive. So you need to really study where you want to go and understand that they have different requirements to where you are. So you probably need to, again, issue your studies around that particular area and see if they do take a prevalence in certifications that can be found with job descriptions. Job descriptions are really good source of information on where there is requirements.

Nox (20:27):

So they may have a particular emphasis in degrees. I know America have a very big emphasis on degrees, UK, not so much. So that's something to look out for. Will experience defeat the purpose of bars we set for skills? Is being overqualified helpful? With lots of certs ? Now that's a double-edged sword. So being really experienced with lots of certifications is a good thing. They may be looking for very particular certifications or they may be looking for somebody with very particular skills because being a master of lots of different things means you're not going to be well. You're not really going to be well-versed in these lots of different things because skill fade happens and you start to get focused in one area. So I'm very focused on the kind of blue team side. So I like to kind of just focus on one different area and make sure that I I'm really qualified in that area. So I'm hireable in that area, but if you kind of do like, you know, you know, jump from OSCP to some malware analysis certification all the way to, you know, blue team certification, if someone may have that kind of emphasis on blue team, but you have all these different certifications everywhere, they may not want that. They may want somebody that's very relevant in that kind of industry in that, not that industry, sorry, in that skillset,

Nox (21:57):

When you take someone's interview, what's the first thing you interviewed, you must know and understand?

Nox (22:04):

When I look when I'm interviewing people, one of the things that I really like is passion. So if they have stuff like lots of like, so, you know, I'm this rank on TryHackMe, I'm this rank on this, or I've done this extra course that shows to me that they're passionate about the industry. And that shows to me that they've got a willingness to learn off their own back. That's something that is quite valuable to a hiring manager, because it says to me that they can work on their own, they can work autonomously, which is really important in the industry. So just say like everyone's off sick one day. I know that in the business in good hands, because the analyst can research and learn themselves. So that's one of the things I look for. Mentoring, you mentioned mentoring. Do you think finding your mentor is a good approach getting industry? Absolutely. Because you can use that mentors connections to help build your own network to the right people. So that mentor might may know lots of CSO's that are currently hiring. So you do have the chance to get yourself a mentor. I recommend it. Can you teach us some British? Do you know what I can barely speak British myself.

Nox (23:24):

I'm

Nox (23:24):

In second year of college and I'm considering a cyber security path, but I'm a complete beginner in this area. What's the best way to start? The best way to start is with the foundation. So your networking, your computing, your security fundamentals, build your foundations first and you know, another selfless plug here, but TryHackMe. Do have really good rooms. The

Nox (23:46):

Complete beginner series is a good way to start as well. How would you recommend gaining a mentor? So there's lots of different platforms out there. One of the ones that I'm a part of quite actively is the cyber mentor dojo. I can leave some details if people want to know more about that, but just so everyone knows that's not actually my project. I'm just quite heavily involved for it as a mentor.

Nox (24:13):

What are your views and company bonds?

Nox (24:15):

I'm not too sure. Sorry, I'm just reading one of the posts. So I do get this question quite, quite a lot about, there being less cyber security jobs in India. It's normally the big consultancies that hire in India for the cyber security roles. So maybe looking at some of the, the, the big consultancies will be a good place to start.

Nox (24:43):

Okay.

Nox (24:46):

I'm thirty years old and an engineer engineering project control manager. I'm looking to get into the industry, just completed a bootcamp and doing security plus prep, how can I translate my existing skills in cyber security?

Nox (25:00):

Security is a mindset. Security is something that we can do, but we don't know that we can do. And I'm going to explain, so let's just say you're a network engineer. You can build a network, you can figure a firewall. You can add devices to this network. What you don't know is that, you know how to do it securely. You know how to connect these devices securely, you know, how to configure this firewall securely with best practices. So it's just applying that security mindset. So you already gained skills. So if you were a project control manager, you've got people skills, you've got leadership skills, which are very crucial for cybersecurity, I may add and they are very needed, but you can also look at what you've done and say, how, how have you done that in a way that increases the security posture of the business, and then translate it that way. That may be a way that you can do it.

New Speaker (25:51):

How should I manage cybersecurity and studies, I am 15.

New Speaker (25:58):

I would say it, you know, don't burn yourself out at that age or any age, don't burn yourself out. Just take it a bit at a time. You've got plenty of time to do your studies. So just take it very slow. Don't burn yourself out and remember sleep is important. So don't find your self up at night on your keyboard at God knows what time because sleep is very important.

