Avaliação da Segurança de Sistemas de Aquicultura 4.0 Através de Testes de Penetração

Dayanne C. S. Portela[1], **Renato V. Mendes**[1], **Obionor O. Nóbrega**[1], **Fernando Aires**[1]

[1]Departamento de Computação – Universidade Federal Rural de Pernambuco (UFRPE) – Recife – PE – Brazil

{dayanne.carolina, renato.mendes, obionor.nobrega, fernandoaires}@ufrpe.br

Abstract. *With the growing demand for food, aquaculture stands out as an important supply source. The adoption of Internet of Things (IoT) systems in this sector optimizes the production process, bringing new opportunities for automation, data collection, and decision-making support. However, this modernization also introduces new cyberattack vectors, which can compromise the integrity of sensitive data and systems. Given this scenario, this work proposes the development and execution of security tests on Aquaculture 4.0 systems, aiming to evaluate and disclose the level of cybersecurity protection currently offered in this domain.*

Resumo. *Com a crescente demanda por alimentos, a aquicultura destaca-se como uma importante fonte de suprimento a nível mundial. Neste contexto, a adoção de sistemas baseados na Internet das Coisas (IoT) otimiza o processo produtivo, trazendo novas oportunidades de automação, de coleta de dados e de auxílio à tomada de decisões. Contudo, essa modernização também introduz novos vetores de ataques cibernéticos, que podem comprometer a integridade de sistemas e de dados sensíveis. Diante desse cenário, este trabalho propõe a proposição e a execução de testes de segurança em sistemas da Aquicultura 4.0, com o objetivo de avaliar e divulgar o nível de segurança atualmente oferecido neste domínio.*

1. Introdução

A aquicultura pode ser definida como a prática de criação de organismos aquáticos, como plantas e peixes, em ambientes controlados [Freitas et al. 2024] [Mahamuni and Goud 2023]. É o setor de produção de alimentos com a maior taxa de crescimento do mundo por atender de maneira eficiente e sustentável à crescente demanda de produção [Bhushan et al. 2024].

A Internet das Coisas, também conhecida como IoT, é um paradigma em crescimento que visa conectar diferentes objetos à Internet, de modo a coletar dados gerados por sensores, controlar dispositivos de forma remota e monitorar ambientes como cidades inteligentes, indústrias e agronegócio [Meneghello et al. 2019]. O seu uso no desenvolvimento da aquicultura se dá pela Aquicultura 4.0, possibilitando automações de processos, redução de custos e aumento de produtividade [Freitas et al. 2024]. A aquicultura 4.0 usa sensores, atuadores, dispositivos e redes de comunicação para realizar monitoramento em tempo real, gerenciamento da qualidade da água e controle do ambiente.

Apesar de existirem dispositivos IoT utilizados especificamente para a aquicultura 4.0 ou agricultura inteligente, ainda assim, eles são comparáveis aos outros dispositivos IoT de outras áreas. Diversos estudos apontam vulnerabilidades a ataques a estes dispositivos que, quando exploradas, podem afetar, por exemplo, uma fazenda, levando à perda de produção devido à falta de segurança dos artefatos.

Inclusive, autores como Nestor Arrega [Arreaga et al. 2023] destacam que a falta de suporte em atualizações e correções, o relativamente baixo poder computacional e a falta de padrões de segurança são algumas das preocupações em relação à segurança dessa área. A alta diversidade desses equipamentos, como os seus tipos de conexão com redes, diferentes *softwares* e *hardwares*, também contribui para a dificuldade de lidar com a segurança desta área.

Considerando esse contexto, conhecer as possíveis vulnerabilidades dos dispositivos que serão utilizados se torna uma ação com reconhecida importância. Desta forma, testes de penetração (também conhecidos como *pentest*) podem ser um excelente método para avaliar o nível de segurança desses dispositivos. Um teste de penetração consiste em uma avaliação autorizada e proativa da segurança de um sistema, e costuma ter o uso de abordagem de simulação de ataques de pessoas hostis [Cai et al. 2022]. Além disso, existe uma diferença nos *pentests* de IoT em comparação aos convencionais, que é o envolvimento de inúmeros componentes, que podem precisar ser testados de maneiras diferentes.

