QINETIQ

Red Team War Stories

Contents

Introduction

The impact of a security breach can be catastrophic for any organisation. This means the security of their information systems and assets is of paramount importance and is usually identified at board level.

A red team exercise is one of the most advanced security assessments an organisation can undertake, accurately simulating the latest targeted attack types and methods used by real world adversaries, across different threat levels. This allows you to evidence your current business critical risk to enable swift improvements, increasing resilience and providing a much higher level of assurance.

The key benefits of Red Teaming are:

- Emulates real world threat actors and vectors in controlled environments.
- Assess the effectiveness of physical controls and human practices.
- Provides real, actionable intelligence against security posture.
- Exercise SOC capabilities in real time with attack methodologies.
- Engagement run over extended period, mimicking a true threat factor.
- Uses network implants, spear- phishing and Open Source Intelligence (OSINT) gathering to help to understand online threat footprint and current risk.
- Ultimately strengthen an organisations defences/blue team.

In this document we share three stories of physical and early stage breaches from our Red Team engagements with customers. All of the exercises resulted in actionable feedback to our customers that they could immediately implement to improve the resilience of their organisation.

Find out more about our range of Advanced Red Teaming Services here.

1 Insider Threat Simulation

QinetiQ were working with a large law firm who were particularly worried about insider threats, as they had recently been targeted in this way. A disgruntled employee had downloaded sensitive information and deleted files and records, with the aim of causing chaos, potential financial loss and at very least significant inconvenience.

Our small group of stakeholders within the law firm had chosen and appointed a member of staff who had been fully briefed on the exercise and most importantly, was instructed to tell no-one, even his line manager. Luckily the first person they asked was happy to help as this reduced the possibility of whispers spreading from anyone who had turned the task down.

We met our contact away from the client site. Upon first impression, the contact was very young (apprentice aged) and very, very nervous about his task. It was hard not to feel sorry for him, though equally it was hard not to suspect we might be being set up to fail. We decided to spend some extra time with him as it would've been a mistake to send him back as he was. After sharing some war stories about other red teams and giving him some tips and tricks of the trade, his initial fear was mostly replaced by excitement as he felt more prepared for the task ahead.

We couldn't wait any longer: suspicions were going to be raised if he wasn't back on site soon. His line manager, of course, was unaware that this trusted member of staff was going to give us the keys to the kingdom.

I'm glad to say that once on site, our contact followed every instruction. He plugged our devices into the internal network which called back to our nearby hotel and we completed all of our objectives completely undetected. In the end we had to reign in him a little and jokingly offered him a job on our team.

While we had waited for our contact to return, we took a look at his laptop, which we had persuaded him to leave with us. As he was a junior employee we weren't expecting him to have privileged access. How wrong we were!

Some of the improvements implemented by the client from this exercise were:

- Locking down networks and sensitive data strictly to those who require access.
    - Surprisingly, network access is still commonly left open in the companies we exercise. Giving privileged access to your entire staff, when you don't need to significantly increases both your risk and threat surface.
- Locking down, ports and internal networks from plug-in devices (especially unrecognised, non-corporate devices).
- Separate guest networks were installed.
- Secure monitoring implemented, configured to detect anomalies e.g. downloading large files/data.
- A more stringent leavers policy was introduced meaning accounts were disabled on the leaving date.

We discovered an almost flat network, with far too much access. They also had an inefficient leaver's policy meaning that disgruntled leavers could easily create havoc, after leaving the organisation.

After reading our report, all of our findings were quickly addressed by our client, driven from the top down and the organisation is significantly more resilient after a single QinetiQ exercise.

2 Cyber Red Team

QinetiQ were chosen to run a remote only cyber red team exercise for a large Insurance firm. The client wants this to be 'black box' - no access information shared with us ahead of the exercise to more accurately simulate "being attacked for real".

