Análise de vulnerabilidade em concentradores de dados de infraestrutura AMI

Ubiratan Alves do Carmo [1], Iony Patriota de Siqueira [2], Manoel Henrique da Nóbrega Marinho [3], Guilherme Ferretti Rissi [4], Samuel Giuseppe Tomasin [5]

[1] uacarmo@gmail.com. Instituto Avançado de Tecnologia e Inovação. [2] iony@tecnix.com.br. Instituto Avançado de Tecnologia e Inovação. [3] marinho75@poli.br. Universidade de Pernambuco. [4] grissi@cpfl.com.br. CPFL Energia S.A. [5] samueltomasin@gmail.com. CPFL Energia S.A.

RESUMO

O desenvolvimento tecnológico dos sistemas computacionais e das comunicações ocasiona uma forte digitalização em todos os setores da sociedade moderna. Conceitos como cidades inteligentes e indústria 4.0 são introduzidos e novos modelos comportamentais são impostos. Essa revolução também está acontecendo nos sistemas de produção, transmissão e distribuição de energia elétrica. Conceitos como geração distribuída, armazenamento de energia, mobilidade elétrica e redes inteligentes afetam sobremaneira o comportamento das pessoas. Para suportar as redes inteligentes é necessário que se tenha uma infraestrutura de medição inteligente (AMI) que suporte os modelos de negócio entre os consumidores e as empresas de distribuição de energia, garantindo a integridade, a confidencialidade e a disponibilidade das informações. Esta pesquisa apresenta os resultados de teste de varredura de vulnerabilidade executado em um concentrador de dados responsável pela aquisição das informações de medidores de energia de consumidores residenciais e industriais. Utilizou-se para os testes a infraestrutura de medição do Instituto Avançado de Tecnologia e Inovação – IATI, que faz parte da infraestrutura de hardware do projeto PA3046, "Desenvolvimento de Plataforma Inteligente com *Cybersecurity Business Intelligence* e *Big Data*", patrocinado pela CPFL Energia e pela Agência Nacional de Energia Elétrica (ANEEL). Os estudos demonstraram a importância de se fazer o gerenciamento de vulnerabilidades desde a fase de implantação até a operação final de um sistema AMI.

Palavras-chave: Vulnerabilidade. Medidores inteligentes. Medição de energia elétrica. Concentradores de dados. AMI.

ABSTRACT

The technological development of computer systems and communications causes an intense digitalization in all sectors of modern society. Concepts such as smart cities, and industry 4.0 are introduced, and new behavioral models are imposed. This revolution is also happening in the systems of production, transmission, and distribution of electric energy. Concepts such as distributed generation, energy storage, electric mobility, and smart grids significantly affect people's behavior. In order to keep business models between consumers and energy distribution companies, an intelligent metering infrastructure (AMI) is needed. This will ensure the integrity, the confidentiality, and the availability of information to support a smart grid. The present research shows the results of a vulnerability scanning test, performed on a data concentrator, which was responsible for the acquisition of information from energy meters of residential and industrial consumers. The testbed was the measurement infrastructure of the Advanced Institute of Technology and Innovation - IATI, which is part of the hardware infrastructure of the PA3046 project, "Development of an Intelligent Platform with Cybersecurity Business Intelligence and Big Data," sponsored by CPFL Energia, and also by the National Electric Energy Agency (ANEEL). Studies have demonstrated the importance of vulnerability management, which must be considered, from the implementation phase to the final operation of an AMI system.

Keywords: *Vulnerability. Smart meters. Measurement of electrical energy. Data concentrators. AMI.*

1 Introdução

Subjaz aos conceitos de cidades inteligentes e Indústria 4.0 o entendimento de que há uma maior demanda de energia elétrica. Sendo assim, não é leviano afirmar que toda a cadeia do processo produtivo vem passando por uma transformação radical desde que tais conceitos se instauraram na sociedade moderna. A possibilidade de armazenamento de energia distribuída também é uma realidade, assim como a forte penetração de geração distribuída com caráter intermitente, que provém de fonte fotovoltaica e eólicas. Nesse cenário, um novo modelo de geração, transmissão e distribuição de energia elétrica está surgindo (GUNGOR *et al.*, 2012). Dentro desse contexto, tornam-se necessárias novas formas de relacionamento entre as empresas de distribuição e os consumidores. A distribuição de energia elétrica é a interface setorial com os consumidores finais, representando o estágio de maior vulnerabilidade do processo de distribuição do sistema elétrico.