A partir disso, este trabalho busca analisar o nível de segurança de sistemas IoT utilizados na Aquicultura 4.0 por meio da utilização de testes de penetração. Através desta avaliação, será possível identificar vulnerabilidades presentes nos dispositivos, sistemas e infraestrutura de rede utilizados nesse domínio, contribuindo para o avanço das práticas de segurança nesses ambientes. O objetivo central consiste em propor e validar uma metodologia que oriente a detecção dessas falhas e vulnerabilidades.

Este artigo está estruturado da forma que se segue. A Seção 2 apresenta os trabalhos relacionados a esta pesquisa. A Seção 3 descreve a metodologia proposta para a realização dos testes de penetração no ambiente IoT. Na seção 4, aborda-se o estudo de caso, ilustrando a aplicação prática da metodologia conduzida em uma solução IoT. Por fim, a seção 5 apresenta as conclusões e trabalhos futuros.

2. Trabalhos Relacionados

Meneghello *et al* [Meneghello et al. 2019] destacam que muitos dispositivos IoT ainda carecem de recursos básicos de segurança, como mecanismos de autenticação robustos e rotinas criptográficas padronizadas. O estudo também analisa os principais protocolos de comunicação utilizados comercialmente, como *ZigBee, Bluetooth Low Energy (BLE), 6LoWPAN e LoRaWAN*, apresentando exemplos de ataques reais observados em dispositivos amplamente utilizados.

Por outro lado, Demestichas *et al* [Demestichas et al. 2020] apresentam ameaças impostas pela introdução de tecnologias inteligentes no setor agrícola, atribuindo essas vulnerabilidades aos problemas de hardware e software dos dispositivos, aos protocolos de comunicação utilizados e à forma de armazenamento e processamento dos dados.

Gupta *et al* [Gupta et al. 2020] realizam um estudo sobre segurança e privaci-

dade na agricultura inteligente, destacando a adoção de dispositivos IoT nesse domínio aumenta significativamente a superfície de ataque, a partir da introdução de vulnerabilidades herdadas do IoT tradicional e dos desafios específicos do ambiente agrícola, como a exposição física dos dispositivos à eventos naturais e agentes externos.

Por sua vez, Bhusan *et al* [Bhushan et al. 2024] realizam uma análise sobre uma grande variedade de ameaças de segurança no contexto da aquicultura, detalhando ataques como repetição (*replay*), *man-in-the-middle*, negação de serviço (*denial of service*), *jamming* e injeção maliciosa. A sua principal contribuição reside na análise estruturada desses riscos, com base na arquitetura de camadas dos sistemas IoT, apresentando as vulnerabilidades e suas respectivas estratégias de contramedidas para aprimorar a segurança nos sistemas de aquicultura.

Métodos já tradicionais de teste de penetração podem não ser suficientes para analisar vulnerabilidades em sistemas baseados na Internet das Coisas. Dispositivos nesse contexto costumam operar em redes interconectadas, nas quais pode ocorrer o comprometimento de todo o sistema mesmo ao ser afetado apenas um dispositivo [Jaafar et al. 2024].

Em [Barybin et al. 2019], é realizado um estudo exploratório, em que foram realizados testes de segurança para detectar vulnerabilidades em dispositivos que utilizam o microcontrolador ESP32, que costuma ser utilizado em dispositivos que podem ser montados por usuários finais e indústrias. Os testes focaram na exploração de vulnerabilidades da rede Wi-Fi, utilizando ferramentas como Aircrack-ng e Wireshark para obter acesso não autorizado a rede e enviar dados falsos para a interface *web* do sistema. Os resultados demonstraram que um atacante com conhecimento básico de ferramentas de rede foi capaz de comprometer o sistema.

Por sua vez, Arreaga *et al* [Arreaga et al. 2023] realizaram três ataques diferentes para testar a falta de um mecanismo de defesa em dispositivos IoT como o Raspberry Pi. Os autores propuseram um modelo de ataque no qual foram utilizadas máquinas virtuais e ferramentas como Wireshark, Metasploit e Ettercap para analisar ataques de negação de serviço, *Man-In-The-Middle* e *backdoor*. Os sistemas utilizados foram considerados vulneráveis a todos os três ataques.

Por fim, Zhukabayeva *et al* [Zhukabayeva et al. 2025] realizaram testes em uma rede Wi-Fi para avaliação de redes de cidades inteligentes. Para isto, foram utilizadas ferramentas como Airmon-ng, Airodump-ng e Wireshark. Os autores conseguiram encontrar vulnerabilidades para ganhar acesso não autorizado na rede, além de terem a possibilidade de injeção de pacotes na rede. Por fim, são destacadas medidas de segurança para aumentar a segurança da rede.

