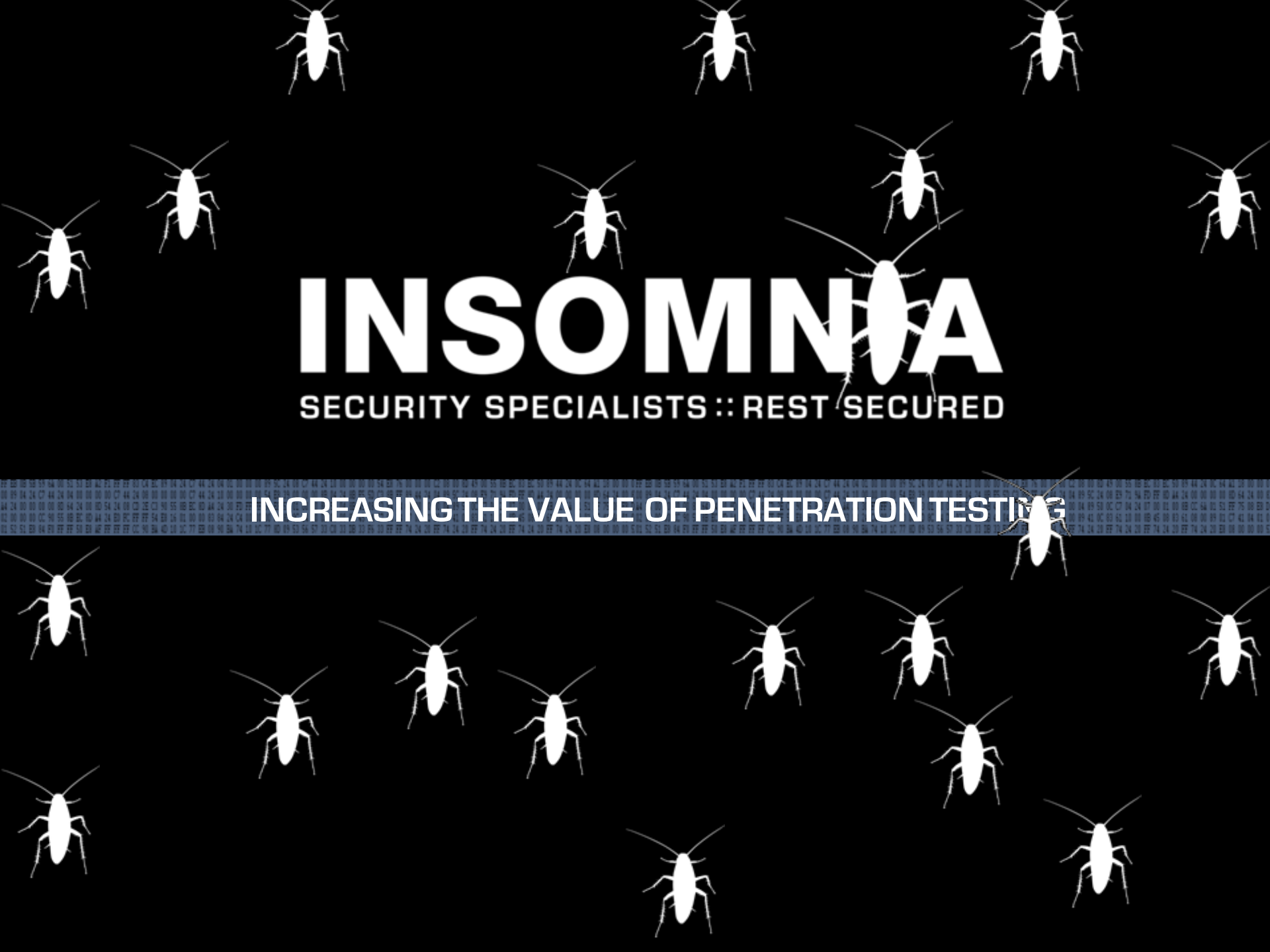

INSOMNIA
SECURITY SPECIALISTS :: REST SECURED
INCREASING THE VALUE OF PENETRATION TESTING

ABOUT YOUR PRESENTER

Brett Moore

- Insomnia Security

New Zealand Company

- Six full time technical staff
- Offices in Auckland and Wellington

Penetration Testing

- Web application reviews
- Red team testing
- Source code reviews

Agenda

- What is penetration testing?
  - Why should this type of testing be used?
  - When should it be carried out
- The value penetration testing
  - Measuring the ROI
  - Value of the result
- Increasing the value of penetration testing
  - Decreasing the time and costs
  - Getting the best possible result
  - Increasing the value of the results

What Is Penetration Testing

An independent evaluation

- To confirm things are secure
- To find flaws in procedures

Third party appraisal

- Ensure target is ‘secure to current levels’
- On-going review

Compliance

- Regulatory assistance
- Legal obligations, Liability

What Is Penetration Testing?

