COMPUTERWORLDUK
THE VOICE OF BUSINESS TECHNOLOGY

What is penetration testing? Meet the security pros breaking into your business for cash

What is penetration testing? Ethical white-hat hackers and security professionals are paid big money to break your business - welcome to penetration testing. Computerworld UK meets some of them.

Tamlin Magee
March 9, 2017

After a brief reconnaissance mission on the web, there's ample data to piece together a convincing enough story to fool a receptionist into trusting you – they hand you the rest of the information you need. (See also: what is a graph database?)

Using this, you conduct a convincing phishing attack by email, and easily bypass a company's rather expensive security systems. You're free to place an exploit where it won't be found and siphon the businesses' data to wherever you like. It's yours. *[You might also like: What is microservices?]*

Image: Flickr/Dan Tentler

Thankfully for this hypothetically hoodwinked company, all this data is safe – because this is the work of a penetration tester, security professionals who use real-world criminal hacking techniques to crowbar open the unguarded gaps in their client's armour.

"If there's a hole it will be found sooner or later – these days, sooner," says Aleksander 'Aleks' Gorkowienko, principal consultant and training manager at pen-testing company 7Safe. "I have absolutely no doubt. If someone does not invest properly in prevention, it's stupidity – I don't have any other words."

Aleks joins me with colleague Steven van der Baan, principal consultant and senior pen-tester, to talk me through the ins and outs of breaking businesses for a living.

It seems that every week there's a high-profile hacking case causing brand damage and putting customers at risk. And there are thousands more cases where attacks aren't reported – or, indeed, slip under the radar.

So there's money to be made having organisations from banks to government department contract pen-testers like 7Safe to conduct thorough security audits.

Penetration testing: Starting a career as a pen-test pro

Both Aleks and Steven were software developers first. Steve's road into penetration testing was through his involvement in Open Web Application Security Project (OWASP), first introduced to him through a colleague, while Aleks had a strong personal interest in security.

Their goal is to recreate the attacks that hackers with a criminal agenda are engaging in on a daily basis, and report their successes or failures back to their clients.

That also means a lot of paperwork, and the resulting screed can often present a brutal education in the realities of cyber-security.

The two encounter different technologies and challenges for every case, from new web apps to relatively ancient systems. Their work varies from SQL injections, placing a query into a database that allows you to manipulate it maliciously; phishing; vishing, where you impersonate someone over the phone to gain information, like keys or a password; XSS attacks and everything in between.

Other firms offer physical penetration testing – that's a dressed-up way of saying breaking into company buildings and compromising everything they've got.

"Reconnaissance in the web is the most basic exercise we can do," Aleks says, referring to 7Safe's social engineering efforts. "We can do phishing and 'vishing' attacks, and we have a system which can collect information about all those clicks."

Penetration testing: Identifying security weaknesses

Aleks recounts a case where his pen-testers made a copy of their client's website, created a form, and sent out legitimate-looking emails to lure them in – designed to fool workers into voluntarily disclosing very sensitive information.

"One of the people on the target list was a guy – he was the only one in the company responsible for the maintenance of this website," Aleks says. "Only he had access to it. He saw the email, clicked the link, filled in the form, pressed the submit button – only afterwards did he ask himself: 'Who the hell created the form?'"

"This is hilarious," he says. "But it's a serious thing. It perfectly demonstrates how deeply we are ingrained in our daily routines. We just click whatever comes."

It's also a prudent example of an often-overlooked weak point: trust.

Beneath the surface of our daily interactions and you'll find a surprising degree are fundamentally based on trust. And when this basic human element is manipulated, it opens opportunities for attackers.

"It is our innate nature to be helpful to people," Steven says. "When you say: 'Please can you help me with this,' your first instinctual reaction is 'maybe I can mean something to them,' rather than 'who are they and what do they want?'"

The nature of the web means there are plenty of opportunities for recon: adding people on Facebook, phoning utility companies for personal information, creating elaborate and believable background stories.

"You're absolutely right," Aleks agrees. "Spear phishing [highly targeted phishing] is more popular than phishing. Real hackers do reconnaissance in the web – Facebook, LinkedIn – and collect information about the target.

"They might write some background information on the person, or create a fake profile to establish connections on social websites.

"It's just a slight deviation from the daily routine for a person who works at the reception desk – they need to be trained enough to identify the deviation and think: 'There's something really fishy here.'"

But equally a threat is plain human error.

"I had a client once where one of the admins wanted to change a little bit inside the database," Steven says. "And they permanently deleted the entire database."

"They said: fortunately, we have our backup procedure. They started to rollout the backup. They destroyed everything through that. They hadn't checked the backup worked – it was only allowed to do a system backup, but not data, so they had the layout of the database and everything else was gone.

"That was definitely not a malicious user."

So, they say, culture is just as important as technical capability.

"A lot of this is dependent on culture, early detection and prevention," Aleks says. "It's prevention, rather than trying to stop the fire when it's already too late."

Penetration testing: Each client presents a new challenge

There is no typical site visit, but each one is prone to surprises.

Some sites will be running relatively ancient legacy systems, in one recent case Windows NT – still running as normal behind a secure perimeter. "It just asks for trouble," Aleks says.

"I was on site for that particular system," counters Steven. "My normal tools didn't work because the system was too old."

Steven tells me he recently found a system where, by manipulating the database with an SQL injection, he was able to read files from the underlying operating system.

Another error elsewhere provided the source code – and after downloading the lot, he located a vulnerability in an obscure part of the system that allowed him to execute whatever code he liked.

"What we find and where we find it, what our end results are, completely depends on the system," he says. "It could be a CRM system – the other day there was a brochure-ware system, where they thought everything was clear but a plugin allowed scripting."

The common factor is that many of these systems tend to be breakable in one way or another.

Rookie errors can be found everywhere – and a problem, according to van der Baan, is that universities are simply not teaching secure code.

"If you're not being taught how to code securely at a university, how can you expect that a developer at a new company will create secure code?" he says. "That type of code usually ends up in a production system."

Both agree that a good security tester needs a strong sense of curiosity – and assert that actually, children are natural pen-testers.

Steven recalls installing Ubuntu on his laptop: "I always lock my system before I step away from it, and my son crawled behind my system. All of a sudden, I saw him have a window open. What the hell did he do? He managed to find the guest account, and he got in from that! He had no clue what he did.

"You have to have this innate curiosity for things. Most of the other things can be taught, but this curiosity is something you must have."