Considerando o contexto de trabalhos relacionados apresentados, este artigo busca realizar uma avaliação experimental das ameaças descritas nos trabalhos anteriores, por meio de um estudo de caso no domínio da Aquicultura 4.0. A maioria dos estudos foca em uma revisão bibliográfica sobre o assunto, com um embasamento mais teórico, enquanto que os trabalhos práticos realizam suas avaliações em outros contextos dentro da área de Internet das Coisas. Deste modo, este trabalho busca avaliar, por meio de testes de penetração, o nível de segurança de sistemas IoT utilizados na Aquicultura 4.0.

3. Metodologia

A metodologia proposta para a avaliação de segurança dos dispositivos IoT utilizados no ambiente de Aquicultura baseia-se em um processo sistemático de testes de penetração estruturado em seis etapas consecutivas, conforme ilustrado na Figura 1. O modelo busca adaptar práticas tradicionais de teste de penetração para ambientes IoT aplicados à aquicultura, considerando características como dispositivos distribuídos, comunicação sem fio, restrições operacionais e diferentes níveis de acesso físico e lógico.

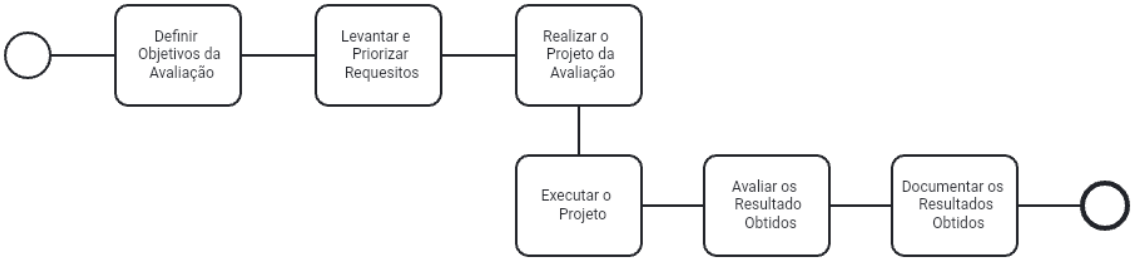

Figura 1. Fluxo do processo metodológico de testes de penetração em ambientes IoT.

O detalhamento de cada uma das fases do processo metodológico adotado é apresentado a seguir.

3.1. Definir os objetivos da avaliação

A definição dos objetivos constitui a etapa inicial da metodologia proposta, sendo responsável pelo estabelecimento do escopo, metas e restrições da avaliação de segurança. Nessa fase, são definidos os objetivos do teste de penetração e os critérios utilizados durante a análise, além do alinhamento entre os responsáveis pela execução da avaliação e os demandantes do projeto.

Também são analisados os riscos operacionais associados à execução dos testes, considerando possíveis impactos na disponibilidade, integridade e funcionamento dos sistemas avaliados. Em ambientes IoT aplicados à aquicultura, essa etapa possui elevada relevância devido à utilização contínua de dispositivos responsáveis pelo monitoramento ambiental e automação da produção, tornando necessária a definição de limitações operacionais para reduzir impactos durante os testes.

3.2. Levantar e priorizar requisitos

Com os objetivos já estabelecidos, esta etapa define quais requisitos de segurança serão testados. O processo inicia-se com a seleção de uma bibliografia de referência, que engloba normas, artigos científicos e relatórios da indústria, para identificar as melhores práticas de segurança. Os requisitos levantados são documentados de forma padronizada, utilizando mapas mentais ou fluxogramas, e priorizados com base nos objetivos do negócio e na criticidade das possíveis falhas, otimizando a execução dos testes e aumentando a efetividade da análise.

3.3. Realizar o projeto da avaliação

O subprocesso de projeto da avaliação (Figura 2) define os elementos necessários para a execução do teste de penetração de forma alinhada aos objetivos estabelecidos anteriormente. Inicialmente, é realizado o mapeamento do ambiente avaliado, incluindo a

identificação dos sistemas, dispositivos, redes e relações de dependência existentes entre os componentes da infraestrutura IoT.

