Tradução do Capítulo do livro The IOT Hackers's Handbook

Gustavo Henrique de Farias Moura

RM556434

Capitulo 2: Performing na IOT Pentest

Realizando um Pentest em IoT

Neste capítulo, aprendemos como realizar um pentest em IoT e entender o primeiro elemento, que é o mapeamento da superfície de ataque. Muitos pentesters ainda não conseguiram migrar para testes de penetração em IoT por falta de conhecimento sobre como realizar um pentest em IoT: Quais são os diferentes componentes envolvidos? Quais ferramentas devem ser usadas? Como executar o pentest como um todo? Este capítulo compartilha insights sobre como realizar um pentest em IoT e responder a essas perguntas. Também cobrimos a primeira fase do processo de teste de penetração, o mapeamento da superfície de ataque, que usamos para avaliar a solução do dispositivo IoT alvo e ter uma estimativa justa de que tipo de problemas de segurança podem estar presentes no produto que estamos testando.

O que é um Pentest em IoT? Um pentest em IoT é a avaliação e exploração de vários componentes presentes em uma solução de dispositivo IoT para ajudar a tornar o dispositivo mais seguro. Ao contrário dos testes de penetração tradicionais, IoT envolve vários componentes, como discutimos anteriormente, e sempre que falamos sobre um pentest em IoT, todos esses componentes precisam ser testados. A Figura 2-1 mostra como se parece um típico engajamento de teste de penetração.

Como em qualquer pentest típico em IoT, nós, como pentesters, precisamos entender o escopo do pentest e quaisquer outras restrições e limitações. As condições de teste de penetração variarão de produto para produto e podem ser qualquer coisa, desde garantir que o teste aconteça entre 22h e 5h (ou durante a noite) até realizar o teste de penetração em um ambiente de staging fornecido pelo cliente. Depois de entender o escopo técnico do projeto, vale a pena mencionar ao cliente que tipo de pentest (caixa branca, caixa preta ou caixa cinza) você ou sua equipe vão realizar para garantir que tanto o cliente quanto você estejam na mesma página. Uma das outras coisas sobre teste de penetração em IoT é a necessidade de múltiplos dispositivos. Muitas vezes, durante um pentest em IoT, certas técnicas que usamos envolvem métodos destrutivos, como remover um chip de uma placa de

circuito para análise, o que provavelmente tornaria o dispositivo inutilizável para análises posteriores.

Após as discussões, o próximo passo é realizar o teste de penetração conforme o escopo e a metodologia desejados. Esta fase do teste de penetração começa com o mapeamento de toda a superfície de ataque da solução, seguido pela identificação de vulnerabilidades e realização de exploração, que é então seguida pela pós-exploração. Os testes concluem com um relatório técnico detalhado. Neste capítulo, cobrimos apenas o primeiro passo, o mapeamento da superfície de ataque. Nos próximos capítulos, veremos as várias formas de identificar e explorar vulnerabilidades, e no capítulo final, veremos como escrever um relatório de teste de penetração para dispositivos IoT.

Mapeamento da Superfície de Ataque O processo de mapeamento da superfície de ataque significa mapear todos os vários pontos de entrada que um atacante poderia potencialmente abusar em uma solução de dispositivo IoT. Este é o primeiro passo, e um dos mais importantes, em toda a metodologia de teste de penetração em IoT. Também envolve a criação de um diagrama de arquitetura de toda a solução do ponto de vista de um pentester. Durante os engajamentos de teste de penetração, frequentemente dedicamos um dia inteiro a esta fase.

Este passo é útil porque ajuda você a entender a arquitetura de toda a solução e, ao mesmo tempo, ajuda a estabelecer vários testes que você executaria no produto, classificados por prioridade. A prioridade dos ataques pode ser determinada pela facilidade de exploração multiplicada pelo impacto da exploração. No caso de um exploit ser extremamente fácil e levar à comprometimento bem-sucedido e recuperação de dados sensíveis do dispositivo, isso seria classificado como uma vulnerabilidade de alta prioridade e alta criticidade. Por outro lado, algo difícil de executar, com resultados não tão úteis durante o teste, seria categorizado como uma vulnerabilidade de baixa criticidade e baixa prioridade. Nos engajamentos, sempre que identificamos uma vulnerabilidade de alta criticidade, notificamos imediatamente o fornecedor sobre a visão geral e o impacto da vulnerabilidade no mesmo dia, em vez de esperar o engajamento ser concluído.