Todas essas inovações somente são possíveis com a introdução de meios de medição e controle compatíveis com a complexidade desses processos. Isso acontece com uma extensão e um nível de penetração antes inimagináveis, pois são utilizados recursos avançados de automação e telecomunicações. Esse movimento fez surgir o conceito de infraestrutura avançada de medição, advindo do inglês *Advanced Metering Infrastructure* (AMI) que utiliza, além dos meios digitalizados para medir a energia consumida ou gerada, recursos avançados de transmissão desses resultados a longas distâncias e, simultaneamente, de milhões de pontos, contribuindo para o controle distribuído de geração e demanda (DUTRA *et al.*, 2013).

Nesse cenário, novos desafios associados ao processo de digitalização surgiram. Entre eles, destaca-se o problema da segurança cibernética associado às redes de comunicações que suportam os sistemas de automação. Em função de sua exposição física, estrutura distribuída, interdependência mútua, e também em função de seu grande impacto social e industrial, a infraestrutura de medição avançada (AMI) está entre os ativos mais vulneráveis à manipulação indevida por meio cibernético, conforme apresentado em Aloul *et al.* (2012), Gui *et al.* (2019) e Park e Kim (2020). Os autores corroboram o fato de que o gerenciamento de vulnerabilidades é de fundamental importância para a perfeita operação de toda a cadeia de informações associada ao processo de medição de energia dos consumidores residências e industriais.

O levantamento de pesquisa bibliográfica indica que os diversos trabalhos abordam as vulnerabilidades e ataques de forma teórica, e que os resultados, na maioria das vezes, são obtidos por intermédio de simulações.

Na arquitetura proposta por Namboodiri *et al.* (2013), para identificar possíveis vulnerabilidades, é realizada uma análise abrangente da segurança sem fio no cenário de rede doméstica baseada em medidor inteligente. Nesse contexto, algumas contramedidas são desenvolvidas. Elas podem ser usadas tanto pela concessionária quanto pelo cliente, integradas em uma estrutura comum denominada de SecureHAN (*Secure Home Area Network*), que pode ser acordada por ambos, concessionária e cliente. Além disso, as experiências de implementação da estrutura SecureHAN, usando hardware de prateleira comercial, são descritas com a inclusão de possíveis desafios.

Liu, Hu e Ho (2014), com o intuito de detectar o custo de anomalias, propuseram uma técnica de contramedida que usa regressão de vetor de suporte e diferença de impacto. Os resultados de simulação demonstram que o ataque cibernético de preços pode reduzir a conta do invasor em 34,3%, aumentar a conta de terceiros em 7,9%, em média, e desequilibrar a carga de energia do sistema de energia local, pois aumenta a relação entre pico e média em 35,7%. Além disso, os resultados demonstram que a técnica de contramedida proposta pode detectar, efetivamente, a manipulação de preços de eletricidade.

Abdullah *et al.* (2015) propõem o estudo da arquitetura das redes de comunicação de *smart grid*, concentrando-se em redes de medição inteligente e discutindo como essas redes podem ser vulneráveis a ataques de segurança. Neste estudo, os autores apresentam os mecanismos atuais que têm sido usados para proteger as redes de medição inteligente do inglês, *Smart Meter Network* (SMN) de determinados tipos de ataques, e indica as questões em aberto relacionadas à segurança cibernética e a privacidade dessas redes, questões. que podem ser tratadas em trabalhos futuro.

A pesquisa proposta neste trabalho, realiza uma análise de vulnerabilidade em um ambiente emulando

uma infraestrutura real de AMI. O estudo apresenta-se como contribuição a uma metodologia de pesquisa de vulnerabilidades para infraestrutura AMI e busca a comprovação de sua existência. A pesquisa realiza varreduras utilizando diferentes ferramentas, o que permite verificar que os resultados obtidos são independentes do tipo de ferramentas ou métodos utilizados.

