IOT PENETRATION TESTING

The IoT (Internet of Things) is one of the latest technology trends. New devices come to market every month. However, there has been a very little attention to their security so far.

The popularity of these devices has made IoT a highly lucrative target for every potential attacker. The number of connected devices has increased in recent years, and hackers have started to create botnets out of some infected devices. Such botnets are often used for a Distributed Denial of Service (DDoS) attack. One example is Mirai, which attacks IP cameras and home routers that become part of the botnet used in DDoS attacks.

IoT includes all products connected to the Internet. Many IoT devices collect and store data during usage, and often share this information with their manufacturers without users being aware of it. IoT devices are often part of a critical infrastructure (IIoT).

SERVICE OVERVIEW

The goal of the penetration test is to identify security vulnerabilities and deficiencies in IoT devices (smart home appliances, toys, smart homes, industrial facilities, SOHO devices, etc.), demonstrate the exploitation of identified vulnerabilities, identify their risk, and recommend solutions to eliminate them.

The penetration test results in a report and customer consultation. The report does not contain any "false-positive" findings, but only verified vulnerabilities and recommendations on how to remove them.

The penetration test can be performed using the BLACK BOX (no information about the tested infrastructure/device), GRAY BOX (partial information about the tested infrastructure/device) or WHITE BOX (full information about the tested infrastructure, including source codes and configuration files of the device / description of settings) method.

The cost of the penetration test depends on the depth of the tests, and the size and complexity of the tested infrastructure / IoT device. The price is determined after customer consultation, which determines the scope, type of test, and other requirements from the customer.

Security of the Internet of Things (IoT) is a major challenge that requires the security evaluation of many vectors, from web and mobile applications, device firmware, network services/protocols, hardware, encryption and cloud services to privacy issues.

Binary House has developed a comprehensive methodology to perform IoT penetration tests that simulate a real attack. Testing can be tailored to specific requirements or specific methodologies. Each IoT test is tailored to the particular tested device. We use a checklist to ensure that all important topics are addressed.

Depending on your specific device and scope, we will perform the following tasks:

- Application and cloud security assessment/test (web/API, mobile apps)
- Infrastructure security assessment/test

- Hardware security assessment/test
- Analysis of communication protocols / firmware / source or binary code
- Wireless communication security assessment/test
- General security assessment