Nox (26:22):

What are some good cybersecurity roles are interesting to you, that seemed harder to fill because people go to flashy pentesting first?

Nox (26:29):

So there is actually a bit of a drought at the senior kind of blue team level and this is because everyone seems to go from junior SOC to pentesting and then senior SOC analysts and senior CERT analysis are very difficult to come by and you in the UK, we're seeing now that this kind of senior blue team level, the pay is just going up and up and up because there's such a drought at that level. So maybe you look at some senior, blue team in kind of level and then see what they kind of earn in your country wherever you may be, because there seems to be quite a drought in there, not just in the UK, but worldwide at the senior blue team level.

Nox (27:12):

If we want to get in the computer science field, particularly cybersecurity at the moment, what would be a good foundation to go for for a degree?

New Speaker (27:20):

So I'm not too sure about degrees in the UK because I didn't have a degree, but I would always say networking, security fundamentals, and computing fundamentals are really good place to start. So you've got your A plus your net plus, and your sec plus, that's going to help you build your foundation. You don't have to take the certifications. You can just do the courses for the knowledge.

Nox (27:42):

OSCP versus CEH first cert for university student?

New Speaker (27:46):

Now OSCP and CEH are vastly different certifications. So CEH is more comparable to security plus, I would ask the question, what do you want to go into that should be your kind of guideline on what you want to do. So I would say OSCP, if you want to be pen tester, that's a certification you want to go for. If you want to be a SOC analyst, you CEH should probably be more aligned to being a SOC analyst in my opinion but it really depends on your country as well because the CEH may not hold any weight. And in some places OSCP doesn't hold weight. It really depends on where you are.

Nox (28:26):

How can you get someone to give you a chance, even at an interview, if you don't have any relative experience?

New Speaker (28:31):

Networking, networking and networking, show people what you're made of, post content that shows your ability and your skills. So people can see that and that's a very important thing to do.

New Speaker (28:45):

What certification is the most valuable in your opinion, when it comes to buying exploitation to better assistant development, security in mind?

New Speaker (28:50):

I'm not too sure on that. So I do apologize but I'm sure potentially I know a very good exploit zero day developer who may be able to help you with that question so I could always ask him, we can connect after this and I can get that information for you.

New Speaker (29:08):

Being a developer and work in it for over 16 years, I am finding it really hard to enter cybersecurity and pen testing since most companies that ask for 3 years experience in these specific roles. Is it a broad issue?

New Speaker (29:20):

Yes, it is a broad issue and I've spoke to many companies in the UK about this and it is a worldwide problem. Lots of companies don't understand cybersecurity so what they do is they copy other job descriptions just to get a kind of feel for what's out there but what they don't realize is that there's people that could do this job, which don't have that experience.

Nox (29:42):

And we're starting to see that kind of gateway drop. So we're starting to see people hired people at the lower levels, just based on skills or based on what they know so it's a very slow process, but it's starting to happen so you should find that you'll be able to break in a lot easier in the coming years but if you're having any problems with that, please just let me know and I will give you my best advice to try and help you with that. Is security plus a good start? So to start with the cybersecurity, absolutely really good foundational knowledge.

Nox (30:20):

I basically want to go to work what you're doing right now, Malware analysis, reverse engineer, any kind of roadmap you can help out with. So I would say if you want to go down that kind of role, I would say SOC analyst is the kind of the, the place where you want to start, but she wants to start seeing how people are alerted to these kinds of, this malware, how they respond to it, how they kind of remediate these problems that are caused by malware and then branch out from there in terms of certifications. I'm not too sure what kind of certifications are out there for malware analysis and reverse engineering. I'm sure there is plenty out there. I think Elearnsecurity may do some, I'm not too sure.

Nox (31:01):

What'd you say for those actively applying for roles and positions, someone like myself who are solely search and work experience, how should we approach these applications that favor someone with a degree I've been told over and over and work colleagues that the recruiter is going to waste someone with, if the recruiter, weighs you over somebody else? Just because they have a degree, I would potentially say that that recruiter is not doing a very good, good job, purely because there's lots of recruiters out there that know that just because you have a degree does not actually mean you possess those skills. It just means that you've done a degree in that area. Good recruiters will really know, if you have relevant certifications, you probably will possess the skills that they require, or wish you've done, maybe a junior networking role.

