Chartered Institute of Information Security

Pulse:

November 2022

CIISEC LIVE 2022

We finally made it to the Craiglockhart Campus in Edinburgh

CIISEC INNOVATION SUMMIT 2022

Themes included Cloud, Supplier Management, Human Behaviours

RANSOMWARE

The subject that cyber professionals can't seem to get away from

Offensive security: more art than science?

‘Offensive security’. Should be easy enough to define, right?

Ben Sandison
Senior Security Consultant, Secure Impact Ltd

Unfortunately, it’s not so simple. The real definition of offensive security depends on who you ask. A typical CISO, for example, probably thinks of offensive security as just one of a dozen processes in their wider security roadmap. Useful, but definitely not the only thing to think about. A compliance officer may see it as one of the many boxes to tick on their way to achieving accreditation, and not worry too much about the specifics of the results themselves. A developer might see it as a process that really validates the time they put in to ensuring their product is rock solid, or as a way of learning how to improve for next time.

To me, a career penetration tester, offensive security is all of these things and more. It’s a method of battle-testing the assumptions and expectations you have and giving as close to true validation of your security controls as is possible without going through a real attack. It’s analogous to crash-testing cars. Sure, it can cost you as much as a car – but wouldn’t you rather have a test dummy explode on impact than lose all your customer data in a breach?

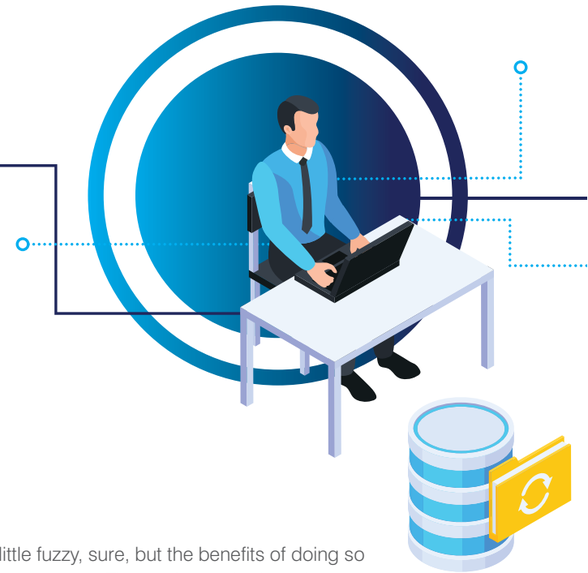
Now that’s out of the way (sort of) let’s go back to the question at hand. Firstly, can offensive security be considered a science? Again, this seems at face value pretty cut and dry. Offensive security is (mostly) to do with computers, machines that outside of a few unique situations are largely considered deterministic. Same input, same output. Sounds like science to me.

Considering it as a science is great. It allows us to apply the strict methodologies which are the basis for compliance and regulatory standards the world over. We can work through a checklist of controls that should be in place, test for a few dozen predefined issues that shouldn’t be there and give a big green tick at the end in the box marked ‘secure’. We know that computers always react in a way that we expect them to, so, problem solved.

The issue with this line of thought is that the problem security programmes aim to solve doesn’t have such a clear-cut solution. The reason is pretty simple – everything involving security also inherently involves humans, and humans are by nature not deterministic. Whether it be the developer who wrote the code being assessed, the end-user who actually interacts with it, or the attacker trying to break it, humans almost never do what you expect them to.

I’m not just talking about social engineering attacks here, though they are something to think about.

Human problems require human solutions, and often the way to get the best out of humans is to let them approach problems without arbitrary restriction. Creativity and ingenuity are some of our best features, so why not use them?



Modern systems are often incredibly complex and built primarily through human ingenuity and creativity. This gives frameworks designed to turn offensive security into a checklist pause, and leads to a necessity for generalisation. Testing for ‘logic-based’ issues for example, could mean almost anything, and is heavily based on context. This is good news for me, as otherwise my job would be done entirely automatically by a vulnerability scanner.

So, offensive security can’t be considered wholly a science. Can it be considered an art? Sometimes. Probably.

In my experience, human ingenuity and creativity comes into it at all levels. Whether it be through a penetration tester seeing a bit of functionality that looks ‘weird’ and following their nose until they find out why, a red teamer spending an afternoon crafting unique payloads designed to evade cutting-edge EDR, or an exploit developer chaining vulnerabilities together in a novel attack to break everything you believed to be true, there is always going to be a requirement for creative thinking.

In the security testing space specifically, treating each engagement as bespoke as opposed to following a strict framework requires a completely different approach. During scoping, for example, rather than asking quantitative questions like “how many dynamic pages are there?”, isn’t it more important to know how those pages are used, where the key functionality is and what the primary business concerns are? When testing, is it more useful to run a suite of predefined tests (again), or to actually look at the target system, use intuition to pick out the parts that are most important and really focus on them? In my experience, the best findings always come from the latter approach.

It sounds a little fuzzy, sure, but the benefits of doing so can often be enormous. Those of you who have been on the receiving end of a penetration test report will know that most of the time the key takeaways are how the results impact your business specifically, and how the risk represented by the vulnerabilities discovered can be contextualised into information that is actually usable going forward. Is a green tick that says you’ve passed really going to do that?

I don’t mean to speak badly of compliance and regulation, they are absolutely critical to ensuring a common baseline level of security. Without them the realm of cyber would still be a wild west, with no real way of enforcing accountability. Outside of that, though, I believe treating them as the gold standard is a mistake that could well be costly.

Human problems require human solutions, and often the way to get the best out of humans is to let them approach problems without arbitrary restriction. Creativity and ingenuity are some of our best features, so why not use them?

Back to the question then: is offensive security more art than science? My answer is a firm yes, but, as often ends up being the case with complicated questions the real answer is ‘it depends’.

SECURE IMPACT