Cybersecurity

Testing

Benchmark cyber readiness with Penetration Testing

A structured security assessment based on IoT and cybersecurity standards and best practices, penetration testing involves discovering and exploiting software vulnerabilities with extensive hacking techniques – including embedded systems analysis and firmware evaluation.

Embedded devices, software and systems

Penetration Testing

Vulnerability assessment of embedded devices, components and software to identify weaknesses that may be exploitable.

Some testing criteria include:

- Vulnerability scanning and binary analysis
- Examining security controls and circumventing features
- Protocol and Packet analysis of communications
- Cryptography attacks
- Denial of Service tests

Advanced Penetration Testing

Next level assessment that delves deeply into pentesting with more complex hacking techniques, including cutting-edge capabilities and vulnerability exploits to validate products and components security hygiene.

Some testing criteria include:

- Spoofing communications
- Replay attacks
- Credential attacks and exposure
- Attempts to elevate privilege
- Customized exploitation

Component and Binary Analysis

Black box reverse engineering of the inner workings of components and binary analysis.

Some testing criteria include:

- Binary analysis on a wide variety of architectures, including:
  - Commercial off-the-shelf processors (Intel, ARM, etc.)
  - Custom microcontroller cores with vendor-specific Instruction Set Architectures

Wireless Communications Protocols

Radio Frequency (RF) protocols and implementation assessments to determine security robustness.

Some testing criteria include:

- Design protocols review
- RF hacking attacks to detect implementation flaws
- Data interception
- Information-leakage vulnerabilities
- Denial-of-Sleep attacks

Some testable protocols include:

- Bluetooth/BLE
- WiFi, WiMAX
- ZigBee
- Z-wave
- LoRa
- Cellular (GSM family), CDMA, LTE
- Software defined radio (SDR)
- Custom RF

Cryptanalysis

Security assessment of the design, implementation and use of cryptography.

Some testing criteria include:

- Manually exploit, credential attacks, and cryptography assessment
- Identification and assessment of cryptographic techniques for communication and storage of sensitive data

UL Cybersecurity Assurance Program (CAP)

Based on the UL 2900 Series of Standards and other industry standards, UL's Cybersecurity Assurance Program (CAP) includes a wide range of service offerings within the following categories:

ADVISORY

TESTING

CERTIFICATION

Cloud and mobile applications

Mobile Application Testing

Vulnerability assessment of mobile applications to identify weaknesses that may be exploitable.

Some testing criteria include:

- iOS and Android support
- Static and dynamic security testing
- Vulnerability scanning and binary analysis
- Assessing software protections

Cloud Penetration Testing

Passive scanning and non-invasive attempts to identify vulnerabilities in the cloud application and infrastructure.

Some testing criteria include:

- Discovery and enumeration of IP-based services
- DNS scanning, enumerate redirect pathways, and enumerate middleware technologies – information leakage identification
- Authentication and authorization investigation
- Packet capture – flows of session traffic and data streams

Advanced Cloud Penetration Testing

Next level of passive scanning and non-invasive attempts that delve deeply into testing protocol details.

Some testing criteria include:

- Database, access and authentication enumeration
- SSL/TLS assessment
- Enumeration of custom services
- Execution chains
- Session and cookie investigation
- Default credentials check
- Browser exploitation

To learn more about UL's Penetration Testing, visit UL.com/cybersecurity or email: ULCyber@ul.com

Empowering Trust™

CYB-082918