Penetration Test & Vulnerability Assessment

Onboarding Guide & What to Expect

Planning & Discovery

1 | Kick-off Meeting & Ground Rules

- Identify Business Objectives
- Agree on Scope of Assessment
- Timing and duration of assessment
- Stakeholder involvement
- Verify if staff should be informed
- Written permission to perform assessment
- Identify known issues or vulnerabilities

2 | Initial Documentation

- Perform walkthroughs to understand the nuances of your business and systems
- Understand technology architecture
- Gather Network diagram, application architecture, and site maps
- Understand key system processes
- Seek insights from management & process owners

3 | Risk Considerations

- Clearly communicate “no-go” systems
- Understand critical applications
- Discuss what-if scenarios
- Black-out dates and times
- Execute procedures in an up-to-date copy of production environment vs. in production

4 | Discovery & Scanning

Leverage a variety of network and/or application scanning tools to gather information, for example:

- Web Application Scanning
- Network Survey & Scanning
- Port Scanning
- Traffic Scanning

Assessment & Exploitation

1 | Identify Vulnerabilities

- Manual vulnerability assessment based upon known exploits and information gathering
- Leverage best practices (i.e., OWASP, SANS Institute, NIST) as a benchmark
- Leverage vulnerability scanning technology to validate vulnerabilities

2 | Vulnerability Exploitation

- Based on identified vulnerabilities, determine suitable targets for exploitation
- Validate that "theoretically vulnerabilities" are in fact exploitable
- Leverage social engineering techniques (when applicable and approved by organization)

Methodology Resources

- https://www.owasp.org/index.php/Web_Application_Penetration_Testing
- https://www.sans.org/reading-room/whitepapers/auditing/conducting-penetration-test-organization-67
- http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

Toolkit Resources

- https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project
- https://www.owasp.org/index.php/Appendix_A:_Testing_Tools
- https://tools.kali.org/web-applications/burpsuite

Assessment Reporting

1 | Develop Assessment Report

- Document assessment findings to clearly articulate findings so that management can reperform and resolve
- Rank issues, identify owners, remediation owners, & remediation strategy
- Seek buy-in from management and key decision makers

2 | Provide Supplementary Documentation

- Provide supplementary documentation to assist management with remediation efforts
    - Uninterpreted Scan Results
    - Third Party resources and whitepapers
    - Important notes taken during the assessment

3 | Provide Third-Party Friendly Report

- Provide redacted report suitable for third parties (if requested)

4 | Read-out with Management

- Ensure that management agrees with and understands potential issues
- Answer questions and discuss next steps

Assessment Clean-Up

1 | Restore Environment to Original State

- Remove any artifacts from environment as result of the assessment:
    - Utilities and devices
    - User accounts
    - Scanning equipment
    - Etc.
- Validate with management that environment has been restored to original state.

Let's Get Started

Shane Peden, Director
Cyber & Vulnerability Assessment Leader
CISA | CISSP | MCSE
Shane.Peden@risk3sixty.com
404.519.8877

Christian Hyatt, Managing Director
CISA | CISM | ISO 27001 Lead Auditor
Christian.Hyatt@risk3sixty.com
404.333.1669