A security review of IT systems

- Network review
- Server hardening
- Application review
- Source code review
- Wireless Review
- Red team testing

INTERNAL

EXTERNAL

WHITEBOX

BLACKBOX

Other areas of review

- Policy, standards
- Physical, processes

What It's Not

It guarantees my systems secure

- It is only part of the solution

I've had it done, why do it again?

- Provides only a snapshot view

Gives a real 'hackers' view

- A real attacker has no limits

The statistical argument

An ever increasing number of numbers

Mar. 26, 2008	Broward School District (Coconut Creek, FL)	A Atlantic Technical High School senior hacked into a district computer and collected Social Security numbers and addresses of district employees.	35,000
Mar. 28, 2008	Antioch University (Yellow Springs, OH)	A computer system that contained personal information on about 70,000 people was breached by an unauthorized intruder three times. The system contained the names, Social Security numbers, academic records and payroll documents for current and former students, applicants and employees.	70,000
Mar. 31, 2008	Advance Auto Parts (Roanoke, VA)	The retailer reported that a "network intrusion" had exposed financial information and was the subject of a criminal investigation. Fourteen of the retailer's stores, including locations in Georgia, Ohio, Louisiana, Tennessee, Mississippi, Indiana, Virginia and New York, are believed to have been affected.	56,000
April 1, 2008	Okemo Mountain Resort (Ludlow, VT) (866) 756-5366	The Ludlow ski area announced that its computer network was breached in by an intruder who gained access to credit card data including cardholder names, account numbers and expiration dates.	28,168

Why Pay For Penetration Testing

Automated Tools

- Why pay someone to use automated tools
- Anyone can run nmap/qualys/nessus

The human factor

- Tools are flawed
- Humans can make decisions
- Logic/functional flaws
- The ‘thinks like a hacker’ mantra

Why Pay For Penetration Testing

Key benefits

- Provides an independent evaluation

- Prevents financial loss
- Provides due diligence and compliance
- Protects brand and reputational value

- Helps with risk analysis and management
- Provides justification for security spend

Measuring The Value

Measuring the ROI

- Difficult to do
- Similar to a health check
- You don't know until someone looks
- Insurance

Information assets

- What is the value of the data you protect
- Loss of reputation
- Data is grouped into security zones
- You should know where your data is

Measuring The Value

Value of the result

- Beyond just the target of the review
- Address the root cause
- Apply against the whole organisation

report states that there is a lack of patches to the server. Wouldn't it be a good idea to have one of the system administrations check other servers for patch levels?

Take this one step further and review the internal patch management procedures, to determine why the servers were allowed to be deployed without proper patching.

When Should It Be Done

Driven by value of information asset

- Now, if you have never done it
- Yearly, internal critical assets
- Yearly, password and account audits
- 6 Months, full perimeter review
- Monthly, automated vulnerability scanning
- Project, all new projects and changes

Back In The Real World

- Intangible ROI is a prohibiter
  - Explaining the need is difficult
  - Use other companies compromise to your advantage
- Remove the adhoc approach
  - Requirements as part of acceptance
  - Servers to be hardened
  - Application secure software development
  - Grade applications to a threshold

Cost vs Gain

Cost is still the prohibter

- Increases the cost of a project
- We want to lower the cost

Independently reviewed

- This could be an internal peer review
- Publicly available checklists

Projects are different

- Have different risks associated with them

Steps To Take Before A Review

Identify the required outcome

- Quantifies time, effort and money
- Going through the motions?
- PCI compliance
- Seriously worried?

Think about the report

- What reporting do you require?
- What will it be used for?
- Is an automated tool report suitable?