During the first morning of the Open Source Intelligence (OSINT) gathering stage, the team found active email and password details and a spoof website, hosted overseas, with log in functionality set-up to harvest credentials. This, worryingly, appeared to have been active for some years, and contained the old company logo, colours and fonts (this was reported to our key technical point of contact (POC) straight away).

On the first morning, using the credentials we'd found, we'd achieved Domain Admin access, ordered our own staff passes and booked our own meeting room through the company's internal booking system.

Upon hearing that we had completed our objective for the remote phase on day one, our technical POC wanted to change the scope of the exercise to include physical access. We were more than happy to oblige. While QinetiQ engagements are tightly and accurately scoped, we are always open to making modifications to achieve both value for money and shared desired outcomes, resulting in a more resilient security posture for our clients. As a threat actor, carrying out a physical access exercise is one of the best parts of our job.

Physical access exercises also get strong buy-in at board-level: to see someone who shouldn't have access sat inside your site helping themselves, undetected, to all kinds of "crown jewels" information is very impactful and strongly drives the momentum for change. Information egress is more commonly achieved through online hacking as threat actors want to avoid getting caught, but the physical piece always resonates with senior management/boards.

We attended on site, had staff passes ready and waiting for us and were shown to the meeting room booked in our "names." We had booked out the room for the full day under the pretence of a large audit taking place and even ordered pizza so we could really make the most of our time on site.

The client was really impressed with the collaborative working, which we employ, even on black-box exercises! We continue to work with this client delivering Cyber Intrusion Exercises (CIE) - white-box testing which evidences what a really bad day may look like, in less time/effort/cost as well as larger red and purple teaming exercises.

Some of the improvements implemented by the client from this exercise were:

- Improved password policies and procedures meaning that old passwords now expire, increasing resilience.
- The client now runs a programme of regular OSINT exercises, utilising a more proactive security approach, rather than entirely reactive experienced during an actual breach. This increases further understanding of potential current threats to the organisation.

3 Physical Breach

QinetiQ were chosen as the trusted security partner to run a full-spectrum red team exercise (including physical breach and simulated cyber-attacks) against a global financial organisation, their first ever exercise of this type.

This was a "Black Box" exercise, meaning no information was provided to QinetiQ up-front. Only a limited 4 or 5 key points of contact within the target organisation were aware that the exercise was taking place. As with any red team exercise, it is key the majority of staff are unaware, as they tend to be on their best behaviour if they believe an audit is taking place. If the organisation then passes with flying colours and relaxes for the rest of the year, little benefit is gained from the exercise and most importantly, a false sense of security is achieved, which can be very dangerous. This complacency then leads to a drastically increased risk of real breaches and the well-known consequences. It's often made worse by a reduction in security budgets in the coming year – driven by the false-positive results suggesting that less investment is needed to maintain a good security posture. We stressed the importance of secrecy around the exercise with our small group of stakeholders at each scoping and pre-exercise, kick-off meetings.

Three testers were deployed for this exercise, with one tester running remote attacks from the comfort of their hotel room, based upon our earlier Open Source Intelligence (OSINT) gathering phase. As a full-spectrum exercise, physical breach was of particular interest and importance to the client so myself and another tester were taking perimeter walks, noting entrances and exits, heavy footfall times, CCTV positions and general staff observations.

Despite our earlier conversations, it immediately stood out that the company we were exercising, sadly, had tipped off their entire staff that an exercise was taking place (later confirmed). This is understandable and is something we often encounter; individuals don't want to look unprofessional to their peers or management. We prefer to work collaboratively with our clients than instil this type of natural fear and from our vast experience as a trusted security partner.

We had been taking perimeter walks since 08:30 and it was now approaching 12:00 without a single staff ID pass observed being worn in public (a great success if this really was common practice!). The organisations' staff on either side of our client's HQ were almost all wearing their passes and would have been much easier targets. The contrast made us feel pretty confident the staff tip-off had taken place! We decided to give this until 12:00 and then change our approach. At 11:50, when we were discussing alternative ideas, a staff member passed us wearing their badge – JACKPOT! The pass was plain enough to memorise rather than risk taking a photo on a phone or from a camera-pen. We passed the formatting instructions to our tester in the hotel room who had designed and printed them by the time we went to pick them up.

