UNIVERSIDADE FEDERAL DE SANTA CATARINA
DEPARTAMENTO DE INFORMÁTICA E ESTATÍSTICA
CURSO DE SISTEMAS DE INFORMAÇÃO

LUIS ARMANDO DA SILVA BROCHADO

SEGURANÇA DE DISPOSITIVOS IOT: ANÁLISE DE VULNERABILIDADES DE UMA CÂMERA IP

FLORIANÓPOLIS - SC
2023

LUIS ARMANDO DA SILVA BROCHADO

SEGURANÇA DE DISPOSITIVOS IOT: ANÁLISE DE VULNERABILIDADES DE UMA CÂMERA IP

Trabalho de Conclusão de Curso de Graduação em Sistemas de Informação, do Departamento de Informática e Estatística, do Centro Tecnológico da Universidade Federal de Santa Catarina, apresentado como requisito parcial para obtenção do grau Bacharel em Sistemas de Informação.

Orientadora: Prof.ª Dr.ª Carla Merkle Westphall

Coorientador: Prof. Ms. Rafael Bosse Brinhosa

FLORIANÓPOLIS - SC
2023

LUIS ARMANDO DA SILVA BROCHADO

SEGURANÇA DE DISPOSITIVOS IOT: ANÁLISE DE VULNERABILIDADES DE UMA CÂMERA IP

Trabalho de Conclusão de Curso de Graduação em Sistemas de Informação, do Departamento de Informática e Estatística, do Centro Tecnológico da Universidade Federal de Santa Catarina, apresentado como requisito parcial para obtenção do grau Bacharel em Sistemas de Informação.

Florianópolis,_____de_____de 2023.

Banca examinadora:

_____
Prof.ª Dr.ª Carla Merkle Westphall - UFSC
Orientadora

_____
Prof. Ms. Rafael Bosse Brinhosa - UFSC
Coorientador

_____
Prof. Ms. Fabricio Bortoluzzi - UFSC
Membro

Florianópolis, 2023

AGRADECIMENTOS

À Universidade Federal de Santa Catarina pela possibilidade do estudo.

A minha orientadora, professora Carla Merkle Westphall, pela orientação, pela disponibilidade e pelo imenso apoio no desenvolvimento deste projeto.

Aos meus pais, pelos ensinamentos, pelo amor e por tudo que me proporcionaram.

À Carla Britto, minha esposa, pelo incentivo e pelo apoio nessa jornada.

À banca de defesa, pelas contribuições e pela disponibilidade de tempo.

BROCHADO, Luis Armando da Silva. **Segurança de dispositivos IoT: análise de vulnerabilidades de uma câmera IP**. 2023. 79 f. Trabalho de Conclusão de Curso (Graduação em Sistemas de Informação) – Universidade Federal de Santa Catarina, Florianópolis, 2023.

RESUMO

Com o aumento exponencial de dispositivos IoT (Internet of Things), é grande a necessidade de recursos para garantir a integridade e segurança dos dados trafegados por estes sistemas, de forma que a evolução não se restrinja somente ao aspecto funcional das aplicações, mas também a proteção dos dados e detecção de vulnerabilidades. Aspectos como limitação de hardware, descontinuação de suporte e atualizações de dispositivos fazem com que o risco de novas vulnerabilidades e ataques seja ampliado, gerando problemas em relação à privacidade e segurança dos usuários destes sistemas. Diante deste cenário, neste trabalho foi realizada uma análise de segurança de dispositivos IoT, a partir da realização de testes de vulnerabilidade em câmeras IP, procurando evidenciar a existência destas falhas e sugerir recomendações para melhorar a segurança dos usuários ao utilizar este tipo de aplicação.

Palavras-chave: Segurança em TI; *Internet of Things; IoT*; Internet das Coisas; Aplicações Web; Interface Web.

BROCHADO, Luis Armando da Silva. **IoT Device Security: Vulnerability Analysis of an IP Camera**. 2023. 79 p. Undergraduate Thesis (Bachelor of Information Systems) – Federal University of Santa Catarina, Florianópolis, 2023.

ABSTRACT

With the exponential increase in IoT (Internet of Things) devices, there is a significant need for resources to ensure the integrity and security of data transmitted by these systems. This ensures that the evolution doesn't only focus on the functional aspect of applications but also on data protection and vulnerability detection. Aspects such as hardware limitations, discontinued support, and device updates expand the risk of new vulnerabilities and attacks, creating problems regarding the privacy and security of users of these systems. In this context, this study aims to analyze the security of IoT devices, based on vulnerability tests on IP cameras, seeking to highlight the existence of these flaws and suggest recommendations to improve user security when using this type of application.

Keywords: IT Security; Internet of Things; IoT; Web Applications; Web Interface.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIAÇÕES E SIGLAS

DDoS	*Distributed Denial of Service*
DoS	*Denial of Service*
HTTP	*Hyper Text Transfer Protocol*
IoT	*Internet of Things*
IIoT	*Industrial Internet of Things*
IP	*Internet Protocol*
OWASP	*Open Web Application Security Project*
SQLi	*SQL Injection*
XSS	*Cross-site Scripting*

SUMÁRIO

1 INTRODUÇÃO

Com o advento da Internet das Coisas, bilhões de dispositivos (THE FUTURE OF IOT, 2019) passaram a utilizar a rede mundial de computadores. Esses dispositivos possuem, além de computadores embutidos, um endereço IP na rede e sensores, entre outros recursos (ZHOU *et al*., 2017). Muitos deles, como câmeras de vigilância e impressoras, possuem todas as suas informações técnicas disseminadas em websites na Internet, como no caso da ferramenta SHODAN (SHODAN, 2019). Do ponto de vista de segurança, surgem questionamentos em relação à possibilidade de que estes dispositivos conectados na rede possam estar de alguma forma distribuindo malware, ou que possuam algum tipo de vulnerabilidade, pondo em risco a privacidade e a segurança dos dados de usuários. Um exemplo de vulnerabilidade problemática em IoT foi o caso do malware conhecido como Mirai, onde falhas de firmware desatualizado foram exploradas para invadir dispositivos, e criar uma rede botnet para efetuar ataques de negação de serviço (DDoS) (ANTONAKAKIS *et al*., 2017).

Questionamentos como estes levam a considerar que, apesar do mundo da Internet das Coisas estar cheio de possibilidades, que incluem desde dispositivos *wearables* até casas inteligentes, existe a necessidade de projetar sistemas com tecnologias de segurança adequadas ao tipo de situação a que estamos expostos.

Porém, segundo Ding *et al.* (2019), a diversidade e a complexidade do ecossistema de Internet das Coisas fazem com a que implementação de mecanismos de segurança em IoT seja uma tarefa árdua, uma vez que as soluções de segurança podem não acompanhar todos os novos desenvolvimentos tecnológicos e gerar uma lacuna entre estes aspectos.

1.1 Motivação

Diante do exposto, muitos desafios se apresentam no que diz respeito a garantir segurança a estas aplicações. Segundo as recomendações do projeto OWASP (*Open Web Application Security Project*) (OWASP, 2019), organização internacional focada em melhorar a segurança de aplicações web, as vulnerabilidades em IoT estão classificadas e associadas a 15 áreas de superfícies de ataque (OWASP IOT, 2019). O projeto OWASP também divulga um ranking chamado OWASP Top 10 que apresenta os riscos de segurança mais críticos de

aplicações web e IoT, as vulnerabilidades relacionadas à superfície de ataque *Interface Web do Dispositivo* tem historicamente aparecido entre as primeiras posições.

Motivado pelo contexto apresentado, este trabalho tem como objetivo realizar um estudo abordando as principais formas de ataque e vulnerabilidades relacionadas à Interface Web de Dispositivos IoT. Será feita uma pesquisa dos testes de invasão existentes para este cenário e as ferramentas utilizadas, e por fim, será realizado um teste prático, apresentando a análise dos resultados e procurando sugerir melhorias para a segurança das aplicações.

1.2 Objetivos

Este trabalho é composto por um objetivo geral e quatro objetivos específicos.

1.2.1 Objetivos gerais

Este trabalho tem como objetivo geral realizar uma análise da segurança relacionada à Internet das Coisas a partir da pesquisa realizada, de experimentos com ferramentas de teste de penetração e da implementação de teste prático com dispositivos IoT.

1.2.2 Objetivos específicos

Os objetivos específicos deste trabalho são:

a. Identificar as principais falhas de segurança relacionadas a interface web de dispositivos IoT;
b. Realizar experimentos com ferramentas de teste de penetração;
c. Realizar teste prático com dispositivos;
d. Analisar resultados dos testes propondo correções de falha e recomendações de segurança.

1.3 Organização do Documento

Este trabalho está dividido em seis capítulos, que são Introdução, Fundamentação Teórica, Trabalhos Correlatos, Desenvolvimento da Proposta, Conclusão e Trabalhos Futuros. Após a Introdução, no capítulo 2, Fundamentação Teórica, são apresentados os principais conceitos que embasam o Desenvolvimento da Proposta. O capítulo está subdividido

em cinco seções secundárias que abordam os conceitos de Internet das Coisas, Segurança em TI e IoT, Vulnerabilidades, Ameaças e Ataques na Interface Web.

O capítulo 3 apresenta os Trabalhos Correlatos, onde é descrito de forma resumida, o conteúdo das tres principais referências para a realização deste trabalho.

No capítulo 4 é realizado o Desenvolvimento da Proposta, que subdivide-se em sete seções. Iniciando pela seleção de dispositivos para a realização dos testes de penetração, passando pela definição das ferramentas e dos ataques a serem realizados e culminando na execução dos testes, análise e considerações finais.

No capítulo 5 é apresentada a conclusão do trabalho, onde é feita uma síntese do que foi realizado. E por fim, no capítulo 6, são apresentados os trabalhos futuros, que são sugestões de temas complementares a este projeto.

2 FUNDAMENTAÇÃO TEÓRICA

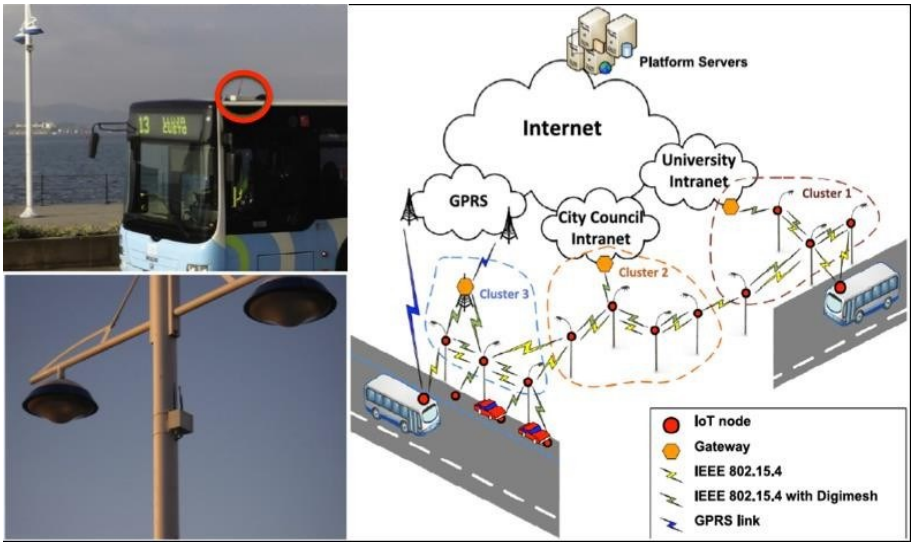
A seguir, será apresentada a base teórica que fundamenta esta pesquisa.

2.1 Internet das Coisas

Segundo Kamienski *et al*. (2016), Internet das Coisas ou IoT (*Internet of Things*) como é também conhecida, se trata de uma grande rede de "coisas": a) que são dispositivos inteligentes, tais como smartphones, *notebooks*, *smartwatches*, eletrodomésticos, veículos; b) e de uma rede sem fio de sensores, que realizam o sensoriamento de uma região ou área para coletar os dados dos dispositivos e enviar para processamento.

Apesar da utilização da IoT ser mais popular nos objetos do cotidiano, como nos *smartphones*, a sua utilização evoluiu bastante na área industrial (IIoT) e comercial, assim como na gestão de infraestrutura pública, nas cidades inteligentes ou *Smart Cities*. Como exemplo para este tipo de aplicação em cidades inteligentes pode-se citar os semáforos inteligentes, sistemas de transporte, estacionamento e iluminação pública, entre outros. Já para aplicação comercial e industrial pode-se indicar os sistemas de monitoramento por câmeras IP para segurança e sensores de monitoramento de máquinas para prevenção e diagnóstico de manutenção (SANTOS, 2016).

Figura 1 - Exemplo de Aplicação IoT em Transporte Público.

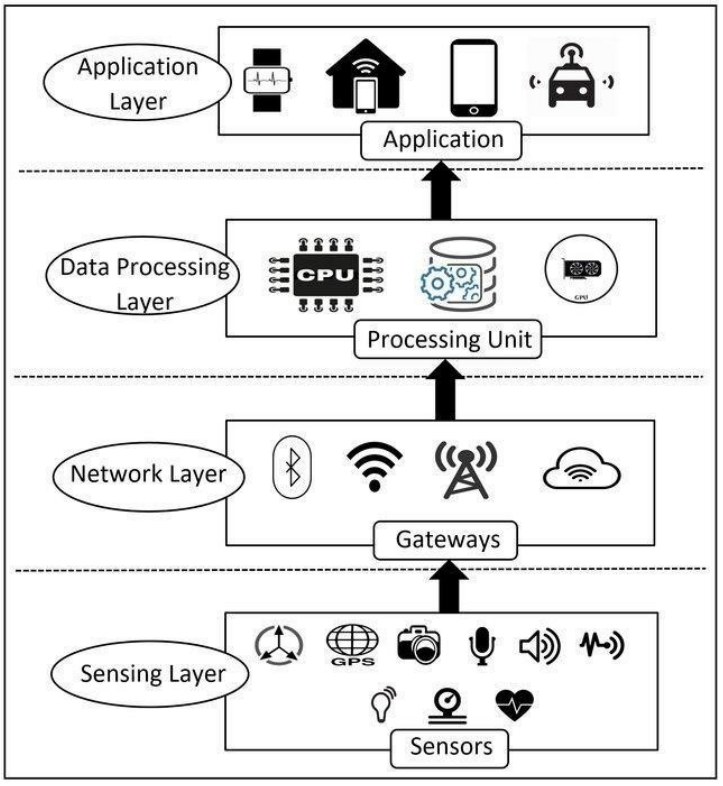


Fonte: (SANCHES *et al.*, 2014).

Conforme a Figura 1, com esta aplicação é possível obter informações em tempo real do transporte público com alertas avisando a chegada do ônibus ao ponto de embarque. A arquitetura da Internet das Coisas pode ser estruturada da seguinte forma, conforme a Figura 2.

No primeiro nível, uma camada contendo os sensores e atuadores. No segundo nível, os gateways, implementando a camada de rede, tipicamente wi-fi ou RFID, por exemplo. No terceiro nível as unidades de processamento, a cloud, por exemplo, onde os dados coletados são analisados e processados. E por fim, as aplicações ou serviços no quarto nível, que exibem as informações processadas para o usuário (SIKDER *et al*., 2018).

Figura 2 - Arquitetura de ambiente IoT.



Fonte: (SIKDER *et al.*, 2018).

2.2 Segurança em TI

Quando tratado do assunto Segurança em TI, conceitos como segurança da informação, segurança de dados, segurança de rede, segurança de computadores, são amplamente abordados, referindo-se a segurança dos dados que trafegam na rede, ou a segurança relacionada ao armazenamento de informações em um banco de dados ou ainda a segurança de uma

aplicação que executa inúmeras funcionalidades manipulando informações sensíveis. Por exemplo, quando o cadastro de um cliente é armazenado em um banco de dados, espera-se que os dados sejam armazenados de forma segura. Espera-se também que ao recuperar estas informações elas estejam precisas, que não tenham sido alteradas por um terceiro não autorizado e que estejam disponíveis a qualquer tempo. Em outro caso, ao enviar um e-mail, espera-se que a mensagem chegue ao seu destino sem ser alterada ou violada, e que o receptor possa ter certeza de que o emissor é quem de fato enviou a mensagem.

Para estes conceitos existem determinados aspectos que a todos são comuns. São as principais propriedades que definem os objetivos da Segurança em Tecnologia da Informação, e que deram origem a regras, políticas e protocolos para orientar a sua aplicação: a Confidencialidade, a Integridade e a Disponibilidade.

Segundo Stallings (2015, p. 6), de acordo com Manual de Segurança de Computadores [NIST95] o conceito de segurança de computadores é definido como "A proteção oferecida para um sistema de informação automatizado a fim de alcançar os objetivos de preservar a integridade, a disponibilidade e a confidencialidade dos recursos do sistema (incluindo software, hardware, firmware, dados e telecomunicações)".

Estes aspectos se estendem ao contexto de segurança em aplicações web assim como para segurança em Internet das Coisas.

De acordo com Stallings (2015, p. 7), a definição para estes conceitos são: *Confidencialidade* refere-se à privacidade dos dados. Significa que dados e informações privados não sejam revelados ou disponibilizados a indivíduos não autorizados.

Já o conceito de *Integridade* refere-se à preservação da autenticidade dos dados ou das informações, impedindo a modificação ou destruição imprópria destas informações de forma não autorizada. Enquanto o conceito de *Disponibilidade* seria a garantia de acesso às informações e dados de forma rápida e contínua.

2.2.1 Segurança em IoT

De acordo com Barros (2021), a IoT é um tema que tem obtido grande notoriedade no mercado, e com isso, a adesão de suas tecnologias por parte das empresas e dos usuários. Com a crescente evolução e expansão no que diz respeito a inovações e sua utilização, observa-se a falta de comprometimento com a segurança dos dispositivos. Ainda de acordo com este autor, este contexto desenvolveu-se em função da falta de previsão de que milhares de dispositivos

passariam a estar conectados em rede, e que a segurança dos dispositivos envolvidos deveria estar implementada. Conforme resultados obtidos por estudos realizados pela Gartner, empresa norte-americana de consultoria na área de TI, até 2022, 50% do orçamento de segurança em IoT serão comprometidos com correção de falhas (PANARELLO *et al*., 2018).

Em um caso que tomou grandes proporções mundiais, empresas como Amazon, Paypal, Spotify e Twitter, ficaram inacessíveis em função de ataques a um servidor de DNS realizados a partir de dispositivos IoT que foram hackeados. Foi o caso do *malware* Mirai que executou uma série de ataques de negação de serviço, inundando de requisições aos servidores e derrubando os serviços destas empresas.

Outro problema relacionado à segurança de IoT, é que o processamento e armazenamento dos dados de usuários são realizados em sua maioria por poucas grandes empresas (PANARELLO *et al*., 2018) e os usuários tendem a subvalorizar a questão da segurança em comparação com a facilidade de uso que lhes é oferecida. Desta forma facilita a ocorrência de ataques sem a necessidade de muito conhecimento por parte dos invasores (GROBELNA; GROBELNY; BAZYDŁO, 2018).

Por outro lado, apesar das técnicas de ataque mais comuns serem conhecidas, e, portanto já protegidas na maior parte dos sistemas, no contexto de IoT, muitas delas ainda são exploradas por se tratar de uma tecnologia mais recente que ainda não possui os mecanismos de segurança necessários implementados (CHECKMARX, 2018).

2.3 Vulnerabilidade e Ameaça

Segundo a OWASP (2014, p. 29) vulnerabilidade é " uma falha ou fraqueza no projeto, implementação, operação ou gerenciamento de um sistema que pode ser explorada para comprometer os objetivos de segurança do sistema". Já, de acordo com a CVE, vulnerabilidade é uma falha ou característica indevida que pode ser explorada para concretizar uma ameaça. Ou seja, vulnerabilidades são alvos elegíveis que um usuário malicioso pode utilizar para efetuar um ataque a um sistema, podendo causar danos ou obter informações de forma não autorizada.

Já o conceito de ameaça, de acordo com Stallings (2015, p. 10), é um potencial evento de exploração de uma vulnerabilidade do sistema, que possa causar dano, instabilidade ou comprometer a segurança deste sistema.

A seguir será abordado o aspecto de vulnerabilidade mais direcionado ao contexto de internet das coisas.

2.3.1 Vulnerabilidades em IoT

Um dos projetos realizados pela OWASP é o OWASP Internet of Things Project, que periodicamente apresenta um relatório com informações sobre as principais vulnerabilidades de IoT, quais as superfícies de ataque a que estas vulnerabilidades estão associadas e um resumo destas vulnerabilidades. Na última versão divulgada, em 2018, as principais apresentadas foram:

- Enumeração de nome de usuário;
- Senhas fracas;
- Bloqueio de conta;
- Serviços não criptografados;
- Autenticação de dois fatores;
- Criptografia mal implementada;
- Atualização enviada sem criptografia;
- Atualizar local gravável;
- Negação de serviço;
- Remoção de mídia de armazenamento;
- Nenhum mecanismo de atualização manual;
- Mecanismo de atualização ausente;
- Exibição da versão do firmware e/ou data da última atualização;
- Extração de firmware e armazenamento;
- Manipulando o fluxo de execução de código do dispositivo;
- Obtendo acesso ao console;
- Componentes de terceiros inseguros.