Steps To Take Before A Review

Get ‘buy in’ from the project team

- The tester is not the enemy
- Bringing in a security specialist
- Help to get those known problems fixed

Do some internal scoping

- Think about what will be tested
- Define the components in detail
- If you don’t know, then how will the supplier

How Not To Do It

Bad scope

No threat modelling

Lack of communication

Steps To Take Before A Review

Internal threat modelling

- Determines the risks to a project
- You are in the best position to do this
- The testing team should ask for this

Do some initial testing

- Use freely available tools, nmap, nessus
- System administrator can check patches
- Doesn't replace an experienced tester

Selecting Your Provider

Trusted advisor

- Included in project meetings
- Trusted service provider

Everyone is not equal

- Different fields of expertise
- Experience means more than qualifications

Team Capability

- Rotate staff for recurring reviews
- Mixed level teams

Selecting Your Provider

Data storage and retention

- Dealing with sensitive information
- Non disclosure agreements
- What is the data storage process?
- Encrypted? … Always?
- What happens after the review

You need to know where your information is

- An information asset stored offsite

Selecting Your Provider

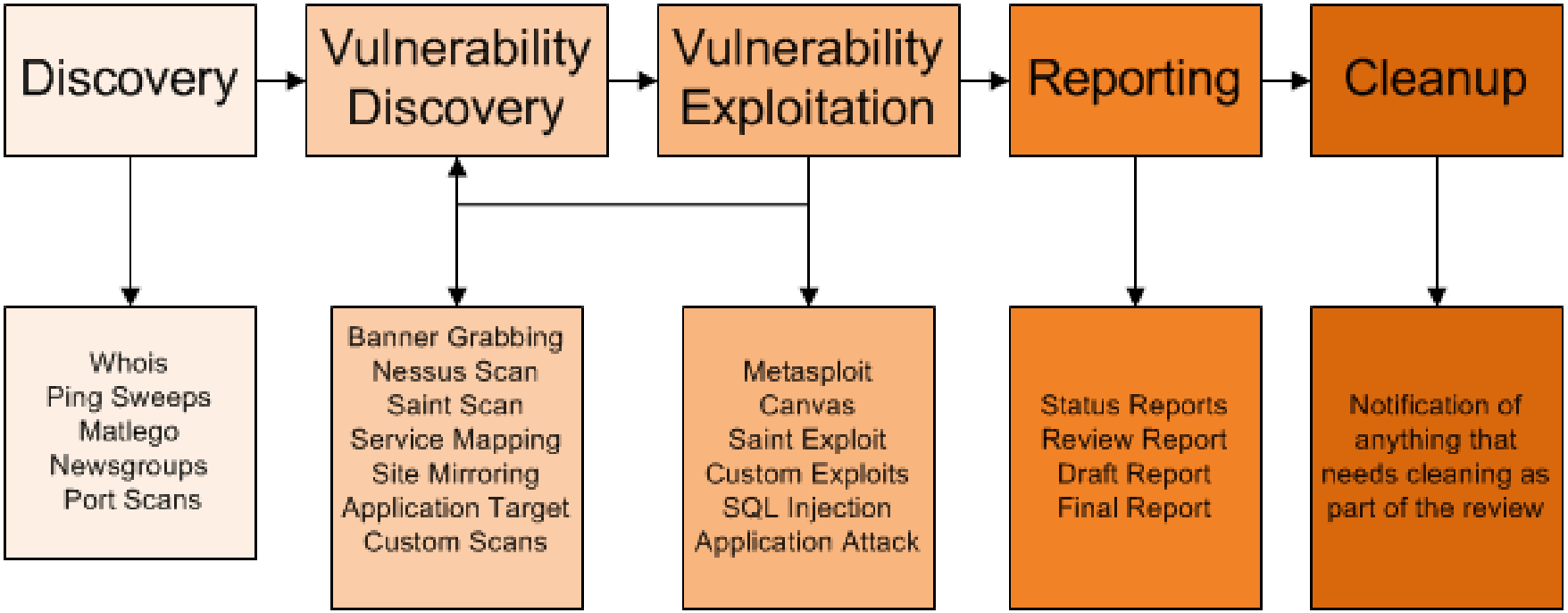
Report type and follow up

- The report is the deliverable
- Detailed analysis and recommendations
- Automated tool output?
- What do you need in the report?
- Is the report style flexible?

…our supplier for a sample report. The information in the report, the way it is presented and the details of both the vulnerabilities and the recommendations, are what you pay for.

Methodology and tools

- A standard approach to testing
- Not a checklist audit
- OWASP, OSSTMM



Selecting Your Provider

Tools

- Commercial tools cost a lot of money
- Testers should use tools
- Should always validate the results
- Use of public exploits allowed?

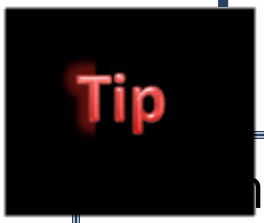
References

- Difficult to get due to NDA
- Your supplier should not be publicly known
- Small IT industry in New Zealand

Before The Review

Scoping is not a sales exercise

- You have picked a supplier
- Costing without scoping is guesswork
- Internal scoping already done
- Supplier can add value through advice
- Experience + methodology = estimate



he person who will be doing the testing involved with the scoping. Allow them to see the target, view some documentation, or view the source code.

