Red Team: A Case Study

Large Insurance Provider

This Large Insurance Provider (The Company) wished to remain anonymous in public-facing documents.

The Company has traditionally conducted annual penetration tests with other providers. However, they were looking to take things further beyond the limitations of a standard penetration test. By expanding the scope, they aimed to gain a deeper, more holistic understanding of their security posture.

The Company's goals

The Company partnered with Volkis to experience how a real attacker might target their business, attempting to breach sensitive Personally Identifiable Information (PII) from the Internet.

1. The Red Team assessment was designed to uncover hidden vulnerabilities and give the Company's Blue Team a live opportunity to respond to a simulated yet highly realistic breach.
2. They wanted to test how the Blue Team would respond once the "breach" was identified, allowing for gaps in incident response process to be plugged and provide staff with as close to real-world experience as possible in dealing with a breach.

Why Volkis was chosen over another consultancy

At first, there was some understandable hesitation among the board members. As the Non-Executive Director shared, "We just wanted to be sure that we could get as much experience as possible" and that "sometimes in the corporate world... we think you have to be big to be good"

But after meeting with Volkis, the Company saw, first-hand, a unique combination of flexibility and professionalism. They realised we could work together to tailor the Red Team engagement to their needs and deliver exceptional results.

The Company enjoyed the direct access to the consultants, the same people who perform the work, rather than dealing with layers of management.

The exercise

The Red Team exercise spanned five months, encompassing multiple campaigns, some successful, others unsuccessful. The team was tasked with emulating an Advanced Persistent Threat (APT), identified as the most likely and potentially damaging adversary to the Company.

Primary Objectives

- Obtain PII of specific customers
- Compromise VIP assets such as payroll or executive network shares
- Map the network topology

Secondary Objectives

- Find configuration documents for an internal asset
- Increase security level of an internal user
- Obtain source code of one or more web modules
- Change bank account details of a supplier
- Change bank account details of an employee
- Download contents of a database table to a network share

Check out our Red Team Methodology

OSINT & infrastructure setup

Open Source Intelligence gathering (OSINT) enabled Volkis to learn as much as possible about the Company without interacting with any of their infrastructure. This process involves Red Team identifying the Company's assets, staff, email addresses, physical addresses, password leaks, documents, and more.

Additionally, custom phishing and Command and Control (C2) infrastructure was built for use in later campaigns.

Even though, during this phase, progress in gaining access to the Company isn't made, the information gathered is valuable for the next stages of the exercise.

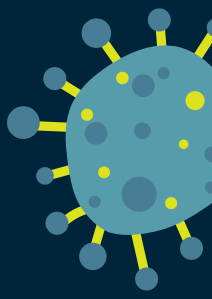
External Campaigns

The Red Team conducted multiple targeted phishing campaigns, each carefully crafted to test the resilience of the Company’s defences. These included fake help desk tickets, insurance complaints with malicious Excel attachments, and online cyber security training requests. The help desk campaign successfully captured a username and password, demonstrating the team's ability to breach the first line of defence, although multi-factor authentication (MFA) remained a barrier against unauthorised access to internet-facing services.

Armed with credentials, the team went on-site to the Company's office, where the wireless network extended into publicly accessible areas. Attempts were made to leverage these credentials for network access, but this was unsuccessful.

Even when campaigns don't achieve their primary goal, they're far from failures. Each attempt gives the Red Team a deeper insight into user awareness levels and the strength of the organisation’s security technologies. This knowledge informs future strategies and helps the Company understand how to better protect against real-world threats.

Implant



As the external campaigns did not result in access to the internal network, and physical intrusion was out-of-scope, the Red Team played a threat card. Threat cards are useful for when the Red Team is unable to progress towards objectives due to limitation that would not be there for real adversaries. Often they are along the lines of simulating an employee or contractor that has fallen victim to a phishing attack or plugging an implant into the internal network, to mimic a workstation that has been infected with malware.

The device was installed on the Company network by a trusted insider, which provided the Red Team with access to the internal network via a VPN connection.

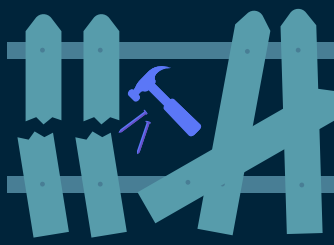
Lateral movement through the network

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

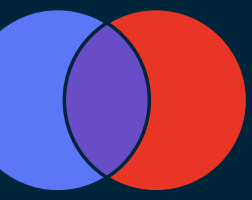
With this level of privilege, the Red Team stealthily deployed benign malware and explored the Company's assets such as documents in Microsoft 365 and data in accounting applications. This helped achieve all but one of the Red Team's objectives.

Incident Response

Once the Red Team had achieved as many of the Company's goals as possible within the given time frame, and the covert phase of the operation had reached its peak, the team turned up the volume on the internal network. The team escalated its activity until their presence was detected by the Blue Team, simulating a "breach" scenario that activated the Company's incident response plan.



This realistic and intense engagement provided the Blue Team with invaluable, hands-on experience. By facing a true-to-life adversary simulation, they were able to identify critical gaps in their defences and strengthen their response capabilities, preparing them for the real threats they might face in the wild.



Purple Team Workshop

After the Red Team exercise wrapped up and the reports were delivered to the Company, Volkis hosted a collaborative workshop with the Company's Blue Team. The session was designed to review the entire exercise from both the offensive and defensive angles, offering valuable insights and key lessons for everyone involved.

While the Red Team exercise simulated a real-world attack, the workshop transformed that experience into a joint effort to boost the Company's security posture. The Red Team guided the Blue Team through each campaign step-by-step, helping them identify which actions were logged, detected, or missed. This hands-on experience was crucial for improving the Blue Team's alerting, reporting, and overall threat response capabilities.

Executive Debrief

The Executive Debrief provided the leadership team with key insights into the Red Team engagement: what was done, the vulnerabilities discovered, and strategic actions that the Company can take to enhance security moving forward.

Were the Company's goals achieved?

YES

The Red Team exercise went beyond just testing defences. It highlighted areas where alerting systems needed fine-tuning, uncovered critical vulnerabilities that had been assumed fixed, and empowered the internal security team to refine and enhance their incident response policies.

With a Volkis Red Team, your organisation doesn't just check a box; you get real-world insights to stay a step ahead of real threats.

> **The report was a lot more comprehensive than we expected. Volkis provided a high level of detail on findings and recommendations... We came out with a lot more learnings and improvement activities then we would achieve out of a standard penetration test.**
>
> *- Company Board Member*

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**