I <3 Reporting

Managing Effective Web Application Assessments

Andrew Evans

A bit about me

- Total corporate InfoSec sellout - 2 years govt.nz, 7 years banking
- Currently working for a Kiwibank as a security jack-of-all-trades
- Formerly penetration testing manager for a very large UK bank

- Disclaimer – These are my own opinions, not those of my employer or my dark mistress, any offense caused to project managers or consultants is intentional. This is entirely based on my own experience, YMMV. WARNING - May contain traces of oddy.
- This powerpoint has very few pretty pictures, because I operate using a total quality management “just-in-time” principle when creating slides.

Penetration Testing - definition

Penetration testing aka Ethical Hacking aka Vulnerability Assessment........

All variations on a theme, I'm not going to go into the debate on what constitutes a penetration test

For this presentation – a consultant driven vulnerability assessment of a web application

Penetration Testing Management

The Value of a penetration test is dependent on a number of things

- Vendor Selection
- Test type selection
- Scope
- Test Preparation
- Logistics
- Reporting

Vendor Selection

- Variable quality - difficult to assess skills
- Build a relationship with a quality supplier, but also consider rotating suppliers
- Not all penetration testers are created equal
- Different levels of expertise
- Different specialisations
- Reassess quality regularly
  - People leave
  - Management changes

Vendor Selection

- What to look for
- Reputation
- Research & Innovation
- Industry/Community Involvement
- Specialised security consultancies
- Lack of corporate bollocks
- Good consultants
- Professionalism and Communication

Consultants vary - Good

Consultants vary - Bad

Consultants vary - Ugly

Test Types

- Vulnerability Scanning
- Infrastructure Testing
- Web Application Testing
- Build and Configuration Reviews
- Code Reviews
- Red Teaming
- Bespoke testing

- What do you need? What is the risk facing your application?

Black Box vs White Box

- Black Box Testing – Testers have no prior information
- White Box Testing – Testers have information and access

- Black Box testing = meh
  - Same results for more time and cost
  - Attackers effectively have an infinite amount of time for information gathering

Scoping

- SCOPE RESTRICTIONS MAKE SECURITY HULK ANGRY
- Test all elements of the application, including third party components if possible
- Have scope restrictions recorded as a finding in the report
  - Not tested = vulnerable
- Scope should be used to define what you care about, save testers time, save $$$
- Also – known things that make production systems go boom

Scoping continued

- Scoping should really be about sizing the test
- How many days/How much it costs
- Scoping is the darkest art of all those practiced by web app pen testers
  - Man day requirements for a web app test based on a variety of things
    - Whether the moon is waxing or waning
    - If Jupiter is in the 7th house
    - Whether the consultant is in need of a shiny new Galaxy S II
    - Size & Complexity of the application
    - Number of user types

Test Preparation

- Set up secure communications
  - PGP, Encrypted zip files at a pinch
- Give your testers as much as possible
  - Credentials – for ALL user types
  - Design Information
  - User Manuals
  - Administrator manuals
  - Software information – OS, Middleware versions, Databases…
  - Source Code

Letters of Authority

Letter of Authorisation

- Blah blah allowed to access system blah blah recognise testing inherently risky blah consultant is in no way responsible for the end of civilisation etc
- Specify system, IP addresses, URLs
- Particularly important for third party systems
- Don’t let the lawyers mess with it too much

- Vital for testing third party systems

Logistics

- Vastly underrated, easily neglected
- Screwed up by everybody, including me
  - Credentials
    - At least two sets for each level of access
    - If there is a separate admin function – specify
    - Accounts will get locked out
  - Make sure the users have relevant test data and structure preloaded if necessary
  - Change Control
  - Network Access/Cabling/Ports
    - Make sure they are in place and working
    - Firewall rules

Logistics

- Technical Contact – for when the system breaks
  - Account lockout
  - General weirdness
  - Explanations of how systems work
- Escalation Contact – for when the technical contact is being a …

- Availability is vital – are you paying $250/hr for a consultant to do nothing?

Logistics Continued

System Availability

- Is it ready for testing?
- Are you going to mess with it during the test period? (hint – DON’T)
- Is it “production ready”
- No really, is it ready for testing. HAVE YOU CHECKED!

- Desk and chair for girly overpaid prima donna consultants
  - Real men sit on top of air con vents in a data centre with a laptop on their knees

Reporting

- This ones for you consultants
  - The report is pretty much the only mechanism for the client to judge the quality of the test
- Introduction
  - Who, what, when, where
- Exec Summary
  - Brief description of findings
  - General commentary on security posture
  - General recommendations
- Pretty Graphs and Diagrams – badness

Reporting continued

- List of findings
  - MUST BE REPEATABLE by a sysadmin or developer
  - List all areas where an issue was found
    - XSS in the following parameters on this page
    - XSS in the following parameters of this other page
    - Keep the core of the report relatively brief - use appendices
  - Actionable Recommendations
    - Where possible, be specific about how to fix a problem
  - Consider the implications of bug chaining
    - Demonstrate bug chaining - A++ would hire again
    - Rate risk accordingly

Reporting continued

- Document everything
  - Scope Restrictions
  - Issues that impacted on tested
  - Cover your arse – if you missed something your client could be very pissed at you later
  - Opinions based on experience

- Report Templates are your friend
  - DO NOT COPY AND PASTE FROM PREVIOUS REPORTS - YOU WILL SCREW UP ONE DAY

Final thoughts

- Work with your pen testing provider
- Learn from them – ask to sit in on some of the testing

- Don’t run before you walk – sort out the basics before doing uber ultra special red team exercises
- Automated tools are largely irrelevant – particularly for web applications

Hackers don’t give a shit

- About your project scope
- It’s managed by a third party
- It’s a legacy system
- It’s “too critical to patch”
- About your outage windows
- About your budget
- You’ve always done it that way
- About your Go-Live Date
- It’s only a pilot/proof of concept
- It’s an internal system
- It’s really hard to change
- It’s due for replacement
- About your Risk Register entry
- The vendor doesn’t support that configuration
- It’s an interim solution
- It’s PCI compliant
- “Nobody else could figure that out”
- You can’t explain the risk to “The Business”