Nox (31:51):

You would probably know how to secure network, how to build a network, how to identify vulnerabilities in networks. So, the good recruiters will look past this and the good companies will also look past this kind of requirement. It's just a case of getting yourself known out there. So if you're actively on LinkedIn, start connecting with different recruiters and just getting some fields out there. So there's plenty of times where I got turned down because I didn't have a degree. There's plenty of times where I've made all the way to the end and decided where I didn't want the job because it wasn't for me. So, you know, it happens, the, the kind of industry is starting to wake up now to realize that there is a lot more out there than just degree holders. There's massive pool of talent that they can tap into and they're starting to do so. Is there a possibility that many remote

Nox (32:40):

Pen testing roles would become opening soon? Now you won't see pen testing roles commonly at the junior level for remote. Normally for junior levels, they want them to be guided, so they're potentially going to be onsite. So that's going to be very rare, especially given the pandemic is going to be even rarer, and they're going to be very competitive as well.

Nox (33:02):

I know

Nox (33:02):

Plenty of recruiters that can help you with that kind of getting visibility into what kind of roles are available. But I think pen testing, remote pentesting roles at junior level are, you know, very, very rare indeed. That's why I say to people maybe take an alternative route for now, especially given the pandemic, just get yourself in the industry and worry about it a little bit later, or just keep hammering away, you know, meshing recruiters, getting yourself seen, Sorry, apologies for the silence. I'm just trying to read and my abilities to read. Isn't so good. So where do you get your information from, for malware analysis? Actually, I have a senior malware analyst in, where I work and I kind of pester him for stuff. So once I get some more good stuff from him, I'll post it in some of the resources channels

Nox (34:13):

Any idea about the cyber security job trend in Australia? like what would be the minimum qualification to land an entry level cyber security role? Well, now they have a very weird situation that I was talking to really Australian recruiter and cybersecurity. So his name was Mitchell Carter. He's really, really good in terms of recruiting for cybersecurity roles in Australia. And I know that they place a heavy emphasis on some certifications. I'm not too sure which one it is. So I may need to clarify with him, but he may be a good contact to reach out, to and find out some more information. If you had the opportunity to move to another one of the five eyes countries, which one would it be? Is Canada part of five eyes? I think they are, Canada would probably be a place where I'd want to go, or America just because I love food and I love donuts and pop tarts. So there's lots of Pop-Tarts and donuts over there. So that'd probably be one place to go.

Nox (35:11):

What do you

Nox (35:12):

Think of DevSecOps as a beginner? Any tips I've seen this as Greenfield, so DevSecOps, it's not really a thing as such. It's more of a strategy, a business strategy, in terms of developing applications securely, commonly we find that they claim that they have DevSecOps, but it falls by the wayside very, very quickly. It is a very, is a growing field and there's lots of people making these DevSecOps roles. If you want to get into that, you probably want to start reading a lot more about it in terms of lots of businesses have different ideas about what DevSecOps actually is and what they hire for. I would say, look around dev ops and see what they're asking for in terms of dev ops, and then try and apply a bit of a security mindset onto that. So maybe get some security certifications as well as doing your dev ops as well.

Nox (36:03):

Okay.

Nox (36:04):

What would you say after doing A levels, a degree in computer science or typically undergraduate, which ones better to go for?

Nox (36:11):

For grad school for computer

Nox (36:14):

Science and then masters in cybersecurity, or does the degree even matter if you have things like OSCP? A degree doesn't matter in the UK. To be honest with you. You can find a job pretty easily without a degree. I've seen many people do it. I've seen people even do, like myself, no certifications in security. I move over to the industry.

Nox (36:32):

It's all about, relevant experience as well.

Nox (36:35):

Well, so let's just say that you've worked in IT for four years. You already know quite a lot about technology at that point. So you're going to be employable in terms of security. It should about having some, maybe some certifications to back it up. So security plus maybe if you want to be a pen tester in the UK, CRT CPSA, OSCP. And I sound like, I'm doing a rap, but that's where you want to go. That will make you employable.

Nox (36:58):

So the degree is not

Nox (37:00):

Going to get you a pen testing role pen testing certifications in that in, in the UK are going to get you that pen testing role.

Nox (37:13):

How can I get better? How can I get a better career in

Nox (37:17):

cyber security and which uni or college? I will say the better career, there's kind of many ways you can approach it. So yes, you could potentially do a degree and then, you know, bulk bolster your credentials, or you could potentially,

Nox (37:31):

Keep doing certifications around your level and build up your network and get a bigger network and then move into other roles because of the people, you know.

