ABSTRACT SECURITY

Date: 9.03.2021.
Interviews with:plaverty9

NoMan29:Hello everyone
Today we are joined with Patrick (@plaverty9)

plaverty9:Woot.

N:Hi Partick, How are you today ?

p:Hey NoMan! Awesome, really looking forward to this!

N:hah i am glad to hear that ! Shall we start ?

p:Let's start!

N:Can tell us who are you ? Maybe some people don't know you so let's start with that.

p:I'm guessing a lot of people don't know me. I'm Patrick Laverty, aka plaverty9 in many places. I'm from the US, east coast. Professionally, I'm a pentester for Rapid7, the people who make Metasploit. I'm also the creator and co-organizer (with Lea Snyder) of the Layer 8 Conference, the first one in the world to solely focus on OSINT and social engineering. This year will be our 4th year of the conference. I also host the Layer 8 Podcast! So please check that out too.

N:Layer 8 podcast is really interesting, cause it is not usual podcast. Can you tell us what we can hear at Layer 8 podcast ?

p:Yeah, for sure. It also focuses on social engineering and OSINT. At my company, we often have little internal conferences where we share info and it seemed like the social engineers had the best stories. I thought that every social engineer has a great story to tell, so I decided to create a podcast where I ask them to tell some story about a great engagement they had, things they learned, hurdles they overcame. We also have OSINT investigators talking about their methods, tools, strategy. I do some interviews, but my preference is to stay out of the way and let the experts talk.

N:Yeah i really like it cause it can be between 20 and 60 min and you hear some interesting story that you may have not heard on conferences. Great job on making that ! Now how did you made conference ? What motivated you ?

p:Ooh yeah...that was a fun one.

N:I will just put this here so people can find you
https://layer8conference.com/

p:I'd been organizing BSides conferences since about 2013 first with BSides Rhode Island with Security Weekly's Paul Asadoorian. But then I got involved with BSides Boston and helped with that one for a few years.

But then I started wanting to do my own thing and one night on Twitter, I saw Rachel Tobac asking if there were any conferences that focused on social engineering. I wasn't aware of any, so I thought, why not? Let's make one. And then Layer 8, in 2018, was born.

N:Haha well that is how great things are made hah

p:It's a lot of fun.

N:And we can say that you are only one conference that is only focused on OSINT and SE

p:Well, Social Engineer dot org now has their Human Hacking conference which has both. There are OSINT conferences and SE conferences, but I think Layer 8 and Human Hacking might be the only ones to just focus on those two things.

N:True, but i think once Chris H said that Human Hacking conference is about people and how we can help them and science behind it . So it is more focused on human (i could be completely wrong about this so don't quote me on this) . But yeah i agree with you

p:I'm attending it this week, so I can let you know when it's done!

N:hah yeah tell us your thoughts on it ! Ok and, how did you held the conference while this pandemic ?

p:Yeah, the pandemic makes things tough. But based on what the awesome people at Black Hills came up with, we were among the early adopters to the online conference. We had three tracks of talks and had nearly 600 people attend virtually over GoToWebinar. We really miss the social aspect, but it's also easier for people who can't travel as easily. Most of the presentations are available on the conference's youtube channel.

N:Oh cool, i am glad that conference was held during this pandemic in safe way. And i think we did't said but when is Layer 8 conference ? What date and what place (in normal conditions)

p:We haven't set that yet for this year. We are working on a few things at the time but I suspect we'll have that info available in a few weeks. If people want more information about the conference and want to stay current on all that, we have the layer8conference.com web site and the @Layer8Conf twitter account, where we publish all of that information. But we're really looking forward to this, our fourth year of the conference and continuing to build it and do great things with it.

N:ah ok then, feel free to post the dates here

p:We've always had great support from the community as well as the villages that we run at the conference. We also have villages, which are like mini conferences at the conference as we partner with TOOOL and the Mental Health Hackers group. TOOOL is the The Open Organization of Lockpickers, where they teach lockpicking, and the MHH have presentations on assisting with better mental health.

N:huh cool! We have some of the TOOOL people here.

p:Awesome, great people, especially Max Power who's been with us for a couple years.

N:How much time does it take you to plan the whole conference ?

p:Oh boy, well I think planning usually starts about 6-8 months in advance with getting a venue, running the CFP committee, finding sponsors and then bringing all the little details together. Then on the day of the conference, it all goes by in a blur, after all that work.

