--------------------ABSTRACT SECURITY--------------------
Date:22.04.2021.
Interview: Bill Graydon

NoMan29: Welcome everyone! Tonight we are joined by one and only Bill Graydon!

Bill Graydon: Hello!

NM29: how are you doing Bill?

BG: Not bad, yourself?

NM29: I am doing ok, shall we start with the interview ?

BG: yep

NM29: ok so most basic question, but yet most interesting one, who are you ? How would you describe yourself?

BG: I always have trouble with this question, there's a lot to condense into a single answer! In terms of what I think this community cares about... my background is somewhat varied, I've done work in computer engineering, cybersec, infectious disease detection and anti-money laundering before coming into my current niche. People now know me for various con talks, and running the lock bypass village - I've applied that sort of thing professionally starting a phys sec firm, which I'm running now.

NM29: That is why i said it is most basic one but yet most interesting one. Wow you have interesting background
And just to make it clear for people who might not know what that is, can you tell us what is LBV or Lock Bypassing Village ?

BG: Yes! So if you aren't familiar with what villages are in general at cons... they're like a con within a con, with talks, workshops, etc. The lockpick village is one of the oldest, and others have popped up over the years but none other than LPV did much phys sec, so we started the Lock Bypass Village at DEF CON in 2019. We schlepped all sorts of door hardware, alarms, etc down to Vegas, and set them up and let people try things! Stuff like under door tool, loiding latches, bypassing car door locks, jumpering out elevator panels, etc. Last year we had to go virtual, so made a bunch of games to try to replicate the hands-on aspect.

NM29: this is the link right ? https://www.bypassvillage.org/

BG: yes sir!

NM29: Nice, so you said that you run the physec firm , is that your primary job?

BG: yep!

NM29: Ok, would you like to share the name of the firm in case someone wants to check it out?

BG: For sure - GGR Security - https://ggrsecurity.com/

NM29: Awesome! So you have been to soo many conferences, what would you say is your favorite?

BG: o I haven't been to all that many actually... particularly not in person now that corona has hit. Of the hacker cons, I've done the most with DEF CON, so that's my answer for now but don't read into it that much... I just don't have as much experience with other smaller cons, so I can't say!

NM29: haha ok then. haha ok then. How did you got into security at all ? Did you know from the start that you like that or was that many trials and errors ?

BG: So I started out during my undergrad, which was in computer engineering, specialising in cybersec, which I found to be very interesting. I then branched out into physical in my masters and subsequent work. Physical has a lot more to be "discovered" that aren't extremely in depth on one area like most cyber 0-days are, so that appeals to me.
It was a few trials and errors but I gravitated pretty quickly towards it

NM29: huh ok that is interesting
ok and what job you had to get or to learn to be here where are you right now ?
or let's say it like this
what set of skills does one need to be where you are now ?
and follow up question, tendies or nuggies ?

BG: Hmm... the skills one is a bit nuanced. There are a lot of hard skills that I would say are indispensible, such as risk management, understanding of business processes and how to do criminology research, and some hard sciences: e.g. resistance of materials to different attacks, etc. But those can be picked up on the job, the softer skills are much more determinative: a passion for security and an adversarial mindset are much more core in my view. Our staff are a wide range of skillsets / types - from detail oriented who work with regulatory compliance, to more “bigger picture” curious types (like myself) who do research, scoping, etc. Some are good with people and work client facing, others aren't and don't and that's ok. But the common elements are that passion for security, and for learning. The more people can cram into their brains on the topic at hand, the more effective they are at finding holes in it.
Tendies.

NM29: Yeah ok so big thing is passion for the Security, everything else you can learn one way or another.

BG: That is a good summary

NM29: You said it better :D Do you look for those skills when looking to hire someone?

BG: 100%. But it is competitive, as you'd imagine - everyone wants to be a red teamer - so we have the luxury of being picky with just about everything. But a perfect match skill wise will still lose out to someone with more learning to do if they don't have that passion, work ethic, and enthusiasm.

NM29: huh yeah i see. And what would say is the good resources for Physical Security and Security in general (beside the LBV website) resource where you can learn some of those skills you said are important.

BG: For both learning, networking and kickstarting your career, I can't praise ASIS enough... join your local chapter, network through there, do the webinars, etc. That and reading books, watching talks, etc... what people all do here already! But that only gets you the hard skills - the nuance of what people actually care about, and the difference between how the hacker community treats physsec and how end users do is stark, so working in the field gives you a perspective that's hard to get another way.