Conforme mencionado anteriormente, as vulnerabilidades apresentadas estão associadas a uma ou mais superfície de ataque. Estas superfícies de ataque são áreas do sistema em que pontos de vulnerabilidade podem ser explorados.

No escopo deste trabalho serão abordadas as vulnerabilidades associadas à superfície de ataque Interface Web de dispositivos, onde ainda segundo a OWASP, as principais são as seguintes, conforme apresentado na Tabela 1.

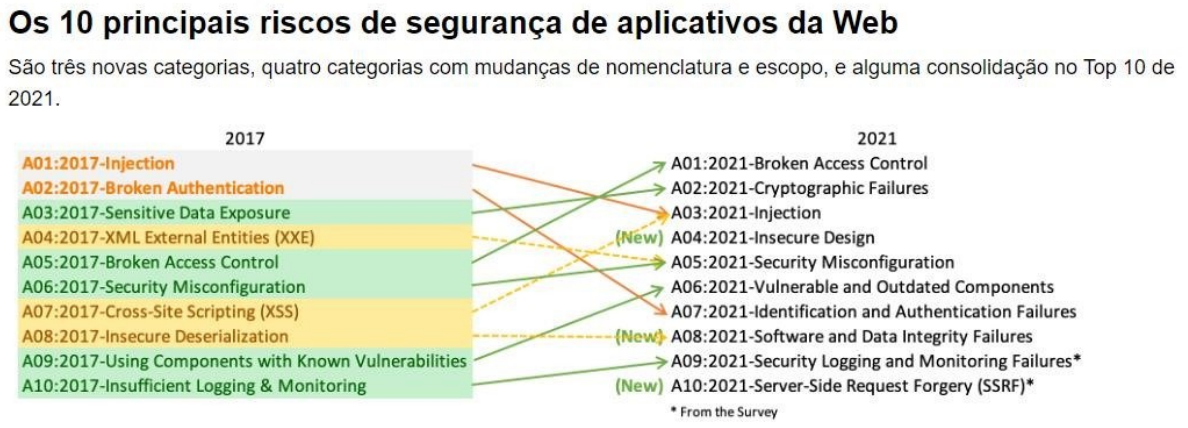
Tabela 1 - Superfície de ataque Interface Web do dispositivo em IoT.

Vulnerabilidade	Resumo
Enumeração de nome de usuário	Capacidade de coletar um conjunto de nomes de usuário válidos interagindo com o mecanismo de autenticação.
Senhas fracas	Capacidade de definir senhas de conta para “1234” ou “123456”, por exemplo.
Bloqueio de conta	Capacidade de continuar enviando tentativas de autenticação após 3 a 5 tentativas de login com falha.
Credenciais padrão conhecidas	Uso de senhas padrão pré-programadas.
Mecanismo de recuperação de senha inseguro	Falta de mecanismos de autenticação de dois fatores, como token de segurança ou scanner de impressão digital.

Fonte: OWASP Internet of Things Project.

De acordo com o relatório OWASP Top 10, que apresenta os dez riscos de segurança mais críticos em aplicações web, foi divulgado um mapeamento entre os relatórios de 2017 e 2021, conforme apresentado na figura 3.

Figura 3 - Mapeamento OWASP Top 10 2017 e 2021.



Fonte: OWASP.

Na figura 3 pode-se observar que, no relatório de 2017, a Quebra de Autenticação ocupava a segunda posição, enquanto que no relatório de 2021 passou para a sétima posição. Já a Quebra de Controle de Acesso ocupava a quinta posição em 2017, e passou para a primeira posição em 2021. Ambas as vulnerabilidades associadas à Interface Web do Dispositivo. Portanto, é possível observar que estas vulnerabilidades continuam figurando entre as mais críticas mesmo após quatro anos de monitoramento.

A seguir serão abordadas as principais formas de ataque para explorar as vulnerabilidades listadas.

2.4 Ataques na Interface Web do dispositivo

Os ataques são tentativas, que utilizam métodos ou técnicas, buscando explorar vulnerabilidades do sistema (STALLINGS, 2015). Podem ser de dois tipos: passivos ou ativos. *Passivo,* quando não interfere no funcionamento do sistema e pode ter somente o objetivo de coletar informações de forma não autorizada. *Ativo,* quando afeta o funcionamento do sistema, podendo até interromper a sua atividade, como é o caso de *ataques de negação de serviço.*

No caso dos ataques às vulnerabilidades listadas da Interface Web do dispositivo, pode haver uma combinação dos dois tipos de ataques, porém na maioria dos casos são utilizados ataques ativos como apresentado a seguir.

Enumeração de nome de usuário:

Este tipo de vulnerabilidade permite ataques interagindo com o mecanismo de autenticação. Em alguns casos, ao enviar credenciais erradas, o sistema lança uma mensagem informando que o nome de usuário está presente no sistema e a senha fornecida está errada, ou vice versa. A partir desta informação, o atacante consegue identificar se o usuário é válido ou não. Uma vez em posse de usuários válidos, pode tentar um ataque de força bruta para acessar o sistema (OWASP WSTG). Um possível cenário de ataque seria quando a interface web apresenta a funcionalidade “Esqueci minha senha”. Que ao informar um usuário inválido o sistema informa: “O usuário *Xyz* não existe”.

Desta forma é possível testar até encontrar um usuário válido. Outro cenário seria a tentativa de um ataque XSS, scripts entre sites, incluindo um script como parâmetro na URL, na barra de endereço do navegador:

```
http://xyz.com/index.php?user=<script>alert(123)</script>
```

Caso o sistema seja suscetível ao ataque XSS, a resposta do navegador é um pop-up de alerta (OWASP IOT). Neste caso, o atacante pode enviar um script para tentar obter informações do usuário.

Senhas fracas:

Esta vulnerabilidade, que é amplamente explorada em Iot, permite ataques com tentativas de autenticação com senhas padrão ou de fácil adivinhação, como 12345, admin, data de nascimento ou nome do animal de estimação. Existem ataques automatizados que utilizam listas de senhas, como ataque do dicionário, que facilmente quebram a autenticação deste tipo de vulnerabilidade.

Segundo Barros (2021, p. 31), "em dispositivos IoT estes ataques ocorrem principalmente através de um protocolo TCP/IP chamado Telnet", sendo necessário que o dispositivo possua a porta 23 aberta e que o atacante possua as informações de usuário e senha. Um possível cenário de ataque seria uma interface que não utiliza proteção contra ameaças ou preenchimento de credenciais, o que permitiria que o atacante executasse várias tentativas até obter os valores válidos.

Atualmente, muitos sistemas já utilizam recursos exigindo senhas mais elaboradas com número mínimo de caracteres, mistura de letras maiúsculas, minúsculas e números, o que minimiza a exploração deste tipo de ataque. Além disso, pode ser utilizado um recurso de autenticação com dois fatores e a atualização de senha periodicamente sem permitir repetição de senhas já utilizadas anteriormente.

Outro cenário possível é um ataque de *man in the middle* onde o atacante monitora o tráfego de rede tentando verificar se as credenciais estão sendo transmitidas em texto plano, não criptografado.

Bloqueio de conta:

Esta vulnerabilidade permite ataques de força bruta, em que a interface não define um limite de tentativas de autenticação. Desta forma o atacante pode efetuar diversas tentativas até obter acesso ao sistema. Para evitar este tipo de ataque deve ser implantado mecanismos de bloqueio de conta, onde após um determinado número de tentativas a conta é bloqueada por um período de tempo. Estes mecanismos devem ter um equilíbrio para tentar garantir o acesso autorizado de usuários e ao mesmo tempo impedir o acesso dos atacantes (OWASP).

Credenciais padrão conhecidas:

Esta vulnerabilidade possui um contexto similar ao de *Senhas Fracas*, pois permite acesso facilitado aos dispositivos, a partir de tentativas de autenticação com senhas padrão.

De acordo com Abdalla (2020), em um caso de estudo de câmeras IP, foi verificado que os dispositivos são fornecidos com uma credencial padrão que é fixada na parte traseira, com a identificação do dispositivo e a senha, que podem ser utilizadas na página do dispositivo online para receber vídeos ao vivo, a menos que seja alterado pelo usuário. Com a inspeção do tráfego de rede foi possível verificar que as informações trocadas entre o aplicativo Android e a câmera são transmitidas como texto simples, permitindo a sua visualização e colocando em risco não somente a segurança da câmera, mas da rede como um todo.

Mecanismo de recuperação de senha inseguro:

Este tipo de vulnerabilidade se refere a uma funcionalidade de autoatendimento onde o usuário redefine a senha de acesso sem a intervenção de um administrador do sistema. O cenário de ataque aqui pode ocorrer se ao redefinir a senha, a ferramenta de redefinição mostrar a senha, permitindo ao atacante a possibilidade de fazer login na conta. Ou ao enviar a senha por e-mail para o usuário, a mesma seja armazenada em texto simples ou em um formato não criptografado (OWASP).

Outro cenário seria se o mecanismo de recuperação de senha for vulnerável a CSRF, Cross-Site Request Forgery, ou seja, através deste ataque, forçar o usuário a executar ações indesejadas. Um exemplo é a identificação de um campo oculto com o e-mail do usuário através de um proxy e fazer um redirecionamento para o e-mail do atacante (ALMEIDA JR., 2021).

3 TRABALHOS CORRELATOS

A seguir, será apresentada a seção acerca dos trabalhos correlatos a esta pesquisa.

3.1 Testing Security for Internet of Things - A Survey on Vulnerabilities in IP Cameras

Este trabalho é uma dissertação de mestrado que aborda a crescente proliferação de dispositivos conectados à Internet, especialmente dispositivos IoT que frequentemente apresentam falhas de segurança. O foco principal da pesquisa é nas câmeras IP , que são dispositivos comuns em residências, ambientes industriais e comerciais.

Os objetivos da pesquisa incluem investigar como dispositivos IoT são localizados por invasores e quais métodos são usados para explorar vulnerabilidades nesses dispositivos. Aplicar esses métodos às câmeras IP para avaliar o impacto na segurança, considerando as perspectivas do usuário e do invasor. E por fim, discutir as consequências e os impactos desses ataques, bem como propor soluções para melhorar a segurança.

A pesquisa destaca a importância da alteração das credenciais padrão em dispositivos, pois muitos deles têm senhas fracas ou até mesmo em branco, o que os torna vulneráveis a ataques. Além disso, explora vulnerabilidades comuns em dispositivos IoT e ressalta a necessidade de os usuários finais influenciarem positivamente a segurança.

A pesquisa também menciona a capacidade de câmeras IP de gerar ataques DDoS devido à sua largura de banda, tornando-as alvos atraentes para invasores. Em última análise, o texto enfatiza a necessidade de conscientização sobre a segurança em dispositivos IoT, como câmeras IP, e destaca a importância da implementação de medidas para proteger esses dispositivos.

3.2 Abusing the Internet of Things: Blackouts, Freakouts, and Stakeouts

O livro “Abusing the Internet of Things: Blackouts, Freakouts, and Stakeouts” (Abusando da Internet das Coisas: Apagões, Surpresas e Vigilâncias), Dhanjani (2015) discorre sobre as vulnerabilidades de segurança e os riscos associados à proliferação de dispositivos conectados à Internet, conhecidos como IoT. Os autores destacam como estes dispositivos podem ser explorados por atacantes para causar invasões de privacidade e outros problemas,

oferecendo dicas essenciais para profissionais de segurança cibernética e pesquisadores envolvidos nesta área.

No capítulo 3, os autores relatam sobre um incidente envolvendo um monitor de bebês fabricado pela marca Foscam, onde os pais foram surpreendidos por um estranho estar conversando com seu bebê através do dispositivo. A partir deste ponto, apresentam uma narrativa mais detalhada e cronológica sobre as vulnerabilidades descobertas por pesquisadores de segurança relacionados a estes dispositivos. Incluindo outra descoberta apresentada em um paper intitulado “Exploiting Foscam IP Cameras” pela empresa Ramparts Security.

Além desta narrativa, o livro aborda também outros temas como, de que forma invasores mal-intencionados podem explorar dispositivos como lâmpadas de LED sem fio, fechaduras eletrônicas, TVs inteligentes e carros conectados.

3.3 IoT-PEN: An E2E Penetration Testing Framework for IoT

Este trabalho é uma qualificação de doutorado motivado pela crescente preocupação com a segurança na Internet das Coisas. Devido à presença de dispositivos com recursos limitados, a falta de foco dos fabricantes em segurança e a descontinuação do suporte e atualizações desses dispositivos, observa-se como resultado uma grande quantidade de dispositivos inseguros na internet e nas redes domésticas, representando um sério risco para a segurança e privacidade das pessoas.

Com base neste contexto, o trabalho propõe o desenvolvimento de um framework de segurança chamado IoPenT, que tem como objetivo realizar testes de invasão em dispositivos IoT, com a capacidade de corrigir automaticamente as vulnerabilidades encontradas nas interfaces web.

Segundo o autor, inicialmente, o trabalho revisa as metodologias existentes e o estado da arte em testes de invasão de dispositivos IoT. Após, é apresentada a proposta do IoPenT e a metodologia para correção semi-automática das vulnerabilidades da interface web. Ao final, é desenvolvida a prova de conceito inicial, na qual é realizado o teste de invasão em um ambiente de smart home.

A proposta do IoPenT é identificar e corrigir falhas de segurança em interfaces web de dispositivos IoT, com um foco específico em ambientes de casas inteligentes. A ideia é criar uma nova interface segura para substituir a interface insegura do dispositivo, reduzindo assim os riscos de ataques, invasões e vazamento de dados.

O trabalho se inspira em trabalhos anteriores, como o framework PENTOS de Visoottiviseth *et al*. (2017) e as regras de segurança propostas por Hossain, Fotouhi e Hasan (2015) para proteção de dispositivos IoT. Muitos dispositivos IoT carecem de atualizações de firmware para corrigir vulnerabilidades, tornando-os alvos fáceis para ataques que soluções tradicionais de segurança, como firewalls, podem não ser capazes de impedir.

Em resumo, o IoPenT é uma proposta inovadora que visa aumentar a segurança dos dispositivos IoT, especialmente em casas inteligentes, através de testes de invasão e correção automática de vulnerabilidades, oferecendo uma solução eficaz para mitigar os riscos associados a dispositivos IoT inseguros.

4 DESENVOLVIMENTO DA PROPOSTA

Nesta seção é apresentada a proposta de desenvolvimento de testes de penetração. A execução dos testes tem a finalidade de avaliar a segurança dos dispositivos evidenciando vulnerabilidades, caso elas existam. Sem a intenção de obter dados privados ou causar algum tipo de dano ao sistema. Segundo Weidman (2014, p. 30), “Testes de invasão ou pentesting envolvem a simulação de ataques reais para avaliar os riscos associados a potenciais brechas de segurança”.

Este desenvolvimento segue o seguinte roteiro: inicialmente, foram selecionados os dispositivos a serem utilizados. Em seguida, definiu-se as ferramentas e os ataques realizados nos testes. Após será realizada a execução dos testes. E, por fim, a análise e as considerações finais.

4.1 Dispositivos

Segundo Syed *et al*. (2020), dispositivos IoT de aplicação residencial são conhecidos por apresentarem baixo controle de segurança. Um exemplo disso são as câmeras IP , que na sua maioria utilizam senhas de administrador facilmente acessíveis ou políticas de senha fracas em relação ao seu tamanho e complexidade. Em função da facilidade gerada por este tipo de vulnerabilidade, este tipo de dispositivos é alvo frequente de botnets.

Ainda de acordo com Syed *et al*. (2020), outro problema encontrado nestes dispositivos são os backdoors, que implementados por desenvolvedores com finalidade de teste durante o desenvolvimento são às vezes esquecidos de serem removidos ou mantidos para fins de manutenção. A descoberta de um backdoor em um dispositivo pode torná-lo um alvo atraente para invasores.

Segundo Kovacs (2016), alguns modelos de câmeras IP Sony permitem que um usuário habilite de forma remota o acesso ao serviço Telnet, enviando uma requisição HTTP. O invasor pode então utilizar este recurso como backdoor, após a autenticação como root, para obter acesso remoto com privilégios.

De acordo com Bjørneset (2017), as câmeras IP da Xionmai Technology foram uma das marcas que tiveram seus produtos explorados. O ataque explorou senhas padrão fracas que foi a principal forma de ataque do malware Mirai.

Já no trabalho de Abdalla e Varol (2020), foi realizada uma pesquisa investigando as vulnerabilidades da câmera “Intelligent Onvif YY HD” que também apresentou problema de utilização de credenciais padrão, permitindo acesso pelo navegador a imagens ao vivo. Também verificou, fazendo uma análise de tráfego de rede, que as informações trocadas entre o aplicativo android e a câmera são transmitidas como texto simples permitindo a sua visualização e colocando em risco não somente a segurança da câmera mas da rede como um todo. Baseado neste cenário, será utilizada a câmera IP como o dispositivo para a realização dos testes neste trabalho.

4.1.1 Pesquisa e seleção do dispositivo

A partir da pesquisa realizada por Dhanjani (2015), foi identificado que câmeras IP da marca Foscam possuem um histórico de ocorrências de falhas de segurança. Trata-se de uma marca chinesa fabricada pela empresa Shenzhen Foscam Intelligent Technology Corporation ou simplesmente Foscam, que além das câmeras IP também produzem monitores de bebês, entre outros produtos.

De acordo com este autor, foi relatado que além das questões de credenciais fracas, foi encontrada uma vulnerabilidade relacionada ao recurso de DNS dinâmico que pode ser explorado para ataques de Phishing. Conforme relatado no artigo de Krebs (2014), a Foscam informou que o problema afetou uma lista de modelos antigos, e que a empresa esperava lançar uma versão atualizada do firmware (Versão 55) para corrigir o bug até 25 de janeiro 2014, uma vez que os problemas identificados estão associados a versão de firmware 11.37.2.54 e anteriores.

Porém, ainda de acordo com Dhanjani (2015), a maioria dos proprietários de dispositivos provavelmente não estava ciente dessa atualização de segurança ou não tomou medidas para aplicá-la, visto que este processo envolvia o download do arquivo para atualização manual, o que nem todos os usuários estão familiarizados. Desta forma os dispositivos continuaram expostos e passíveis de exploração, conforme relataram os pesquisadores de segurança, “Encontramos exatamente nenhuma câmera disponível que executa o firmware mais recente oferecido pela Foscam. Isso pode indicar que os usuários finais que sabem como corrigir também sabem que é melhor não conectar uma câmera IP à Internet, ou pode indicar que ninguém corrige suas câmeras”.

Com base nestas informações, optou-se pela realização dos testes com os dispositivos da marca Foscam e que a obtenção de dispositivos seria feita de duas formas: seleção de dispositivos pela plataforma Shodan e aquisição de um dispositivo para testes locais.

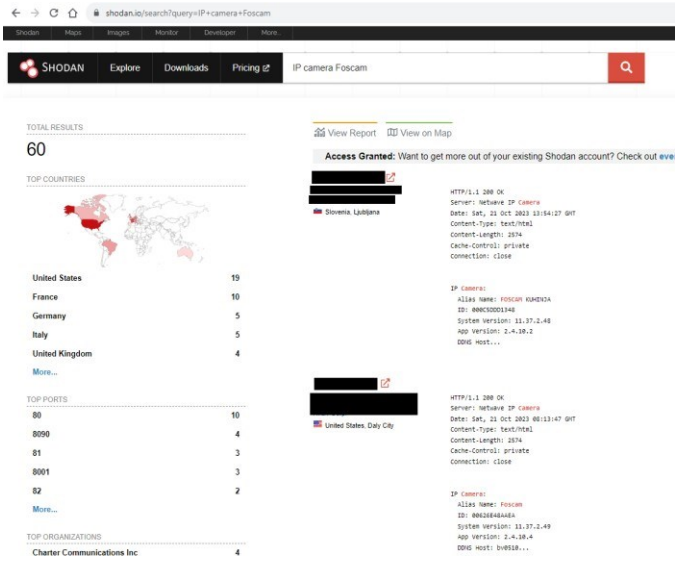
Para a aquisição do dispositivo foi realizada uma pesquisa na internet por câmeras IP, usadas, da marca Foscam. Foi adquirido o modelo FI9900EP (Figura 4), encontrado na plataforma de ecommerce Mercado Livre, que das opções encontradas foi a avaliada em melhor estado para a finalidade.

Figura 4 - Câmera IP Foscam modelo FI9900EP.

Fonte: Acervo pessoal do Autor.

Para a seleção dos dispositivos remotos foi realizada uma pesquisa na plataforma Shodan utilizando várias combinações de filtro, como por exemplo: “camera ip Foscam”.

Figura 5 - Pesquisa plataforma Shodan.



Fonte: Acervo pessoal do Autor.