Nox (37:44):

Ah this question, bug bounties. So all I don't rate bug bounties at all. I think bug bounties are a way for companies to get cheap labour and just basically turn around to people and say, hey, look, we couldn't find the bug here. We're not going to pay you, but at the end of the day, bug bounty is a very good experience that you can put on your CV, but

Nox (38:08):

Wouldn't waste too much

Nox (38:08):

Time, you know, spending loads of time finding a bug that you might not get the pay out for, because at the end of the day, that could be useful, purely more studying and bolstering your own career and getting that salary, or even, you know, making your own consultancy and actually doing a pen test for that company instead of, doing a bug bounty. Cause sometimes I just don't know, what it is about, I just see something very morally kind of wrong bug bounties. If it's something you're doing, please put it on your CV because people will want to know about it.

Nox (38:45):

Okay. Any more questions as far as getting ourselves out there, do you find blogs to be the best option or are there more creative forms? Yes. So when I tell Pete, when I tell him I mentees to get on LinkedIn, I say, make a video, introducing yourself to people. This is going to get more views is going to let people know what you're about and you know, who you are. Yeah. Podcasts are really good as well. I love listening to a good podcast. So when you, when you're trying to get yourself out of there, yeah. Get creative, get yourself out there, which college or university did your cyber security started with? So I didn't actually go to college or university. I was home-schooled and a little tiny bit of public school here, but I wasn't in any higher education. That's why, you know, I'd like to give back to people that don't have that kind of opportunity or they're struggling to break in at that level because is possible, is very doable. And there's just different ways you have to go about it. Sorry, I'm just trying to find some more questions.

Nox (39:52):

Apologies if I've skipped over your questions. I do apologize. so any tips for beginners to get started? Just get started, you know, just pick up network plus download packet tracer, mess around with packet tracer for a bit, learn a bit networking, bit of computing, it's really going to get you far, get yourself and TryHackMe, do some rooms. That's really going to push you forward. When I'm in interviews, I love to ask people about their TryHackMe experiences, because for me, that's a talking point and I get to learn about what that kind of person knows, what they've done. So that's also something to bear in mind. So I'm just reading your question, So, the only experience you have is CTF's, which don't count and vulnerable machines on TryHackMe they do count. So I always put at the bottom of my CV, any CTF that I'd done and what position I came or rank on TryHackMe or any kind of like completion certificates that you have.

Nox (40:58):

But get yourself out there, get yourself on LinkedIn, get yourself known, talk to recruiters, tell them what you've done. Cause if the recruiter doesn't know that you've done, that they can't tell the client, or if it's not on your CV, the person won't know that you've done that. So if you think that it may be relevant, get it on your CV, get yourself known, Any advice for making your CV?

Nox (41:26):

That's going to be more for recruiters in your local area about what the CV should look like because every kind of different, you know, it depends on where you are. So in the UK, we like to keep the CV relatively short. Anything more than I think is about two pages. It doesn't get really seen, they don't like long text and stuff like that. But again, it depends on where you are on how they like your CV to be formatted, but my kind of rule of thumb, is let's keep it to two pages, keep it relevant. If you think it should be in there, put it in there.

Nox (42:07):

When recruiters pick the person for the job. Is it the most whoever that has the most certs wins? Absolutely not. Best one wins as Paul just mentioned there, the best one does win. I've interviewed someone that had OSCP says they have CEH as well and they had a degree in cybersecurity and we didn't pick them purely because they had no soft skills. They weren't able to talk the talk and it was very difficult to kind of work with them and kind of like get the answers out of them. I mean, we asked them a very basic security question and they kind of explained it in a very, very long-winded way. It didn't make sense in the end and we had this, the other guy that came in and he had like, literally nothing, and he had like security plus and he was brilliant.

Nox (42:51):

He was excellent. So we picked them, if there's no more questions, think it'd be a, quite a good point to end it there guys. I'm going to stick around for a bit. so I might jump into one the general chat channels, or stick around more general chat and answer any further questions, but thank you everyone for listening. Thank you to TryHackMe for this opportunity to talk. So I was just reading the chat, but thank you for this opportunity and thank you everyone for attending my talk. I hope it's helped and hope you have an easy time breaking into the industry. I really am thankful for this and thank you all for your support. Have a great evening, morning or afternoon wherever you are and take care.