Niru: Adopt an attacker mindset

Hi, I'm Niru, and I lead the red team at Google.
The red team at Google simulates attackers that are trying to hack into Google.
They function as a sparring partner for the blue team, that is, the teams that build security controls, detection pipelines, or respond to incidents.
So we help test all of those by simulating adversaries.
So we hack into Google to make it harder to hack into Google.
So it's like, hey, we found these issues with your system, now here are some recommendations we have, and how can we help you fix this?
Thinking like an attacker is approaching a problem like an adversary.
I generally have a predisposition to think like an attacker. [LAUGH].
It started when I was a kid and I used to play video games, and I used to ask, oh, do I have to beat the game in the way it's intended?
Do I have to get the objective in the standard path?
Looking at a system and asking the question, can I break into it?
How do I break into it?
What is likely to fail?
If it fails, what does that give me?
It's about taking apart systems and trying to understand it.
Threat modeling is integral to almost anything a security professional does.
It's about challenging assumptions.
It's about approaching things from a different perspective.
Rather than looking at the system from the perspective of a developer who is thinking about, how do I build the system in a way that works for people?
You're putting on the hat of an attacker and saying, if I looked at the system, how would I break into it?
It's important for all security professionals to think like an attacker because you code more defensively, you build things more defensively, and you break things more offensively.
And what that means is you're building in this resilience into the system, and you're building in all these safeguards that are going to help protect the data, the systems, and the people.
In order to build my attacker mindset, what I did is I would go pick people's brains.
What that means is I can grab time with them and say, hey, how do you approach the system?
What are the assumptions you're making?
How do you build out the security safeguards that you're thinking about?
My advice for people who are trying to build their own attacker mindset is go talk to people, be it in local meetups, in conferences,
find yourself a CTF group and play these competitions with them.
See how each person in the team approaches certain things and solves for it.
Almost everything we do on a daily basis is online these days, like banking is online, grocery shopping is online, the electricity grid, the water supplies.
All of this has happened in a short span of time, and now people are taking a step back and say, what does that mean for us?

And cybersecurity folks are the ones who help make sure these systems are locked down and protected against these adversaries.
If you're inquisitive, if you like taking things apart, if you like solving things, if you want to help make things secure, you should join cybersecurity.

Revision #1
Created 2023-08-21 10:12:28 UTC by naruzkurai
Updated 2023-08-21 10:14:19 UTC by naruzkurai