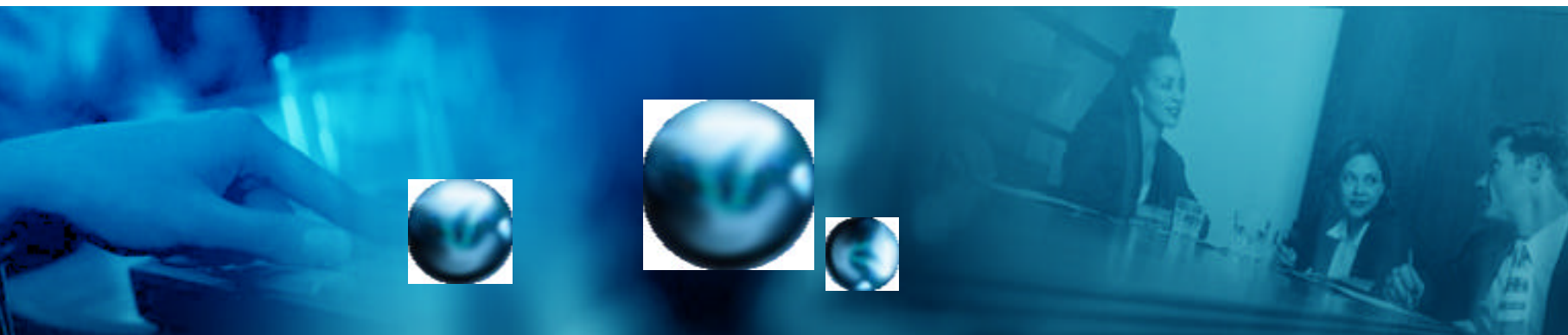


Penetration Testing

(as part of Corporate Governance)



The why, what and how

Mark Hofman

Shearwater/SANS Institute



Agenda

1. Penetration Testing Defined

2. Why?

3. What?

4. How?

5. Common Issues

6. Questions



PENETRATION TESTING

Probing systems in order to breach or circumvent security



PENETRATION TESTING

Probing systems in order to breach or circumvent security

Goal – Identify weaknesses and provide information on mitigation



Difference between Hacking and
penetration testing

PERMISSION!



Pen Testing Defined

- One step beyond Vulnerability Assessment
- Can/Should include Risk Assessment Components
- Can be focussed on specific elements
 - applications
 - infrastructure
 - Specific Controls



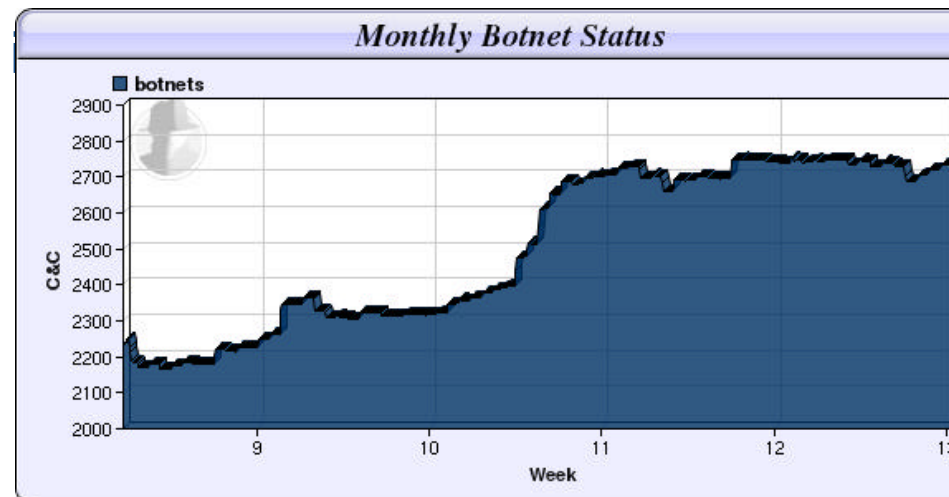
Why?

- Because
 - Someone says so (Standards)
 - Payment Card Industry Data Security Standard
 - ISO/IEC 27001
 - SOX
 - ACSI 33
 -
 - Someone is checking up (Corporate Governance/Audit)
 - We better find things before (Proactive management)
- For each the focus and deliverable may be different



Why? (warning, FUD page)

- Bots, Bots and Bots.
 - Tracking 2700 botnets, average 165,000 drones
 - Tasked with compromising systems, spamming, phishing
- Three major attacks currently happening
 - Injection Attacks ASP & PHPBB sites
 - Approx 591,000 sites
- SPAM
- Vulnerabilities
 - many/day





What?