N:soo planing for 6 months to get one good conference
that is a loot work you have to give to make everything as best as possible .

p:Yeah, and we're still a little one. Big things like defcon take a really large group, full time. It is, it's not really hard exactly, it's just a lot of little moving pieces with things you can't forget. Like being sure you have the right dongles or adapters for the speakers to connect to the projector.

N:Yeah i imagine how much preparation there is for DefCon or CCC (Germany one)

p:Or remembering to have lanyards for badges.

N:And is it easier to make online conferecne or is it same amount of stress and work ?

p:It's the same amount of work but the day of the conference is more stressful because online has a single point of failure.
When you have an in-person venue, you have rooms where people show up and talk to each other. When it's online, there are technical issues where a speaker might have a power outage at their designated time (that happened) or attendees who paid to go, can't log in for some reason.
You don't have most of those issues when it's in-person.
As long as you have a venue, speakers, attendees, you have a conference.
When it's online, that venue part is a little harder.

N:huh yeah, you would think that is easier as you don't have all the physical work, but as you said there is stress there too.

p:Yeah, there's definitely stress in both, but it also might have been the novelty of it last year and not knowing exactly if it'd all go well that was stressful.
Now there have been so many online conferences, we've all learned from each other on mistakes to not make again.

N:yeah at least that .
And how many people are behind the Layer 8 conference ?

p:There are two main organizers, myself and Lea Snyder. And then we have five people on the CFP committee.
And that's about it.

N:ok wow that is a small group.

p:Yeah, Lea and I have learned that a smaller group works better. When you have too many, there's often disorganization with people going in different directions and doing their own thing. So I like to call us benevolent dictators. We're nice, but we make sure things are done a certain way.
As the conference grows, we might need to expand. Especially in the area of finding partners.

N:I like that name and that philosophy. Smaller and controlled, smart

p:That's always the hardest part, finding financial backing, especially when you're an unknown name. If you're known, like a BSides, everyone loves to associate with that and wants to be a part of it. When you're new and no one's heard of you, a lot of partners take a wait and see approach.
But I think we're starting to win people over to see that we're for real, not a scam and offering real value to the community.

N:Yeah but i can see that you have some great partners like Innocent life foundation !
and Trust Sec

p:Yes! The ILF is awesome. They recently asked me to be one of their ambassadors which I was honored to accept, so that lets me tell people all about the awesome work that they do.

N:oh wow that is really awesome ! Congrats on that !
So you mentioned that you might expand, so do you have any plans for expanding the conference ?

p:I would love to, but I also think it needs to be controlled. Even after the first year, people were suggesting expansion and growth. But I'd rather people leave the conference thinking "I want more next year!" instead of "Eesh, that was just too much."

N:yeah, as i said small and controlled

p:So the first year, we had about 150 people at a college campus in Rhode Island and then the second year, we grew to a little more than 300 at the Rhode Island Convention Center. And then last year, we got bigger again with the online conference.
So we'll see what kind of growth we can pull off when we get past COVID times.
I'd love to be able to run multiple instances of the conference in multiple locations. So we'll have to see what that brings.

N:huh that would be interesting, something like BSide

p:Maybe, though BSides is enormous and is a general security conference. We're a niche with the SE and OSINT specifics, so we don't reach as wide of an audience. Though everyone in security should probably be interested in our focus.
I would also like to branch out of security as SE and OSINT involve lots of professions.
My friend TinkerSec always says that he learned his best social engineering while doing sales.

N:you could do like a tour like today we are in NY in two days we are in LA and soo on.. but that would be a lot of work and planing

p:That sure would, but also be pretty awesome. Those big cities are pretty expensive for conferences. Little known fact, those box lunches that you get at conferences with a sandwich, chips, cookie, in a mid-size city can easily cost the conference $20-25 each.
In the big cities, that quickly gets in the neighborhood of $40 each.

N:oh wow, double the price
well bigger city bigger prices

p:Yep, that is the tradeoff, you can get more people at bigger cities, but big cost too. That's one of the reasons that Defcon is in Vegas in the summer.

N:but for now you are doing really great ! even if you are ''small'' conferences.

p:Thanks, we're having a lot of fun with it and the focus is really on helping the community and sharing information.

N:yeah well that is the goal of conference !
now why is it named Layer 8 ?

p:Oh good one, I get asked that a lot.
It is based on the OSI model of networking where Layer 1 is the physical layer, the actual wires, all the way through Layer 7, the applications that we interact with on the computer. So because we are focused on the security of the human, we figured that is the next layer after the application, so Layer 8!

N:yeah that makes sense :smiley:
Now i will stop asking you the questions about the conference haha
You said that you work as PenTester, right ?

p:I do. I work for Rapid7 as a pentesting consultant. So I get to test other companies all the time.