Na figura 5 é possível ver em alguns resultados o Alias Name: Foscam, além de outras informações como a versão do sistema , o nome do servidor , localização da câmera e protocolo HTTP entre outras informações. O IP foi coberto pela tarja por questão de privacidade. A utilização da plataforma Shodan, mesmo criando uma conta gratuita, limita os resultados em duas páginas por dia, o que dificulta o trabalho de pesquisa, já que nem todos os resultados atendem os requisitos. A pesquisa tem como um dos objetivos avaliar a segurança da interface web do dispositivo. Em alguns casos, ao tentar acessar a interface é lançada mensagens de erro como “Não é possível acessar este site”, ou "401 - Unauthorized”, “Não Autorizado”. Portanto foram necessárias inúmeras tentativas até encontrar resultados satisfatórios. Dos resultados encontrados foi selecionado um dispositivo para a realização dos testes de forma remota.

4.2 Ferramentas

Esta seção aborda uma breve descrição das ferramentas utilizadas na realização dos testes de penetração.

4.2.1 Shodan

É uma ferramenta de busca especializada em dispositivos conectados à Internet, que indexa e cataloga dispositivos online revelando informações como banners de serviços, portas, sistemas operacionais, localização geográfica e vulnerabilidades. É uma ferramenta valiosa para profissionais de segurança cibernética, por permitir a identificação de vulnerabilidades e com isso avaliar a exposição a ameaças. Da mesma forma, é bastante utilizada pelo meio acadêmico para pesquisas e experimentos.

4.2.2 Kali Linux

É uma plataforma de testes de penetração baseado em uma distribuição Linux, que disponibiliza ampla gama de aplicações e ferramentas de teste, que vai desde escaneadores de porta, como o Nmap, crackeadores de senhas, como John the Ripper ou Hydra, até ferramentas de análise de tráfego de rede como Wireshark, sendo uma das plataformas mais conhecidas e

utilizadas para estudo em segurança computacional e auditoria forense. As demais ferramentas utilizadas para a realização dos testes de penetração são provenientes deste pacote.

4.2.3 Owasp Zap

Zap, da abreviação de Zed Attack Proxy, é uma ferramenta de testes de penetração utilizada para identificar vulnerabilidades em aplicações web. Dentre os recursos disponibilizados esta ferramenta apresenta scanner automatizado, servidor proxy interceptador e rastreadores web tradicionais e AJAX.

A utilização do scanner automatizado, por exemplo, é bem simples. Bastando informar a url da aplicação a ser escaneada e definir o tipo de spider a ser utilizado; se tradicional e com ou sem AJAX. Após a conclusão do escaneamento pode ser gerado um relatório com os resultados. Este relatório apresenta alertas categorizados por nível de risco, conforme Figura 6, e pode ser customizado quanto ao seu formato, pdf ou html por exemplo, e seleção dos conteúdos a serem apresentados de acordo com a necessidade do usuário.

Figura 6 - Categoria dos níveis de risco.

Fonte: ZAP.

4.2.4 Hydra

É um cracker de logon de rede que vem pré-instalado no pacote da Kali Linux e que possibilita testes de ataque de força bruta e ataque de dicionário. É uma ferramenta projetada para utilização exclusivamente em protocolos de rede online como SSH, HTTP, RDP ou em formulários HTML. Pode ser utilizado por comandos no terminal ou por interface gráfica, xHydra. Em ambas as formas é necessário informar pelo menos três parâmetros: usuário(s),

senha(s) e o recurso a ser atacado. Porém existe uma série de parâmetros adicionais que podem ser informados para refinar a precisão do ataque.

4.2.5 Wireshark

É uma aplicação que analisa o tráfego de rede monitorando a entrada e saída de dados de diversos protocolos. Além disso, é um *snnifer* de pacotes, o que significa que realiza a captura de mensagens enviadas e recebidas de seu computador podendo fazer o armazenamento e apresentação dos seus conteúdos. Possui recurso de captura ao vivo e análise offline, e suporte de descriptografia de vários protocolos como IPsec, Kerberos, SSL/TLS, WEP, WPA/WPA2.

4.3 Ataques Realizados nos Testes

Nesta seção são apresentados os ataques selecionados para a realização dos testes de invasão. Para a realização dos testes, foram escolhidos os ataques relacionados às vulnerabilidades apresentadas pela OWASP Top 10 e que estão associados à interface web. E ataques relatados por pesquisas anteriores, como os registrados na CVE, Common Vulnerabilities and Exposures, e que estão associados aos dispositivos selecionados.

Relativo às vulnerabilidades apresentadas pela OWASP Top 10, foi mencionado a enumeração de nome de usuário, senhas fracas e bloqueio de conta, conforme mencionado na seção 2.3.1, Tabela 1 e descritos com mais detalhes na seção 2.4 . Os ataques associados a estas vulnerabilidades são aqueles realizados por ferramentas que interagem com os mecanismos de autenticação, como Hydra ou John The Ripper. São ataques de dicionário e de força bruta, além da interação do atacante com o mecanismo de autenticação diretamente na interface web para testar a capacidade de definição de senhas de baixa complexidade.

Já relativo a ataques anteriores às câmeras IP Foscam, segundo Bjørneset(2017), uma lista de ataques foi coletada a partir do livro “Abusando da Internet das Coisas”, Dhanjani (2015), e do material da apresentação de Sergey Shekyan e Artem Harutyunyan (2013), na conferência *Hack in the Box*, que ocorreu em Amsterdam. Estes pesquisadores realizaram uma pesquisa mais avançada chegando a efetuar modificações no firmware de determinadas versões para transformar a câmera em hospedeiro de software malicioso. A lista inclui os ataques a seguir.

4.3.1 Path Directory Traversal

Catalogado na CVE como CVE-2013-2560 é um ataque a aplicativos web onde é realizada uma tentativa de exploração adicionando caminhos de diretórios ao final da url com **“ ../ ”**. De acordo com o CVE, no caso das câmeras Foscam, o ataque foi identificado em firmwares anteriores à versão 11.37.2.49, adicionando “//../proc/kcore” no final do endereço, por exemplo, http://[IP Address]/proc/kcore .

Segundo Dhanjani (2015), “De acordo com os pesquisadores, um atacante de posse do endereço IP da câmera, pode acessar a memória completa do dispositivo através de uma URL específica (http://[Endereço IP]/proc/kcore). Uma vez com acesso ao arquivo ‘kcore’, o atacante pode abrir esse arquivo em um editor hexadecimal para obter o nome de usuário e senha. Com essas credenciais em mãos, o atacante pode controlar a câmera do dispositivo.”

4.3.2 Authentication Bypass (Ataque de Forced Browsing)

Registrado na CVE como CVE-2014-1911, utiliza a mesma técnica do Path Directory Traversal, de modificação da URL acrescentando parâmetros, porém nesse caso se refere a obtenção de acesso a serviços ou conteúdos sem autorização, ignorando os mecanismos de autenticação. Segundo Bjørneset (2017), o caso referente às câmeras Foscam ocorre em versões anteriores a 11.37.2.55 o sistema permitiu a obtenção de vídeos e imagens gravadas do dispositivo sem autenticação de usuário, somente digitando o endereço IP da câmera seguido por /videostream.asf? ou /snapshot.jpg? no navegador ou no VLC Media Player.

4.3.3 Envenenamento de DNS Dinâmico

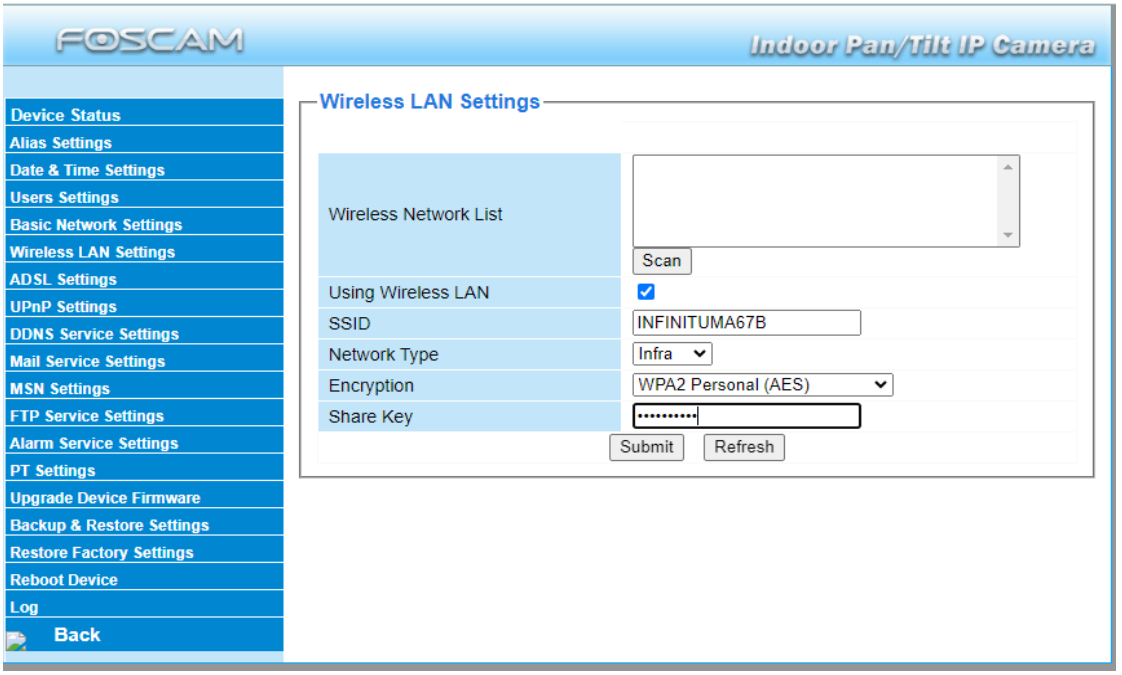
Este é um ataque mais complexo que prevê uma série de passos incluindo o controle de envio de informações entre o usuário e o servidor para a obtenção das credenciais de acesso. Mas de forma mais resumida,o invasor de posse do endereço do DNS dinâmico, caso realize uma exploração bem sucedida, modifica a associação do IP no servidor DNS para um IP de seu controle, desta forma disponibiliza uma página falsa de login para o usuário acessar e com isso obter as credenciais do dispositivo. No caso da Foscam esta ação foi possível em função do sistema de nomes de domínio seguirem um padrão fornecido pela empresa de fácil adivinhação,

“XXYYYY.myfoscam.org" onde XX são caracteres alfabéticos e YYYY é um número de quatro dígitos variando de 0000 a 9999. É fácil perceber, portanto, que um domínio entre AA0000 e ZZ9999 “.myfoscam.org" é um potencial DNS dinâmico de uma câmera para acesso remoto. Catalogado na CVE como CVE-2014-1849.

4.3.4 Cross Site Scripting (XSS)

Registrado na CVE como CVE-2013-5215, este é um ataque em que elementos HTML e scripts podem ser inseridos em um formulário, chamado de Persistido, pois o *script* é enviado ao servidor para ser executado posteriormente, ou pela barra de endereço do navegador, chamado de Refletido pois são executados no lado do cliente na requisição. Estes scripts podem ser um código malicioso para gerar um ataque de phishing ou para induzir o usuário a ações indesejadas. No caso das câmeras IP Foscam esta foi uma vulnerabilidade apontada que permitiu a exploração da interface nos campos de configuração Wireless LAN Settings, figura 7, portanto existente apenas para os modelos que possuem esta opção.

Figura 7 - Interface de configuração wireless da câmera IP Foscam.



Fonte: Acervo pessoal do Autor.

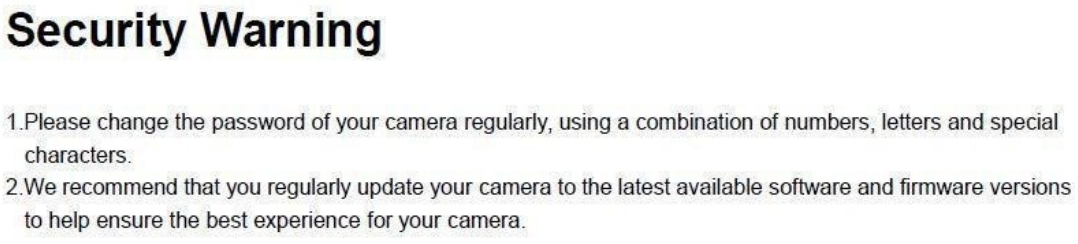
4.4 Instalação e Configuração da Câmera local

Antes da execução dos testes de fato, foi realizada a instalação e a configuração da câmera local para que os procedimentos pudessem ser realizados de forma padronizada para todos os dispositivos.

A câmera local é uma Foscam modelo FI9900EP que foi adquirida para a realização de testes locais. Ao receber o produto foi realizada uma verificação para avaliar se o dispositivo estava funcionando corretamente. O que verificou-se positivo. Para realizar a instalação da câmera foi feito o download do manual do usuário do modelo, e constatado que se trata de uma "Outdoor HD IP Camera", ou seja, é um modelo desenhado para monitoramento exterior como pátios, supermercados ou escolas. Também foi verificado que utiliza conexão na rede via cabo Ethernet, ou seja, é conectada ao roteador via cabo.

Avançando pelo manual, verificou-se que logo no início, antes das seções de instalação e utilização, apresenta um aviso de segurança informando ao usuário para alterar regularmente a senha utilizando combinações de números, letras e caracteres especiais. E recomendando a atualização regular da câmera para as últimas versões de software e firmware disponíveis (Figura 8). Esta mensagem chamou atenção, visto que os itens de segurança abordados estão relacionados à vulnerabilidades selecionadas para os testes. E também porque demonstra preocupação do fabricante com a segurança do produto.

Figura 8 - Aviso de segurança informado no manual do usuário.



Fonte: Foscam.

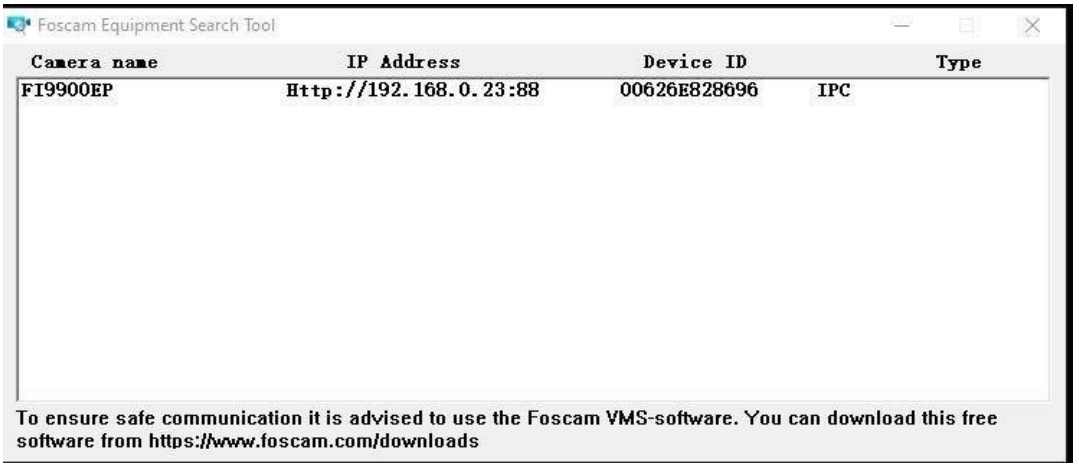
Continuando o processo de instalação, foi verificado que na parte inferior possui uma etiqueta com algumas informações do dispositivo (Figura 9). Entre elas, as credenciais padrão, usuário “Admin” e senha em branco, conforme consta no manual.

Figura 9 - Etiqueta com credenciais padrão de fábrica.

Fonte: Acervo pessoal do Autor.

Então, foi realizada a conexão da câmera na rede, via cabo Ethernet pelo roteador, e à energia elétrica. Após, foi realizado o download de uma ferramenta auxiliar do dispositivo, "Equipment Search Tool", a partir do website oficial da Foscam, para ser instalada no computador, conforme orientado no manual. Essa ferramenta serve para identificar o dispositivo na rede e acessá-lo, além de possibilitar a visualização de algumas configurações.

Figura 10 - Interface da ferramenta auxiliar da câmera IP no computador.

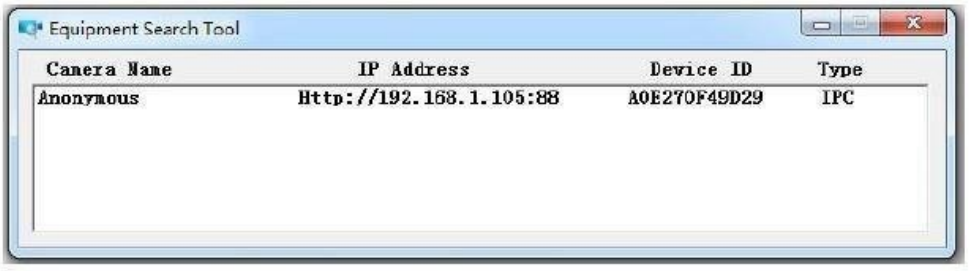


Fonte: Acervo pessoal do Autor.

Ao acessar a aplicação é mostrado o dispositivo conectado à rede, o endereço IP e o MAC Address (Figura 10). Foi verificado que na parte inferior da tela da aplicação apresentou

uma mensagem informativa para baixar o software Foscam VMS, com o objetivo de garantir a segurança na comunicação. Foi verificado também que no manual do usuário do modelo, esta mensagem não é apresentada na ilustração da ferramenta, o que pode indicar duas possibilidades, de que a utilização do software foi incluída em uma atualização de versão posterior ou o manual do usuário não foi atualizado (Figura 11).

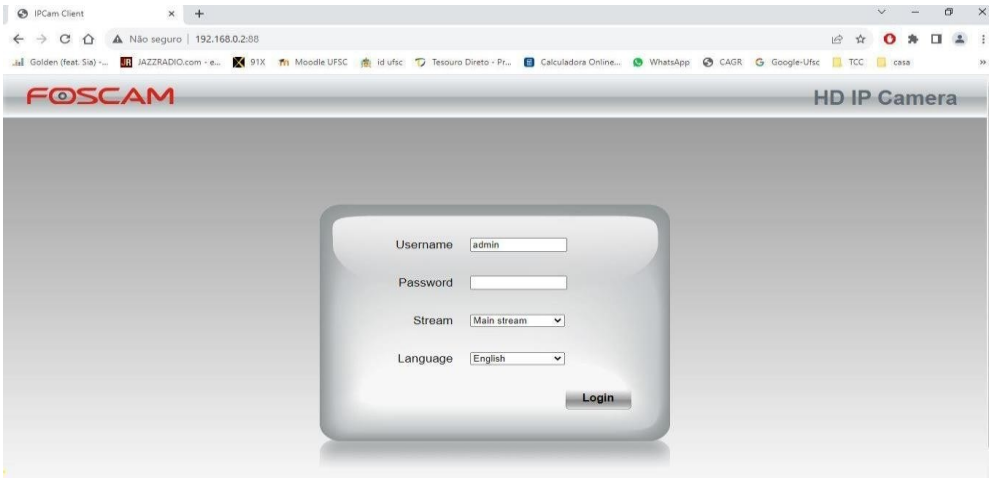
Figura 11 - Ferramenta auxiliar da câmera IP no manual do usuário.



Fonte: Acervo pessoal do Autor.

Efetuando um duplo clique no registro da câmera, na tela do Equipment Search Tool, é aberta a tela de login no navegador.

Figura 12 - Interface de login no navegador.



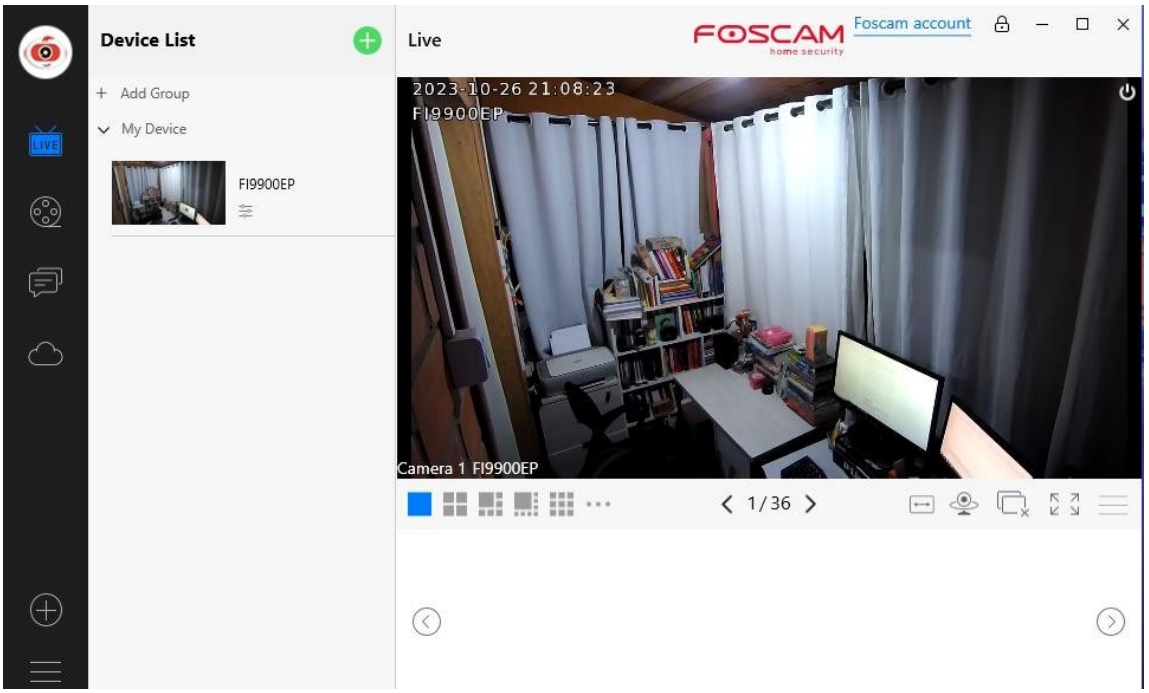
Fonte: Acervo pessoal do Autor.

