# Testing the system

I.G.Batten@bham.ac.uk

# “Tiger Teaming”

- aka Red Team, “ethical hacking”, penetration testing, etc, etc.
- Very popular, very trendy, probably great fun to do

# Objective

- People with skill are employed to “break” your security
- Tests both security policy and security execution
- Can be done by your own staff, by small outside companies, or offered as a service by large audit and security companies
    - Who might outsource it, of course

# Positive Results

- If they don’t break in, you presumably don’t have gaping open doors in your security
- Provides some confidence that your security policy is capable of providing some security
    - Of course, that assumes the tiger team aren’t idiots

# Negative Results

- Shows you that there is at least one flaw in your security, how it was exploited and (ideally) how to fix it.
- Might be policy, might be implementation, might be execution…but you should be able to figure it out.

# Problems

- Tiger team **motivations** are potentially different
- Tiger team **resources** and economic **incentives** aren’t realistic
  - (particularly, “give up and try the next company” less attractive to them)
- Tiger team **legal position** different
  - Less likely to use firearms and kidnapping: they don’t have a “Get out of jail free” card

# Freedom to Break Law?

- Extremely unlikely tiger team will be granted permission to commit criminal offences
- Companies can give *de facto* permission by failing to report or provide evidence, but cannot give *de jure* permission in case of assault, document fraud (in UK law, at least, possession of forged ID documents is an offence in its own terms) etc.

# Problems

- More likely to end up finding obscure technical weaknesses whose economic value to an attacker may not be great
- Less likely to find internal process and personnel weaknesses, as not their focus
- Also cannot blackmail, bribe or otherwise suborn staff without possible legal consequences
- Great fun for managers, though.

# War Gaming

- Like a tiger team, but a paper exercise
- Instead of trying to break into the real enterprise, an exercise is conducted in a room, with the paperwork to hand, and referees to adjudicate “battles”.
- Has the disadvantage of being entirely unrealistic
- Has the advantage of allowing examination of illegal acts
- Expensive, and not as exciting for managers

# Hostile Audit

- Usually there is tacit understanding with auditors that they aren’t there to tear the whole system apart
- Most auditors are being paid by the people being audited, and want repeat business
- Sometimes you can get auditors who don’t have those sort of constraints, for example internal security people in a large multi-national
- They can “white box” examine systems and processes and report

# Learning Lessons

- Main problem with all these approaches is **WHAT DO I DO NEXT?**
- Is a security system which consists of patches applied to fill individual holes worthwhile?
- Hence continuous improvement needs to look at root causes

# Exercise

- Suppose a tiger team penetrated the network by using a security vulnerability on a machine which hadn’t been patched.
- That’s all you know: “there was a machine, it wasn’t patched”.
- What might be the reasons it wasn’t patched?

# Causes

- Failure of patching
- Failure to try to patch
- Failure to include in list of machines to match
- Failure to include in list of machines that matter
- Failure to firewall
- Failure to audit
- …

# Root Cause Analysis

- Is the solution:
  - apply the patch?
  - revisiting patching policy?
  - revisit security awareness?
  - revisit top-level security policy?
  - What else?

# Not on Asset Register

- Just add it to the asset register?
- Look at the scope document?
- Check how the asset register was built?

# AAIB / RAIB

- Air accident investigation board (used to be “branch”)
- Rail accident investigation board
- Their reports are detailed, dispassionate and find root, root causes

# G-BJRT, June 1990

- Windscreen failed on a BAC 1-11 flying out of Birmingham airport
- Pilot partially sicked out (this is not a real photograph, it's a reconstruction)
- Problem was traced to careless use of bolts that fitted but weren't long enough, uncalibrated torque wrenches, a whole host of issues
- "84 of the 90 windscreen retention bolts were 0.026 inches (0.66 mm) too small in diameter, while the remaining six were 0.1 inches (2.5 mm) too short."

# Root Cause Analysis

- Time consuming
- Expensive
- “What’s the point, we know anyway?”
- Absolutely vital