Agora que você tem uma ideia básica do que fazer no mapeamento da superfície de ataque, vamos aprofundar isso e entender os detalhes exatos de como realizar este processo.

Como Realizar o Mapeamento da Superfície de Ataque Assim que você obtém um novo alvo, reserve um tempo para entender o dispositivo primeiro. Começar uma avaliação com informações incompletas ou parciais é um dos maiores erros que um pentester pode cometer. Isso significa passar por todos os canais possíveis e coletar informações, como documentação e manuais do dispositivo, recursos online e postagens sobre o produto e qualquer conteúdo disponível ou pesquisa anterior sobre o dispositivo.

Anota-se os vários componentes usados no dispositivo, tipo de arquitetura de CPU, protocolos de comunicação usados, detalhes do aplicativo móvel, processo de atualização de firmware, portas de hardware, suporte de mídia externa em dispositivos e praticamente tudo o mais que você puder encontrar. Muitas vezes as coisas não são tão óbvias quanto parecem inicialmente, e é por isso que você deve aprofundar-se em cada uma das várias funções que o dispositivo oferece.

Quando olhamos para uma solução IoT, a arquitetura inteira pode ser dividida em três categorias amplas:

1. Dispositivo embarcado.
2. Firmware, software e aplicativos.
3. Comunicações por rádio.

Nosso objetivo ao analisar o dispositivo IoT para mapeamento da superfície de ataque seria categorizar a funcionalidade e as ameaças de segurança correspondentes a cada categoria. Consideramos qual deve ser o processo de pensamento ao categorizar as vulnerabilidades potenciais de acordo com as categorias mencionadas. Cada uma das categorias mencionadas a seguir serve como uma lista de verificação durante o processo de mapeamento da superfície de ataque e ajuda a identificar as áreas nas quais a exploração adicional é necessária.

Dispositivo Embarcado O primeiro componente que examinamos durante o mapeamento da superfície de ataque é o próprio dispositivo. Isso inclui, mas não está limitado a, análise de hardware, avaliação da configuração de segurança do dispositivo, processos em execução, interface de entrada e saída (GPIO) e métodos de interação com o usuário.

Avaliação de Hardware Para realizar uma avaliação de hardware, é necessário abrir o dispositivo. Uma vez dentro, você pode coletar informações importantes, como o tipo e a marca dos chips usados, a quantidade de memória, a quantidade de armazenamento, os dispositivos de comunicação integrados (por exemplo, Wi-Fi, Bluetooth, Zigbee) e o tipo de CPU. Essas informações podem ser úteis durante a análise de vulnerabilidade e na identificação de possíveis falhas de segurança.

Configuração de Segurança Avaliar a configuração de segurança envolve verificar se o dispositivo usa a configuração padrão de fábrica, se o acesso físico ao dispositivo é protegido (por exemplo, selado) e se a configuração do usuário é segura. Um dispositivo IoT é considerado mais seguro se ele não usa configurações padrão de fábrica e requer autenticação forte (por exemplo, usando senhas complexas) para acessar o dispositivo e configurá-lo.

Processos em Execução Identificar quais processos estão em execução no dispositivo pode ajudar a entender sua funcionalidade e determinar quais serviços e interfaces estão disponíveis. Isso também pode ajudar a identificar quaisquer processos suspeitos ou desnecessários que podem representar riscos de segurança.

Interface de Entrada e Saída (GPIO) As interfaces de entrada e saída permitem que o dispositivo interaja com o ambiente externo. Para dispositivos IoT, isso pode incluir interfaces como pinos GPIO (General Purpose Input/Output), UART (Universal Asynchronous Receiver/Transmitter) e I2C (Inter-Integrated Circuit). O acesso a essas interfaces pode permitir a um atacante manipular o dispositivo ou acessar dados confidenciais.

Métodos de Interação com o Usuário É importante entender como os usuários interagem com o dispositivo, seja por meio de uma interface gráfica de usuário (GUI), linha de comando (CLI), aplicativo móvel ou outro método. Isso pode revelar áreas onde a segurança pode ser reforçada, como autenticação de usuário e controle de acesso.

Essa é uma visão geral do que é feito durante o mapeamento da superfície de ataque em dispositivos embarcados. No próximo capítulo, continuaremos com a discussão sobre mapeamento de firmware, software e aplicativos.