VULNERABILITY MANAGEMENT AND RESEARCH PENETRATION TESTING OVERVIEW

Len Kleinman
Director ATO Trusted Access
Australian Taxation Office
What is Vulnerability Management?

“The on-going approach to the collection and analyses of information regarding vulnerabilities, exploits and possible inappropriate communications in identifying the level of IT risk the ATO may be facing at any one instant in time.”

*Vulnerability Centric – Evidence based*
Vulnerability Management:

Security Testing:
- Penetration Testing
- Security Assessments
- Red teaming
- Production System testing
- Verification testing

Threat Intelligence:
- Incident response
- Monitoring and alerting

Innovation Development
Vulnerability Management and Research – Anatomy of VMR

- Technical Forensics
  Detailed analysis and extraction of artefacts to gain in depth working knowledge

- Incident Response
  Prepare, Identify, Contain, Eradicate, Recover, Lessons Learned

- Penetration Testing
  Liaison, Testing, Reporting, Debriefing, Signoff, Handover

- Security Assessments
  Security evaluation of a particular technology

ATO
Whole of Government
3rd Party Providers
Vulnerability Management and Research – Anatomy of VMR

- **Strategic Technical Advice**
  - Liaison, POGs, Reporting, Technical Advice, Projects

- **Technical Forensics**
  - Detailed analysis and extraction of artefacts to gain in-depth working knowledge

- **Incident Response**
  - Prepare, Identify, Contain, Eradicate, Recover, Lessons Learned

- **Penetration Testing**
  - Liaison, Testing, Reporting, Debriefing, Signoff, Handover

- **Security Assessments**
  - Security evaluation of a particular technology

- **Threat Intelligence**
  - SIC and monitoring services

- **Network Security Monitoring**
  - "Eyes on glass" near real-time monitoring of ATO ICT environment

- **Data Mining / Log Analysis**
  - Using SAT, conduct data mining and log analysis for incident detection

- **Research Whitepapers**
  - Prepare white papers on current IT Security related topics

- **Phishing**
  - The notification, analysis, tracking and recording of phishing attacks

- **Research**
  - Research on new vulnerabilities, tools, patches, attack and defence techniques

- **Inter-Branch Advice and Collaboration**
  - Branches include MCL, SNC, ME&I, OCIO, SPS, CS&I

- **International and Inter-Agency Collaboration**
  - Agencies include AFD, Defence, DSD, AGIMO, AusCERT, ACMA, IRS, Resuce (HMFG, NZ IRC)
Vulnerability Management and Research – Anatomy of VMR

**Provision of Technical Knowledge**
- Coordinating/Assembly of technical/security content

**Penetration Testing**
- Liaison, Testing, Reporting, Debriefing, Signoff, Handover

**Security Assessments**
- Security evaluation of a particular technology

**Threat Intelligence**
- SIC and monitoring services

**Network Security Monitoring**
- "Eyes on glass" near real-time monitoring of ATO ICT environment

**Data Mining / Log Analysis**
- Using SAT, conduct data mining and log analysis for incident detection

**SAT** (Security Analysis Toolkit)
- Suite of tools to facilitate Information Gathering, Analysis, Alerting and Reporting
  - SOS WebFrontend
  - Presentation and Analysis of source/log data
  - SAT DB (High Performance storage of source/log data)
  - SOS DB (High Performance storage of alert data)

**SAT Download**
- Acquisition of source/log data for analysis
  - Internet
    - Internet traffic logs
    - Antivirus
    - Intrusion Detection logs
    - IDS/IPS
    - Behavioural analysis of traffic
  - Email
    - Inbound and outbound emails
  - Active Directory
    - Microsoft Active Directory logs
  - Secum Token
    - Secure Token for VPN and VDI

**Incident Response**
- Prepare, Identify, Contain, Eradicate, Recover, Lessons Learned
- Analyse and Remediate
  - Detect and Collate

**Technical Forensics**
- Detailed analysis and extraction of artefacts to gain in depth working knowledge

**Strategic Technical Advice**
- Liaison, PoCs, Reporting, Technical Advice, Projects

**International and Inter-Agency Collaboration**
- Agencies include AFU, Defence, DSD, ASIO, AUSTRAC, ACMA, Interpol, NZISD

