



Red Team Attacks Fact Sheet v2.4



TIME TO GET REAL

Cyber-attacks are more targeted and financially motivated than ever before. The random whiz-kid and activist hackers have made way for disciplined and well organised criminal groups for hire to the highest bidder, costing Australian businesses millions each year.

The public and market expectations for security has and is continuing to grow rapidly. Legislation is also catching up and Australian Company Directors are now personally liable for breaches involving customer data, hence, driving cyber security up on the executive agenda.

Red Team attack simulations are the most realistic way to test the resilience of not only your IT controls (i.e. firewalls) but also of your people, processes and facilities. Our attacks will expose tangible and non-repudiable flaws in your security to be remediated.



HOW IT WORKS

Simulating a team of skilled and motivated attackers, the Privasec Red Team will craft and relentlessly execute a series of real-life attack scenarios to breach your security by any means possible (within the boundaries of the law and what is agreed with you). Thinking outside the box like a potential attacker, they will combine intelligence gathering, social engineering, hacking, physical intrusion and other deceptive techniques to compromise your defences and gain access to your most critical information.



RED TEAMING VS. PENETRATION TESTING

As opposed to traditional testing, Red Team attacks are multi-layered and focus on the objectives rather than on the method, allowing our team to think outside the box to create innovative scenarios you may not have planned or prepared for, allowing to you to identify blind spots in your defence strategy.

A Red Team attack scope primarily defines the don'ts (i.e. what cannot be done) rather than the do's, leaving our Red Team as unrestricted as an attacker would be.



METHODOLOGY

1. Your lead consultant will discuss the objectives of the assessment as well as the methods, techniques and systems excluded and included from the scope of the exercise. You can also ask for specific methods to be included if you need to test a particular process or policy (access card cloning, random dropping of USB infected sticks, etc).
2. Timeframes will be discussed and agreed prior to commencement and will depend on the level of sophistication desired.
3. You will be notified one day prior to commencement by your lead consultant. Our Red Team will remain anonymous to not influence the results of the attack one way or the other.
4. Our Red Team will conduct reconnaissance activities, including physical surveillance, intelligence gathering, cyber scanning, to identify potential gaps in security controls and craft targeted and concerted attack scenarios which they will then execute.
5. You will be provided with regular updates on the progress of the exercise.
6. At the conclusion of the exercise, a formal report will be presented to you, detailing step by step, the attacks carried out along with supporting evidence. The results of each scenario tested and prioritised recommendation to reduce your exposure to future attacks will also be provided.



NON-REPUDIATION

The effectiveness of Red Team attacks comes from its 'clear-cut' evidencing of security weaknesses. It bypasses the risks/potentials and other 'ifs' to deliver very tangible evidence which cannot be argued against.



GET THE BALL ROLLING

To discuss how our Red Team can help you test your defences and/or train your staff, call us on 1800 996 001 or email us at info@privasec.com. Our direct and flexible approach means we can get your Red Team attack going in as quickly as 24 hours.

Privasec

GRC
GOVERNANCE
AND INFORMATION
SECURITY PARTNERS

RED
RED TEAMING &
ADVANCED ETHICAL
HACKING

+61 1800 996 001 (AU)
+65 6610 9597 (SG)
+64 9 222 4725 (NZ)

info@privasec.com

www.privasec.com

New South Wales Office
Level 12, 234 George Street
Sydney 2000
NSW, Australia

New Zealand Office
Level 4, 17 Albert Street
Auckland CBD 1010
New Zealand

Victoria Office
Level 6, 276 Flinders Street
Melbourne 3000
VIC, Australia

Singapore Office
10 Anson Road
International Plaza #34-06
Singapore 079903

Queensland Office
Level 6, 200 Adelaide Street
Brisbane 4000
QLD, Australia

Malaysia Office
B-5-8 Plaza Mont Kiara
Mont Kiara 50480
Kuala Lumpur, Malaysia