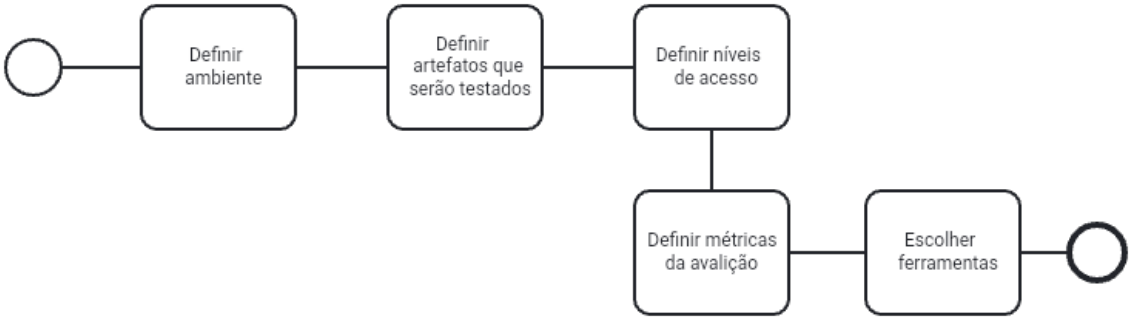

Figura 2. Fluxo do subprocesso de projeto da avaliação.

Após o mapeamento do ambiente, são definidos os artefatos a serem avaliados, priorizando dispositivos e serviços considerados críticos para o funcionamento do ambiente analisado. Em cenários de aquicultura IoT, esses artefatos podem incluir sensores ambientais, como sensores de pH e temperatura responsáveis pelo monitoramento da qualidade da água; gateways de comunicação, dispositivos embarcados, serviços em nuvem e protocolos de comunicação utilizados na transmissão de dados.

A metodologia adota os níveis de acesso propostos pelo OWASP IoT Security Testing Guide [OWASP Foundation 2024], considerando diferentes capacidades de interação física e lógica com os dispositivos avaliados. Os níveis físicos incluem acesso remoto, local, não invasivo e invasivo, enquanto os níveis de autorização abrangem acesso não autorizado, baixo privilégio, privilegiado e acesso de fabricante.

Além disso, são estabelecidos os objetivos específicos de cada caso de teste e as métricas utilizadas para avaliação dos resultados. Essas métricas podem incluir indicadores qualitativos e quantitativos, como severidade das vulnerabilidades, complexidade de exploração, impacto operacional e quantidade de falhas identificadas. Por fim, realiza-se a seleção das ferramentas utilizadas durante a avaliação. Essa escolha considera os objetivos definidos anteriormente e as características do ambiente analisado, podendo envolver ferramentas voltadas à análise de firmware, monitoramento de rede, exploração de vulnerabilidades e análise de protocolos de comunicação.

3.4. Executar o projeto

O subprocesso de execução integra as fases de descoberta e exploração, com base na metodologia empregada pela NIST[Scarfone et al. 2008]. Inicialmente, são realizadas atividades de reconhecimento do ambiente, incluindo identificação de dispositivos, mapeamento de serviços, análise de portas abertas e coleta de informações sobre os sistemas avaliados.

Em seguida, é conduzida a análise de vulnerabilidades, utilizando as informações coletadas durante a etapa de reconhecimento e bases de vulnerabilidades conhecidas, permitindo identificar falhas relacionadas a firmware desatualizado, autenticação inadequada, ausência de criptografia, falhas de segmentação de rede e exposição indevida de serviços.

Após a etapa de descoberta, são realizadas tentativas controladas de exploração das vulnerabilidades identificadas. Essa fase pode incluir obtenção de acesso ao sistema, escalonamento de privilégios, movimentação lateral e coleta de evidências relacionadas ao impacto das falhas exploradas. Todas as atividades são executadas respeitando as restrições previamente definidas no planejamento da avaliação.

Durante a etapa de ataque em ambientes da Internet das Coisas, é comum a exploração de vulnerabilidades arquiteturais que comprometem não apenas o dispositivo, mas também toda a rede. Conforme aponta [Demestichas et al. 2020], a negligência na atualização de firmware expõe os equipamentos a falhas públicas já conhecidas, permitindo que invasores assumam o controle do dispositivo ou extraiam dados sensíveis.

3.5. Avaliar os resultados obtidos

A avaliação dos resultados consiste na análise das evidências coletadas durante a execução dos testes de penetração. Essa etapa busca verificar o nível de exposição do ambiente avaliado, identificar os ativos mais vulneráveis e analisar os impactos associados às falhas identificadas.