The ID pass passed all the observation checks of a genuine-looking staff pass but we knew it wouldn't scan. We had decided against cloning RFID at this point (until next time) as this was a 1st engagement and we wanted to evidence the art of the possible, using more simple methods for the client to be able to bench-mark and improve upon.

This demonstrated that although the whole company staff were tipped off, it merely delayed our attempt for only a few hours on the first morning.

Back at the target site, the reception area was eerily quiet, too quiet with just me and my colleague. This left us pretty exposed - with a pass we knew wouldn't swipe and would arouse suspicion if the integrity was scrutinised. I approached the receptionists with a cover story that I worked for the local newspaper and engaged them both in conversation, asking questions back and forth between the two to keep their focus on me. As I was doing this we'd already prepared my colleague with a tray of coffee cups and he was waving his hip awkwardly at the anti-tailgate barrier sensor, his fake but genuine-looking pass clipped on to his belt (at this stage we didn't have a company branded lanyard). As my colleague acted more and more frustrated, I glanced over my shoulder to direct the receptionist's attention that way, and as I'd hoped, the receptionist opened the barrier for my flustered looking colleague. We were in!

He then chose an unoccupied meeting room, plugged into the network and hacked from the inside. Again, this was useful as a benchmark because we didn't need to physically risk breaching the client site - we'd already been successful from our hotel room, managing to set-up persistent access and exfiltrate sensitive data (previously agreed with the client), all without detection.

On his way out of the building, my colleague was able to help himself to one of the branded lanyards. If we did need to re-enter the site on further phases this would have further enhanced our credibility as genuine members of staff.

Following the report being issued, we worked with the client to address the issues we identified. By the time the board level presentation was delivered, we had worked closely with the Information Security team and they had already implemented some quick-fixes which rapidly reduced the significant risks. A positive and true representation narrative for the board is never a bad thing and this also pointed firmly to where the security budget still needed to be directed, backed by our evidence based findings.

It was fed-back by the board that this was their most valuable security spend of the financial year.

We're pleased to have been working with this client for almost a decade and each full-spectrum red team exercise is getting harder, something we love to see! This isn't a tick-box audit, it's sincerely about making your blue teams and your organisation much more resilient, all of the time, not just during an exercise.

Some of the improvements implemented by the client from this exercise were:

- An increase in ID and integrity checks at building entrances/exits.
- An organisation-wide improvement of security awareness culture, once the results had been shared of the very successful physical "breach".
- Upon reflection, the client agreed it was more beneficial to work with us on these exercises (rather than tipping off the entire workforce) to obtain a true picture and to not "game" the security exercise. This resulted in better value for money, as well as accurate evidence-based findings to benchmark, maintain and improve upon.

Conclusion

How secure is your organisation?

Our Full Spectrum Red Team exercises are specifically designed to help you identify the points of weakness that put your business and your people at most risk of attack.

Advanced Intrusion Exercise (AIE) – safely emulates nearly any potential threat actor from insider threats to nation state level, dependent on our client's needs or business type.

Multi Scenario Advanced Attack Simulation (MSAAS) – this exercise is delivered over a longer period of time (e.g. 6-9 months) allowing a more stealth based approach, mimicking real world adversaries as closely as possible compared to more traditional and common time bound exercises.

Red Team Cyber Attack Simulation – we safely emulate the cyber only elements of a targeted attack, network implants, spear-phishing, and internet based attacks.

Purple Teaming – designed to team up our Red Team specialists with your Blue Team defenders to identify tools, signatures and techniques used by threat actors before they become a problem.

For more information about how your organisation could benefit from our expert capability to deliver simulated attacks, visit our Advanced Red Teaming Services website or email us at cyber@QinetiQ.com

QINETIQ