O objetivo da pesquisa é realizar testes de vulnerabilidades no concentrador, com foco na tecnologia Ethernet, e na análise dos resultados obtidos. A avaliação da rede PLC-Prime e de outros meios de comunicação, como RS-232/485 e porta óptica, estão fora do escopo deste estudo. Os autores, consideraram que a zona desmilitarizada (do inglês, *DeMilitarized Zone* – DMZ), ou *perimeter network*, é uma rede que faz parte de esquema de segmentação. Ela tem a função de isolar a rede interna de um acesso externo (NAKAMURA e GEUS, 2007), está localizada nas dependências da concessionaria, usando esquemas de segurança como servidores fortificados (*Hardening*), monitoramento, e controle de fluxo através de esquemas de *firewall,* sob um controle ativo da equipe de TI. É menos atrativa a ataques cibernéticos do que os concentradores de dados que estão instalados em locais públicos, e sem nenhum controle de acesso físico por parte da concessionaria.

Este artigo está estruturado da seguinte forma: na seção 2 estão contextualizadas abordagens do tema infraestrutura de medição inteligente e vulnerabilidades, por meio do referencial teórico; a seção 3 discorre sobre os métodos utilizados nesta pesquisa; na seção 4 são analisados os resultados encontrados e, por fim, são apresentadas as conclusões na seção 5.