Foram realizadas inúmeras tentativas de acesso pelo navegador, porém sem sucesso. Foi tentado acesso por navegadores diferentes, como Google Chrome, Mozilla Firefox e Microsoft

Edge, mas sem sucesso. Foi realizada a tentativa de resetar a câmera para os padrões de fábrica, mas da mesma forma não foi possível logar na interface web pelo navegador. Dessa forma, foi necessário realizar a instalação do software Foscam VMS, conforme informado na tela da aplicação “Equipment Search Tool”, para conseguir acesso à câmera.

De acordo com o portal da Foscam, Foscam VMS, sigla que significa Video Management System, é uma aplicação desktop que permite a visualização das câmeras em tempo real, a gravação de imagens e o gerenciamento de configurações como, endereço IP, parâmetro de imagem e acesso local ou remoto. Com suporte para adicionar múltiplas câmeras de forma mais segura e com mais opções que o navegador.

Figura 13 - Interface Foscam VMS.



Fonte: Acervo pessoal do Autor.

Dessa forma, ficou concluída a instalação da câmera local para a realização dos testes.

4.5 Execução dos Testes

A execução dos testes práticos seguirá o seguinte roteiro. Primeiro será realizada uma coleta de informações do dispositivo. Após, serão executados os testes de vulnerabilidade para avaliar se os casos relatados ainda persistem. E por fim, será realizada uma análise dos

resultados relatando a experiência obtida com cada dispositivo, que será utilizada para a conclusão do trabalho.

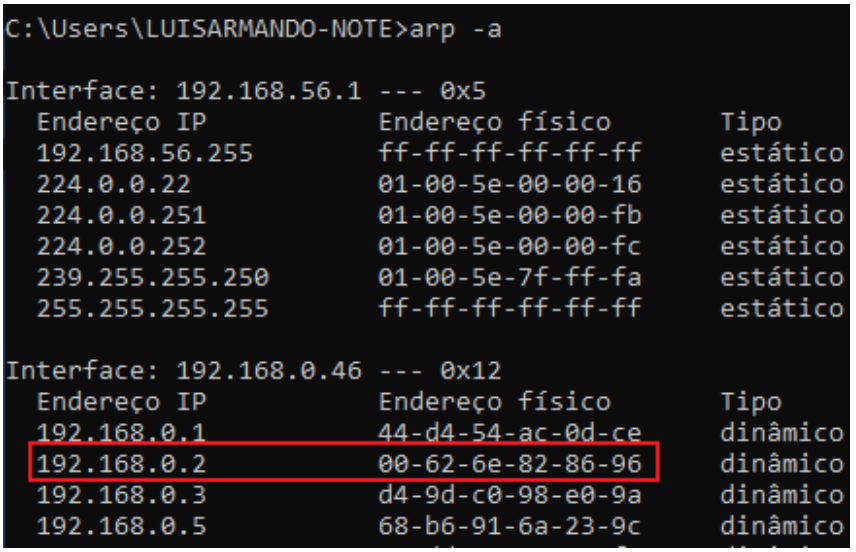
4.5.1 Dispositivo Local

Conforme informado na seção 4.1, o dispositivo local é uma câmera IP modelo FII9900EP, com conexão via cabo Ethernet. Com o dispositivo conectado iniciamos a execução dos testes.

4.5.1.1 Coleta de Informações

Iniciamos a coleta de informação identificando o protocolo IP do dispositivo a partir do MAC Address fornecido na etiqueta da câmera, conforme foi mostrado na Figura 9, seção 4.4.

Figura 14 - Endereço IP e físico do dispositivo na rede local.

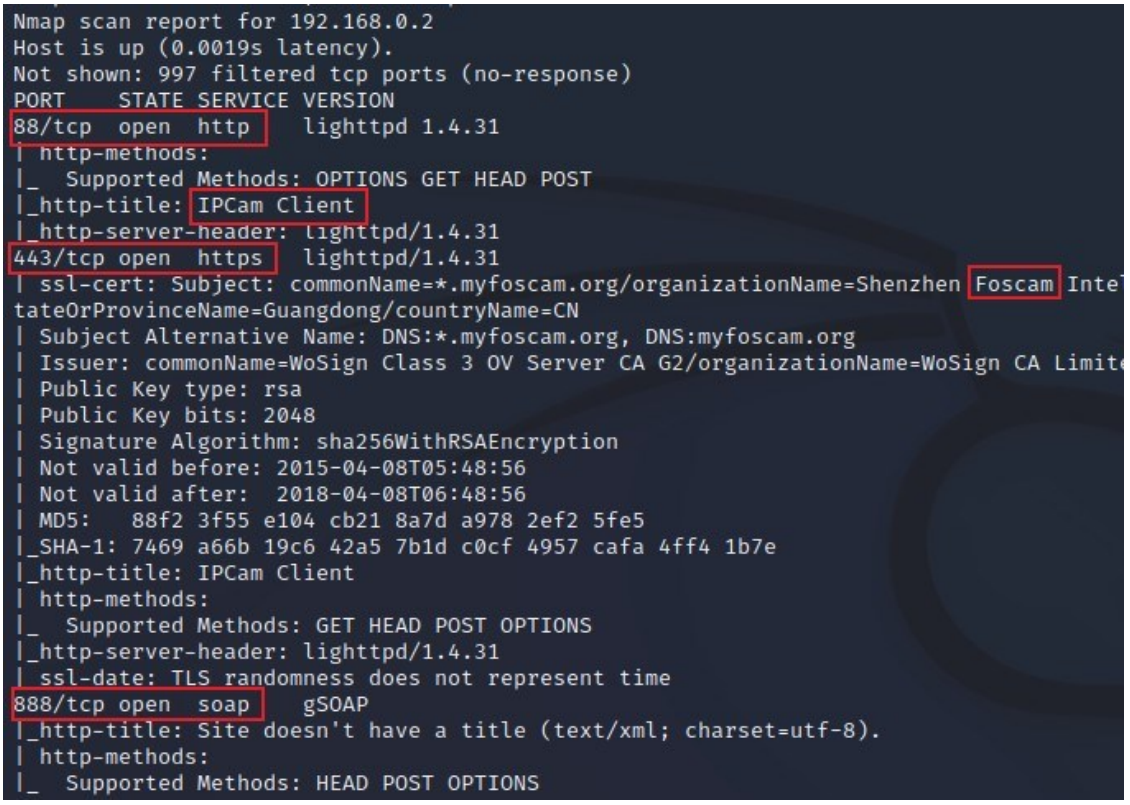


Fonte: Acervo pessoal do Autor.

Após, foi realizado o escaneamento com a ferramenta Nmap, utilizando o comando: # nmap -v -A -sV 192.168.0.2. O resultado apresenta informações como, portas abertas, o protocolo associado a elas, o tipo de serviço e os métodos suportados.

Foram encontradas 3 portas TCP abertas no dispositivo. A porta 88 utilizando o serviço HTTP, a porta 443 com o HTTPS e mostrando que utiliza criptografia com chave pública do tipo RSA de 2048 bits, e uma porta 888 que utiliza o serviço SOAP.

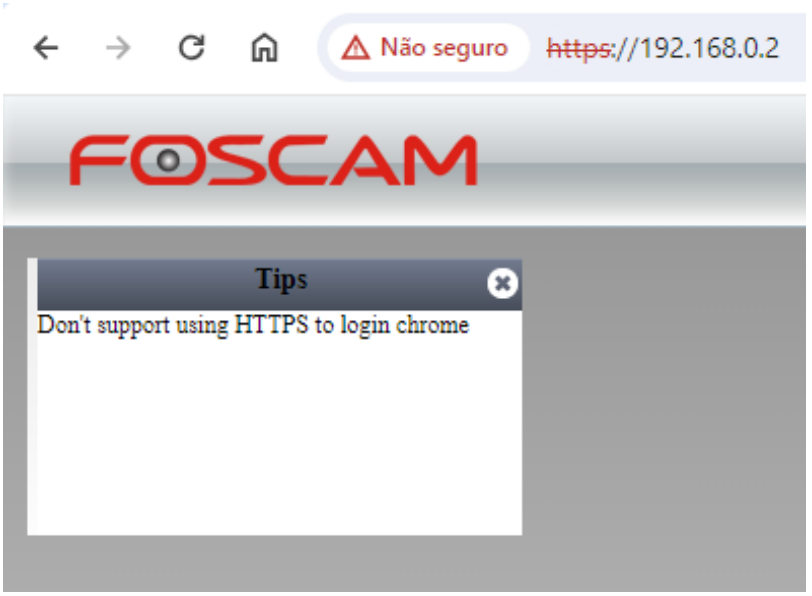
Figura 15 - Escaneamento de informações do dispositivo local na rede.



Fonte: Acervo pessoal do Autor.

Destas portas, tentando acesso pelo navegador, somente a 88 apresentou a tela de login. A porta 443 apresentou um aviso de site inseguro com certificado inválido. Conforme o resultado do Nmap, este certificado expirou em 08-04-2018. Ignorando a mensagem e avançando é apresentada uma mensagem que o dispositivo não suporta HTTPS para logar no Chrome. Mesmo tentando em outros navegadores a mesma mensagem é apresentada. A porta 888, segundo o manual de usuário, é utilizada pelo protocolo ONVIF que é um recurso de comunicação para gravação de vídeo em câmeras IP.

Figura 16 - Mensagem ao acessar a porta 443 pelo navegador.



Fonte: Acervo pessoal do Autor.

Em seguida, foi realizada uma varredura no host por vulnerabilidades utilizando a ferramenta Owasp ZAP, na porta 88, que foi a que apresentou acesso à interface web. Foram apresentados 3 alertas de vulnerabilidade de risco médio, conforme mostra a Figura 17.

Figura 17 - Alertas no relatório do Owasp ZAP.

Alerts

Name	Risk Level	Number of Instances
Content Security Policy (CSP) Header Not Set	Medium	9
Missing Anti-clickjacking Header	Medium	5
Vulnerable JS Library	Medium	1
Private IP Disclosure	Low	4
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	75
X-Content-Type-Options Header Missing	Low	71
Information Disclosure - Suspicious Comments	Informational	52
Modern Web Application	Informational	3
User Agent Fuzzer	Informational	72

Fonte: Acervo pessoal do Autor.

De acordo com a descrição apresentada no relatório, Content Security Policy (CSP), é uma camada adicional de segurança que ajuda a detectar e mitigar certos tipos de ataques, incluindo Cross Site Scripting (XSS) e ataques de injeção de dados. É um conjunto de padrão de cabeçalhos HTTP que permite definir quais fontes de conteúdo os navegadores podem carregar naquela página. Os tipos de conteúdo são javascript, frames HTML, css e imagens entre outros. Segundo o relatório, estas diretivas não estão definidas para a interface do dispositivo, aumentando a possibilidade de ameaça. O ataque de Cross Site Scripting já foi abordado na seção 4.3.4.

Missing anti-ClickJacking header, segundo o relatório, também se refere a falta de definição de diretivas no cabeçalho HTTP de resposta do servidor ao navegador, que previne ataques de ClickJacking.

Segundo a Kaspersky, “um ataque de clickjacking permite que um hacker insira uma camada invisível na interface do usuário, entre seus comandos e o que você vê na tela do dispositivo." Desta forma a vítima pode ser direcionada para um ambiente controlado pelo hacker ou os dados informados serem capturados.

A vulnerabilidade apontada como “Vulnerable JS library“ se refere a bibliotecas do framework Jquery desatualizadas. Não é fornecido muitos detalhes referente a falhas de segurança relacionadas, mas apresenta uma lista de identificadores CVE. Dentre eles, um dos mais atuais, CVE-2020-7656, se refere a uma função que não valida a inclusão de tags “<script>” permitindo ataques de Cross Site Scripting.

4.5.1.2 Testes de Vulnerabilidade

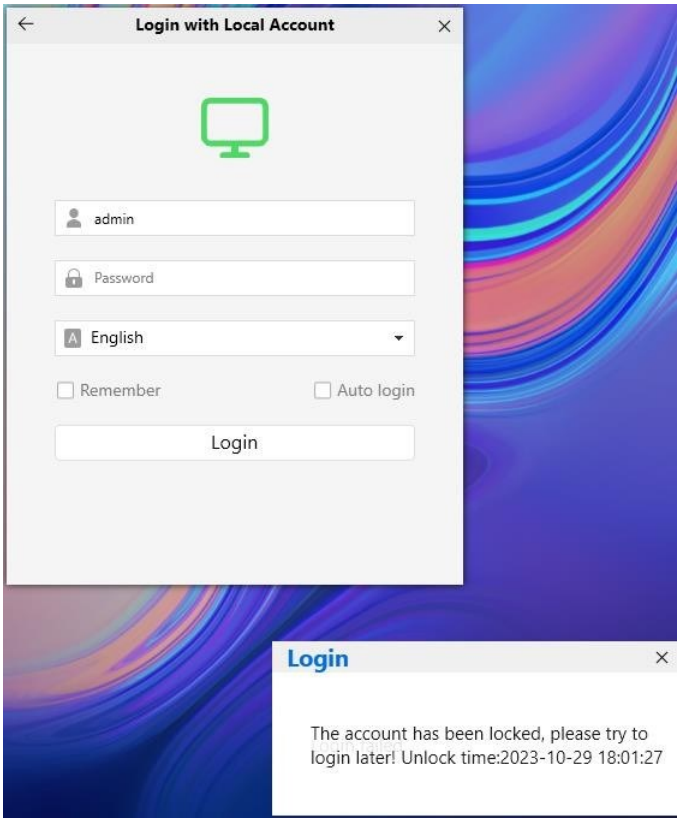
Após a coleta de algumas informações do dispositivo e realizar a varredura para verificar a existência de alerta de vulnerabilidades, realizamos a execução dos testes na câmera IP local, modelo FII9900EP, de acordo com a lista de ataques selecionados.

Em relação aos testes associados a autenticação na interface web, neste modelo não foi possível logar-se pelo navegador, conforme informado na seção 4.4 . O acesso só foi possível pelo app Foscam VMS, instalado no computador.

- **Enumeração de Usuário e Bloqueio de Conta**

Foi realizado o ataque de tentativas de login, e verificado que o sistema possui um mecanismo que bloqueia o login por 30 minutos após 10 tentativas, dificultando bastante este tipo de ataque, conforme apresentado na figura 18. Da mesma forma, com o sistema de bloqueio, fica dificultada a enumeração de usuários. Além disso, em função da interface não ser acessível pelo navegador, é um fator que dificulta a possibilidade de ataques deste tipo. Portanto a falha não foi identificada.

Figura 18 - Mecanismo de bloqueio de conta ao exceder o número de tentativas.



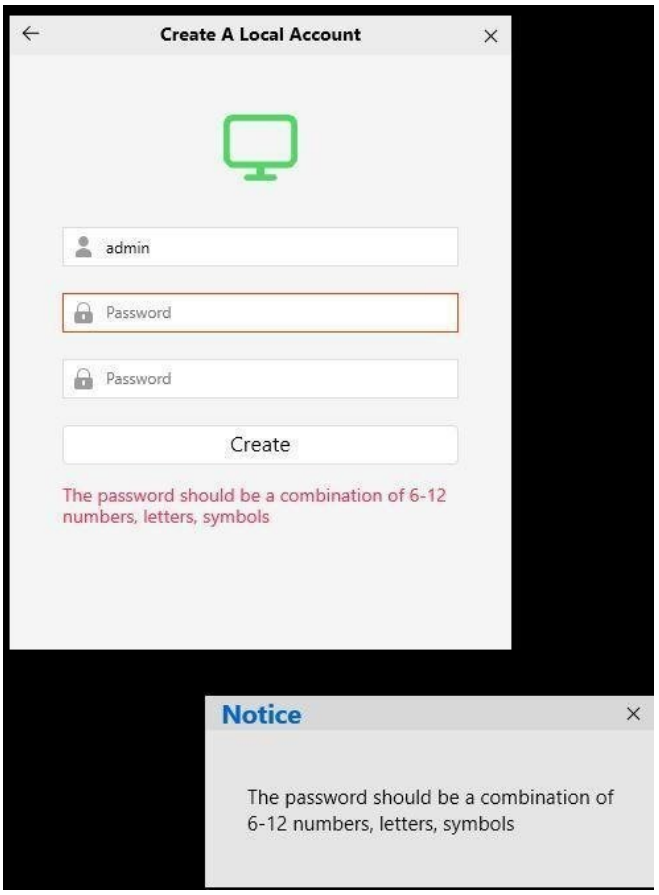
Fonte: Acervo pessoal do Autor.

- **Credenciais Padrão e Senhas Fracas**

A câmera possui credenciais padrão de fábrica definidas como usuário “admin” e senha em branco. Esta informação está no manual do usuário assim como na etiqueta na parte inferior da câmera. Porém, após instalar e acessar pela primeira vez, é apresentada uma tela para criar uma conta local. Tentando acessar com as credenciais padrão de fábrica, o sistema não permitiu,

informando que a senha deve ser uma combinação de 6 a 12 números, letras ou símbolos. Portanto, o problema de credenciais padrão para este modelo da câmera está solucionado.

Figura 19 - Validação para criação de credenciais no app Foscam VMS.



Fonte: Acervo pessoal do Autor.

Já em relação a senhas fracas, o sistema permitiu criar a conta de acesso à interface web com as credenciais usuário “admin” e senha “admin1”. Desta forma, observa-se que a vulnerabilidade continua existindo, uma vez que senhas desta natureza são de fácil adivinhação.

- **Path Directory Traversal e Authentication Bypass**

Para a travessia de diretório foi realizada a tentativa de ataque pelo navegador inserindo o comando: http://192.168.0.2:88//../proc/kcore o qual apresentou erro 404 - Not Found.

Figura 20 - Ataque de passagem de diretório via navegador.

Fonte: Acervo pessoal do Autor.

Mesmo que o acesso ao dispositivo não esteja sendo realizado pelo navegador, pela perspectiva do atacante pode servir como superfície de ataque, uma vez que existe a tela de login e o código é disponibilizado pelo servidor.

Foi realizado também o teste pelo terminal, mas também resultou sem sucesso.

Figura 21 - Ataque de passagem de diretório realizado pelo terminal.

Fonte: Acervo pessoal do Autor.

Para o ataque de Authentication Bypass foi realizado o teste inserindo os endereços no navegador porém sem obtenção de sucesso. Foram testados os comandos relatados em experiências anteriores, onde a falha foi detectada.

http://192.168.0.2:88/snapshot.jpg?

http://192.168.0.2:88/snapshot.cgi?user=&pwd=

http://192.168.0.2:88/get_status.cgi

http://192.168.0.2:88/vars.htm

Da mesma forma que o Path Directory Traversal apresentou o erro 404 - Not Found.

- **Envenenamento de DNS Dinâmico**

Este ataque foi realizado nas câmeras Foscam em função da disponibilização de um serviço de DNS pela própria empresa, onde o sistema de domínio segue uma nomenclatura padrão de fácil adivinhação. No modelo FI9900EP, que é o do dispositivo sendo testado, esse serviço não é disponibilizado, apresentando somente provedores de serviço de domínio de outras empresas como No-IP, DynDns e outras, como opção. Portanto esta falha, da forma como foi identificada, não ocorre mais.

Figura 22 - Interface de configuração DDNS no app FoscamVMS.

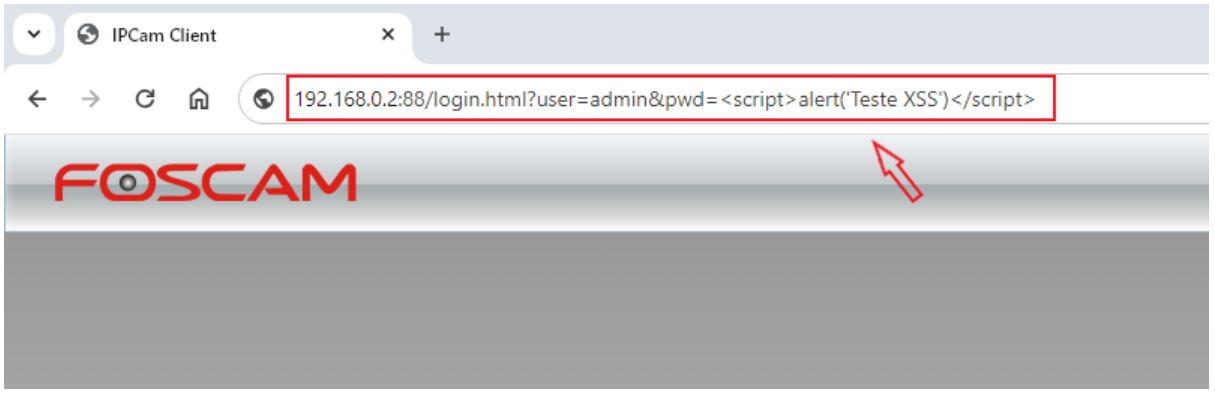
Fonte: Acervo pessoal do Autor.

