Dhruv Verma
LinkedIn: https://www.linkedin.com/in/vdhruv7/
Please check our study group workbook for previous interviews.

1. How did you get started in Cyber Security and what advice would you give a beginner?

- Very good question. I was always interested in “hacking” and finding my way around certain restrictions on the internet. I got started with cyber security by interning at a security consulting firm during my undergraduate years. My advice:
    - Don’t get overwhelmed. This is a vast field and it can be easy to get lost.
    - There are different aspects to professional cyber security which are covered overall by the following security positions. Take your time to look at the different kind of work, and get into what interests you:
        - Security Engineer
        - Security Analyst
        - Security Consultant

2. What is your specialty in Cyber Security and how can a student pursuing OSCP certification get expertise in it?

- I work as a security consultant at NCC Group, where we perform a wide range of penetration tests. Personally, I specialize in red team operations and network penetration tests. OSCP is a great way to get into network security, which is the first step in becoming a red teamer.

3. What is your top advice when it comes to passing OSCP or similar certification.

- Good question. I suppose i can split this into two overall things:
    - Understand what the certification is trying to teach you. In the case of OSCP, it is all about enumeration, exploitation and escalation. However, the main focus is on enumeration. ENUMERATE, ENUMERATE and ENUMERATE some more.
    - The final exam for the OSCP can be quite stressful. Planning your exam time can play a MAJOR role in if you pass or not. There is a high chance that you will get stuck on a box, or go down some weird rabbit hole. Personally, I scheduled my exam to begin at 4 PM on a Saturday. That way, i have a good 8-9 hours before 1 AM, where i can take a break and get about 4-5 hours of sleep. Wake up around 6 AM on Sunday and still have the whole day ahead of me to complete my challenges.

4. What is the best book or tool you can share to illustrate OSCP challenges

- Honestly, I did not follow a certain book. My best advice would be to read OSCP blogs, some of those point out great sources, great enumeration scripts, tricks and techniques.
- Hack the box is a great way to know what's coming.
- Do CTFs. Get into the CTF mind set.
- Overall, you need a set of tools to be able to enumerate a linux OS and a Windows OS. You need as much information as you can get.

5. What is a life hack that you'd like to share? Where else in your life do you feel like a ‘hacker’?

- Great question. I feel like my answer is “Everywhere”. Your thinking of everyday actions changes when you are a hacker. From ordering food online, to talking to the customer service over the phone, to someone asking you to email them your credit card information. I can’t think of a certain example as of right now though. Just to be clear, the word “hacker” is sometimes misunderstood to be unethical, and that is not how i mean it in this sentence.

6. What is the biggest mistake you have ever made and how did you recover?

- Two points:
    - OSCP related: I did not take any screenshots during my BOF machine only to realize that I had to take one for every step of the way. Luckily I had enough time to redo . Amateur hour, right?
    - On a very difficult red team engagement, I finally had access to an employee’s email (after tons of social engineering, forcing their 2FA, etc). For some reason, I thought that they would not detect mail forwarding rules.
        - I tried to send an email to IT from the employees email asking them for a new VPN profile with a forwarding rule set to forward all replies to me.
        - Immediately got flagged and the employee got a huge red alert on their email and phone.
        - Since i had already social engineered them before, i could get a handle on it and got away without them reporting it. But it was a very close call.
        - The employee was a security engineer. If they reported me, my life would have become exponentially difficult from there on out.

7. What is the most difficult hacking assignment you’ve ever done?

- Almost every new project, in some way, turns out to be the most difficult hacking assignment i’ve ever done. I can think of one such instance where I was on a red team engagement with a very strong client. They had strong host based

defenses. Network defenses, a blue team watching our every move. We managed to gain a shell on their boxes by social engineering an employee, over a phone call, to give us their VPN profile. From here, we had to fight off a very strong EDR, which reset credentials for all power users every day. It took us 2-3 days before we owned their entire network.

8. What's your work routine like, and how do you manage keeping up-to-date while staying on top of your work?

- My work in itself involves a lot of studying and researching. Every other week I am put up against something i've never heard of. The first few days go in studying and learning everything about that piece of software, and then, breaking it. Overall, I spend a few hours of my day everyday catching up, researching. I also almost always have a personal project i'm working on.

9. How rapidly does your workflow change? I.e. how long from settling on a specific set of tools or methods to altering them to better fit your use case, can you give an example.

- The workflow does not change much. There is an overall guideline as to how we would approach a pentest. However, each pentest is different, and there is not a specific way you can approach it. There is an overall idea about what tools we would need, or what methodology we would need to follow, but that changes on projects. I've had to modify tools such as "Responder" multiple times on engagements to fit my needs. Ideally, never run a script or a tool which you haven't read up on. Make sure you understand what it does, before you run it.

10. Favorite linux desktop environment? (xfce/gnome/mate/lxde/i3/pantheon/unity/etc)

- I use a Mac :).

11. What did you do to practice your weak areas for OSCP? (e.g. BOF, Priv Esc., etc.)

- Hack the box is a great way to train. I mainly practiced on any CTF I could get my hands on (network related). The OSCP machines in themselves are a great practice. Try to find your way through them without attempting to google for hints. My weakest area was Windows Priv Esc. It is also a great practice to read up on blogs, follow other pentesters, and know the right way to enumerate. Priv escs become easy when you can enumerate well.

12. What is the hardest part of the OSCP Certification or getting an equivalent Certification?

- OSCP requires dedication. In my personal opinion, this isn't a certification you can just start - leave for a few months - and come back to. You need to be open to lots of reading, lots of head scratching, uncounted rabbit holes. It may take days or sometimes weeks to crack a box, but you need to keep going with it

with a strategy in mind. On the second hand, you need to plan out your exam day well.

13. What non-technical things do you do in your spare time to unwind or generally step away from the screen a little bit?

- I have been a gamer for a long time (even professional back in the day), but that is not very “away” from the screen. I spend my team go-karting, riding my motorcycle or street racing.

14. Do you hack professionally? If not do you have any advice to help transition from hacking as a hobby to professional work?

- I do. They are a little different, in the sense that when you’re getting into it professionally, your job is to provide value to the client (again, depending upon what role you choose. I am talking from a consulting mind frame). Professionally, your job is not to go in, destroy everything and walk out. Our job is more to make the world a safer place. It is important to know why something is broken, and how you could go about fixing it (not by knowing exactly what code you’d write, but more around why the problem exists).

15. What would you tell yourself if you could go backwards in time one day before you took OSCP?

- I’d tell myself to relax. I was way too stressed.

16. How did you stay focused enough and maintain enough endurance(and tolerance) of a 48 hour exam?

- I did not sleep the 24 hours of my exam. Just the excitement/stress of it all had me all pumped up. Without being super repetitive about what i say, i believe it is all about how you time your exam. You have to be careful to not let yourself feel down when you are unable to crack a box, and you have to be careful to be well rested before your exam begins.