Abstract Security

1. Can you tell us who are you?

- Yea man, well kinda. So obviously we all use handles in this space my handle is paint parrot, its not spelt how it sounds as I use a little leet speak when I type it. Also I vary it too keep some air of mystery around it. But feathers aside, who am I? So in a nutshell I am a former member of the British Army, a hacker, a red teamer, social engineer and just someone who always gets into places they shouldnt be. anything more than that isn't really public.

2. What is your job ? How would you describe it?

- What my job now, or my job on the Darknet Diraies epsiode? Then I was doing the murky world of corporate intelligence, kinda. I guesss it was more Human intelligence, source recruitment and handling. But other than the episode I can't go into much unless you have direct questions on things. So feel free to have a think and ask more dude. But now I work for a cyber security consultancy, so my day to day is pen testing and red teaming. I'll be honest the pen testing is bread and butter. The physical intrusion and social engineering stuff doesnt come around as reguarly, but it's better like tghis more stability day to day you know. Like red teaming is sexy and a great area of info sec, but in the UK it is not as huge as it is in US for example. There's a lot of factors involved cost, shared office space so technically would break the law to gain un authorised access to communal areas shared by companies. Lot's more red tape.

3. What made you learn about security ?

- Well I guess with the military and since then there has always been an element to security. Be it the senisitive nature of the work I did and the information I handled in the miltary or after leaving and falling into the physical security world before the intelligence industry. thinking about it whatever I do or have done has a large ammount of security involved. I guess thats why I am pretty well rounded and fit into the red team or hacker space very well.

4. What would you recommend for someone to start learning about security

- Shit. What a question. So I guess first thing is first pick an area that appeals, you know. Security as a whole is all encompassing, its multi spectrum. It dominates the physical and the cyber space. But both rarely from a companies perspective go hand in hand. What I am trying to say is look at your own strengths, use that past experience and see where it translates. Not everyone is mentally able to social engineer targets, same as not everyone can hack secure enviroments. Play to your strengths and intrests, if you are pasionate own that, passion goes a long way in this industry.

5. What set of skill does one need for a job like yours ?

- Errrm I would be honest I do not feel I could answer this one. I have imposter syndrome on a daily basis, there is always people better than me. Be humble be willing to learn.

6. What set of skills you look for when hiring ?

- Well I do not get involved with hiring as such, but when I was running cover surveillance teams etc in the past area, it was all down who they knew and reccoemended them. I would also arrange to meet them but have a couple of my team surveil them to the meeting to see how they carried themselves and get an idea of who they were. It was very much would you work or not depending on the task. You want the ultimate grey man, someone who doesnt stand out or have a pressence. with the social engineering side its similar. they need to not stand out and only project whats useful for a cover or pretext.

7. Which resources do you recommend for Physical Security?

- Just understand it, how security is implemented. why? Defence in depth and the weaknesses regardless. Look and take in everything around you. Think like a bad guy.

8. Do you think that it is better to generalize and try and do a bit of everything, or specialize in one area?

- Well once again this kinda depends on your situation and location, so look at jobs, compaines or whatever in your area. try to apply yourself to suit whats local unless you can relocate. Take it now companies will only relocate you at there expense if you are top of your field. Look at it like this, if you live in Silicone Valley tech jobs are everywhere right so it's an easier area to progress into. If you live in the middle of the African bush not so much. Same applies for physical sec or red team. Review where you are and be prepared to move at your own expense. The internet has made the world smaller for sure, but not that small.

9. What is in your opinion more important, right certification or knowing right people?

- Having the ability to do the job and communicate that knowledge onwards. No point being awesome if you cant explain why. Yea contacts and networking help obviously.

10. Do you have any regime of training your skills set? if so, can you share it with us?

- Not really, just mix and talk with people its a hard thing to explain. Just understand your town and surroundings, like really understand. It's a hreally hard thing to convey aside from teaching various inteligence mindsets.

11. What is the biggest success in your career?

- The case in the DD episode hands down. Was a big one.

12. If you could start all over again, would you choose this path again ?

- I think ask me in 15 years, if im broke and living alone maybe not, I got goals right. Look SE has a downside, you become slightly manipluative by nature. thats not always cool.

13. Is there any interesting story from your lab/office/training space
that you can share? I am sure there are many but what is some that sticks
with you the most.

- Thats a listen to DD episode 80 man, there isnt much more I would say outside of that. But yes a lot more went on.