- **Cross Site Scripting (XSS)**

Os ataques de Cross site Script são realizados com injeção de códigos javascript que é interpretado pelo navegador. Como o modelo não utiliza o navegador para acesso da interface e o ataque depende da interação do usuário com esta interface, é improvável que o mesmo ocorra. Além disso, segundo Bjørneset (2017), a vulnerabilidade foi identificada na interface de configuração de rede wireless, injetando scripts no campo SSID. Porém o modelo que está sendo testado é de conexão via cabo e não possui esta interface.

Mesmo assim, foi realizado um teste de XSS Refletido, no navegador ,interagindo com a tela de login. Foi testada a entrada da URL http://192.168.0.2:88/login.html?user=admin&pwd=<script>alert('Teste')</script>. Porém, ao enviar a requisição não houve sucesso na tentativa e a tela abriu normalmente. Foram feitas outras tentativas com algumas variações mas o resultado foi o mesmo.

Figura 23 - Simulação de ataque de Cross Site Script pela URL.



Fonte: Acervo pessoal do Autor.

4.5.2 Dispositivo Remoto

Após a experiência com o dispositivo local, procurou-se buscar dispositivos com as características dos modelos que apresentaram as falhas relatadas anteriormente.

Realizando a pesquisa pela plataforma Shodan, foi selecionado um dispositivo que atendeu a estes requisitos. Trata-se de uma câmera IP de modelo 8910W com o firmware de versão 11.37.2.48. De acordo com Bjørneset(2017), muitas das vulnerabilidades das câmeras Foscam foram identificadas no modelo 8910W com firmware anterior a versão 11.37.2.55.

4.5.2.1 Coleta de Informações

Ao acessar o detalhamento de um registro pesquisado no Shodan é possível obter as informações necessárias para avançar nos testes. As informações disponibilizadas são similares ao resultado do escaneamento realizado pela ferramenta Nmap, conforme mostra a figura 24.

Figura 24 - Resultado da pesquisa na plataforma Shodan.

Fonte: Acervo pessoal do Autor.

O dispositivo apresenta uma porta TCP aberta utilizando o serviço HTTP. Possui um servidor Netwave IP Camera, MAC address 000C5DDDBC51 e firmware versão 11.37.2.48.

Realizando a varredura do host com a ferramenta Owasp ZAP, foram apresentados 3 alertas de risco médio, conforme apresentado na figura 25.

A vulnerabilidade de Content Security Policy Header Not Set já foi apresentada na seção 4.4.1.1, assim como Missing Anti-clickjacking Header. Se tratam de informações que devem estar definidas no cabeçalho das páginas HTTP para prevenir contra ataques de Cross Site Script e Clickjacking.

Em relação a Weak Authentication Method, se refere ao mecanismo de autenticação utilizado, que transmite as credenciais pela rede de forma insegura. Pela seção detalhada do relatório, pode-se observar que a interface utiliza HTTP Basic e o envio dos dados da página é feito via método GET, conforme mostrado na figura 26.

Figura 25 - Resultado da pesquisa na plataforma Shodan.

Alerts

Name	Risk Level	Number of Instances
Content Security Policy (CSP) Header Not Set	Medium	28
Missing Anti-clickjacking Header	Medium	24
Weak Authentication Method	Medium	1
Timestamp Disclosure - Unix	Low	2
X-Content-Type-Options Header Missing	Low	27
Information Disclosure - Suspicious Comments	Informational	28
Modern Web Application	Informational	3

Fonte: Acervo pessoal do Autor.

Figura 26 - Detalhamento da vulnerabilidade do ZAP Scanning Report.

Medium	Weak Authentication Method
Description	HTTP basic or digest authentication has been used over an unsecured connection. The credentials can be read and then reused by someone with access to the network.
URL	http:/ /check_user.cgi
Method	GET
Attack	
Evidence	www-authenticate: Basic realm="ipcamera_000C5DDDBC51"
Other Info	
Instances	1
Solution	Protect the connection using HTTPS or use a stronger authentication mechanism

Fonte: Acervo pessoal do Autor.

4.5.2.2 Testes de Vulnerabilidade

A câmera modelo FII8910W, realiza o acesso a interface web pelo navegador, e portanto a maior parte dos testes são realizados por este ambiente.

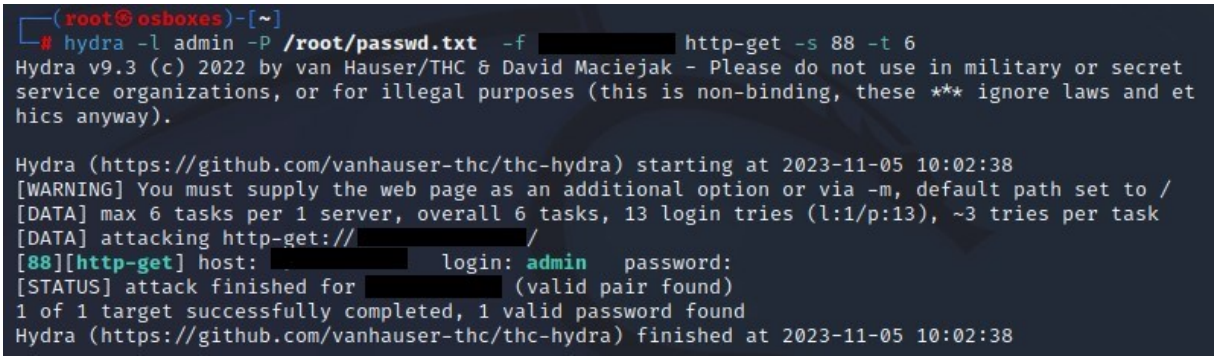
- **Enumeração de Usuário e Bloqueio de Conta**

Foram realizadas inúmeras tentativas de acesso com credenciais diferentes e não foi identificado mecanismo de bloqueio de conta no sistema. Por não limitar as tentativas de autenticação, considera-se que a vulnerabilidade é existente e o ataque possível de ser realizado.

Foi realizado um teste com a ferramenta Hydra, utilizando um pequeno arquivo contendo 13 senhas, com o objetivo de validar a possibilidade de ataque, pois já era conhecida a utilização de senha em branco. Para isso foi utilizado o seguinte comando # hydra -l admin -P /root/passwd.txt -q <IP_ADDRESS> http-get -s 1200 -t 6

Com este teste foi constatado que o dispositivo é passível de exploração para um ataque de dicionário.

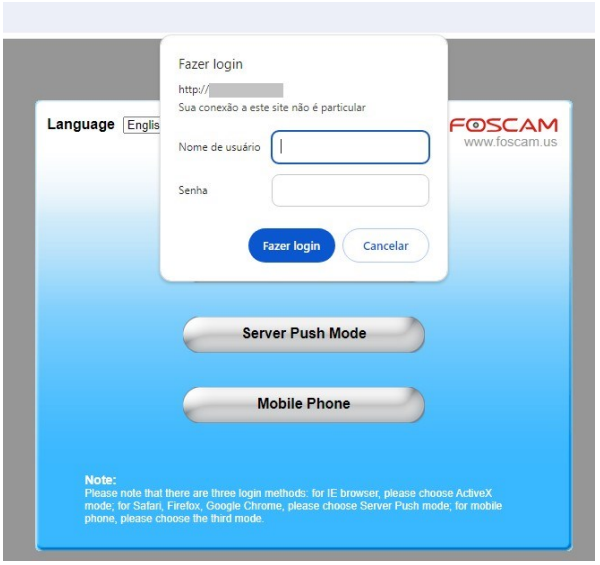
Figura 27 - Resultado da ferramenta Hydra (imagem meramente ilustrativa).



Fonte: Acervo pessoal do Autor.

Já referente a enumeração de usuário, o sistema não disponibiliza mecanismo de recuperação de senha ou mensagens informando que o usuário ou senha são inválidos. Desta forma, não ficou evidenciada a possibilidade de um ataque de enumeração.

Figura 28 - Tela de login da interface web.

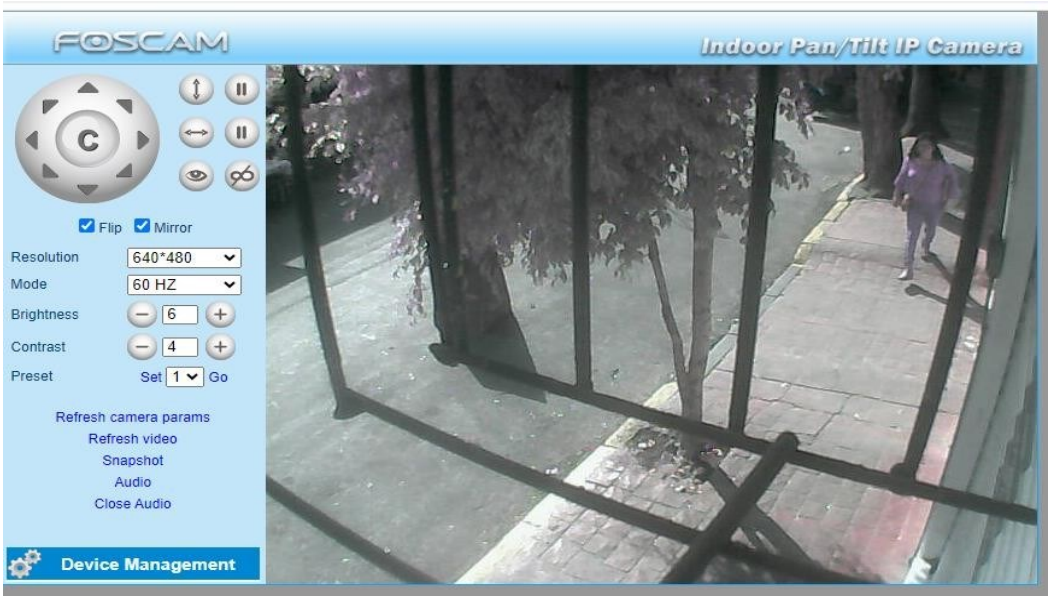


Fonte: Acervo pessoal do Autor.

- **Credenciais Padrão e Senhas Fracas**

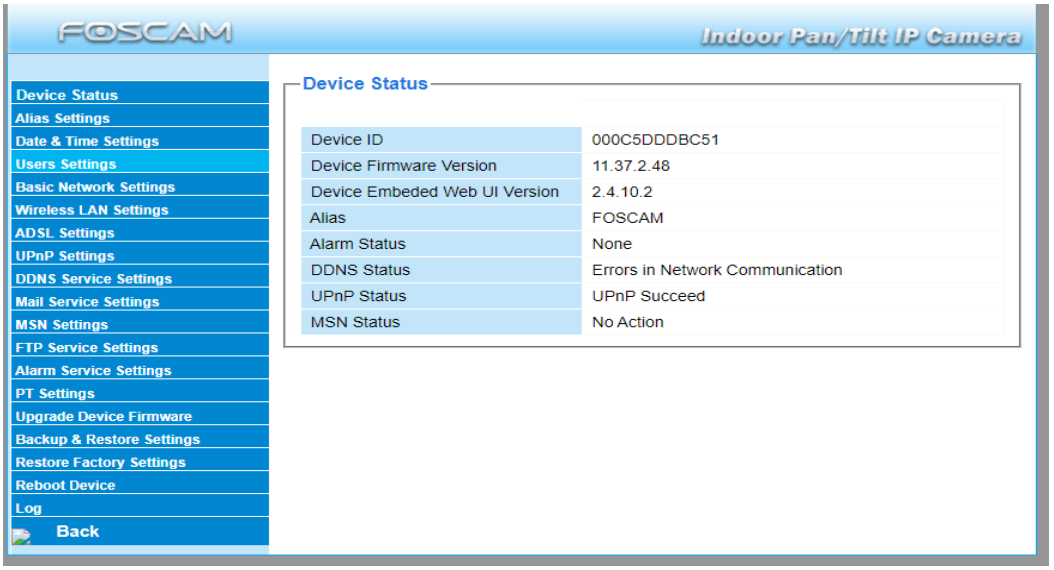
Ao utilizar as credenciais padrão para logar no sistema foi obtido acesso na primeira tentativa. Portanto, foi confirmada a existência da vulnerabilidade. Com acesso concedido, o atacante pode não somente acessar as imagens da câmera mas também as configurações e controle do dispositivo.

Figura 29 - Acesso às imagens da câmera.



Fonte: Acervo pessoal do Autor.

Figura 30 - Acesso às configurações da câmera.



Fonte: Acervo pessoal do Autor.

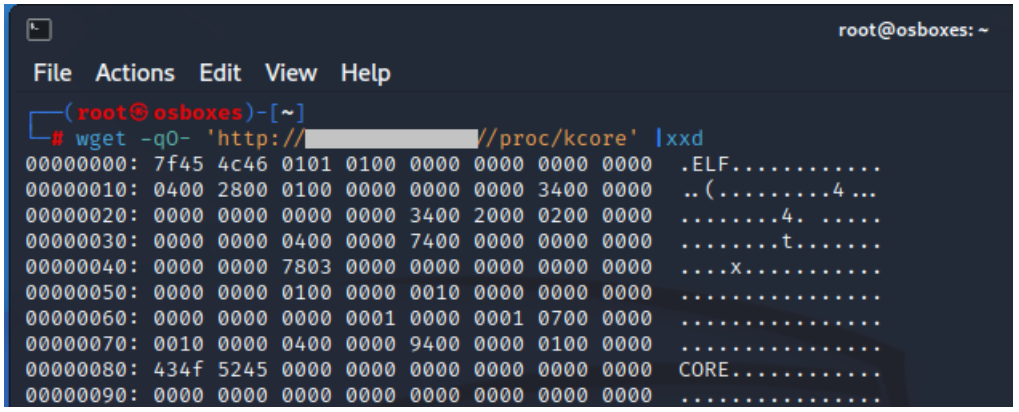
Segundo Dhanjani (2015), “Os dispositivos Foscam eram conhecidos por terem a combinação padrão de nome de usuário "admin" e senha em branco, que a maioria dos usuários provavelmente não alterava.” O texto descreve como uma consulta no Shodan revelou a quantidade de pessoas e organizações que não alteraram suas credenciais, colocando em risco a privacidade”. Desta forma, fica evidenciado que as duas falhas permanecem ativas neste dispositivo.

- **Path Directory Traversal e Authentication Bypass**

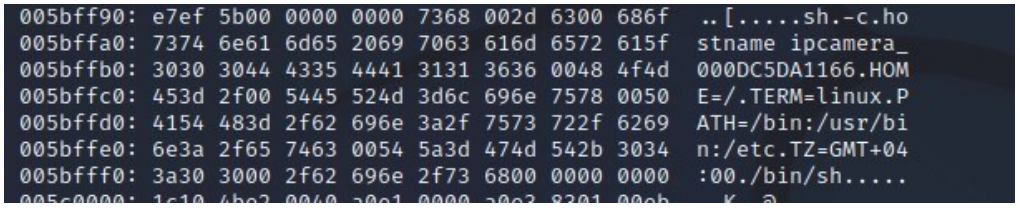
Foi realizado o teste pelo terminal utilizando o comando wget -qO- 'http://<IP_ADDRESS>//proc/kcore'|xxd. Segundo Dhanjani (2015), com este ataque foi possível obter a memória do dispositivo. O resultado é apresentado nas figuras 31a e 31b.

Figura 31 a,b - Ataque de Path directory traversal.

a)



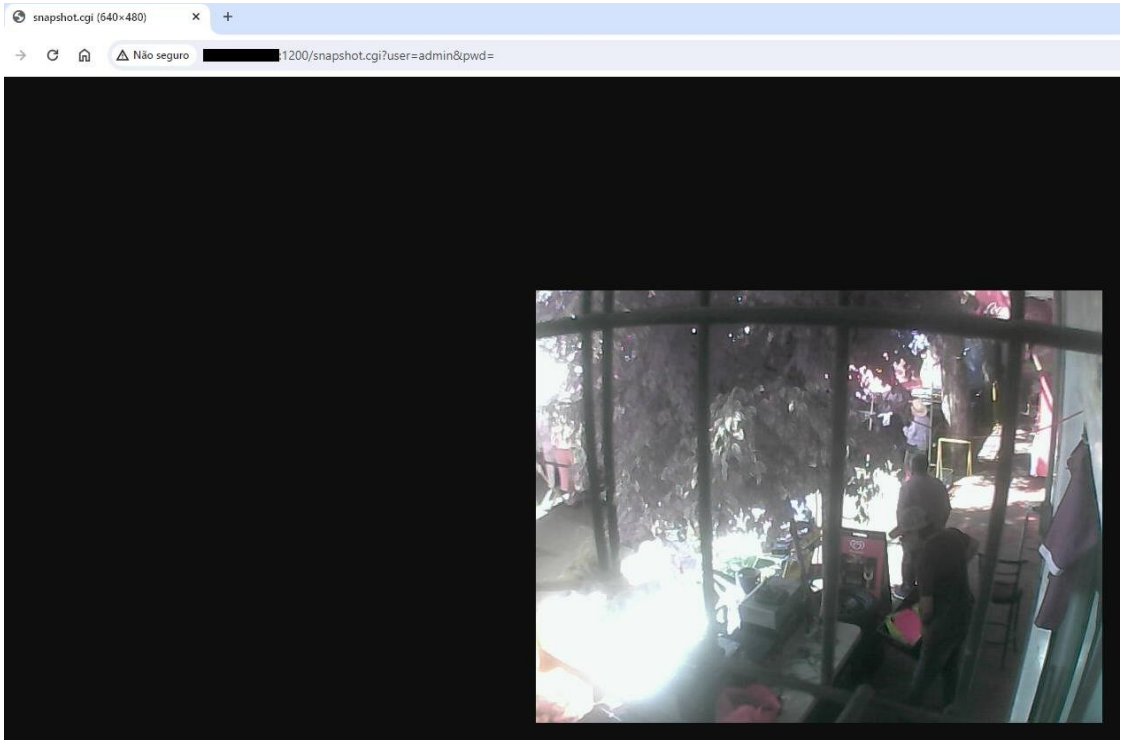
b)



Fonte: Arquivo pessoal do autor.

Em outro teste utilizando a URL http://<IP_ADDRESS>/snapshot.cgi?user=admin&pwd= foi possível obter um print da câmera, sem acessar a interface. O que evidencia uma vulnerabilidade ativa na interface, conforme apresentado na figura 32.

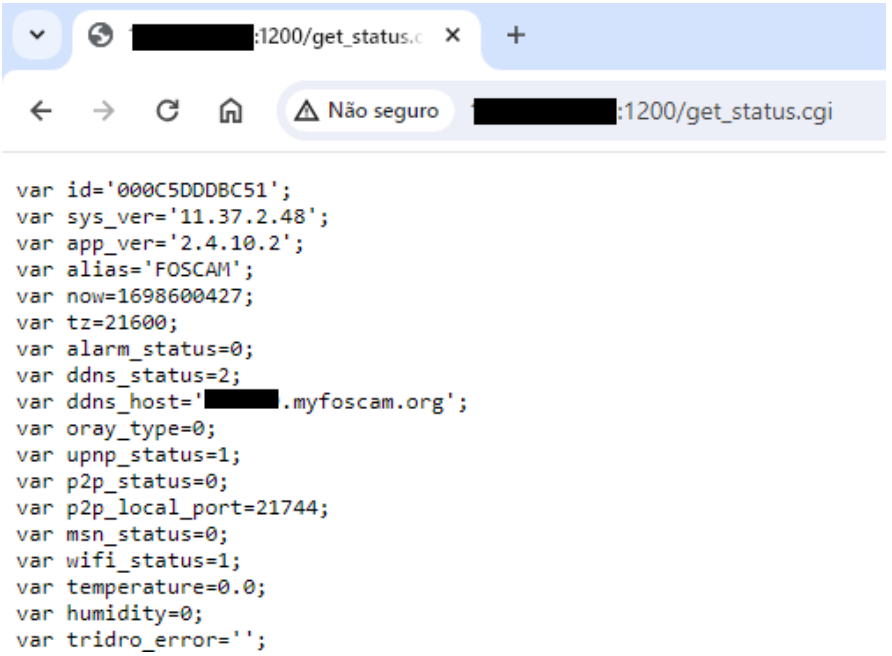
Figura 32 - Snapshot obtida a partir de modificação da URL.



Fonte: Arquivo pessoal do autor.

