Understanding the threat
Edward Farrell
Overview

- About us
- The problem we face
- What we don't understand about threats
- employing adversarial thinking
- Adversarial tradecraft to consider
About our team

- Penetration Testing
- Red teaming
- Threat emulation
- Digital assurance
- consulting & advisory
Shortfalls in our approach to (cyber) security

- ill defined terms of reference (what is cyber)
- Inward thinking on security
- We never contextualise
- We’ve forgotten why we’re here
This isn't a talk on specific threat actors.
Understanding the threat

- Thinking about the wrong threat
- Addressing signs & symptoms (root cause)
- Poor response practice (to all threats)
- Taking purely a PRA or “bad guy” approach

source: National Research Council
Causes of security issues

Pinkerton's paradox
There will never be a 1 size fits all threat
Contextualising the threat

Questions to ask:

- Where does the business derive its ability to sustain itself?
- what are critical processes or capabilities for this to occur
- what are the requirements for these processes
- What would make this the worst day for the organisation
- What would cause this to happen?
- How do we define & understand the problem at hand?
The application of adversarial thinking to understand threats
Historical applications of introducing adversarial thinking
Why we use adversarial thinking & methodologies

- Employs an open, honest framework of systems and processes
- Identifies and evaluates how the target environment appears
- Shapes our response to meet the likely threats & risks
- Rehearses our defence
- Efficiency

source: defence.gov
In cybersecurity, red teams exist to critically evaluate the technical, operational & procedural security of an organisation as they appear from an adversarial role or point of view.
Different approaches in cyberspace

source: little bobby comic strip
Why we’ve avoided the practice in Australia

Never had a demand/threat warranting the requirement for tradecraft or complexity (or so we think)

Risk adverse

Inward drive of the cybersecurity market

.AU focuses on the tech because purchasing power is driven by technologists

Product driven technology (what gets sold)

Old paradigms & control

Diversity of thought
Red Team - Characteristics

Digital

Social

Physical
### A client's subjective framing

<table>
<thead>
<tr>
<th>Currently</th>
<th>should be</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scare the boss for money</td>
<td>Are we getting value out of our activities?</td>
</tr>
<tr>
<td>prove I’m resistant to an “elite” attack</td>
<td>am I doing things right?</td>
</tr>
<tr>
<td></td>
<td>Rehearsing the defence</td>
</tr>
</tbody>
</table>

- Scare the boss for money
- Prove I’m resistant to an “elite” attack
- Rehearsing the defence
Poor planning
Poor execution

Craft does not scale
Setting up a red team for success

- Individual traits
  - Wheaton's rule
  - Be proficient!!!
  - humility
- Research, technology and business (what is the context)
- Establish control measures
- Communications, time and planning material
- Get creative
Some of our tradecraft
Good afternoon,

The following are your bank login credentials.

You can access your account by going to our website at https://CustomerLogin and enter the following: (These are not case sensitive)

**Company ID:**

**User ID:**YZUO

**Password:**welcome5
Search returned 1 results (1.8 seconds)

<table>
<thead>
<tr>
<th>Email</th>
<th>Username</th>
<th>Password</th>
<th>Leak Source</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:edward.farrell2@gmail.com">edward.farrell2@gmail.com</a></td>
<td>-</td>
<td>K00w0ng12</td>
<td>linkedin</td>
</tr>
</tbody>
</table>
Social engineering & manipulation
Over the air from the fire escape
Overcoming physical obstacles
Paths not seen
The accessibility of disruption
The drop box

• Useful for

• Close access when a place is under regular observation

• secondary link when you get caught

• MITM

• any foothold
Engineering a C2 network

- whereas most tech or assurance engagements are short lived, we take a bit of time to engineer

- Not all that expensive

- cost is in time, effort & understanding context
USB Drop

- Leonardo USB ATmega32U4
- Programmable Arduinos
- U$5.39 each
Challenge assumptions & call problems out