RSC
Ripple Software Consulting

PenTest +
Communication Planning

Author: Joseph Lee
Email: joseph@ripplesoftware.ca
Mobile: 778-725-3206

Communication Planning

Define communication path

- Makes it easier to answer questions or requests for information from company employees, etc.

Establish a regular communication schedule

- Daily or weekly meetings depending on length of engagement

Communication triggers

- Circumstances that merit immediate communication to management
  - Completion of testing stage
  - Discovery of critical finding
  - Discovery of indicators or prior compromise

Goal reprioritization

- Sometimes plans must be re-organized
- Must communicate with stakeholders and organization properly
- Senior managers need to be consulted about any changes to engagement scope or rules

Recommending mitigation strategies

- Advisory about controls that could have prevented any gained access to unauthorized resources
- Advisory for re-thinking authorization scopes
- **People**
  - Awareness campaigns
- **Process**
  - Implementing new processes
  - Implementing formal processes
- **Technology**
  - Implementing new technical controls to prevent unauthorized access, block

malware, etc

Remediation Advisory

Shared local administrator credentials

- **Shared accounts** are bad idea because they **prevent accountability and repudiation**
- **Shared admin accounts** are even greater risk
- Penetration testers / attackers will attack admin accounts as priority
- Use **password management application** / tools to store passwords securely
- **Microsoft's Local Administrator Password Solution (LAPS)** is a tools for managing admin passwords and stores them in **Active Directory**

Weak password complexity

- Users often create weak passwords
- Use **strong, complex, pseudo-random passwords** with high **key-space**
- **Set technical policies** for minimum password length, password change duration, and high complexity for high key-space

Plaintext passwords

- Passwords stored in databases must be encrypted
- Web-sites must use HTTPS to prevent passwords and session cookies from being stolen

No multi-factor authentication

- Use **2nd factor, one-time-passwords (OTP)** or physical tokens
- Combine **two or more factors / mechanisms** when authenticating physical restricted areas, or applications / systems
- **Something you know –** Passwords, pin numbers
- **Something you have –** Physical object such as phone with authenticator app, key fob, access cards, smart-cards
- **Something you are –** Biometric such as facial recognition, fingerprint scanning, retina-scanning

SQL injection

- One of the most common findings in penetration testing
- Solutions include:
  - Proper user input validation
  - Using parameterized queries / prepared statements

Unnecessary open services

- Un-required services should be removed, uninstalled
- Open searches increase attack surface

Writing A Penetration Testing Report

Document your work

- Processes, scans, systems and services
- Other findings
- Changes made to systems or services
- Data saved, collected, or extracted

Recommending Remediation

- Provides road map to mitigating any discovered vulnerabilities
- Some vulnerability scanners provide direct remediation instructions

Written Penetration Testing Report

- **Executive Summary**
    - At start of report
    - Conveys all important information
    - Clear and understandable to non-technical person
    - Audience is not necessarily technically savvy
    - Explain what you discovered and describe risks to business operations
    - Keep short such as 1-2 pages
    - Write this section last
- **Findings and Remediation**
    - Describe security issues, and offers suggestions on how to remediate
    - Includes classifications of risk such as: **critical, high, medium, moderate, low**
- **Methodology**
    - Includes the highest level of technical information
    - Explain types of tests you performed, observations, results, sample data
    - Audience is the CSO, or IT department, technically savvy people
    - Limit amount of code in the report
    - Code or other large data information can be included appendix
- **Conclusion**
    - Summarize conclusions and reiterate mitigations

Secure Handling and Disposition of Reports and Data

- Reports often contain extremely sensitive information
- Could serve as a road map for attacker seeking to gain access
- Reports should only be transmitted and stored in encrypted form
- Paper copies should be kept in physically restricted area, safe, or locked cabinet
- Digital and paper documents should be destroyed when no longer needed

Post Report Activities

- Revisit documentation of the penetration tester
  - Remove any **changes to systems**
  - Remove **shells** installed
  - Remove **tester created accounts, credentials, or back-doors**
  - Remove any **tools installed** during the penetration test
- Gain client approval of the report
- Have final meeting with clients to discuss any remediation or final questions
- Possible to **re-scope** and do more testing
- Possible the client wants more information than provided in the report
- Document any **lessons learned** by the pen-tester for future engagements

Attestation for regulatory requirements

- Regulatory or contractual commitments may have formal attestation from the penetration testing team / organization