Os resultados obtidos são comparados com as métricas definidas durante o projeto da avaliação, permitindo analisar aspectos como severidade das vulnerabilidades, complexidade de exploração e impacto sobre disponibilidade, integridade e confidencialidade dos sistemas.

Além disso, as vulnerabilidades identificadas podem ser classificadas com base em métricas consolidadas, como o *Common Vulnerability Scoring System* (CVSS) [FIRST 2019], auxiliando na priorização das ações corretivas e na definição de estratégias de mitigação adequadas ao ambiente avaliado.

3.6. Documentar os resultados obtidos

O subprocesso de documentação consolida os resultados obtidos durante a avaliação de segurança. O relatório gerado deve apresentar, de forma estruturada, os objetivos da avaliação, o escopo definido, a metodologia aplicada, os testes executados e as vulnerabilidades identificadas, incluindo evidências técnicas das falhas, descrição dos impactos e recomendações de mitigação compatíveis com as características do ambiente. As recomendações devem considerar viabilidade operacional, custo de implementação e impacto sobre os sistemas IoT. Além do detalhamento técnico, o relatório deve utilizar linguagem acessível ao demandante, permitindo compreensão adequada dos riscos e das medidas recomendadas.

4. Estudo de caso

O estudo de caso foi conduzido em um ambiente IoT fornecido pela *Smart Rural*[1], startup especializada em soluções para Aquicultura 4.0. A plataforma desenvolvida pela empresa é voltada ao monitoramento em tempo real de ambientes de produção de peixes, camarões e aves de postura, por meio de dispositivos conectados para aquisição e transmissão de dados operacionais. Devido à dependência de comunicação contínua e monitoramento remoto, o ambiente apresenta características relevantes para avaliação de segurança em sistemas IoT aplicados ao setor aquícola.

[1] https://www.smartrural.com.br/

4.1. Definição dos objetivos da avaliação

Nessa fase, foi definido que os testes de penetração teriam como objetivo avaliar o nível de segurança da infraestrutura IoT analisada, identificando vulnerabilidades presentes nos dispositivos, serviços e mecanismos de comunicação utilizados pela solução. Além disso, a avaliação buscou analisar o nível de maturidade da segurança do sistema, considerando os mecanismos de proteção implementados e a exposição do ambiente a potenciais ameaças.

Também foram analisados os riscos operacionais associados à execução dos testes, considerando possíveis impactos sobre a disponibilidade e funcionamento da solução monitorada. Como o ambiente é utilizado para monitoramento contínuo da produção, eventuais interrupções poderiam comprometer temporariamente o funcionamento do sistema e o acesso às informações operacionais. Para minimizar esses impactos, os testes foram conduzidos em um ambiente separado de validação, utilizando dispositivos específicos para avaliação de segurança, de forma a reduzir riscos de paralisação e interferências no ambiente operacional da solução IoT.

4.2. Levantamento e Priorização de Requisitos

Após a definição dos objetivos da avaliação, foi realizado o levantamento dos requisitos de segurança considerados relevantes para o ambiente IoT analisado. Essa etapa foi conduzida com base em trabalhos científicos e referências da literatura relacionados à segurança em sistemas IoT e ambientes de aquicultura inteligente, buscando identificar práticas e requisitos aplicáveis ao contexto da solução avaliada.

Considerando as características operacionais do ambiente, a confidencialidade das informações transmitidas e armazenadas pelos dispositivos foi definida como um dos principais requisitos de segurança a ser priorizado durante a avaliação. Isso ocorre devido à natureza dos dados coletados pelos sensores e à arquitetura distribuída da solução, que envolve múltiplos dispositivos embarcados, ampliando a superfície de exposição a potenciais ataques voltados à obtenção de informações sensíveis.

4.3. Projeto da Avaliação

A etapa de projeto da avaliação teve como objetivo estruturar tecnicamente os testes de penetração realizados no ambiente IoT empregado no estudo de caso. Inicialmente, foi realizado o mapeamento da infraestrutura, identificando dispositivos embarcados, serviços expostos, protocolos de comunicação e relações de dependência entre os componentes da solução. A partir desse levantamento, foram definidos os artefatos priorizados para análise e os níveis de acesso a serem considerados durante a execução dos testes.

A solução IoT analisada tem como objetivo o monitoramento da qualidade da água em ambientes de produção aquícola. A arquitetura utiliza sensores de pH e temperatura conectados a um dispositivo com a placa ESP32, que transmite os dados via protocolo LoRa para um *gateway*, os dados coletados. Este realiza o processamento e encaminhamento dos dados por rede Wi-Fi para um servidor, que os disponibiliza em plataformas *Web* e *mobile* para visualização pelos usuários, conforme apresentado na (Figura 3).

