Tightening IT Security

Security Review and Penetration Testing of Complex Environment

By Anton Bolshakov

KIT 2015, April

About Me

Anton (aka blshkv)

- 15 years in security business, 13 years in Singapore
- Network, Wireless, Radio, Mobile, Application, VoIP penetration testing and forensics
- Industries: Financial, Medical, Transportation, Oil&gas in Apac region
- Current: ITDefence.asia
- Developer of Pentoo Linux

Regulatory Authority

- Technology Risk Management Guidelines
- Frameworks / Checklists
- Incident Notification and Reporting
- Examples: Monetary Authority Singapore / Hong Kong / India

PPDR

- Predict - What system need to be protected
- Prevent – Adequate protection against threats
- Detect – Identify presence of undesirable event
- Respond – Specific decisions and activities
- Recover – Restore services

Kill Chain

1. Secure Design
2. Software Development Circle
3. Remote Access Standards and Network Security Management
4. Standards, Application Security Engineering Guidelines, Network Security Engineering
5. Guidelines, Guidelines for Change Requests

0-day stops here

Kill Chain

6. Hardening
7. Implementation manual
8. Host based intrusion prevention
9. Data loss prevention
10. Antivirus (Windows sucks)
11. Patching & vulnerability management
12. Log review

0-day stops here

Kill Chain

11. Intrusion detection, DoS/DDoS protection
12. ID management
13. Change control
14. Health check
15. **Penetration Testing**
16. Decommissioning

0-day stops here

Penetration Test

- Not an Audit / PCI
- Discover Known and Zero Day Vulnerabilities
- White (Glass) box vs Black-box
- UAT / Production
- Public / Internal attack vectors

Penetration Test

- 50% Application Penetration Test
- 30% Network Penetration Test
- 15% Mobile Security Review
- 10% Wireless/RFID/NFC Penetration Testing
- 5% Firewall/DB/Router Configuration Review
- VoIP/PBX Penetration Testing
- Systems: ATM/CCTV/Printers

Web Application Test

- OWASP Top XX
- Tools: Automated scan vs manual tools
- Manual Source Code Review

Web Vulnerabilities

In 100 projects:

- 90% Cross-site Scripting
- 60% Broken Session Management
- 50% Improper Error handling
- 40% Insecure Config Management
- 30% SQL Injeciton
- 30% Unvalidated Input
- 20% Broken Access Controls
- 10% Denial of Service
- 5% Buffer Overflow

Network Penetration Test

- PTES Open Standard / NIST
- Vulnerability Assessment vs Pentest
- External / Internal Networks
- Network topology review

Mobile Security Review

- Internet Banking – do not keep locally
- Internal Applications
- MDM Solutions - BYOD
- Android / iOS

Summary

- Pushing factors: Regulators and Hackers
- Success story: Processes
- Final exam: Penetration Testing

Contacts

anton.bolshakov@itdefence.asia

Questions please