Outra ação que foi possível, foi adicionar o comando /get_status.cgi na URL, após o endereço do dispositivo. http:///<HOST>/get_status.cgi, que conforme relatado por Bjørneset (2017), nas câmeras Foscam são utilizados alguns comandos CGI, que se estudados pelo atacante, podem ser usados para realização de ataques. Com este comando foi possível acessar uma página sem autenticação com informações sensíveis do dispositivo, conforme mostra a figura 33.

Figura 33 - Acesso a página por modificação na URL.



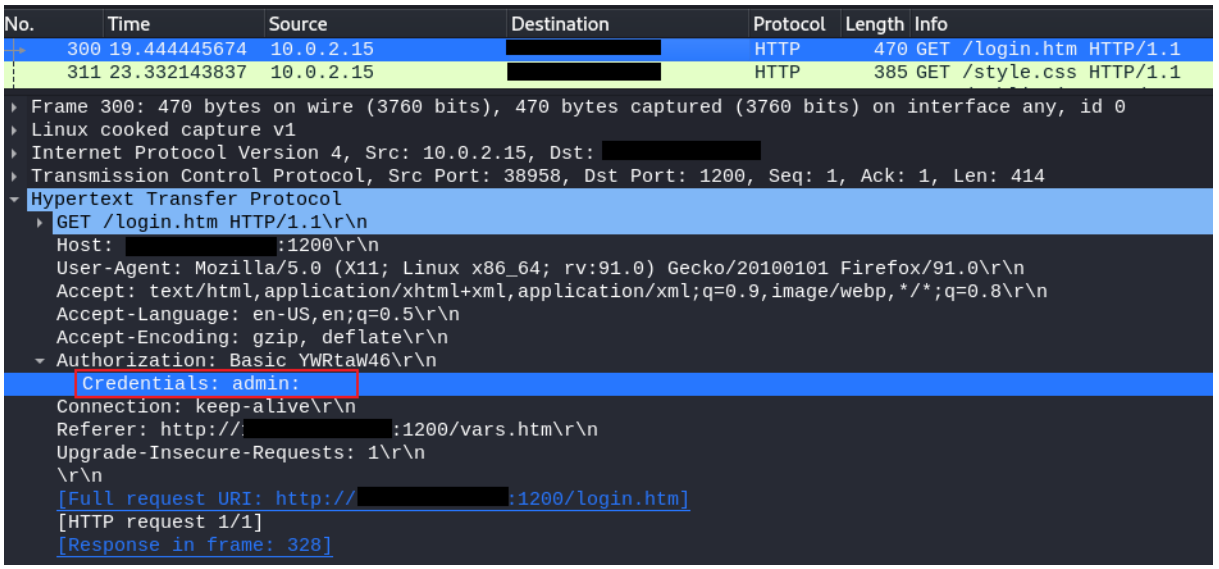
Fonte: Arquivo pessoal do autor.

- **Envenenamento de DNS Dinâmico e Eavesdropping**

Conforme mencionado na seção 4.3.3, este tipo de teste envolve ações que necessitam permissão e consentimento do usuário para realizar, como modificar o IP de associação do dispositivo no servidor DDNS e disponibilizar uma página falsa de login para o usuário acessar. Portanto, não será realizado. Este tipo de teste seria possível no dispositivo local, que na verdade foi adquirido com a finalidade de ter mais liberdade para realização de testes mais invasivos como este. Entretanto, o modelo encontrado não apresenta mais esta vulnerabilidade conforme relatado na seção 4.5.1.2.

Porém, uma das etapas do ataque consiste em monitorar a rede para obtenção das credenciais quando o usuário acessa a página disponibilizada pelo atacante. Este ataque, conhecido como Eavesdropping, foi realizado com sucesso utilizando a ferramenta Wireshark e realizando a interação com o mecanismo de login na interface web. O tráfego de rede foi capturado durante a realização do login, e depois analisado filtrando os pacotes com protocolo HTTP contento o IP do dispositivo como destino.

Figura 34 - Captura de pacote na rede contendo as credenciais do usuário expostas.



Fonte: Arquivo pessoal do autor.

Conforme mostra a figura 34, as credenciais estão expostas no pacote capturado, pois são transmitidas em texto plano ou base64, que pode ser convertido para texto facilmente . Esta vulnerabilidade foi detectada pela ferramenta Owasp ZAP na varredura do dispositivo, e apresentada com a descrição de Weak Authentication Method.

Pelo authentication bypass realizado foi possível acessar algumas configurações do dispositivo acessando a página get_status.cgi. Nela pode-se observar que o serviço de DDNS está ativo e o host configurado. Desta forma pode-se concluir que o ataque não está descartado.

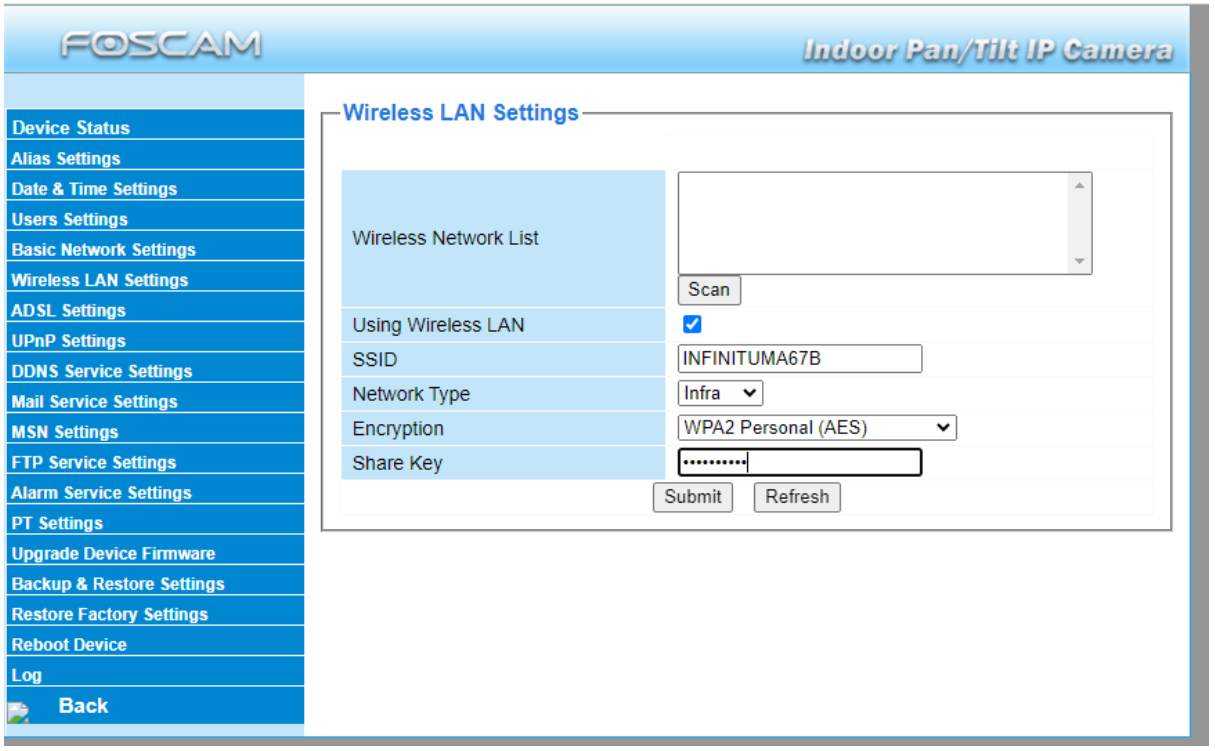
- **Cross Site Scripting (XSS)**

O caso relatado referente às câmeras Foscam se trata de XSS persistido, onde o código malicioso é injetado em um campo de formulário e gravado no banco de dados da aplicação. Quando a tela era acessada, o código era executado.

Para a realização deste teste, aplica-se o mesmo contexto do envenenamento de DNS. A injeção de script malicioso na aplicação do cliente, mesmo que para a finalidade de pesquisa, necessita de permissão e consentimento. E, portanto não será realizado.

Porém, no relatório gerado pela ferramenta Owasp ZAP foi detectada a vulnerabilidade de Content Security Policy Header Not Set, indicando a possibilidade de ataques de Cross Site Scripting pela ausência desta diretiva definida no cabeçalho HTTP. Portanto, será considerada como identificada a vulnerabilidade.

Figura 35 - Tela de configuração wireless na interface web do dispositivo.



Fonte: Arquivo pessoal do autor.

Segundo a CVE, o ataque foi realizado na tela de configuração de rede Wireless, onde foi injetado script no campo SSID pelo atacante, para ser executado ao acessar a tela pelo usuário.

4.6 Análise dos Testes

A análise de segurança foi feita a partir de testes de penetração realizados com dois dispositivos. Um deles, dentro da rede local e outro de forma remota.

A aprovação nos testes, não evidencia que um atacante experiente não consiga explorar as vulnerabilidades abordadas. Somente que nos testes, da forma como foi executado, obteve resultado positivo.

A forma de execução foi obtida a partir dos trabalhos correlatos referenciados, nas orientações de uso das ferramentas utilizadas e na pesquisa sobre as vulnerabilidades abordadas em órgãos como a OWASP e a CVE.

Com base nos resultados dos testes realizados, é possível identificar várias implicações em termos de segurança.

No modelo FI9900EP, dispositivo local que é um modelo mais recente, apresentou correções em falhas anteriormente exploradas, e teve um número menor de falhas identificadas, resultando em maior aprovação na maioria dos testes. Foi identificada a vulnerabilidade de senhas fracas, além de problemas de segurança na porta 88 incluindo vulnerabilidades de Content Security Policy não definido e Missing Anti-clickjacking header, conforme apresentado na tabela 2.

Apesar de ter sido implementado um recurso obrigando o usuário a cadastrar uma senha ao configurar o dispositivo, não foi exigida uma complexidade mínima para descaracterizar como vulnerabilidade de senhas fracas. Segundo a OWASP, esta é uma falha considerada de severidade Alta, pois pode causar impactos graves, resultando em perda ou corrupção de dados, negação de acesso e pode levar ao comprometimento total do dispositivo e/ou contas de usuário.

Tabela 2 - Vulnerabilidades testadas no modelo Foscam FI9900EP.

Dispositivo Local	Modelo	FI9900EP				
Ataque/ Vulnerabilidade	**Status**	**CVE**	**CWE**	**CVSS Score**	**Severidade**	**# OWASP IOT Top10**
Enumeração de Usuário	não identificado		CWE-287		Alta	A03
Bloqueio de conta	não identificado		CWE-307		Alta	A03
Credenciais padrão	não identificado		CWE-521		Alta	A01
Senhas fracas	identificado		CWE-521		Alta	A01
Path Directory Traversal	não identificado	CVE-2013-2560	CWE-35	7.8	Alta	
Authentication bypass	não identificado	CVE-2014-1911	CWE-287	7.8	Alta	
Envenenamento DDNS	não identificado	CVE-2014-1849	CWE-255	10.0	Crítico	
Cross Site Scripting	não identificado	CVE-2013-5215	CWE-79	4.3	Média	
Content Security Policy Não Definido	identificado		CWE-693		Média	

Anti-clickjacking	identificado		CWE-1021		Média	
header						
Autenticação Insegura	não identificado		CWE-326		Média	

Fonte: Elaborado pelo autor.

Já no modelo FI8910W, dispositivo acessado de forma remota e que possui registros de vulnerabilidades já exploradas, foi possível reproduzir a maioria dos ataques efetuados anteriormente, com exceção de Enumeração de Usuário, conforme apresentado na tabela 3.

Tabela 3 - Vulnerabilidades testadas no modelo Foscam FI8910W.

Dispositivo remoto	Modelo	FI8910W				
Ataque/ Vulnerabilidade	**Status**	**CVE**	**CWE**	**CVSS Score**	**Severidade**	**# OWASP IOT Top10**
Enumeração de Usuário	não identificado		CWE-287		Alta	A03
Bloqueio de conta	identificado		CWE-307		Alta	A03
Credenciais padrão	identificado		CWE-521		Alta	A01
Senhas fracas	identificado		CWE-521		Alta	A01
Path Directory Traversal	identificado	CVE-2013-2560	CWE-35	7.8	Alta	
Authentication bypass	identificado	CVE-2014-1911	CWE-287	7.8	Alta	
Envenenamento DDNS	não descartado	CVE-2014-1849	CWE-255	10.0	Crítico	
Cross Site Scripting	identificado	CVE-2013-5215	CWE-79	4.3	Média	
Content Security Policy Não Definido	identificado		CWE-693		Média	
Anti-clickjacking header	identificado		CWE-1021		Média	
Autenticação Insegura	identificado		CWE-326		Média	

Fonte: Elaborado pelo autor.

Em relação às informações apresentadas na tabela, pode-se verificar que o dispositivo possui cinco vulnerabilidades de severidade Alta e uma Crítica, passíveis de serem exploradas. Além de outras quatro de severidade Média. E das falhas exploradas anteriormente, todas permanecem ativas.

Foi possível acessar o dispositivo com as credenciais padrão, e ter acesso às imagens e às configurações da câmera. Desta forma o atacante passa a ter controle total do dispositivo.

No caso da vulnerabilidade Envenenamento de DDNS, de acordo com a CVE, "A câmera IP Foscam 11.37.2.49 e outras versões, ao usar a opção Foscam DynDNS, gera credenciais com base em nomes de subdomínios de câmeras previsíveis, o que permite que invasores remotos falsifiquem ou sequestrem câmeras arbitrárias e conduzam outros ataques modificando registros de câmeras arbitrárias no servidor DNS Foscam".

Considerado de severidade crítica, este problema pode ocasionar o sequestro de inúmeros dispositivos para a criação de botnets.

Mesmo não tendo sido possível executar o ataque, pois necessitaria de consentimento do proprietário do dispositivo, foi considerado como não descartado pois todas as características e configurações necessárias foram identificadas para a sua realização.

O ataque de Path Directory Traversal que foi identificado e considerado de severidade Alta, possibilitou o acesso à memória do dispositivo. Este tipo de ataque pode possibilitar a injeção de arquivos maliciosos, como é o caso de LFI, sigla para Local File Inclusion, ou Inclusão de Arquivo Local em tradução livre.

Segundo Chauan (2023), " LFI é um tipo de vulnerabilidade de aplicativo da web que permite que um invasor acesse e execute arquivos em um servidor web, que podem conter código malicioso." Este tipo de vulnerabilidade pode levar a um RCE, Remote Code Execution, que é a execução de código de forma remota. Ainda de acordo com Chauan (2023) "os ataques LFI a RCE são um sério problema de segurança que pode permitir que invasores assumam o controle total de um servidor web."

Com base nos dados apresentados pode-se fazer algumas considerações em relação às falhas de segurança encontradas nos dispositivos:

- **Credenciais Padrão e Senhas Fracas** (Dispositivo Local e Remoto): A presença de credenciais padrão ou senhas fracas em dispositivos são vulnerabilidades de severidade Alta. Isso pode permitir que invasores acessem e controlem os dispositivos, comprometendo a privacidade e a segurança dos usuários, além da possibilidade de execução de outros ataques. É essencial que

os fabricantes implementem medidas fortes de autenticação como credenciais com maior complexidade, e incentivem os usuários a alterar as senhas padrão.

- **Content Security Policy (CSP) Não Definido** (Dispositivo Local e Remoto): A falta de definição de CSP em dispositivos pode aumentar o risco de ataques de Cross Site Scripting (XSS) e injeções de dados. É vital que os fabricantes configurem políticas de CSP para restringir quais fontes de conteúdo podem ser carregadas em suas interfaces da web, aumentando a segurança.
- **Métodos de Autenticação Inseguros e Exposição de Credenciais de Usuário** (Dispositivo Remoto): O uso de métodos de autenticação inseguros, como o envio de credenciais via HTTP Basic, pode expor informações de autenticação a terceiros. O fato de que as credenciais do usuário são transmitidas em texto simples ou codificadas em Base64 em tráfego de rede revela uma vulnerabilidade crítica. Os desenvolvedores devem adotar métodos de autenticação seguros, como HTTPS, para proteger a transmissão de informações de autenticação e garantir que as informações de autenticação sejam protegidas usando criptografia forte e métodos de transmissão seguros
- **Path Directory Traversal e Authentication Bypass** (Dispositivo Remoto): A detecção dessas vulnerabilidades indica que os dispositivos podem ser vulneráveis a ataques de manipulação de URL e comprometimento da integridade dos sistemas. Os fabricantes devem implementar controles de segurança adequados para evitar essas ameaças, como validação de entrada e restrições de acesso.

Por fim, pode-se concluir que em modelos mais recentes foram realizadas correções procurando solucionar as falhas de segurança encontradas anteriormente. Por outro lado, os modelos mais antigos, que continham estas falhas e não foram atualizados, continuam sendo potenciais alvos de ataque e passíveis de exploração.

4.7 Recomendações de Segurança

- **Atualização de Firmware e Senhas**: Os fabricantes devem liberar atualizações de firmware para corrigir as vulnerabilidades identificadas, incluindo a eliminação de credenciais padrão. Os usuários devem ser incentivados a aplicar essas atualizações e a alterar as senhas padrão para senhas fortes e únicas.

- **Configuração Adequada de Content Security Policy**: Os fabricantes devem configurar de forma adequada a Content Security Policy para restringir as fontes de conteúdo permitidas e evitar ataques de XSS. Isso é especialmente importante em dispositivos que têm interfaces web.
- **Implementação de Métodos de Autenticação Seguros**: A implementação de métodos de autenticação seguros, como HTTPS, é crucial para proteger as informações de autenticação durante a transmissão dos dados. Além disso, métodos de autenticação robustos devem ser utilizados para reduzir o risco de ataques.
- **Validação de Entrada e Restrição de Acesso**: Os fabricantes devem implementar validação de entrada e restrição de acesso adequadas para evitar ataques de Path Directory Traversal e Authentication Bypass. Isso inclui filtrar e validar todos os inputs do usuário.
- **Criptografia dos Dados**: A utilização de criptografia forte dos dados é fundamental para proteger informações sensíveis. Os fabricantes devem garantir que as comunicações entre os dispositivos e os clientes sejam seguras e criptografadas. Importante atentar-se para a não utilização de algoritmos ultrapassados
- **Educação do Usuário**: Os fabricantes devem educar os usuários sobre a importância da segurança, incluindo a necessidade de alterar senhas padrão, manter dispositivos atualizados e estar cientes das práticas de segurança recomendadas.

5 CONCLUSÃO

Neste trabalho são apresentados os principais conceitos de segurança em IoT, dando ênfase à Interface Web dos dispositivos, que historicamente vem sendo um dos vetores de ataque mais explorados.

Além disso, foi realizada uma análise de segurança dos dispositivos IoT, a partir da realização de testes de penetração com duas câmeras IP.

O objetivo da análise foi avaliar se as principais vulnerabilidades listadas na OWASP Top 10, relacionadas a interface web, podem ser reproduzidas, assim como as vulnerabilidades identificadas anteriormente nestes dispositivos. O que se confirmou em ambos os casos.

A partir disso, foram propostas recomendações de segurança como, atualização de firmware e senhas, e implementação de métodos de autenticação seguros.

As câmeras IP foram o exemplar escolhido dentre centenas de dispositivos IoT para fazer esta avaliação. Porém, outras categorias de dispositivos inteligentes também são portadores de falhas de segurança e alvo frequente de ataques.

Das vulnerabilidades identificadas, pode-se destacar a de credenciais padrão e senhas fracas que figuram em primeiro lugar na lista da Owasp IoT Top 10 como , Weak Guessable, or Hardcoded Passwords. Apesar do trabalho frequente da indústria de software buscando solucionar este problema, continua sendo fonte recorrente de vulnerabilidade em dispositivos IoT. Problemas de firmware podem estar associados, ao não implementar uma rotina que force o usuário a alterar as credenciais padrão ou a criação de credenciais com complexidade suficiente para não ser adivinhada.

Outras vulnerabilidades importantes identificadas foram Path Directory Traversal e Authentication Bypass, ambas relacionadas a permitir acesso não autorizado a recursos do sistema adicionando caminhos de diretórios no final da URL. A exploração destas falhas possibilitou ao atacante acessar a memória do dispositivo e arquivos com informações sensíveis.

Evidenciou-se também a existência de métodos de autenticação inseguros, com as credenciais sendo enviadas em texto plano pela rede. Desta forma, mesmo solucionando o problema de senhas fracas a segurança na parte de autenticação estaria comprometida.

Por fim, ficou evidenciado que os dispositivos mais antigos, que não tiveram atualização de firmware continuam sendo passíveis de exploração e contribuindo para um ambiente IoT inseguro. Nas recomendações de segurança é mencionada a importância da ação de fabricantes e usuários para mitigar este problema.

Do lado dos desenvolvedores e fabricantes, também é necessário maior preocupação com a segurança, procurando melhor equalizar este aspecto com as questões funcionais e comerciais.

Ademais, foi verificado que algumas das formas de ataque utilizadas são de certo modo simples e que não necessitam muito conhecimento técnico para executá-las, o que as torna ainda mais críticas em função da facilidade de disseminação. Ao mesmo tempo, o conhecimento e as ferramentas estão cada vez mais acessíveis, favorecendo a ação dos atacantes.