- Perimeter,
 - i.e. Internet facing services
- Internal Network
 - Discover new/unknown services
 - Identify issues
 - Highlight broader issues
 - New server deployment
 - Part of verifying security baseline
- Applications
 - New applications
 - Review existing deployments



How?

- Decide what needs to be checked and why?
- Who will do it?
 - Scanning Services
 - External expertise
 - Internal expertise
- What will be delivered?
- Agree boundaries



How? Typical process

- Often follows same steps as hackers
 - Passive recognisance
 - Active recognisance
 - Attack
- Other steps
 - Research
 - Review
 - Report

Methodologies

- OSSTM
- ISACA
- SANS



How? Typical process

- Often follows same steps as hackers
 - **Passive recognisance**
 - Active recognisance
 - Attack
- Other steps
 - Research
 - Review
 - Report

Google Hacking
Domain Name Services
Other Public Information



How? Typical process

- Often follows same steps as hackers
 - Passive recognisance
 - **Active recognisance**
 - Attack
 - Port Scanning
 - Spidering
 - Service Identification
 - Vulnerability scanning
 - Email
- Other steps
 - Research
 - Review
 - Report



How? Typical process

- Often follows same steps as hackers
 - Passive recognisance
 - Active recognisance
 - **Attack**
- Other steps
 - Research
 - Review
 - Report

Attempt Exploits



How? Typical process

- Often follows same steps as hackers
 - Passive recognisance
 - Active recognisance
 - Attack
- Other steps
 - Research
 - Review
 - Report



HOW? (tools)

Free

- Nessus
- Wikto
- Paros
- Webscarab
- NMAP
- Metasploit
- Hping2
- Cain

Advantages – Cost, often leading edge

Disadvantages – Reporting, Extra Surprises

Not so free

- Qualis
- Foundstone
- IIS/IBM
- Trend
- Nessus
- Core Impact

Advantages – typically much better reporting
Scheduling, automation.

Disadvantages - Cost



How? (the report)

- Value is in the report
- It should
 - Use internally defined risk criteria (if available)
 - It should assign a level of risk
 - Exploitable from the internet?
 - Script kiddies exploits?
 - Observed in the wild?
 - Value target?
 - Provide relevant findings
 - Contain raw results
 - Measure effectiveness of controls
 - Provide recommendations
 - Highlight underlying causes



Common Issues

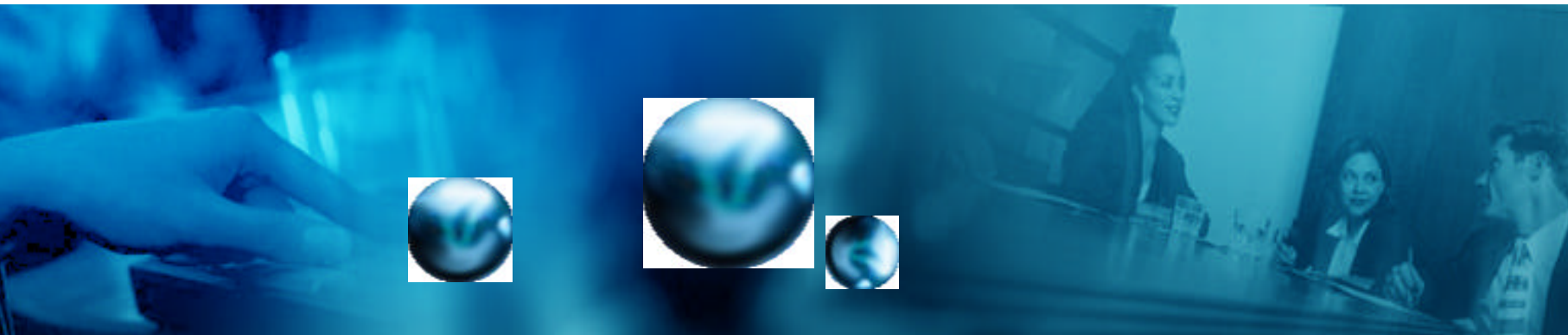
- Not Conclusive
- May provide false sense of security
- Can break things
- Hitting wrong targets
- Limited time



Consider Using Pentests

- SDLC
 - To verify security applications as they are built
- Security Management
 - Hardening of servers
 - Provide Metrics
 - Verify patching
 - Verify controls
- Audit
 - Verify effectiveness of controls
 - Gain insight to the security posture of the organisation.

Questions



mhofman@shearwater.com.au