**Research Whitepapers**
- Prepare whitepapers on current IT Security related topics

**Phishing**
- The notification, analysis, tracking and recording of phishing attacks

**Research**
- Research on new vulnerabilities, tools, patches, attack and defence techniques

**Inter-Branch Advice and Collaboration**
- Branches include MOC, SIC, MEBC, CCIO, SPS, CSBS

**Verification and Confirmation**
- Retesting of previously discovered vulnerabilities
  - Testing SHP mitigations
  - Testing IR mitigations

**Covert Penetration Testing**
- Holistic Whole of Organisation Security Testing

**Production Security Testing (PST)**

**Training and Skilling**
- Mentoring, wargames, continued development of technical skills, Professional Certifications, High level conferences (e.g. Blackhat and Defcon)

**Outsourcer Engagement**
- ESMC, HPES, MNS etc.
  - Evaluation of outsourcer’s tools and processes
  - Investigation of new Security Products in liaison with outsourcer
  - Security Technical Working Group
  - Appraisal of IT Security service delivery

**SAT (Security Analysis Toolkit)**

**Analysis Engines**
- Automated detection

**Development**
- Tool development

**Sandboxing**
- Automated drive-by download malware analysis

**Workflow**
- Workflow scheduling, recording and statistics

**Static file analysis**
- Automated email attachment malware analysis

**AutoDoc**
- Automated Report Generator

**FPC**
- Full Packet Capture – all data in and out of the ATO

**Hash Compare**
- Compare files with other known bad files from external sources

**Pen Test Networks**
- Networks to facilitate all areas of VMR work
What is a Penetration Tester?

► An Out-of-the-box thinker
► One who bends computers to their will
► What’s with the hats?

Black = Cracker, script kiddie

White = Ethical Hacker / Corporate Hacker

Grey = Full disclosure and Hactivist
What is a Penetration Test?

“A program of systematic testing that identifies weaknesses inherent in IT systems. System owners and Security administrators use the results of the testing to improve the security posture of the application/system and therefore improve the overall ATO IT environment.”
How we developed our capability – The Journey

- Started small – focus was on **reporting** on vulnerabilities
- Decision to develop hands on capability
  - **Application** focus
  - Collaborative effort with a provider
- Applied relevant training and skilling program
- Developed our risk matrix
- Extended scope to include network security testing
- Extended to full system testing as per NIST definition
- Extended function to Red teaming
- Extended function to production systems testing
How we developed our capability – The Journey

- NIST definition of System NIST SP800-42 Guideline on Network Security Testing:

  **System** – A system is any of the following:
  + Computer system (e.g., mainframe, minicomputer)
  + Network system (e.g., local area network [LAN])
  + Network domain
  + Host (e.g., a computer system)
  + Network nodes, routers, switches and firewalls
  + Network and/or computer application on each computer system.
How is a Penetration Test performed?

- Penetration Test Team coordinates with the project manager
- Client Consensus Statement – Set and manage expectations
- Penetration Test results peer reviewed
- Draft report circulated for review by relevant stakeholders
- Once a Penetration test is finalised, it is approved and signed by:
  - Senior Director VMR
  - The CTO/AC Trusted Access; and
  - The system owner
- VMR conducts de-briefing sessions with the System Owners
  - Flows into the education and compliance aspects
  - Any residual risk is accepted by the System Owner
Plan & Organise
Perform pen test on new or significant version change system

Document & Escalate
Articulate cause and propose a course of action

Continuous Improvement
Check and re-check by regularly testing, even Production systems

Communication & Remediate
Report and brief identified risks to permit treatment

Evaluated state of security posture for the system and the organisation

Application Standards
Best Practice
Legislation and Policy
VMR’s penetration testing is normally conducted in four phases:

<table>
<thead>
<tr>
<th>Test Phase</th>
<th>Planning and Reconnaissance Phase</th>
<th>Information Gathering. Setting up and setting expectations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Probing Phase</td>
<td>Vulnerability Identification</td>
<td></td>
</tr>
<tr>
<td>Attack Phase</td>
<td>Exploitation of identified vulnerabilities through penetration Optional - social engineering Optional - physical penetration</td>
<td></td>
</tr>
<tr>
<td>Reporting Phase</td>
<td>Detailed reporting on the activities, results and recommendations as a result of testing</td>
<td></td>
</tr>
</tbody>
</table>
## Structure of a Pen Test: Incorporating DREAD model