Em resumo, a identificação e a correção das vulnerabilidades destacadas nos dispositivos são cruciais para garantir a segurança dos usuários e a integridade dos sistemas. Fabricantes, pesquisadores e usuários desempenham papéis importantes na mitigação dessas ameaças, garantindo que os dispositivos estejam atualizados, configurados corretamente e protegidos contra possíveis ataques. A segurança deve ser uma consideração central no desenvolvimento e uso de dispositivos IoT. E espera-se que os resultados deste trabalho contribuam para a evolução da Internet das Coisas nesta direção.

6 TRABALHOS FUTUROS

Um futuro trabalho poderia utilizar outros métodos de teste de penetração, como o PTES, sigla para Penetration Testing Execution Standard, e o Mitre Attack Framework, como alternativa e complementar ao que foi utilizado, para a realização de testes com as câmeras ou com outros dispositivos. No caso das câmeras, poderia realizar um comparativo de resultados ampliando as análises já realizadas.

O PTES é um método abrangente de teste de penetração que apresenta uma metodologia padronizada em sete seções principais, em que cada seção aborda uma etapa específica do processo, desde a preparação até a documentação dos resultados.

Enquanto o Mitre Attack Framework é uma base de conhecimento acessível globalmente de táticas e técnicas adversárias baseadas em observações do mundo real. Onde a sua base de conhecimento é utilizada como base para o desenvolvimento de modelos e metodologias de ameaças específicas de diversos setores na segurança cibernética (MITRE.org).

Um outro trabalho futuro poderia avançar na exploração de firmwares das câmeras utilizando a ferramenta Binwalk, e analisar a segurança deste recurso, uma vez que estes dispositivos disponibilizam a atualização de forma manual. De acordo com a Kali.org, o “Binwalk é uma ferramenta para pesquisar uma determinada imagem binária em busca de arquivos incorporados e código executável. Especificamente, ele foi projetado para identificar arquivos e códigos incorporados em imagens de firmware”.

REFERÊNCIAS

ABDALLA, P. A.; VAROL, C. Testing IoT Security: The Case Study of an IP Camera. *In*: INTERNATIONAL SYMPOSIUM ON DIGITAL FORENSICS AND SECURITY (ISDFS), 8., 2020, Beirut, Lebanon. **Proceedings** […] Beirut, Lebanon: IEEE, 2020. p. 1-5. DOI: 10.1109/ISDFS49300.2020.9116392. Disponível em: https://ieeexplore.ieee.org/document/9116392 Acesso em: 20 ago. 2023.

ALCHIERI, E. A.; BARRETO, P. S; CAETANO, M. F.; GONDIM, J. J.; LEITE, C. Pentest on Internet of Things Devices. *In*: LATIN AMERICAN COMPUTING CONFERENCE (CLEI), 45., 2019, Panama City. **Proceedings** […] Panama City: IEEE, 2019. p. 1-10. Disponível em: http://clei2019.utp.ac.pa/storage/app/uploads/public/5d8/cff/bd1/5d8cffbd16f09903219768.pdf. Acesso em: 21 jul. 2022.

ALMEIDA Jr., J. A. **Pentest em Aplicações Web**. São Paulo: Casa do Código, 2021. 267 p.

ANTONAKAKIS, M. *et al*. Understanding the mirai botnet. *In*: SECURITY SYMPOSIUM SECURITY, 26., 2017, Vancouver. **Proceedings** […] Vancouver: USENIX, 2017. p. 1093-1117.

BARROS, E. **Estudo de vulnerabilidades em dispositivos IOT TCP/IP**. 2021. Monografia (Graduação) – Universidade Federal do Rio Grande do Sul, 2021. Disponível em: https://lume.ufrgs.br/handle/10183/222479# Acesso em: 20 ago. 2023.

BJORNESET, K. J. **Testing Security for Internet of Things** - A Survey on Vulnerabilities in IP Cameras. 2017. 132 f. Master's Thesis (Mestrado) - University of Oslo, 2017. Disponível em: https://www.mn.uio.no/ifi/english/research/groups/psy/completedmasters/2017/Kim_Jonatan_Wessel_Bjorneset/kim_jonatan_wessel_bjorneset_testing_security_for_internet_of_things_a_survey_on_vulnerabilities_in_ip_cameras.pdf Acesso em: 23 ago. 2023.

BRINHOSA, R. **IoPenT**: Framework para Penetration Testing de dispositivos IoT. 2019. Projeto de Qualificação (Doutorado) - Programa de Pós-graduação em Ciência da Computação, Universidade Federal de Santa Catarina, Florianópolis, 2019.

BURSZTEIN, E. Inside the infamous Mirai IoT Botnet: A Retrospective Analysis. **CLOUDFLARE Blog**, [*s.l.*], 14 dez. 2017. Disponível em: https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/ Acesso em: 25 jul. 2022.

CHAUAN, Aditya. Inclusão de arquivo local (LFI) para RCE. Disponível em: https://aditya-chauhan17.medium.com/local-file-inclusion-lfi-to-rce-7594e15870e1
Acesso em: 03 dez. 2023.

CVE. Disponível em: https://www.cve.org/ResourcesSupport/Glossary#. Acesso em: 21 jul. 2022.

CVE Details. Disponível em: https://www.cvedetails.com/cve/CVE-2014-1849/ Acesso em: 03 dez. 2023.

DHANJANI, N. **Abusing the Internet of Things**: Blackouts, Freakouts,and Stakeouts. Califórnia: O'Reilly Media Company, 2015. 274 p.

DING, A. *et al*. Ethical Hacking for Boosting IoT Vulnerability Management: A First Look into Bug Bounty Programs and Responsible Disclosure. *In*: ICTRS '19: EIGHTH INTERNATIONAL CONFERENCE ON TELECOMMUNICATIONS AND REMOTE SENSING, 19., 2019, Rhodes, Greece. **Proceedings** […]. Rhodes, Greece: ICTRS, 2019 p. 49-55. DOI: https://doi.org/10.1145/3357767.3357774

EXPLOITING Foscam IP Cameras. Disponível em: https://docplayer.net/11352485-Exploiting-foscam-ip-cameras-contact-rampartssecurity-com.html . Acesso em: 18 out. 2023.

GARTNER. **Gartner Glossary**. [*S.l.*: s.n.], 2021. Disponível em: https://www.gartner.com/en/information-technology/glossary/internet-of-things. Acesso em: 21 jul. 2022.

GROBELNA, I.; GROBELNY, M.; BAZYDŁO, G. User awareness in IoT security. A survey of Polish users. *In*: AIP PUBLISHING LLC, 1., 2018. **AIP Conference Proceedings**. [*S.l.*]: AIP Publishing, 2018. v. 2040, p. 080002.

GUPTA, A.; GUZMAN, A. **IoT Penetration Testing Cookbok**: identify vulnerabilities and secure your smart devices. Birmingham: Packt, 2017. 361 p. Disponível em: https://books.google.com.br/books?id=rEFPDwAAQBAJ. Acesso em: 30 abr. 2021.

GUPTA, A. **The IoT Hacker's Handbook**: a pratical guide to hacking the internet of things. Walnut: Apress, 2019. 320 p. Disponível em: https://dx.doi.org/10.1007/978-1-4842-4300-8. Acesso em: 22 jul. 2022.

JOHARI, R.; KAUR, I.; TRIPATHI, R.; GUPTA, K. Penetration Testing in IoT Network. *In*: 2020 5Th INTERNATIONAL CONFERENCE ON COMPUTING, COMMUNICATION AND SECURITY (ICCCS), 5., 2020, Patna, India. **Proceedings** [...]. Patna, India: IEEE, 2020. v1, n. 1, p. 1-8. DOI: http://dx.doi.org/10.1109/icccs49678.2020.9276853.

KAMIENSKI, C. *et al*. Computação Urbana: Tecnologias e Aplicações para Cidades Inteligentes. *In*: SIQUEIRA, F. *et al*. **Minicursos do SBRC 2016**. Salvador: Sociedade Brasileira de Computação (SBC), 2016. p. 12-14.

KOVACS, E. Backdoor Found in Many Sony Security Cameras. **Wired Business Media**, [*s.l.*], 2016. Disponível em: https://www.securityweek.com/backdoor-found-many-sony-security-cameras. Acesso em: 20 set. 2023.

KREBS, B. **Krebs on Security**. Disponível em:http://krebsonsecurity.com/2014/01/bug-exposes-ip-cameras-baby-monitors/ Acesso em: 18 out. 2023.

OWASP IOT - OWASP Internet of Things Project - OWASP. [s.d.]. Disponível em: https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project. Acesso em: 20 jul. 2022.

OWASP Teste para alteração de senha fraca ou funcionalidades de redefinição. Disponível em: https://wiki.owasp.org/index.php/Testing_for_weak_password_change_or_reset_functionalities_(OTG-AUTHN-009). Acesso em: 25 jul. 2022.

OWASP Teste para CSRF. Disponível em: https://wiki.owasp.org/index.php/Testing_for_ CSRF_(OTG-SESS-005). Acesso em: 25 jul. 2022.

OWASP WSTG - Web Security Testing Guide v. 4. Disponível em: https://owasp.org/www-project-web-security-testing-guide/assets/archive/OWASPTestingGuidev4.pdf. Acesso em: 25 jul. 2022.

PANARELLO, A. *et al*. Blockchain and iot integration: A systematic survey. **Sensors, Multidisciplinary Digital Publishing Institute**, [*s.l.*], v. 18, n. 8, p. 2575, 2018. DOI: https://doi.org/10.3390/s18082575

SANTOS, P. **Internet das Coisas:** o desafio da privacidade. Setúbal: Instituto Politécnico de Setúbal, 2016. p. 8-14.

SANCHEZ, L. *et al*. Smartsantander: Iot experimentation over a smart city testbed. **Computer Networks**, [*s.l.*], v. 61, p. 217-238, 2014.

SHEKYAN, S.; HARUTYUNYAN, A. **Turning your surveillance camera against you**. Qualys, Inc, 2013. Disponível em: https://www.slideshare.net/SergeyShekyan/d2-t1-sergey-shekyan-and-artem-harutyunyan-turning-your-surveillance-camera-against-you Acesso em: 20 jul. 2023.

SHODAN. [s.d.]. Disponível em: https://www.shodan.io/. Acesso em: 21 jul. 2022.

SIKDER, A. *et al*. A Survey on Sensor-based Threats to Internet-of-Things (IoT) Devices and Applications. **arXiv**:1802.02041, 2018. DOI: https://doi.org/10.48550/arXiv.1802.02041

STALLINGS, W. **Criptografia e segurança de redes**: Princípios e práticas. 6. ed. São Paulo: Pearson Education do Brasil, 2015. 558 p.

SYED, R. *et al*. Threat model for securing internet of things (IoT) network at device-level. **Internet of Things**, [*s.l.*], v. 11, 2020. DOI: https://doi.org/10.1016/j.iot.2020.100240.

THE FUTURE OF IOT: 10 Predictions about the Internet of Things | Norton. [s.d.]. Disponível em: https://us.norton.com/internetsecurity-iot-5-predictions-for-the-future-of-iot.html. Acesso em: 22 jul. 2022.

ZAP - Zed Attack Proxy. Disponível em: https://www.zaproxy.org/getting-started/. Acesso em: 29 out. 2023

ZHOU, J. *et al*. Security and privacy for cloud-based IoT: Challenges. **IEEE Communications Magazine**, [*s.l.*], v. 55, n. 1, p. 26-33, 2017. DOI: 10.1109/MCOM.2017.1600363CM

APÊNDICE

Segurança de Dispositivos IOT: análise de vulnerabilidades de uma câmera IP

Luis Armando da Silva Brochado[1]

[1]Departamento de Informática e Estatística, Centro Tecnológico da Universidade Federal de Santa Catarina – UFSC, Brasil

luisarmandosb@gmail.com

Abstract. *With the exponential increase in IoT (Internet of Things) devices, there is a significant need for resources to ensure the integrity and security of data transmitted by these systems. This ensures that the evolution doesn't only focus on the functional aspect of applications but also on data protection and vulnerability detection. Aspects such as hardware limitations, discontinued support, and device updates expand the risk of new vulnerabilities and attacks, creating problems regarding the privacy and security of users of these systems. In this context, this study aims to analyze the security of IoT devices, based on vulnerability tests on IP cameras, seeking to highlight the existence of these flaws and suggest recommendations to improve user security when using this type of application.*

Resumo. *Com o aumento exponencial de dispositivos IoT (Internet of Things), é grande a necessidade de recursos para garantir a integridade e segurança dos dados trafegados por estes sistemas, de forma que a evolução não se restrinja somente ao aspecto funcional das aplicações, mas também a proteção dos dados e detecção de vulnerabilidades. Aspectos como limitação de hardware, descontinuação de suporte e atualizações de dispositivos fazem com que o risco de novas vulnerabilidades e ataques seja ampliado, gerando problemas em relação à privacidade e segurança dos usuários destes sistemas. Diante deste cenário, neste trabalho foi realizada uma análise de segurança de dispositivos IoT, a partir da realização de testes de vulnerabilidade em câmeras IP, procurando evidenciar a existência destas falhas e sugerir recomendações para melhorar a segurança dos usuários ao utilizar este tipo de aplicação.*

1. Introdução

Este trabalho se trata de uma análise de segurança em dispositivos IoT, motivado pela existência de uma grande quantidade destes dispositivos conectados à internet, com falhas de segurança e suscetíveis à exploração por atacantes. Onde os prejuízos inerentes a este problema impactam a vida das pessoas e das empresas, ocasionando uma série de situações como, risco à privacidade, distribuição de malware, sequestro e roubo de dados, além de prejuízo financeiro.

Apesar das possibilidades oferecidas pela IoT, incluindo dispositivos wearables e casas inteligentes, destaca-se a necessidade urgente de projetar sistemas com tecnologias de segurança adequadas para enfrentar os desafios presentes. Ding *et al*. (2019) mencionam que a diversidade e complexidade do ecossistema de IoT tornam a implementação de mecanismos de segurança uma tarefa árdua, podendo gerar lacunas diante dos constantes desenvolvimentos tecnológicos.

Diante desse contexto, o trabalho propõe um estudo focado nas formas de ataque e vulnerabilidades relacionadas à Interface Web de Dispositivos IoT. A pesquisa abrange testes de invasão existentes para este cenário e as ferramentas utilizadas, culminando em um teste prático com análise de resultados e recomendações para aprimorar a segurança dessas aplicações.

2. Conceitos Básicos

2.1. Internet das Coisas

A Internet das Coisas (IoT) é uma rede de objetos físicos com tecnologia embarcada, conexão na rede e sensores que coletam dados dos dispositivos e enviam para processamento. São dispositivos inteligentes, como smartphones, smartwatches e câmeras. Embora seja comumente associada a objetos do cotidiano, como smartphones, a IoT também desempenha um papel significativo nas áreas industrial e comercial, bem como na gestão de infraestrutura pública, incluindo cidades inteligentes. Exemplos de aplicações em cidades inteligentes incluem semáforos inteligentes, sistemas de transporte e monitoramento de máquinas para segurança e diagnóstico de manutenção.

A arquitetura de um dispositivo IoT, conforme descrita por Sikder *et al*. (2018), é estruturada em quatro níveis. No primeiro nível, temos sensores e atuadores que coletam dados. O segundo nível é composto por gateways, responsáveis pela implementação da camada de rede, utilizando tecnologias como Wi-Fi ou RFID. O terceiro nível abrange unidades de processamento em nuvem, onde os dados coletados são analisados e processados. Por fim, no quarto nível, encontramos as aplicações ou serviços que apresentam as informações processadas para os usuários.

2.2. Segurança em IOT

De acordo com Barros (2021), observa-se a falta de comprometimento com a segurança dos dispositivos IoT, em função da falta de previsão de que milhares de dispositivos passariam a estar conectados em rede, e que a segurança destes dispositivos deveria estar implementada.

Conforme resultados obtidos por estudos realizados pela Gartner, empresa norte-americana de consultoria na área de TI, até 2022, 50% do orçamento de segurança em IoT serão comprometidos com correção de falhas (PANARELLO *et al*., 2018).

Outro problema relacionado à segurança de IoT, é a subvalorização da segurança por parte dos usuários em relação às facilidades de uso que lhes são oferecidas. O que facilita a ocorrência de ataques sem a necessidade de muito conhecimento por parte dos invasores. (GROBELNA; GROBELNY; BAZYDŁO, 2018).

2.3. Vulnerabilidade em IOT

As vulnerabilidades são falhas de segurança do sistema que podem ser exploradas por um usuário malicioso para efetuar um ataque. A OWASP, sigla de Open Web Application Security Project, é uma organização internacional focada em melhorar a segurança de aplicações web.

Um dos projetos realizados pela OWASP é o OWASP Internet of Things Project, que periodicamente apresenta um relatório com informações sobre as principais vulnerabilidades de IoT, quais as superfícies de ataque que estas vulnerabilidades estão associadas e um resumo destas vulnerabilidades. A Tabela 1 apresenta as vulnerabilidades associadas à superfície de ataque Interface Web, de acordo com a OWASP.

Vulnerabilidade	Resumo
Enumeração de nome de usuário	Capacidade de coletar um conjunto de nomes de usuário válidos interagindo com o mecanismo de autenticação.
Senhas fracas	Capacidade de definir senhas de conta para “1234” ou “123456”, por exemplo.
Bloqueio de conta	Capacidade de continuar enviando tentativas de autenticação após 3 a 5 tentativas de login com falha.
Credenciais padrão conhecidas	Uso de senhas padrão pré-programadas.
Mecanismo de recuperação de senha inseguro	Falta de mecanismos de autenticação de dois fatores, como token de segurança ou scanner de impressão digital.

Tabela 1. Superfície de ataque Interface Web do dispositivo em IoT.

Fonte: OWASP Internet of Things Project.

As superfícies de ataque são áreas do sistema em que pontos de vulnerabilidade podem ser explorados. No escopo deste trabalho são abordadas as vulnerabilidades associadas à superfície de ataque Interface Web de dispositivo.

3. Desenvolvimento

No desenvolvimento da proposta foram realizados os testes de penetração que seguiram o seguinte roteiro: inicialmente, foram selecionados os dispositivos a serem utilizados. Em seguida, definiu-se as ferramentas e os ataques realizados nos testes. Após será realizada a execução dos testes. E, por fim, a análise e as considerações finais.

A execução dos testes tem a finalidade de avaliar a segurança dos dispositivos evidenciando vulnerabilidades, caso elas existam.

3.1. Dispositivos

As câmeras IP são dispositivos conhecidos por apresentarem baixo controle de segurança e na sua maioria utilizarem credencias padrão ou senhas fracas. Um exemplo disso são as câmeras

Xionmay Technology e Intelligent Onvif que foram exploradas por ataque de credenciais padrão, além das câmeras Sony que permitiram um atacante habilitar acesso ao serviço Telnet de forma remota utilizando este recurso como backdoor.

De acordo com Dhanjani(2015), as câmeras da marca Foscam possuem um histórico de ocorrências de falhas de segurança. Em função da possibilidade de encontrar os dispositivos e reproduzir algumas das falhas, foi escolhida a câmera Foscam para a realização dos testes de penetração.

A obtenção de dispositivos foi realizada de duas formas: seleção de dispositivos pela plataforma Shodan e aquisição de um dispositivo para testes locais.

Para a aquisição do dispositivo local foi realizada uma pesquisa por câmeras IP, usadas, da marca Foscam, sabendo-se que os modelos mais antigos foram os que apresentaram as falhas. A ideia de realizar testes com um dispositivo local foi de ter mais liberdade, podendo realizar alguns tipos de ataques que de outra forma seria necessária a permissão e consentimento do proprietário.

Para a seleção dos dispositivos remotos foi realizada uma pesquisa na plataforma Shodan. Com o aprofundamento da pesquisa foi verificado que a maioria dos problemas de segurança nas câmeras Foscam ocorreram com modelos e versões de firmware específicos.

A partir disso foi procurado encontrar estas características na pesquisa para tentar reproduzir estes casos. Dos resultados encontrados foi selecionado um dispositivo para a realização dos testes de forma remota.

3.2. Ferramentas

Para a realização dos testes foram utilizadas as ferramentas Shodan, Kali Linux, Owasp ZAP, Nmap, Hydra e Wireshark. Shodan é uma ferramenta de busca especializada em dispositivos conectados à Internet, que nos seus resultados apresenta informações como, portas abertas, IPs, protocolos e vulnerabilidades, entre outras informações.

Já a Kali Linux é uma plataforma de testes de penetração que disponibiliza grande variedade de aplicações e ferramentas de teste, incluindo as demais ferramentas utilizadas nesta implementação, Owasp Zap, Hydra e Wireshark.

3.3. Instalação e configuração da câmera local

A câmera local é uma Foscam modelo FI9900EP. Trata-se de um modelo desenhado para monitoramento exterior como pátios, supermercados ou escolas, e utiliza conexão via cabo Ethernet. Foi verificado também que na parte inferior da câmera possui uma etiqueta com informações técnicas como modelo, MAC add, as credenciais padrão de fábrica e outras informações.