Os testes foram conduzidos sob o contexto de acesso físico invasivo, conforme a nomenclatura do OWASP IoT Security Testing Guide [OWASP Foundation 2024]. As

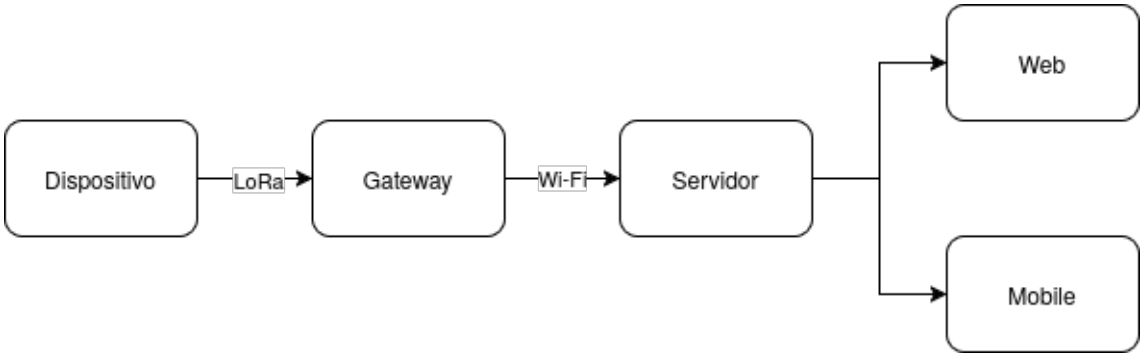

Figura 3. Arquitetura do sistema da SmartRural

métricas utilizadas incluíram o número de vulnerabilidades encontradas, a severidade das falhas identificadas, a complexidade dos ataques realizados e a complexidade de mitigação dos problemas encontrados. Para a execução, foram utilizadas ferramentas como *Burp Suite* para análise das aplicações, *esptool* para interação com os dispositivos ESP32 e *binwalk* para análise de firmware, e um ambiente baseado no sistema operacional Kali Linux, devido à disponibilidade de ferramentas específicas para testes de penetração.

4.4. Execução dos Testes

A execução dos testes abrangeu os dispositivos, o *gateway* e a aplicação web da solução, realizados de forma sequencial e respeitando as restrições operacionais definidas no planejamento.

A avaliação foi iniciada pela análise do firmware dos dispositivos embarcados utilizados. Foi identificado que o dispositivo ainda possuía interfaces de depuração do tipo JTAG habilitadas, possibilitando interação direta com os componentes internos do ESP32. Embora o sistema apresentasse um mecanismo de proteção responsável pelo desligamento automático do dispositivo após alguns segundos conectado via cabo, observou-se que essa proteção não impedia completamente a realização de análises físicas no equipamento.

A partir dessa condição, foi possível utilizar a ferramenta *OpenOCD-ESP32* para manter o dispositivo em estado de interrupção da execução, permitindo acesso ao sistema antes da finalização do mecanismo de proteção implementado. Com isso, foi realizada a extração do firmware utilizando a ferramenta *esptool*, possibilitando a obtenção de uma cópia da memória flash do dispositivo. A ausência de mecanismos de criptografia do firmware permitiu a inspeção direta das partições do dispositivo e a identificação de parâmetros de configuração da rede LoRa por meio do comando *strings* sobre o arquivo binário extraído.

Na avaliação do *gateway*, identificou-se a presença de uma porta USB-C acessível externamente e sem qualquer mecanismo de proteção físico ou lógico. Por meio dessa interface, foi realizada a extração do firmware utilizando a ferramenta *esptool*, sem que qualquer barreira de segurança fosse encontrada durante o processo, evidenciando a ausência de mecanismos de proteção contra leitura da memória flash do dispositivo.

A análise do firmware extraído, realizada por meio do comando *strings* sobre o arquivo binário, revelou informações críticas armazenadas em texto claro, incluindo o endpoint da API utilizada para comunicação com o servidor e as credenciais da rede Wi-

Fi à qual o *gateway* se conecta. A exposição dessas informações representa um vetor de ataque de alto impacto, uma vez que um agente mal-intencionado com acesso físico ao dispositivo poderia obter controle sobre a comunicação do *gateway* e ganhar acesso à rede local onde o sistema está implantado.