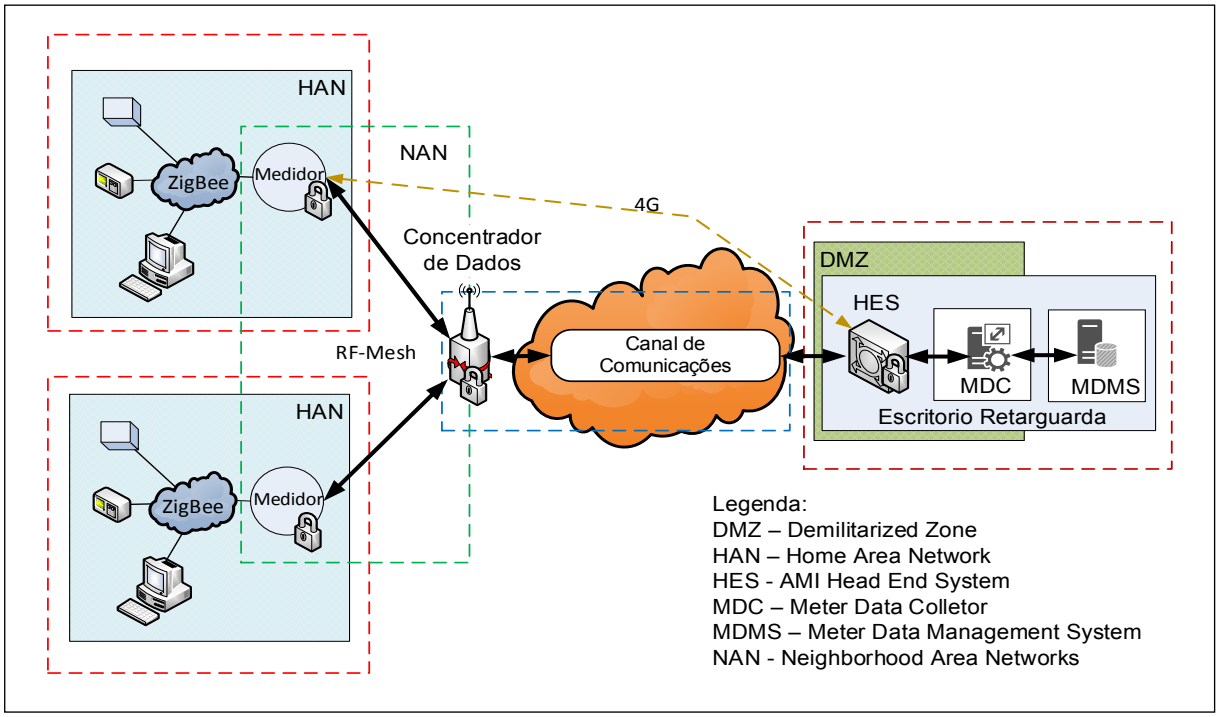
2 Infraestrutura de medição inteligente

A infraestrutura de coleta de informações, denominada de AMI, é um sistema que adquire sinais provindos de diversos tipos de sensores e analisa o uso de informações de consumo de eletricidade, gás, refrigeração e água dos consumidores residenciais e industriais (XIAO, 2013). Essas informações são adquiridas a partir dos dispositivos de medição associados ao tipo de serviço utilizado pelo usuário. As medições são realizadas sob demanda ou seguindo um cronograma definido. A arquitetura do sistema de medição inteligente, é composta de medidores avançados (do inglês, *Smart Meter* – SM). Trata-se de uma rede de comunicação bidirecional para transferir os dados entre os medidores avançados e o sistema de gerenciamento de dados de medidores (em inglês, *Meter Data Management* – MDM), conforme Sorebo e Echols (2011). Os sistemas de gerenciamento de medidores são instalados nos escritórios das empresas de distribuição.

A arquitetura da infraestrutura AMI é composta dos seguintes domínios (NAMBOODIRI *et al.*, 2013; ABDULLAH *et al.*, 2015): i) redes residenciais, termo avindo do inglês *Home Area Network* (HAN), que são sub-redes formadas pelos eletrodomésticos e pelos dispositivos inteligentes. Por exemplo: *smart plugs*, sistemas de controle de refrigeração, e displays de informação para o usuário, o que possibilita o gerenciamento do consumo de energia e a forma de faturamento de sua residência; ii) redes de vizinhança, avindo do termo em inglês, *Neighborhood Area Network* (NAN), são compostas dos SM das diversas residências e de um concentrador de dados, que funciona como *gateway*, que recebe informações dos medidores e as envia para o centro de medição da concessionária de energia; iii) *backhaul* de comunicações é uma rede de telecomunicações hierárquica que compreende os links intermediários entre a rede principal, ou a rede de *backbone*, e as pequenas sub-redes de borda. No caso específico de AMI, considera-se *backhaul* toda infraestrutura de comunicações desde o concentrador de dados até a concessionária de distribuição.

O fluxo de comunicações de uma infraestrutura AMI é iniciado no medidor e se comunica por uma interface com o concentrador de dados da rede doméstica (do inglês, *in-home-display*), trocando informações com os eletrodomésticos, e por outra interface com os concentradores de dados da rede de vizinhança. Esse concentrador coleta as informações de um conjunto de residências e transmite por meio da rede WAN (*Wide Area Network*) até o conjunto consolidador (do inglês, *head-end system*), e o MDMS (*Meter Data Management System*) que recebe as informações, realiza o tratamento adequado e as distribui para as aplicações do sistema de medição da concessionaria de energia. A Figura 1 ilustra uma arquitetura teórica de uma infraestrutura AMI, conforme literatura.

Figura 1 – Topologia de uma infraestrutura de redes de medição inteligentes



Fonte: Adaptado de Sorebo e Echols (2011).

2.1 Vulnerabilidades

A segurança cibernética da infraestrutura AMI visa atender aos fundamentos de segurança de confidencialidade, integridade e autenticidade das informações em todas as etapas do processo de medição inteligente (SKOPIK *et al.*, 2012). A estratégia de garantir a segurança cibernética em cada domínio, em associação com as etapas, além de garantir a segurança em todo o percurso dos dados, permite tratá-la de forma diferente para cada um dos tipos de tecnologia de comunicação utilizados. Portanto, cada domínio possui vulnerabilidades e problemas de segurança diferentes.

A vulnerabilidade é definida como uma condição que, quando explorada por um atacante, pode resultar em uma violação de segurança (WEIDMAN, 2014). Essas vulnerabilidades podem ser ocasionadas por mecanismos de segurança inadequados, sistemas mal configurados e pessoas mal-intencionadas. Destacam-se como principais vulnerabilidades encontradas em sistemas computacionais as injeções de falhas, as quebras de autenticação, a exposição de dados sensíveis, os erros de configuração de segurança e as quebras de controle de acesso.

O gerenciamento de vulnerabilidades é a prática cíclica de identificar, classificar, remediar e mitigar vulnerabilidades. O mapeamento de vulnerabilidade consiste na identificação e análise das possíveis fraquezas do sistema (MORENO, 2017). É uma atividade essencial, pois garante a segurança cibernética de sistemas computacionais e, no caso do estudo, da infraestrutura AMI. As ameaças são ataques realizados por pessoas mal-intencionadas, que têm como objetivo explorar as vulnerabilidades encontradas.