Nas pesquisas, os relatos referentes aos problemas de segurança nas câmeras Foscam que ocorreram na interface web, tiveram o seu acesso pelo navegador. Porém, após instalar e configurar a câmera, não foi possível logar na interface web pelo navegador. Dessa forma, foi necessário realizar a instalação do software Foscam VMS, conforme orientado no manual do usuário, para obter acesso às imagens e às funcionalidades da câmera.

3.4. Execução dos Testes

3.4.1 Dispositivo local

Coleta de Informações

A execução dos testes foi realizada primeiramente com o dispositivo local. Inicialmente foi realizada a coleta de informações utilizando a ferramenta Nmap, para escanear portas abertas, protocolos, serviços e métodos suportados. O Nmap é uma das ferramentas disponibilizadas na Kali Linux e os comandos são feitos via terminal. Foram encontradas 3 portas abertas sendo uma delas, a porta 88, com protocolo HTTP e suporte ao método GET que é um dos focos dos testes de vulnerabilidade a ser realizado. As outras portas são, a 443 com HTTPS que é um protocolo seguro e a outra, 888, com SOAP que é utilizado no protocolo Onvif , um padrão de comunicação de câmeras IP para utilização com imagens.

A seguir foi realizada uma varredura por vulnerabilidades com a ferramenta Owasp ZAP, na porta 88. No relatório gerado como resultado foi apresentado um alerta com 9 tipos de vulnerabilidades. Destes foram considerados os de risco médio para análise nesta pesquisa, pois são os que apresentam mais probabilidade de serem explorados por atacantes.

Das vulnerabilidades encontradas, *Content Security Policy (CSP)* not set e *Missing anti-ClickJacking header* são diretivas utilizadas em navegadores modernos que se habilitados adicionam uma camada adicional de segurança evitando determinados ataques com Cross site scripting e ClickJacking. A outra vulnerabilidade é a *Vulnerable JS Library* se refere a bibliotecas do jQuery desatualizadas e não será considerado para esta pesquisa.

Testes de Vulnerabilidade

Com a utilização do app Foscam VMS, a maior parte dos ataques não obteve sucesso neste modelo. Foi implementado um mecanismo de bloqueio de conta ao exceder o número de 10 tentativas, bloqueando o login por 30 minutos, o que dificulta que falhas como *Enumeração de Usuário* e de *Bloqueio de Conta* ocorram.

No caso de *Credenciais Padrão* e *Senhas Fracas*, foi implementada uma validação obrigando o usuário a cadastrar uma senha, o que já altera o padrão de fábrica que é senha em branco. Porém, o sistema permite cadastrar credenciais como usuário “admin” e senhas fracas como “admin1”. Portanto, para o teste de senhas fracas, o modelo falhou.

Nos demais testes realizados, *Path Directory Traversal*, *Authentication Bypass, Envenenamento de DNS Dinâmico e Cross Site Scripting,* da forma como os testes foram conduzidos, não se identificou falha de segurança.

3.4.2 Dispositivo remoto

Para a realização dos testes com o dispositivo remoto foi selecionada uma câmera de modelo 8910W, com o firmware de versão 11.37.2.48, que é um dos modelos que apresentaram falhas relatadas anteriormente.

Coleta de Informações

A coleta de informações foi obtida com o resultado da pesquisa na plataforma Shodan, que apresenta resultado similar ao da ferramenta Nmap, onde foi possível identificar que a porta 1200 está aberta, possui protocolos TCP e HTTP habilitados, o nome do servidor, MAC address e versão do firmware.

Da mesma forma, foi executada a varredura com a ferramenta Owasp ZAP na porta 1200. O resultado foi bastante parecido com a diferença de uma vulnerabilidade de risco médio que foi a Weak Authentication Method. Na descrição da vulnerabilidade no relatório, menciona que a autenticação está utilizando uma conexão insegura e que as credenciais podem ser lidas por alguém com acesso à rede. As outras vulnerabilidades de risco médio apresentadas foram *Content Security Policy (CSP)* not set e *Missing anti-ClickJacking header,* falhas também identificadas no dispositivo local.

Testes de Vulnerabilidade

Em relação aos testes de vulnerabilidade com o dispositivo remoto, foi possível fazer o login com as credenciais padrão de fábrica, e ter acesso às imagens da câmera e às configurações. Portanto, ficou evidenciado que as falhas de *Credenciais Padrão e Senhas Fracas* permanecem ativas.

Também ficou evidenciado que o dispositivo não possui sistema de bloqueio limitando o número de tentativas de autenticação. Desta forma considera-se que o *Bloqueio de Conta* é uma vulnerabilidade possível de ser explorada.

Outras falhas identificadas foram o *Path Directory Traversal* e *Authentication bypass*, que são tentativas de exploração adicionando caminhos de diretórios no final da url. Com este ataque foi possível acessar dados da memória do dispositivo, sendo possível em alguns casos obter as credenciais de acesso do sistema.

Em outro caso, adicionando um comando CGI ao final da URL, foi possível acessar uma página sem autenticação com informações sensíveis do dispositivo.

Sabendo-se que o dispositivo utiliza o protocolo HTTP, enviando as requisições via GET, foi realizada uma captura de pacotes na rede, com a ferramenta Wireshark no momento do login, para testar a possibilidade de ataque de Eavesdropping. Com este teste, foi verificado que as credenciais são enviadas em texto plano, evidenciando mais uma falha de segurança no dispositivo.

4. Análise dos testes

A análise de segurança foi feita a partir de testes de penetração realizados com dois dispositivos. Um deles, dentro da rede local e outro de forma remota.

A aprovação nos testes, não evidencia que um atacante experiente não consiga explorar as vulnerabilidades abordadas. Somente que nos testes, da forma como foi executado, obteve resultado positivo.

A forma de execução foi obtida a partir dos trabalhos correlatos referenciados, nas orientações de uso das ferramentas utilizadas e na pesquisa sobre as vulnerabilidades abordadas em órgãos como a OWASP e a CVE.

Com base nos resultados dos testes realizados, é possível identificar várias implicações em termos de segurança.

No modelo FI9900EP, dispositivo local que é um modelo mais recente, apresentou correções em falhas anteriormente exploradas, e teve um número menor de falhas identificadas, resultando em maior aprovação na maioria dos testes. Foi identificada a vulnerabilidade de senhas fracas, além de problemas de segurança na porta 88 incluindo vulnerabilidades de Content Security Policy não definido e Missing Anti-clickjacking header, conforme apresentado na tabela 2.

Apesar de ter sido implementado um recurso obrigando o usuário a cadastrar uma senha ao configurar o dispositivo, não foi exigida uma complexidade mínima para descaracterizar como vulnerabilidade de senhas fracas. Segundo a OWASP, esta é uma falha considerada de severidade Alta, pois pode causar impactos graves, resultando em perda ou corrupção de dados, negação de acesso e pode levar ao comprometimento total do dispositivo e/ou contas de usuário.

Dispositivo Local	Modelo	FI9900EP				
Ataque/ Vulnerabilidade	**Status**	**CVE**	**CWE**	**CVSS Score**	**Severidade**	**# OWASP IOT Top10**
Enumeração de Usuário	não identificado		CWE-287		Alta	A03
Bloqueio de conta	não identificado		CWE-307		Alta	A03
Credenciais padrão	não identificado		CWE-521		Alta	A01
Senhas fracas	identificado		CWE-521		Alta	A01
Path Directory Traversal	não identificado	CVE-2013-2560	CWE-35	7.8	Alta	
Authentication bypass	não identificado	CVE-2014-1911	CWE-287	7.8	Alta	
Envenenamento DDNS	não identificado	CVE-2014-1849	CWE-255	10.0	Crítico	
Cross Site Scripting	não identificado	CVE-2013-5215	CWE-79	4.3	Média	
Content Security Policy Não Definido	identificado		CWE-693		Média	
Anti-clickjacking header	identificado		CWE-1021		Média	
Autenticação Insegura	não identificado		CWE-326		Média	

Tabela 2. Vulnerabilidades testadas no modelo Foscam FI9900EP.

Fonte: Elaborado pelo autor.

Já no modelo FI8910W, dispositivo acessado de forma remota e que possui registros de vulnerabilidades já exploradas, foi possível reproduzir a maioria dos ataques efetuados anteriormente, com exceção de Enumeração de Usuário, conforme apresentado na tabela 3.

Dispositivo remoto	Modelo	FI8910W				
Ataque/ Vulnerabilidade	**Status**	**CVE**	**CWE**	**CVSS Score**	**Severidade**	**# OWASP IOT Top10**
Enumeração de Usuário	não identificado		CWE-287		Alta	A03
Bloqueio de conta	identificado		CWE-307		Alta	A03
Credenciais padrão	identificado		CWE-521		Alta	A01
Senhas fracas	identificado		CWE-521		Alta	A01
Path Directory Traversal	identificado	CVE-2013-2560	CWE-35	7.8	Alta	
Authentication bypass	identificado	CVE-2014-1911	CWE-287	7.8	Alta	
Envenenamento DDNS	não descartado	CVE-2014-1849	CWE-255	10.0	Crítico	
Cross Site Scripting	identificado	CVE-2013-5215	CWE-79	4.3	Média	
Content Security Policy Não Definido	identificado		CWE-693		Média	
Anti-clickjacking header	identificado		CWE-1021		Média	
Autenticação Insegura	identificado		CWE-326		Média	

Tabela 3. Vulnerabilidades testadas no modelo Foscam FI8910W.

Fonte: Elaborado pelo autor.

Em relação às informações apresentadas na tabela, pode-se verificar que o dispositivo possui cinco vulnerabilidades de severidade Alta e uma Crítica, passíveis de serem exploradas. Além de outras quatro de severidade Média. E das falhas exploradas anteriormente, todas permanecem ativas.

Foi possível acessar o dispositivo com as credenciais padrão, e ter acesso às imagens e às configurações da câmera. Desta forma o atacante passa a ter controle total do dispositivo.

No caso da vulnerabilidade Envenenamento de DDNS, de acordo com a CVE, "A câmera IP Foscam com versão 11.37.2.49 e anteriores, ao usar a opção Foscam DynDNS, gera credenciais com base em nomes de subdomínios previsíveis, o que permite que invasores remotos falsifiquem ou sequestrem os dispositivos e realizem outros ataques modificando os registros das câmeras no servidor DNS Foscam".

Considerado de severidade crítica, este problema pode ocasionar o sequestro de inúmeros dispositivos para a criação de botnets.

Mesmo não tendo sido possível executar o ataque, pois necessitaria de consentimento do proprietário do dispositivo, foi considerado como não descartado pois todas as características e configurações necessárias foram identificadas para a sua realização.

O ataque de Path Directory Traversal, que foi identificado e considerado de severidade Alta, possibilitou o acesso à memória do dispositivo. Este tipo de ataque pode possibilitar a injeção

de arquivos maliciosos, como é o caso de LFI, sigla para Local File Inclusion, ou Inclusão de Arquivo Local em tradução livre.

Segundo Chauan (2023), “LFI é um tipo de vulnerabilidade de aplicativo da web que permite que um invasor acesse e execute arquivos contendo código malicioso em um servidor web.”

Com base nos dados apresentados pode-se fazer algumas recomendações em relação às falhas de segurança encontradas nos dispositivos, a saber:

1. **Atualização de Firmware e Senhas**: Os fabricantes devem liberar atualizações de firmware para corrigir as vulnerabilidades identificadas, incluindo a eliminação de credenciais padrão. Os usuários devem ser incentivados a aplicar essas atualizações e a alterar as senhas padrão para senhas fortes e únicas.
2. **Configuração Adequada de Content Security Policy**: Os fabricantes devem configurar de forma adequada a Content Security Policy para restringir as fontes de conteúdo permitidas e evitar ataques de XSS. Isso é especialmente importante em dispositivos que têm interfaces web.
3. **Implementação de Métodos de Autenticação Seguros**: A implementação de métodos de autenticação seguros, como HTTPS, é crucial para proteger as informações de autenticação durante a transmissão dos dados. Além disso, métodos de autenticação robustos devem ser utilizados para reduzir o risco de ataques.
4. **Validação de Entrada e Restrição de Acesso**: Os fabricantes devem implementar validação de entrada e restrição de acesso adequadas para evitar ataques de Path Directory Traversal e Authentication Bypass. Isso inclui filtrar e validar todos os inputs do usuário.
5. **Criptografia dos Dados**: A utilização de criptografia forte dos dados é fundamental para proteger informações sensíveis. Os fabricantes devem garantir que as comunicações entre os dispositivos e os clientes sejam seguras e criptografadas. Importante atentar-se para a não utilização de algoritmos ultrapassados
6. **Educação do Usuário**: Os fabricantes devem educar os usuários sobre a importância da segurança, incluindo a necessidade de alterar senhas padrão, manter dispositivos atualizados e estar cientes das práticas de segurança recomendadas.

5. Conclusão

Neste trabalho são apresentados os principais conceitos de segurança em IoT, dando ênfase à Interface Web dos dispositivos, que historicamente vem sendo um dos vetores de ataque mais explorados.

Além disso, foi realizada uma análise de segurança dos dispositivos IoT, a partir da realização de testes de penetração com duas câmeras IP.

O objetivo da análise foi avaliar se as principais vulnerabilidades listadas na OWASP Top 10, relacionadas a interface web, podem ser reproduzidas, assim como as vulnerabilidades identificadas anteriormente nestes dispositivos. O que se confirmou em ambos os casos.

A partir disso, foram propostas recomendações de segurança como, atualização de firmware e senhas, e implementação de métodos de autenticação seguros.

Das vulnerabilidades identificadas, pode-se destacar a de credenciais padrão e senhas fracas que figuram em primeiro lugar na lista da Owasp IoT Top 10 como, Weak Guessable, or Hardcoded Passwords.

Outras vulnerabilidades importantes identificadas foram Path Directory Traversal e Authentication Bypass, ambas relacionadas a permitir acesso não autorizado a recursos do sistema adicionando caminhos de diretórios no final da URL. A exploração destas falhas possibilitou ao atacante acessar a memória do dispositivo e arquivos com informações sensíveis.

Evidenciou-se também a existência de métodos de autenticação inseguros, com as credenciais sendo enviadas em texto plano pela rede. Desta forma, mesmo solucionando o problema de senhas fracas a segurança na parte de autenticação estaria comprometida.

Por fim, ficou evidenciado que os dispositivos mais antigos, que não tiveram atualização de firmware continuam sendo passíveis de exploração e contribuindo para um ambiente IoT inseguro. Nas recomendações de segurança é mencionada a importância da ação de fabricantes e usuários para mitigar este problema.

Do lado dos desenvolvedores e fabricantes, também é necessário maior preocupação com a segurança, procurando melhor equalizar este aspecto com as questões funcionais e comerciais.

Ademais, foi verificado que algumas das formas de ataque utilizadas são de certo modo simples e que não necessitam muito conhecimento técnico para executá-las, o que as torna ainda mais críticas em função da facilidade de disseminação. Ao mesmo tempo, o conhecimento e as ferramentas estão cada vez mais acessíveis, favorecendo a ação dos atacantes.

Em resumo, a segurança deve ser uma consideração central no desenvolvimento e uso de dispositivos IoT. E espera-se que os resultados deste trabalho contribuam para a evolução da Internet das Coisas nesta direção.

6. References

Abdalla, P. A. and Varol, C. (2020). “Testing IoT Security: The Case Study of an IP Camera”, In: *Proceedings of International Sumposium on Digital Forensics and Security.* Beirut, Lebanon, IEEE, p. 1-5. DOI: 10.1109/ISDFS49300.2020.9116392

Alchieri, E. A. *et al*. (2019). “Pentest on Internet of Things Devices”, In: *Proceedings Latin American Computing Conference*. Panama City, IEEE, p. 1-10.

Almeida Jr., J. A. (2021). *Pentest em Aplicações Web*. São Paulo: Casa do Código.

Antonakakis, M. *et al*. (2017). “Understanding the mirai botnet”, In: *Proceedings Security Symposium Security*. Vancouver, USENIX, p. 1093-1117.

Barros, E. (2021). *Estudo de vulnerabilidades em dispositivos IOT TCP/IP*. Monografia (Graduação). Universidade Federal do Rio Grande do Sul, Porto Alegre, Brasil.

Bjorneset, K. J. (2017). *Testing Security for Internet of Things - A Survey on Vulnerabilities in IP Cameras*. (Master’s Thesis). University of Oslo, Oslo, Noruega.

Brinhosa, R. (2019). *IoPenT*: *Framework para Penetration Testing de dispositivos IoT*. (Projeto de Qualificação de Doutorado). Universidade Federal de Santa Catarina, Florianópolis, Brasil.

Bursztein, E. (2017). “Inside the infamous Mirai IoT Botnet: A Retrospective Analysis”,

https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/

Chauan, A. (2023). “Inclusão de arquivo local (LFI) para RCE”, https://aditya-chauhan17.medium.com/local-file-inclusion-lfi-to-rce-7594e15870e1

CVE (2022), “Glossary”, https://www.cve.org/ResourcesSupport/Glossary#.

CVE Details (2014), https://www.cvedetails.com/cve/CVE-2014-1849/

Dhanjani, N. (2015). *Abusing the Internet of Things*: *Blackouts, Freakouts, and Stakeouts.* Califórnia, O'Reilly Media Company.

Ding, A. *et al*. (2019). “Ethical Hacking for Boosting IoT Vulnerability Management: A First Look into Bug Bounty Programs and Responsible Disclosur”, In: *Proceedings ICTRS '19*. Rhodes, Greece, ICTRS, p. 49-55.

Exploiting Foscam IP Cameras (2023), https://docplayer.net/11352485-Exploiting-foscam-ip-cameras-contact-rampartssecurity-com.html.

Gartner. (2021). “*Gartner Glossary”,* https://www.gartner.com/en/information-technology/glossary/internet-of-things.

Grobelna, I., Grobelny, M. and Bazydło, G. (2018). “User awareness in IoT security. A survey of Polish users”. In: *AIP Conference Proceedings*. AIP Publishing, v. 2040, p. 080002.

Gupta, A. and Guzman, A. (2017). *IoT Penetration Testing Cookbok*: identify vulnerabilities and secure your smart devices. Birmingham, Packt.

Gupta, A. (2019). *The IoT Hacker’s Handbook*: *a pratical guide to hacking the internet of things*. Walnut, Apress.

Johari, R. *et al*. (2020). “Penetration Testing in IoT Network”, In: *Proceedings International Conference on Computing, Communication and Security*. Patna, India, IEEE, v.1, n. 1, p. 1-8.

Kamienski, C. *et al*. (2016). “Computação Urbana: Tecnologias e Aplicações para Cidades Inteligentes”. In: *Minicursos do SBRC 2016,* editado por F. Siqueira *et al*. Salvador, Sociedade Brasileira de Computação (SBC), p. 12-14.

Kovacs, E. (2016). “Backdoor Found in Many Sony Security Cameras”, https://www.securityweek.com/backdoor-found-many-sony-security-cameras.

Krebs, B. (2014). “Krebs on Security”, http://krebsonsecurity.com/2014/01/bug-exposes-ip-cameras-baby-monitors/.

Owasp Iot - Owasp Internet of Things Project (2022), https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project.

Owasp Teste para alteração de senha fraca ou funcionalidades de redefinição (2022), https://wiki.owasp.org/index.php/Testing_for_weak_password_change_or_reset_functionalities_(OTG-AUTHN-009).

Owasp Teste para CSRF (2022), https://wiki.owasp.org/index.php/Testing_for_CSRF_(OTG-SESS-005).

Owasp Wstg - Web Security Testing Guide v. 4, (2022), https://owasp.org/www-project-web-security-testing-guide/assets/archive/OWASPTestingGuidev4.pdf.

Panarello, A. *et al*. (2018). “Blockchain and iot integration: A systematic survey”. *Sensors, Multidisciplinary Digital Publishing Institute, 18*(8), 2575.

Santos, P. (2016), *Internet das Coisas: o desafio da privacidade*. Setúbal, Instituto Politécnico

de Setúbal, p. 8-14.

Sanchez, L. *et al*. (2014). “Smartsantander: Iot experimentation over a smart city testbed”. *Computer Networks*, *61*, 217-238.

Shekyan, S., and Harutyunyan, A. (2013). *Turning your surveillance camera against you*. Qualys, Inc.

Shodan. [s.d.], https://www.shodan.io/.

Sikder, A. *et al*. (2018). “A Survey on Sensor-based Threats to Internet-of-Things (IoT) Devices and Applications”. *arXiv*:1802.02041.

Stallings, W. (2015). *Criptografia e segurança de redes*: *Princípios e práticas*. 6. ed. São Paulo, Pearson Education do Brasil.

Syed, R. *et al*. (2020). “Threat model for securing internet of things (IoT) network at device-level”. In: *Internet of Things*, v. 11.

The Future of Iot (2022). *The Future of Iot: 10 Predictions about the Internet of Things*. Norton. [s.d.].

Zap - Zed Attack Proxy (2023), https://www.zaproxy.org/getting-started/. Acesso em: 29 out. 2023

Zhou, J. *et al*. (2017). “Security and privacy for cloud-based IoT: Challenges. *IEEE Communications Magazine*, *55*(1), 26-33.