N:Only digital side or the physical one too ?

p:We do physical engagements but that is the one type of social engineering that I have not done just yet. I've done email and phone calls, but nothing physical. Post-COVID times, I likely will try some of that. It seems like so much fun, if you're properly prepared.

N:yeah preparing for it is the biggest part. As our member (@autom8on) said '' study hard, fight easy''

p:Yeah, when I talk with people who do physical engagements, they often say that they might spend 3-4 days out of the 5 allotted just on prep.

N:yeah, that is what i heard people say too. You can always ask if you have questions here for phys sec, but i think you already know that

p:I definitely will! Thank you.
I'm looking forward to trying it. I think I have a pretty innocent looking face, so people should let me in.

N:Now i always like to ask this question, why security ? What brought you to it ?

p:It was actually accidental.
I was working at a university as a web application developer. And I had a little bit of interest in it. I'd been to conferences and seen some interesting things, but never really got much of a chance to do security stuff. But my cubicle was right next to the university's CSO and we talked a lot, I told him how I thought it was an interesting area to learn about. There werent' many people at that school focused on IT security, so I could see some pretty big gaps. Then one day, the web server got DoS'd. We had to figure it out. The CSO told me it was my chance and to run forensics on it.
I had so much fun with that, I turned it into a conference talk and it just grew from there.

N: huh interesting way of getting in security !

p:Turned out, the web server had a few leaky web pages which let people install web shells on the server. To the point that there were way, way too many of them on there. They had .htaccess files directing google to index their bad sites they'd installed. And one day there were just so many of those that Google was indexing so many things that it overloaded the web server and took it down.
So yeah, we really got DoS'd by Google.
(inadvertently)
After that, I got to do an internship with Security Weekly which was so much fun. Paul and the team are awesome there.
He's grown so much since I was an intern with them.
I have this picture during one of the shows which is just Paul, Larry and me in Paul's basement. Now, Security Weekly is comparable to any professional TV studio.

N:That is really awesome way to get into security. You can always say i have stopped Google and became the security guy ahah
or i have fixed what Google didn't

p:Yes! That's a great way to put it. I shut down Google!

N: hahahahaha yeahh
Now you always have interview with other people if they have any interesting story that they want to share, so let's turn that around,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.

p:Well let's see, I just posted a big one from an internal network penetration test on my twitter account, that one was fun. But it does often seem like the social engineering stories are the best ones.
I still really like my first one, which is even before I was working for Rapid7
I was doing side work for another pentest company doing mostly web application testing.
But then they asked me to do a phone calls/vishing engagement. They just said "do your best"

N: they are more interesting cause many people understand it, and when talking about digital ones only people who that work on know it understand it hah

p:They gave me names and phone numbers of 50 people.
So what I did was to find that company's VPN web page, the one where you can log in to get access into a network and copied it onto a server that I owned, and was serving it from an IP address.
Then I started calling.
I was calling people as "Patrick from IT" because we'd had a breach, some of our password database got leaked and I was told to have people check if theirs was in the breach.

N: hahaha that is a classic hahah

p:So I'd explain to people that since it'd just happened, we just now threw up this web page where they can check.
Don't tell me your password, just go to [IP address] and log in. It'll tell you if your password was in the breach and whether we need to worry.
Of course for everyone, it just said no, you're safe
But the main part was to capture username and password.

N: hahah you are safe, but actually not hahah

p:One of the things that I learned from that is to do the phone calls late on a Friday, as I was much more successful than when I tried Monday morning.
People were tired, just wanted to go home and get me off the phone.

N: yeah well who would bother to think about security on Friday ?

p:Exactly.

N: that story is a classic one but i have heard that tactic succeeded so many tiimes!

p:I just tried to make it as easy as possible for them. But it was a lot of fun, and then I was hooked.

N: yeah you have tasted the blood

p:I know people have seen the videos where the SE using background noises, so I tried that on the last one. But unfortunately, no one picked up. I was tasked with trying to get a company to add a subdomain to a configuration record.

N: well you have tactic for another time

p: So my story was that my company's CEO and the director of IT were in front of a crowded room of investors and the board. I had background noise of just people talking, like in a big room at a conference. I wanted to see if I could go into a panic and tell them the CEO is not happy because someone messed up and the subdomain wasn't working.
But yeah, maybe next time.