14. Is there any story from your work that you would like to share with
us?

-No comment

15. What is something that you have notice in your field of work that you think everyone should know?

- I wont name names, but there is some people in this space that now thrive on the fame. To me fame prevents you doing your job right. To be a succesful SE or red teamer means the ability to blend in and be that grey man. fame ruins that. My take away is be humble dont pretend to be an expert, stay grey and just take everything around you, all the time.

16. Many countries with less developed security industries suffer from social engineering attacks, which cost them a lot of money. Nevertheless, a common argument given is that ther eare many other issues that need to be adressed before social engineering attacks. How would you respond to
this argument?

- Without researching the statistics so feel free to correct me after this. But I feel like Social engineering attacks are present in every culture or contry regaless of economic develpment. I think all that changes is the complexity of the attack. Like thats Social Engineering 101 right? Make the pretext fit your target audience? I don't want to say that some countries or demographic get hit harder more than others. But take the UK for example the stats im sure will show the ederly are hit more by SE attacks than anyone else, simply due to the technology is new to them. they are used to being more trusting in general. Its a bad area, Se can do some real good in the world and be used to highlight security weaknesses but at the same time some threat actors are comitting the lowest crimes possible.

17. What is something that you came acrosss that is persistant with peoples secuirty ? Or nationstate secuirty?

- You want the honest truth on this... people. People are the one constant. this is why Human Intellegence or HUMINT and Social Engineering will always be viable. People are inherently the weakest link and always will be, it's human nature that is exploitable.

18. What do you look for when trying to manipulate someone ? How do you aproach it ?

- So in the intelligence circuit you have what is called the MICE model, so it's in a simple way human vulnerabilties hard coded into us. Money, Ideology, Coecian and Enviromental / Emmotional. Basically it's somerthing that can be exploited given the right set of circumstances to almost everyone. We don't have the time here to go into all of them in detail. But when you look at a potential target you want to assess what vulnerabilites are present and how you can exploit them, same as a network right. Damn its hard to explain.

19. Is there any story behind your handle P41ntP4rr0t?

- Yea but it is a little lack lustre, seriously there isnt a great story here. So I was getting involved in a few things discord included and it wasn't appropriate to use my real name. So I used a random word generator. that gave me Paint, I thought it needed more and I had just switched to Parot OS as my main OS from Kali so I grabbed that. ThenI realised Parrot OS had a parrot background with a kinda paint splash and that was it, I liked that picture and I used it a few times and it stuck. Is it as cool as some out there hell no, but it came from a need and then my profile grew and before I knew it was too late to change. If I was to change it I would probs go with "ThatGuyD4V3" because everyone knows a Dave right?

20. What is the one thing about your job that makes your heart beat faster?

- I think I got past the part of the rush, that's partly why I made the move into the more technical side of things. I got to a point where I wasnt feeling challenged or that "rush" so I changed path slightly. Pentesting kinda fullfils that but im still missing something.

21. What is one question that you wished someone would asked you, but never did?

- What I really wanted to be when I grow up. No one every asks. I'm older than you might think and in my mind I still havent grown up.

22. What is your favorite part in your work? And what is your least favorite?

- Oh damn I'm not sure. Never really given that much thought to be honest. ask me again in few years.

23. In your opinion, how will the world of InfoSec or Security change in next few years?

- So as security professionals we are behind the curve, like everything we do is reactive according to the threat landscape and current threat actor tactics. If I was a real betting man I would say its the IoT and wearable tech space. Think of it for a second, every person is becoming a walking networkinterconected devices worn and carried on bascially a private LAN. Our whole lives and most senitive pieces of data are held on that, from private images to banking information.

24. What is one myth that you hear constantly, about your work or something related to it, that you want to debunk?

- My big gripe is training companies and the monoply they hold. I get you need a benchmark. But seriousily in the UK CREST is the main certification body and I hate it. The material is outdated and you have to pay to re-sit the same outdated exams every three years. It is all a scam. The industry needs an overhual. Lets be real for a second do the "attackers" have certs? Not fucking likely, so what are them certs really worth? the guys that hacked Talk Talk wer like 14 and from the Welsh Valleys if I remember rightly. did they have CREST or OSCP or CEH? Nope. Is it a good benchmark? I dont think so....

Thanks for speaking with me man. Hope everyone gets something out of this. Laters!

-P41ntP4rr0t