Na infraestrutura AMI, a lista de ameaças vai desde o vazamento do estilo de vida dos usuários até a provocação de um apagão regional. Podem ser citadas, como exemplo de ameaça, as seguintes situações (SOREBO; ECHOLS, 2011):

a) Observação e espionagem da vizinhança: nesse tipo de ataque um homem no meio pode escutar e monitorar os dados de um determinado consumidor. Nesse caso, o atacante tem a capacidade de levantar o perfil do uso de energia do consumidor e, como consequência, o padrão do estilo de vida dele;

b) Adulteração de pacotes: os pacotes transmitidos podem ser capturados, alterados e reenviados para o destino. Os consumidores mal-intencionados podem desejar alterar os dados do medidor para adulterar o valor do consumo de energia;

c) Medidores comprometidos e concentradores de dados: as informações de um medidor inteligente podem ser hackeadas. Sua identidade e chave secreta podem ser roubadas e usadas para bisbilhotar a rede e outros medidores;

d) Bloqueio de serviço: o invasor pode enviar pacotes com erros ou inundar e degradar o serviço. Em uma rede congestionada, o provedor de serviços da concessionária de energia pode perder seu controle;

e) Comprometimento do sistema de gerenciamento de dados de medidor (MDMS): nesse cenário, um comprometimento do MDMS pode ocasionar o vazamento dos dados dos usuários, o que gera o descrédito da empresa concessionária de energia diante de processos judiciais. Nesse caso, haverá a possibilidade de comprometimento dos dados da medição de faturamento e a geração de prejuízos financeiros.

A necessidade de manter a privacidade dos dados de consumo e dos usuários, pela regulamentação, impõe à infraestrutura AMI requisitos de criptografia das informações coletadas no medidor. O gerenciamento de vulnerabilidades é uma etapa essencial para garantir a conformidade dos requisitos de segurança na tecnologia da informação (TI) aderente às regras e regulamentos legais, corporativos e contratuais relacionados às infraestruturas AMI.

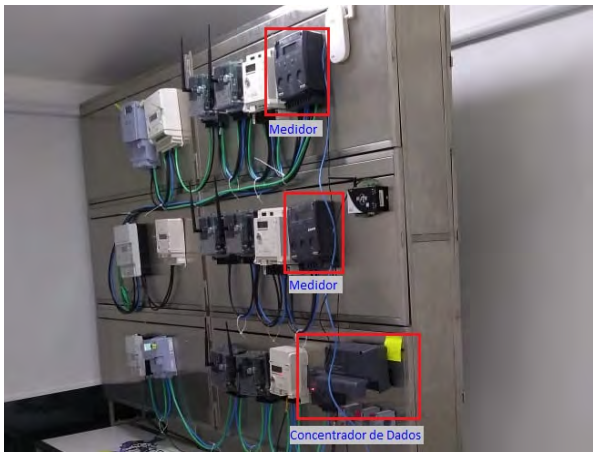
Nesse contexto, a conformidade com os requisitos de segurança se refere, principalmente, à garantia da informação, com respeito à sua disponibilidade, ao seu armazenamento e à privacidade dos dados do usuário. Controlar e melhorar a segurança de uma infraestrutura AMI é um processo contínuo que consiste em pelo menos três etapas: descoberta do estado atual, melhorias desse estado e análise das medidas tomadas.

3 Método da pesquisa

A metodologia utilizada foi a realização de varredura de vulnerabilidades de um concentrador de dados de AMI comercial, na sua configuração padrão de *firmware*, utilizando ferramentas de varredura de vulnerabilidades de código aberto e comercial em sua versão de distribuição para comunidades. O cenário de teste foi a rede da infraestrutura de medição inteligente, baseado na arquitetura ilustrada na Figura 1, pertencente ao Instituto Avançado de Tecnologia e Inovação (IATI), localizado na cidade de Recife. Esse laboratório faz parte da infraestrutura de hardware do projeto PA3046, "desenvolvimento de plataforma inteligente com *Cybersecurity Business Intelligence* e *Big Data*", patrocinado pela CPFL Energia e pela Agência Nacional de Energia Elétrica (ANEEL).