Por fim, foi realizada a avaliação da aplicação Web. Os testes indicaram a presença de mecanismos de controle de acesso adequados, não sendo identificadas falhas críticas relacionadas à autenticação ou autorização.

4.5. Avaliação dos Resultados

Após a execução dos testes, os resultados obtidos foram analisados para identificar o nível de exposição do ambiente avaliado e os impactos associados às vulnerabilidades encontradas. Ao todo, foram encontradas cinco vulnerabilidades distribuídas entre os dispositivos embarcados e a aplicação Web, conforme apresentado na Tabela 1.

Tabela 1. Vulnerabilidades identificadas

Componente	**Vulnerabilidade**	**CVSS**	**Compl. Exploração**	**Compl. Mitigação**
Dispositivo	Interface de depuração JTAG habilitada	6.1 Médio 3.1/AV:P/AC:L/PR:N/ UI:N/S:U/C:H/I:H/A:N	Média	Baixa
Dispositivo	Ausência de criptografia do firmware	4.6 Médio 3.1/AV:P/AC:L/PR:N/ UI:N/S:U/C:H/I:N/A:N	Baixa	Baixa
Gateway	Porta USB-C exposta sem proteção	6.1 Médio 3.1/AV:P/AC:L/PR:N/ UI:N/S:U/C:H/I:H/A:N	Baixa	Média
Gateway	Ausência de criptografia do firmware	4.6 Médio 3.1/AV:P/AC:L/PR:N/ UI:N/S:U/C:H/I:N/A:N	Baixa	Baixa
Gateway	Credenciais armazenadas em texto claro	6.2 Médio 3.1/AV:L/AC:L/PR:N/ UI:N/S:U/C:H/I:N/A:N	Baixa	Média

A avaliação dos dispositivos revelou um nível de exposição moderado. A presença de interfaces JTAG habilitadas, associada à ausência de criptografia do firmware, torna possível a extração e análise do conteúdo armazenado na memória flash, bem como a potencial modificação e regravação do firmware, comprometendo a confidencialidade e a integridade do dispositivo. A complexidade de mitigação de ambas as vulnerabilidades é considerada baixa, uma vez que o próprio ESP32 oferece mecanismos nativos para desabilitar as interfaces de depuração e habilitar a criptografia do firmware, o que representa, portanto, falhas de configuração corrigíveis sem necessidade de alterações de hardware.

O *gateway* apresentou o maior nível de exposição entre os componentes avaliados. A porta USB-C sem proteção torna trivial a extração do firmware por qualquer pessoa

com acesso físico ao equipamento. Agravando essa condição, a ausência de criptografia do firmware e o armazenamento de credenciais em texto claro resultaram na exposição de informações sensíveis. Essa combinação de vulnerabilidades aumenta a criticidade, pois, ao contrário das demais falhas identificadas, seu impacto ultrapassa os limites do próprio dispositivo, comprometendo outros componentes da infraestrutura. De posse dessas credenciais, um agente mal-intencionado poderia acessar a rede local, interceptar ou manipular a comunicação entre o *gateway* e o servidor, e comprometer toda a solução IoT. A mitigação envolve tanto medidas de proteção física quanto a adoção de criptografia do firmware e de armazenamento seguro de credenciais.

A aplicação Web demonstrou um nível de maturidade de segurança superior ao dos dispositivos embarcados, com mecanismos de controle de acesso adequados e sem falhas críticas de autenticação ou autorização identificadas durante os testes.

De forma geral, os resultados obtidos indicam que a solução avaliada apresenta vulnerabilidades relevantes, concentradas principalmente nos dispositivos embarcados, onde falhas de configuração e a ausência de mecanismos de proteção básicos resultaram no maior nível de exposição identificado. A facilidade de exploração das vulnerabilidades do *gateway*, em particular, evidencia que o acesso físico aos dispositivos representa um vetor de ataque crítico em ambientes IoT aplicados à aquicultura, reforçando a necessidade de considerar não apenas a segurança lógica, mas também a proteção física dos equipamentos implantados nesses ambientes. Os resultados foram devidamente documentados e repassados à SmartRural, esperando-se que contribuam para elevar o nível de maturidade de segurança da solução.