<table>
<thead>
<tr>
<th>Consequence</th>
<th>Consequence Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insignificant</td>
<td>No injuries, low financial loss</td>
</tr>
<tr>
<td>Minor</td>
<td>First aid treatment, on-site release immediately contained, medium financial loss</td>
</tr>
<tr>
<td>Moderate</td>
<td>Medical treatment required, on-site release contained with outside assistance, high financial loss</td>
</tr>
<tr>
<td>High</td>
<td>Extensive injuries, loss of production capability, off-site release with no detrimental effects, major financial loss</td>
</tr>
<tr>
<td>Very High</td>
<td>Death, toxic release off-site with detrimental effect, huge financial loss</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Likelihood Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Almost certain</td>
<td>Is expected to occur in most circumstances</td>
</tr>
<tr>
<td>Likely</td>
<td>Will probably occur in most circumstances</td>
</tr>
<tr>
<td>Possible</td>
<td>Might occur at some time</td>
</tr>
<tr>
<td>Unlikely</td>
<td>Could occur at some time</td>
</tr>
<tr>
<td>Rare</td>
<td>May occur only in exceptional circumstances</td>
</tr>
</tbody>
</table>
### Structure of a Pen Test:

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Consequences</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Insignificant</td>
</tr>
<tr>
<td>Almost certain</td>
<td>H</td>
</tr>
<tr>
<td>Likely</td>
<td>M</td>
</tr>
<tr>
<td>Possible</td>
<td>L</td>
</tr>
<tr>
<td>Unlikely</td>
<td>L</td>
</tr>
<tr>
<td>Rare</td>
<td>L</td>
</tr>
</tbody>
</table>

- **E**: extreme risk; immediate action required
- **H**: high risk; senior management attention needed
- **M**: moderate risk; management responsibility must be specified
- **L**: low risk; manage by routine procedures
Diversity and variety is very important
   - Rotation within the team.

Early notification
   - Don’t do it!

“Mini” pen test
   - No such thing. Do they mean a vulnerability scan?

Verification test
   - Do not accept in blind faith.
   - Prepare for the growth.

Recruit appropriately.
The Challenge:
What is it good for? The “Value” component

- Tests exposure of **known** security threats and vulnerabilities to both internal and external attack.
- Provides a **snapshot** in time of what security looks like. Sets a benchmark.
- Assesses monitoring and **escalation** procedures.
- Provide advice, solutions and recommendations to enhance the ATO’s security posture at both the **enterprise** and/or **process** level.
What are the benefits? The “Value” Component

- Improved information security knowledge and understanding around the real threats and vulnerabilities in ATO systems and processes.
- Proactive identification of potential risk and provision of assistance in mitigating these risk immediately.
- Assist in the decision making process e.g. Go Live!
- Education opportunity, ….BUT
  - Only for those who want and can be educated.
Problems, Issues and Concerning Observations

- Too many **Generalist** playing in the **specialist** space.
  - Everybody wants in!
  - Terminology matters.
- Increasing sophistication of attacks.
- Is **not** assurance/compliance/audit work – It can be part of a program where level of assurance is derived from an interpretation of the results. Assurance is subjective.
- Massive gap in technical understanding by persons in a position of responsibility and accountability.
Vector of attack that allows the risk to be realised
Takeaways

✓ Have a thorough documented methodology.
✓ Ensure you can articulate the “value”.
✓ Quality of Results = methodology + skill + reporting
  ➢ Clear reporting = ability to remediate.
✓ No substitute for capable, qualified, compatible staff.
✓ Hands on Testing cost more then “check-box testing” but is reflective of reality, cost more i.e. time and money.
✓ Volatile environment – increase sophistication of attacks, increased requirement for expertise, increase requirement to maintain skills.
Our expectation is that a penetration test of systems being relocated from X Data Centre to Y Data Centre is unnecessary as these systems are being moved within network boundaries that have been previously tested.

That vulnerability has always been there therefore…

“The system was built in 2002 and the secure coding standards being applied are the 2012 standards. Therefore, we will not be fixing the vulnerabilities identified as the standard is after the build date.”
That vulnerability is not within the scope of the XXX application and we should not be held responsible.

“…their observed vulnerability for cross site scripting is a common website condition, even evident in the current XXX website, and hence there was an expectation set that there would be no change to the XXX Web Site to resolve this.”

“This vulnerability will not be addressed as part of XXX Upgrade, as mentioned in previous updates the vulnerability was via open ports which is a potential vulnerability for all apps.”