O Laboratório é composto de medidores inteligente, infraestrutura de comunicações e de um sistema de gerenciamento de dados de medidor (MDMS), tendo a capacidade de emular uma infraestrutura de medição inteligente, desde a aquisição do consumo, o sistema de comunicações, até o centro de medição. A Figura 2 ilustra o ambiente do laboratório de medição inteligente do IATI.

Figura 2 – Laboratório de medição inteligente do IATI



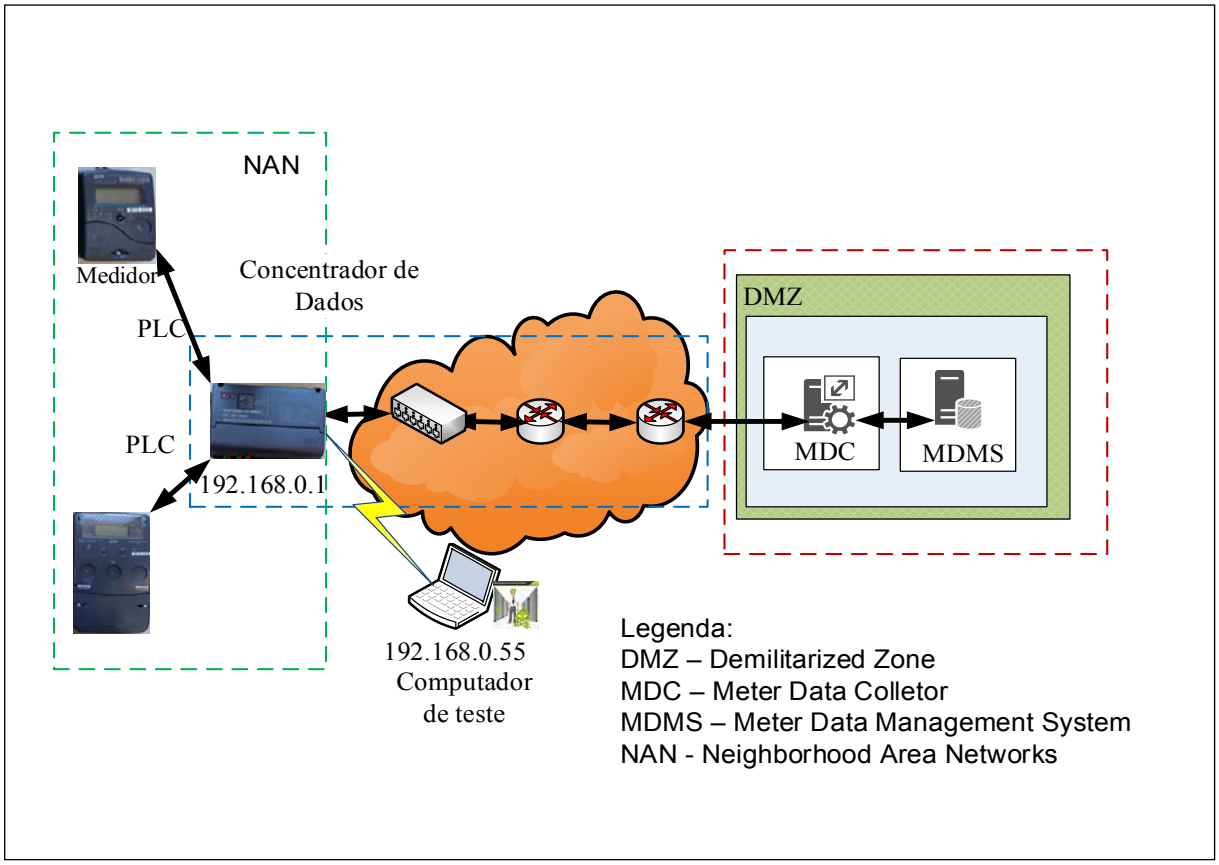
Fonte: Arquivo pessoal dos autores.

Nesse cenário, o concentrador de dados utiliza o padrão de comunicações *Power-Line Communication* (PLC) em conformidade com a especificação *PoweRline Intelligent Metering Evolution* (PRIME) para adquirir os dados dos medidores inteligentes, e utiliza o meio de comunicação Ethernet para conexão com o *Backhaul* de comunicações.

