HP World
September 2002

Vulnerability Assessment and Action

Scott S. Blake, CISSP
Vice President, Information Security
BindView Corporation

Agenda

- Introduction
- Analyzing a Vulnerability
- Types of Assessment Programs
  - Basic Vulnerability Assessment
  - Advanced Vulnerability Assessment
  - Application Vulnerability Assessment
- Understanding the Limitations of Technology
- Conclusion

Introduction

- Fear, Uncertainty, and Doubt
  - 90% report security breach, up from 42% in 1996
  - 74% cite the Internet as a frequent source of attack, up from 59%
  - Reported Losses totaled over $455 million
  - Fraud and theft cost the most, 55 respondents reported losses of over $286 million
  - 34% reported breaches to law enforcement, up from 16% in 1996
  - 21% didn't know if their web server had been attacked

    - From the 2002 CSI/FBI Survey

Introduction

- The Risk Management Equation:

  Risk = (Threat + Vulnerability) * Value

Introduction

- Understand your Threat Model
  - Insider Fraud
  - External Thieves, Spies, etc.
  - Customers
  - Ankle-Biters
- Design an Appropriate Security Policy
  - Identify Key Assets
  - Identify Risks and Threats
  - Build and Maintain Countermeasures
  - Continually Re-assess

Introduction

- Vulnerability Assessment Technologies
  - Network-Based
    - Mostly Non-Credentialed
    - Inferential v. “Live Fire”
    - Generally Does Not Play Well with Others
    - Sometimes Finds Things Host-based cannot
  - Host-based
    - Depends on Administrative Access
    - Often Requires Code on Box
    - Generally More Accurate than Network-based
    - Sometimes Finds Things Network-based cannot
  - Issues
    - Scalability, Reliability, Manageability

Analyzing a Vulnerability

- Notifications
  - Monitor Open Sources
- Triage Function
  - Affected Platforms
  - Impact of Exploit
  - Map Vulnerability to Risk
  - Prioritize
- Determine Action
  - Apply Patch?
  - Shut down service?
  - Reconfigure?
  - Emergency or Regular Procedure?

Analyzing a Vulnerability

- Consider Organizational/Functional Issues
  - Who found the vulnerability?
  - Who needs to take the action?
  - Have business continuity issues been considered while analyzing the priority?

Basic Vulnerability Assessment

- Goal: Stop the Ankle-Biters
- Network Assessment of Internet-facing systems
  - Find and close the Big Holes
- Actions:
  - Strip out unnecessary services
  - Apply the important patches
  - Minimize user accounts
  - Tighten ACLs

Basic Vulnerability Assessment

- How To:
  - Consider Outsourcing
  - Run a network scanner daily or weekly
  - Keep the scanner up to date
  - Establish baseline configuration
  - Alert staff when there are exceptions

Advanced Vulnerability Assessment

- Goal: Stop External Attackers and Insider Fraud
- Mostly Host-based Assessment
- Actions:
  - Minimize user privileges
  - Maintain security standards on workstations and servers
  - Automate vulnerability discovery

Advanced Vulnerability Assessment

- How To:
  - Define security policies and standards
  - Scan regularly (at least monthly) for exceptions
  - Respond swiftly to exceptions on a tiered basis
  - Maintain a test lab for patches, verify them quickly
  - Keep the scanner up to date
  - Consider Outsourcing the scans
  - Distribute the information load

Application Vulnerability Assessment

- Goal: Stop Customers and Attackers
- Usually a consulting engagement
- Actions:
  - Design for Security in the Beginning
  - Code Review
  - Ethical Hacking, aka Adversary Testing

Application Vulnerability Assessment

- How To:
  - Consider Outsourcing
  - Involve security staff in earliest design phases
  - Use peer code review within development
  - Use outside experts for security code review
  - Engage reputable firm for adversary testing

Understanding the Limitations of Technology

- Firewalls
  - Must have holes to function
- Intrusion Detection
  - Limited to known signatures
  - May be subject to attack/evasion
- Anti-Virus
  - Limited to known signatures
  - Must be kept constantly updated
- Encryption
  - VPN/SSL only provide transmission security, not endpoint
  - Data storage encryption good, but key management is the bottleneck
- Vulnerability Assessment
  - Limited to known signatures
  - Balance reliability v. impact on targets

Conclusion

- Understand the Threat Model
- Constantly Search for Vulnerabilities
- Combine Threat and Vulnerability to Manage Risk
- Use Technology, but Know the Limits

Q&A

Questions?