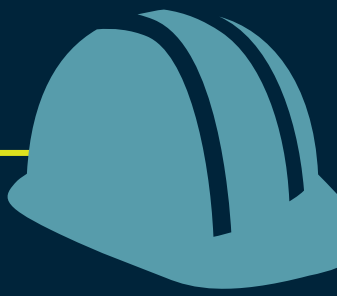
Red Team: A Case Study



Tier 1 Construction Company

The Company wished to remain anonymous in public-facing documents, but can provide a private reference upon request.

The Company had previously performed multiple penetration tests with other providers. Having received consistently clean results, with few vulnerabilities identified, the Company wanted to step things up and perform a long-term Red Team exercise to test the end-to-end security of their business.

Company's goals

The Company had three simple, but broad goals:

1. Identify issues and improvements to the Company's security processes.
2. Identify any vulnerabilities that may have been missed during previous security assurance activities.
3. Test the response of the SOC, and the security team.

> **We're not trying to tick a box. We're trying to find out how we can improve our posture.**
>
> *- Company's CIO*

Rather than perform a Red Team with a limited scope, the Company chose to holistically target the entire business. Attackers would not limit their scope when attacking a target, and the ability to think like hackers and mimic adversaries was essential to achieving the Company's goals.

"We don't want people to go to the dark side, but we were happy for the boundaries to be certainly pushed," emphasised the CIO.

Why Volkis was chosen over another consultancy

When asked, the CIO explained, "There was a sense of competence. 'These guys sound like they know what they're doing', we said."

Our passion, transparency, and empathy, play a big role in all of our work. But they are especially important during a Red Team exercise, due to the level of trust required. We are hackers! We love what we do and use our skills to help those around us.

Comparing us to larger companies, the CIO said, "If you go to the KPMGs and those groups, you're buying respectability, at least at a board level....But our experience is, often dealing with the bigger groups, you're paying for layers of cost and management."

This is where our size and team structure shine. Our consultants are well versed in both technical and human skills, meaning one person is accountable for the entire Red Team exercise, from organisation to execution, and communication throughout.

> **[With Volkis] we would be dealing with the people who were actually going to run it...That was important to us.**
>
> *- Company's CIO*

The exercise

The Red Team exercise ran for 5 months with multiple campaigns attempted throughout; some successful, others not. The Red Team were tasked with emulating a ransomware group as the most likely and damaging adversary to the Company.

Primary Objectives

- Show the ability to deploy ransomware on any system, server or workstation.
- Show the ability to impact day to day operations.
- Access and show the ability to delete backups.

Secondary Objectives

- Access sensitive information or information that may be perceived as sensitive by the public.
- Show the ability to perform invoice/financial fraud by changing details of a subcontractor.

Check out our Red Team Methodology

OSINT & infrastructure setup

This was the first, and most important, campaign as it would setup the rest of the Red Team exercise for success. Open Source Intelligence (OSINT) gathering was a valuable step for the Red Team and allowed us to discover the Company's assets, staff, email address, physical addresses, password leaks, documents, and more.

Additionally, bespoke phishing and, Command and Control (C2) infrastructure was setup to be leveraged in later campaigns.

Though there was not much progress in the way of gaining access into the Company, the information gathered would be invaluable in later stages of the exercise.

Gaining internal entry

Multiple phishing campaigns were performed with the goal of gaining user credentials. This campaign was partially successful, providing a username and password, but not a multi-factor authentication (MFA) token, preventing access to Internet facing services.

These credentials were taken on-site to the Company's office and used to access the wireless network. This was successful and gave the Red Team access to internal network and its systems. An implant device would later be left in a secret location for persistent remote access.

Lateral movement through the network

By chaining a printer misconfiguration with lateral movement techniques such as "Pass-the-Cert", the Red Team managed to gain Domain Admin privileges.

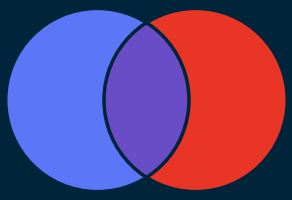
With this level of privilege, the Red Team stealthily deployed benign malware and explored the Company's assets such as documents in Microsoft 365 and data in accounting applications. This helped achieve all but one of the Red Team's objectives.

Failed campaigns

The Company's detection and response capabilities were effective. Throughout the Red Team exercise, we were detected several times and kicked off the network. However, through multiple persistence techniques and a flaw in the Company's incident response process, we were able to maintain internal network persistence.

Purple Team Workshop

After the exercise had wrapped up and a report was sent to the Company, a 2.5 hour workshop was performed with both the Volkis Red Team and the Company's Blue Team. The aim was to discuss what had occurred from both perspectives, giving each team the opportunity to learn from the other. Though the Red Team exercise is adversarial by nature, the workshop was light-hearted as we all ultimately had the same goal in mind: strengthen the Company's security.



Were the Company's goals achieved?

YES

The results of the Red Team exercise helped the Company close some obscure, but large gaps in their incident response process, along with some previously undetected vulnerabilities.

"We have already closed out the majority of issues," explained the CIO when asked about the progress just 2 weeks after the Red Team exercise concluded.

> **We had a lot more exposed than we thought we had... We didn't expect that you'd be able to traverse as well as you did across our environment.**
>
> *- Company's CIO*

VOLKIS™

Curious about your company's security posture?

Reach out for an obligation free chat about what a Red Team exercise might look like for you!

If you don't feel ready for a Red Team exercise, feel free to contact us about our other services that can help in the meantime.

info@volkis.com.au **www.volkis.com.au**