Even an initial scan of an environment can help estimation

Before The Review

Time and project slippages

- Have a set timeframe for the review
- Communicate slippages with supplier
- Who pays for downtime?

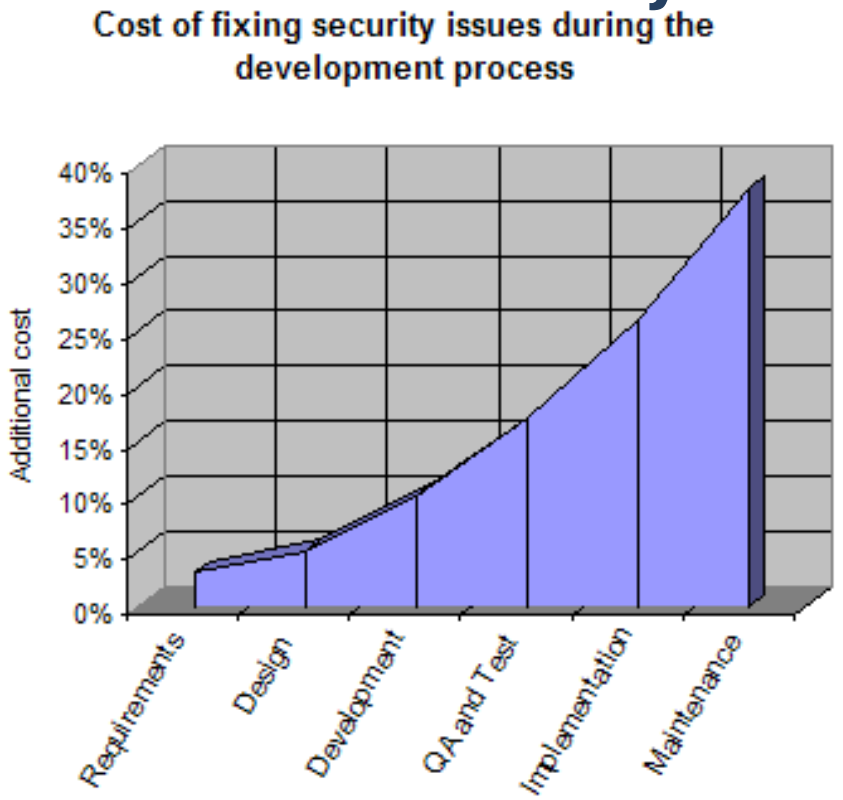
e there is communication at least a week prior to the start of the review, even if there are no slippages.

There are activities that can happen before the review that will help increase the value of the work to be done

Before The Review

Get the review team involved early

- Secure development lifecycle
- Still left till the 'security signoff'
- Security from the start saves money



Before The Review

Bring the review team up to speed

- Not only technical aspects of components
- How they fit into your environment
- Understand the risks to the business
- Any related documentation

is used more efficiently when the reviewer works closely with the project team.

During The Review

Black box review is less effective

- Real attacker is not limited
- Limit time spent on zero knowledge attack

Give them what they need

- You want the best possible result
- Host access, network docs, server logs
- Source code,
- More effective, More accurate

During The Review

Be ready for them

- Have all information ready
- If possible, send through before the start
- Confirm credentials and access

Have suitable access available

- Are they going to be onsite?
- They will want to connect their laptops

ester will be limited if they are not able to use their tools properly. This will increase time and reduce accuracy.

During The Review

Freeze the project

- Or at least communicate outages
- Prevents confusion
- Don't fix vulnerabilities silently

Become involved with the tester

- Open communication
- Verbal status reports every couple of days
- Project team could learn something

After The Review

Review the report

- This is what you have paid for
- Are you happy with the report
- Any areas need clarification

Understand the root causes

- Lack of procedure and process documents
- Prevent the same issues in other projects
- Apply mitigation to other projects

After The Review

Meet with the project team

- Have a team meeting to discuss report
- Congratulate, do not persecute
- Pass lessons learnt to other projects

Consider security training

- Security is a specialised field
- Education is an effective defense
- Courses, books, online material

After The Review

Take action

- Most important
- Not another dust gatherer
- If overwhelmed, seek help

Consider regression testing

- Depending on results
- Should not take the supplier long

In Summary

- Decrease time, increase value
- Maximise the use of results
- Scope accurately for best effect
- Do basics ourselves
- Have trusted suppliers
- Get them involved early with projects
- Open book approach to testing
- A report that works for us
- Understand the root causes of issues
- Open communication between parties

www.insomniasec.com