Os ensaios de varreduras de vulnerabilidade dos dispositivos de forma individual em bancada proporcionam a possibilidade de implantação das correções (*patches*) antes de sua entrada em produção, facilitando os trabalhos de comissionamento no campo. O concentrador sob estudo oferece como serviços de acesso por meio da porta Ethernet, um servidor web na porta 80, comunicação via Telnet na porta 23, aplicação PLC *PRIME Manager* na porta 7919, o serviço central de web na porta 8080, destinado à comunicação máquina a máquina, e um serviço de transferência de arquivo na porta 21.

A pesquisa utilizou duas ferramentas: a ferramenta de código aberto, *Open Vulnerability Assessment Scanner* (OpenVAS) e a ferramenta NESSUS. As ferramentas foram hospedadas em uma máquina virtual Kali Linux versão 7.0 em um computador de teste, conforme pode ser observado na Figura 3. A escolha dessas ferramentas, dentre as várias existentes no mercado, foi decorrente da sua popularidade, da facilidade de documentação, do número de *plugins* que definem os tipos de assinaturas que vão ser verificadas, e a cobertura dos números de CVE, em inglês, *Common Vulnerabilities and Exposures*, existente em sua base de vulnerabilidade.

Figura 3 – Topologia da rede de teste de varredura do concentrador de uma AMI



Fonte: Elaborado pelos autores.

A ferramenta OpenVAS é um *scanner* de vulnerabilidades com capacidade de realizar testes não autenticados e autenticados, testes de diversos protocolos industriais, e protocolos de Internet de alto e baixo nível. Além disso, a ferramenta permite ajustes de desempenho para verificações em larga escala e possui uma poderosa linguagem de programação para implementar qualquer tipo de teste de vulnerabilidade (GREENBONE NETWORKS, 2019).

Esse *scanner* executa, de forma eficiente, testes de vulnerabilidade de rede (termo oriundo do inglês, *Network Vulnerability Test* – NVT), os quais são suportados com atualizações diárias mediante um *feed* de NVT de um serviço comercial, com mais de 30.000 tipos de vulnerabilidades administrados pela *Greenbone* Networks, desenvolvedora do OpenVAS.

O *scanner* Nessus, assim como o OpenVAS, apresenta vários recursos para realizar as funções de escaneamento. Pode-se citar, por exemplo, varreduras com e sem credenciais, em redes IPv4, IPv6 ou híbrida e cobertura para os dispositivos de rede, tais como, *firewall*, roteadores e *switches* (NESSUS, 2020). Esse *scanner* também apresenta a capacidade de operação em sistemas virtualizados. O Nessus é desenvolvido e suportado pela *Tenable Network Security*.

Com o avanço das ameaças aos sistemas computacionais, o governo dos Estados Unidos da América, criou o *National Vulnerability Database* (NVD) que é um repositório de dados de gerenciamento de vulnerabilidades, baseado em padrões, cuja representação é embasada no protocolo denominado de *Security Content Automation Protocol* (SCAP). Esses dados permitem a automação do gerenciamento de vulnerabilidades e define parâmetros que permitem a medição do nível de segurança e análise de conformidade com as normas. O NVD inclui um banco de dados com referências a uma lista de verificação de segurança. Nessa lista estão incluídas falhas de software relacionadas à segurança, a configurações incorretas, à identificação de produtos e a métricas de impacto. Todas as vulnerabilidades registradas no NVD recebem um identificador administrado pelo serviço *Common Vulnerabilities and Exposures* (CVE) (MELL; SCARFONE; ROMANOSKY, 2007). Baseado no resultado das análises das vulnerabilidades, uma métrica de vulnerabilidade é definida, denominada de *Common Vulnerability Scoring System* (CVSS). Essa métrica é uma estrutura aberta que apresenta as características e a gravidade das vulnerabilidades de softwares.

O CVSS consiste em três grupos de métricas: base, temporal e ambiental. As métricas do tipo base produzem uma pontuação que varia de 0 a 10 e que pode ser modificada em função das pontuações das métricas temporal e ambiental. O *National Cybersecurity* FFRDC[1](NCF), operado pela *Mitre Corporation*, mantém o sistema de CVE com financiamento da Divisão Nacional de Segurança Cibernética do Departamento de Segurança Interna dos Estados Unidos (*National Cyber Security Division of United States Department of Homeland Security)*.

