PACKETLABS

PCI Testing Methodology

1 Methodology

Packetlabs' security testing methodology is based on industry standards and is primarily aligned with NIST SP800-115 to ensure compliance with most regulatory requirements. Below, the key tasks within the methodology have been outlined. Included in this methodology are current threats and vulnerabilities experienced within the last year.

At minimum, Packetlabs will retain all penetration testing related artifacts (i.e. testing results, remediation activity results, reports) for a period of three (3) years. Please note, it is the Customer's responsibility to retain these artifacts for any period beyond the minimum three (3) years to meet internal and/or regulatory compliance requirements.

1.1 Information Gathering

- Review the architecture, network topology and configuration
- Identify time restrictions for automated and manual testing
- Identify any restricted hosts (i.e., systems and devices not to be tested)

1.2 Discovery and Vulnerability Assessment

1.2.1 Infrastructure Security Testing

- Passive traffic analysis to identify insecure network protocols
- Comprehensive port scanning, fingerprinting of services and applications
- Automated vulnerability scanning of target systems to identify publically known operating system and application vulnerabilities (network-based and/or authenticated scans)
- Manual validation of findings, removing false-positive items and low-confidence findings
- Manual vulnerability testing using commercial and/or custom tools
- Extensive manual testing for vulnerabilities within the following areas:
  - ✓ Network and routing configuration
  - ✓ Client-side applications
  - ✓ System configuration
  - ✓ OS and third-party applications
  - ✓ Authentication
  - ✓ Database security
  - ✓ Cryptography
  - ✓ Management devices

1.2.2 Application Security Testing

- Comprehensive mapping & manual crawling of the web applications to ensure coverage
- Automated discovery of vulnerabilities using various commercial grade tools
- Manual validation of automated security testing results
- Extensive manual testing for OWASP Top 10 vulnerabilities including but not limited to:
  - ✓ Configuration and Deploy Management
  - ✓ Identity Management
  - ✓ Authentication
  - ✓ Authorization
  - ✓ Session management
  - ✓ Input validation
  - ✓ Error handling
  - ✓ Cryptography
  - ✓ Business logic
  - ✓ Client-side components

1.2.3 Segmentation Testing

- Comprehensive validation of segmentation through conducting port-scans
- Attempt to bypass segmentation controls using various techniques
- Identify and report on accessible network paths in and out of the CDE

1.3 Application and Network Layer Penetration Testing

- Exploit vulnerabilities on affected hosts utilizing penetration-testing tools and manual testing techniques
- Attempt to escalate privileges and/or gain unauthorized access
- Attempt to pivot from compromised systems to other internal systems

1.4 Reporting

- Executive summary detailing the overall state of the environment
- Detailed report outlining findings coupled with prescriptive control recommendations
- Root cause analysis of findings outlining common themes observed with recommendations to improve security within the environment