5. Conclusões e Trabalhos Futuros

Este trabalho apresentou uma metodologia para a realização de testes de penetração em ambientes IoT aplicados à aquicultura, visando adaptar práticas consolidadas de avaliação de segurança às características específicas desses sistemas. A metodologia proposta foi aplicada em um estudo de caso envolvendo uma solução IoT voltada ao monitoramento aquícola, permitindo a identificação de vulnerabilidades relacionadas aos dispositivos embarcados, mecanismos de comunicação e configurações de segurança do ambiente analisado.

Os resultados demonstraram que os dispositivos embarcados, em especial o gateway, apresentaram o maior nível de exposição, com vulnerabilidades relacionadas à ausência de proteção física, falta de criptografia do *firmware* e armazenamento de credenciais em texto claro. A aplicação web demonstrou nível de maturidade superior. Como limitações, destacam-se a ausência de equipamentos de rádio apropriados para testes sobre o protocolo LoRa e a necessidade de análises mais aprofundadas sobre a comunicação entre os dispositivos e o *gateway*.

Como trabalhos futuros, pretende-se expandir a aplicação da metodologia para outros ambientes IoT com características operacionais distintas, permitindo avaliar sua adaptação em diferentes contextos e arquiteturas. Além disso, também se propõe a realização de testes específicos envolvendo outros protocolos de comunicação, como LoRa e LoRaWAN, incluindo análises relacionadas à segurança da transmissão de dados e resiliência da comunicação sem fio.

Referências

Arreaga, N. X., Enriquez, G. M., Blanc, S., and Estrada, R. (2023). Security vulnerability analysis for iot devices raspberry pi using pentest. *Procedia Computer Science*, 224:223–230. 18th International Conference on Future Networks and Communications / 20th International Conference on Mobile Systems and Pervasive Computing / 13th International Conference on Sustainable Energy Information Technology.

Barybin, O., Zaitseva, E., and Brazhnyi, V. (2019). Testing the security esp32 internet of things devices. In *2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC ST)*, pages 143–146.

Bhushan, A., Aimen Fathima, S., and Shanthala, P. T. (2024). Aquaculture iot security landscape: A comprehensive analysis of threats and mitigation strategies. In *2024 5th International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)*, pages 587–593.

Cai, B., Xie, S., Liang, Q., and Lu, W. (2022). Research on penetration testing of iot gateway based on risc- v. In *2022 International Symposium on Advances in Informatics, Electronics and Education (ISAIEE)*, pages 422–425.

Demestichas, K., Peppes, N., and Alexakis, T. (2020). Survey on security threats in agricultural iot and smart farming. *Sensors*, 20(22).

FIRST (2019). Common vulnerability scoring system v3.1: Specification document.

Freitas, F. A. d., Nóbrega, O. d. O., Lins, F. A. A., Santos, J. F. D., Galvez, A. O., and Santos, E. P. D. (2024). A low-cost iot-based solution for water quality monitoring in aquaculture 4.0. In *2024 IEEE 10th World Forum on Internet of Things (WF-IoT)*, pages 517–522.

Gupta, M., Abdelsalam, M., Khorsandroo, S., and Mittal, S. (2020). Security and privacy in smart farming: Challenges and opportunities. *IEEE Access*, 8:34564–34584.

Jaafar, A. G., Ismail, S. A., Habir, A., Ariffin, K. A. Z., and Yusop, O. M. (2024). A raise of security concern in iot devices: Measuring iot security through penetration testing framework. *International Journal of Advanced Computer Science and Applications*, 15(5).

Mahamuni, C. V. and Goud, C. S. (2023). Unveiling the internet of things (iot) applications in aquaculture: A survey and prototype design with thingspeak analytics. *Journal of Ubiquitous Computing and Communication Technologies*.

Meneghello, F., Calore, M., Zucchetto, D., Polese, M., and Zanella, A. (2019). Iot: Internet of threats? a survey of practical security vulnerabilities in real iot devices. *IEEE Internet of Things Journal*, 6(5):8182–8201.

OWASP Foundation (2024). IoT Security Testing Guide.

Scarfone, K., Souppaya, M., Cody, A., and Orebaugh, A. (2008). Technical guide to information security testing and assessment. Special Publication 800-115, National Institute of Standards and Technology.

Zhukabayeva, T., Ahmad, Z., Adamova, A., Karabayev, N., Mardenov, Y., and Satybaldina, D. (2025). Penetration testing and machine learning-driven cybersecurity framework for iot and smart city wireless networks. *IEEE Access*, 13:86144–86166.