**PENETRATION TEST EM DESPOSITIVOS IOT**

**2021**

**Introdução**

Nesse documento, serão introduzidos conceitos de penetration test (pentest) em dispositivos de IoT (Internet of Things). Os pentests em dispositivos IoT são métodos de invasão que avaliam e exploram vulnerabilidades no sistema, afim de aprimorar a segurança dos dispositivos e seus sistemas.

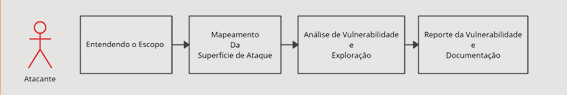
**1 - Sobre os Dispositivos IoT**

Dispositivos de Internet of Things, em português “Internet das Coisas”, são dispositivos interconectados a uma rede, que possuem propósitos variados. Esses dispositivos físicos variam: carros, luzes, TVs, portas, campainhas, fornos microondas, e até prédios. Todos possuem características semelhantes: uma tecnologia embarcada, sensores e conexão com a rede, e são capazes de reunir e transmitir dados.

O IoT é uma extensão da Internet atual que permite que quaisquer dispositivos, desde que possibilitados, se conectem à rede mundial de computadores. Essa conexão permite o controle remoto destes dispositivos, primariamente. Mas nem tudo são flores: com esse número de possibilidades, os dispositivos IoT possuem diversos riscos que devem ser explorados e investigados.

**2 - Ciclo do Teste de Intrusão**

O ciclo do teste de intrusão não foge do padrão já utilizado:



Abaixo, uma explicação detalhada de cada passo:

* **Entendendo o Escopo**:

A primeira etapa do pentest envolve um reconhecimento completo do analista do escopo trabalhado. Aqui, ele estabelecerá o planejamento, objetivo, testes, logística, implicações legais, além do método mais viável para se utilizar: **Black Box**, **Grey Box** ou **White Box**;

* **Mapeamento da Superfície de Ataque**:

O mapeamento consiste basicamente em um estudo detalhado sobre o alvo. Ele se inicia com técnicas de reconhecimento do alvo, como o OSINT (Open Source Intelligence), uma database de dados públicos, onde o analista pode encontrar informações pertinentes para a intrusão.

O estudo de um novo dispositivo pode – e vai – levar muito tempo. Portanto, é importante coletar e avaliar o maior número de informações possível. Leia documentações, manuais, fórums, procure por informações públicas, redes sociais – qualquer coisa que ajude é válida.

Anote todos os componentes de hardware usados no dispositivo, como tipo de arquitetura, protocolos de comunicação, detalhes de apps, firmware, portas, etc. Novamente, tudo que seja pertinente.

Na página seguinte, abordaremos as três categorias onde a arquitetura dos dispostivos IoT se dividem.

**2.1 - Arquitetura dos Dispositivos**

* **Dispositivo integrado;**

É uma parte essencial do dispositivo – a “coisa” da Internet das Coisas. Pode ser várias coisas e ter vários propósitos, como um sensor, um emissor, um transmissor, receptor, etc.

Algumas de suas vulnerabilidades incluem:

Portas seriais expostas;

Mecanismo de autenticação inseguro usado nas portas seriais;

Capacidade de despejar o firmware em JTAG ou através de chips Flash;

Análise de energia e ataques baseados em canal lateral

* **Firmware, softwares;**
* **Comunicações de rádio;**