NM29: yeah i agree.
and while on topic of learning and experience, the questions i also like is what do you think is more important certs or experience ?
certs without experience ; experience without certs

BG: Experience for sure. Certs can be hacked. Most require some experience, so it's hard to have a cert without experience - most that don't have some angle to them, so piling on a bunch of non-experience-requiring certs will give you a skewed view

NM29: hah yeah i expected you to say that hah, do you have any certs ?

BG: None at the moment. They are most valuable when you need to prove yourself, e.g. applying for jobs, which I haven't needed to do in some time! In my opinion, a lot of them are kinda cash grabby, and maintaining more than one gets very expensive and time consuming. I'll likely get / resume a few as I progress to giving expert witness testimony, where they do provide significant value - that's a few years out though.

NM29: mhm ok that is fair. And yeah i agree that some are more cash grabby
while on topic of skills, do you think one should generalize or focus on one area ?

BG: So I personally generalise, because I like to see the big picture, and I manage a lot of specialists in varied fields - we make it one of our value propositions to be extremely interdisciplinary, to see the connexions between different systems.
That's not to say everyone needs to though. From the perspective of a client / facility manager, there is a lot of benefit to hiring a firm that has a wide range of expertise, but this is critical: they don't care

if the individual consultants they work with are all fully rounded out; so long as the firm overall is. So my answer is "you do you". If you are interested in one area and nothing else, there's nothing wrong with specialising in that and nothing else, and working for a bigger firm where you can just do that all day. If you're interested in a broad spectrum, that's great too, and the interdisciplinary approach will definitely serve you well at a smaller company, or moving up the ranks quickly anywhere.

NM29: huh that is interesting answer.
i like it !
and what is something that you came across that is persistent in the field of PhySec?

BG: Hmm... so coming to phys sec from cyber, and from the hacker community takes quite a paradigm shift. There's an enormous difference in threat models that people often don't appreciate:
* Cyber, your adversaries are all over the world, all attacking at once, and you are subject to the worst of the worst.
* Physical, bad actors can only be in one place at once, and they risk their persons and freedom if caught. So you don't need to defend against absolutely every niche attack... it's a lot more about threat modeling and making business decisions on what costs are justified to harden your infrastructure.

So with that preamble... one thing that's "persistent" is the viewpoint that "I don't care about that attack vector", or "I don't care enough to do anything about it". For many lower level clients, their preferred answer to a lot of vulns is "if someone does that, insurance will cover it". It's a big shift from the hacker community where any little vuln is worth delving so deeply into.

NM29: huh that is very interesting. I mean you come from both areas so you know it best. It is logical that it is that way. Interesting
and what is one myth that you have came across, in your work, that you want to debunk ?

BG: different communities have different myths. The hacker community tends to overemphasise vulns, and the end user community tends to underestimate them. E.g., on the topic of calling a lock "unpickable": we love to bash on anyone who does this, but for certain applications, good locks are "effectively unpickable", in that picking is so unrealistic of an attack that you're better off focussing on forcible, etc. E.g., for extremely high security targets, we don't focus on whether you can get in, but when. If a lock offers a 60 minute delay (as some safes are rated for, e.g.), that's as good as impenetrable if you detect the intrusion and respond in less than that time.

On the flip side, the end user community often takes "unpickable" literally, and relies on locks exposed to the public for long periods of time with no intrusion detection or response. In that case, does it really matter if a bad actor picks or forces it open, if you have no

response? So there's a false sense of security there, and a false sense of insecurity amongst hackers.

NM29: i must say that i enjoy your answers as you really explain them good.
Now, what would you say is your biggest success in you career ?

BG: Interesting question... I've worked on some pretty neat engagements, but the one that I'm personally most proud of, and that frankly took the most hard work was the very first paid pen testing gig :slight_smile: Going from 0 to 1 is a whole lot harder than 1 to 100.

NM29: yeah hah nicely said !
We have seen form your responses that you have manyy skills, do you have any regime of training your skills set? If so, could you share it with us?

BG: Reading, watching talks etc is a good way to get started, but to properly learn, you have to do it. So when I see a skill that I think is particularly needed, I'll buy the tools for it, and hack at them until I've recreated the extent of the published literature on it myself, then try to go beyond it. Often that's the basis for talks I give, when I discover something worthwhile that way. We try to make that a community thing at GGR... once one of us has gone to that level of depth in a particular skill, teaching the others and giving them the equipment and mentorship to pick it up themselves 10x faster.

NM29: that is really smart, one who has highest level of knowledge teaches others in same community or team and that way you all keep improving

BG: yeah!

NM29: will we are on the topic of your team and community, Is there any interesting story from your lab/office/work that you could share with us ?