N: huh nice pretext
now you are in InfoSec for some time
In your opinion, how will the world of InfoSec or Security change in next few years?

p:Oh boy, predictions. Everything changes just so fast, it's super hard to keep up. But also the field of security is probably starting to mature a little bit more, it's more of a priority. I also think some parts of securing things are getting easier in that they're getting outsourced.
So rather than every company needing to know how to keep every possible service safe, you can outsource parts of it to other companies who focus on that.
And then many companies can also get secured quickly when a new issue comes up, like the recent Exchange vulnerability.

N: yeah, true.

p:If you run your own exchange servers, you gotta stay on top of that and patch it. If you run O365, I think MS was on top of it and probably patched it before the vuln was public.
Similar for things like AWS and Azure.

N: yeah i understand

p:So I think there might be less and less of "do it yourself" and more outsourcing. That might help with cost and security.

N: nicely said !

p:Now if one of those places mess up, it's gonna be a disaster.

N: And what is one myth that you hear constantly, about your work or something related to it, that you want to debunk?

p:Well, I'll say that 8 characters is not nearly long enough for a password. Also, you can't just blanket tell people "a longer password is better" because humans will always find a way around that. I was testing one company and they had a policy where the password needed to be a minimum length of 15 characters. Sounds strong, right? Until they saw that people were still using Password1Password1!
Or keyboard walks.

N: oh wow....that is new level....

p:It's a struggle that I empathize with, but in the end, humans are often the main attack vector in.

N: as someone said, human is weakest and the strongest part of Security

p:Yes, definitely. You can lock everything down, but if a human is compromised, all your security is gone.
Because you also have to balance security with usability.

N: yeah

p:The old "Don't put a $100 lock on a $10 bike" thing

N: hah yeah
What is your favorite part in your work? And what is your least favorite?

p:My favorite part is learning new things. It seems that every week, in virtually every engagement, there are new things to learn. This week, I'm digging in to a web application and really learning how to use the browser's developer tools even more.
I think my least favorite is just being away from home. Some people on my team love to travel. I don't mind a little bit, but I still love to be home.

N: huh interesting. And what is in your opinion more important, right certification or knowing right people?

p:but also, sometimes writing the report isn't the best part.
Neither. Knowing the right stuff.

If you know your stuff, that will come through in your interviews. I just interviewed a handful of people and that really showed.
If you have certifications but can't really talk your way through an interview, you're not going to get hired.

N: and what did you look for, beside good skills for job ?

p:Same with knowing people. Friends might get your foot in the door, but you gotta know what you're doing.
Other than having a solid understanding of the necessary level of skills, I like it when someone can admit "I don't know". I tell people that my goal in technical interviews is to get to a point where either you or I say "I don't know anymore" because that's how deep we went. I also really like to ask people to be able to explain something to me like I'm only a little bit technical. For example, you did a "pass the hash" technique in my network. What does that mean? Tell me like I'm the CEO.
If you can't really explain it in that way, you might not really understand it thoroughly.

N: hah interesting .

p:I like to go by "Learn it, do it, teach it". If you can teach something, then you really understand it.

N: yeah that is on the top of the pyramid of knowledge

p:As you teach something, people will ask you questions or force you to teach it in various ways that forces your solid understanding.

N: What is one question that you wished someone would asked you, but never did?

p:I don't know that there is one, as if I have something to say, I'll often say it and not wait to be asked. But that's an interesting one that I'll think a little more about and see if I can come up with something. Sorry that's a lame answer.

N: no don't worry, it is not a lame answer, it is a good thing, it is better to say what is on you mind then to keep it in you
and never say it
and last question, do you think that it is better to generalize and try and do a bit of everything, or specialize in one area?

p:Well, it depends. It depends on what phase you're in of your career. If you're just starting out and have no experience, I tell people to pick an area that interest them and dig in. Start learning all about it. And if you want to be in security, which to me is about breaking things, you first need to learn how to build them. So when starting out, find something you like and learn how to build it really well. Then when you start getting into security, try everything. See what you like. There's so much to dig in to. And then eventually you can decide if you like one area, like maybe physical security, or IoT, or car hacking or social engineering and focus on that, or keep the diversity of things, so it doesn't get boring for you.

N: huh interesting answer. I quite like it. And i agree with you.
Now
we will take a little brake and we will come back to see what questions our members have for our guest !
If anyone have any questions for our guest, post it in #💬general-sec

p: Awesome, I look forward to that. And earlier, I alluded to an internal network pentest that I wrote up for people. I don't know if that's an area of interest, but if they want to see it, it's here:
https://twitter.com/plaverty9/status/1368960812816216068

N: Awesome, we will take a look at it! There is no questions, thanks for the interview!

p: THanks for having me !

END