BG: hmm... a lot of the most interesting are covered by NDAs! I guess one general phenemenon on jobs that would be funny if it weren't so bad is bad security culture when encountering workers in secured areas. More than once, I have had them start explaining to me why they were there. On one occasion, after UDTing into an area, we re-closed the door and decided to document the process for the client. While doing this, one of the occupants came up and, evidently aware of what we were doing, was like "oh I can let you in if you're locked out".

NM29: hahaah ok why are security guards stories soo good haha

BG: I have an answer to that, it's a little un-PC though.

NM29: we will talk about that some other time haha
In your opinion, how will the world of PhySec and InfoSec change in next few years?

BG: interesting question... infosec will continue to evolve proportional to the number of people working in it. Same underlying phenomenon as Moore's law, on computer speed... with enough people working on it, the rate of progress in the field becomes a statistical phenomenon. For physsec, as I mentioned, the threat model is everything. So the spread of vulns will increase - 99.99% of facilities will remain the same, because their threats won't change. For the top most secure places, it will evolve, but much more slowly since far fewer people are working on it, and many of those who do don't publish. I think surveillance technology will be the biggest disruptor though: behavioural biometrics, tracking movement throughout a space, etc. Automating what we previously needed guards to do.

NM29: we will see how much you are right in future

BG: true - this answer is always a risky one to give lest I be quoted 10 years on being like "look how wrong this guy was"
if you ever talk to researchers in quantum computation, they'll refuse to predict for that reason

NM29: haha well you wouldn't be quouted as being wrong, you will just represent how people were thinking in the past and how far we have come.

BG: that's the most diplomatic wording for "wrong" I've heard all day

NM29: Talking about future in public will just leave kinda a qoute on how people think right know and what they expect
Ok now as i know members have questions for you so i will just ask you one last question, where can people find you ?

BG: So my main public social media is twitter: https://twitter.com/access_ctrl. I put things on github sometimes too - https://github.com/bgraydon (a lot of backlog still to add there). My brother and I also started a YT channel, currently with 0 content, which we'll get around to uploading to eventually https://www.youtube.com/channel/UCzZK3vjJL9rKNPXNoCPFO5g

NM29: Awesome, now let's jump to the questions from the members

Member question 1: Here's a question for Bill, because multiple people may be interested to know: if someone wants to get involved with helping to run in person/virtual events for the LBV, how do they do so?

BG: Great question! I wish we'd known about this server earlier for this reason! The official way is to email humans@bypassvillage.org, but just DM me and I'd be happy to get you looped in!

MQ 2: got one for Bill as well, what was a "i cant believe that worked" moment on an engagement/job/etc...

BG: I can remember thinking this on many occasions... trying to recall specifics now though! I guess one recurrent one is with passcodes... the number of times the default, or one of the top 10 is used is shocking.

Or getting a brute force in <5 mins. Or seeing it posted on a sticky note in the room, visible from the outside through a window.

MQ 3: do you consider lock bumping to be bypass? what about comb picks?

BG:Bumping I consider to be in the realm of picking... often the mechanics are the same as raking, for certain types of locks. Comb picks gets more into bypass, it kinda straddles the line though. But these are just my opinions, and I am by no means a source of truth on it. And that presupposes a prescriptivist approach to the definitions of those words.

MQ 4: does he come across situations where he needs to kind of prove to the client that something is a risk, like is common in cyber sec?

BG:On occasion. We're often hired by the CSO or a director under him, and asked to pen test not because it's the best way to audit the business, but because it's the best way to convince the board to invest in their security! When it comes to "proving the risk", it's not enough to just show that a vulnerability is possible. Our job is to a) show that, b) determine under what circumstances it's a vulnerability, c) determine the likelihood that it's actually used, d) determine the damage if it is, e) determine the options and costs (both financial and otherwise) to mitigate, and f) to make a recommendation, providing all necessary information for the decision makers in a company to make the final decision. That's our job as consultants: not just to hack it, tell them what we did, and call it a day.

MQ 5: Are you starting a UK arm ?

BG: Not currently in the pipeline, but possibly >5 years out. I have a lot of respect for how security and resilience are done in the UK, and try to bring that school of thought to our North American work. With no offence to Americans, but the predominant approach there is throw more money, overwhelming force and draconian measures at threats. The UK actually applies their brains to the problem.

MQ 6: Do you think the USA is historically based on a more adversarial approach to testing, whereas, the U.K. pen test industry grew out of gov/military and was more based around trusted consultancy?

BG: he USA's approach, in my view, is defined by "9/11 reactionism". It isn't particularly big in red team testing either - despite the term originating there, the vast majority of infrastructure protection is not done that way. It's done by hardening the heck out of things, militarising the guard force, and relying on shows of force and military tactics against adversaries that work like traditional enemy forces. Both are trusted consultancy, but with very different foci.

----------END----------