As ferramentas empregadas para o desenvolvimento dessa pesquisa, utilizam tanto o CVE quanto o CVSS para identificação, classificação e pontuação das vulnerabilidades encontradas durante o processo de varredura.

4 Resultados da pesquisa

Esta seção apresenta os resultados obtidos nos ensaios de varredura de vulnerabilidades. Esses resultados foram extraídos dos relatórios de verificação de segurança emitidos por meio das aplicações OpenVAS e Nessus.

4.1 Resultados do OpenVAS

O OpenVAS define o indicador de qualidade de detecção, termo oriundo do inglês, *Quality of Detection* (QoD), que descreve a confiabilidade da detecção de vulnerabilidade executada. Sua graduação é na escala de 0% a 100%. Apenas resultados com QoD superior a 70% são considerados na elaboração dos relatórios emitidos pela ferramenta. Durante as varreduras, foi utilizada a configuração padrão dos filtros do OpenVAS. A Figura 4 ilustra os parâmetros de configuração da tarefa de varredura de vulnerabilidade do OpenVAS.

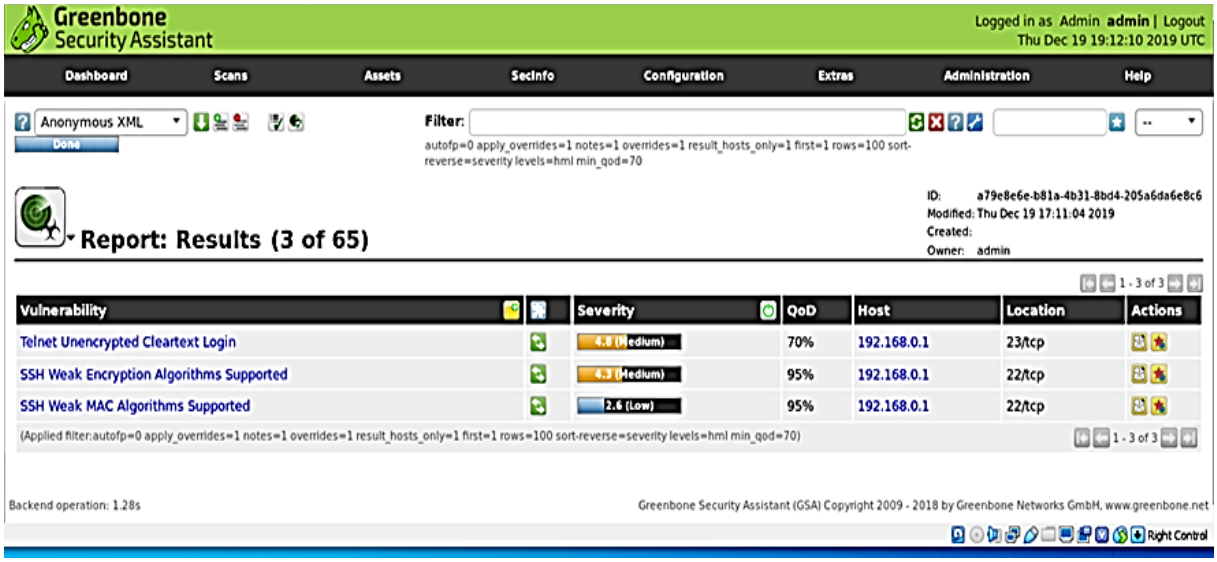
O OpenVAS, por meio de varreduras com duração de 34 minutos e 43 segundos, detectou 65 ocorrências de vulnerabilidades. Aplicando-se o critério de QoD superior a 70%, apenas três vulnerabilidades, foram consideradas relevantes, duas foram percebidas como de severidade média e uma foi vista como de severidade baixa, todas associadas aos serviços de acesso remoto Telnet e SSH. A Figura 5 ilustra a tela do OpenVAS com um fragmento do relatório das vulnerabilidades encontradas.

Figura 4 – Tela de resumo de configuração de tarefa do OpenVAS

Fonte: Resultados da pesquisa.

1 Federally Funded Research and Development Centers (FFRDCs).

Figura 5 – Tela do OpenVAS apresentando o resumo do relatório de varredura



Fonte: Resultados da pesquisa.

O detalhamento dessas vulnerabilidades é listado e discutido:

a) A vulnerabilidade, *SSH Weak Encryption Algorithms Supported*, associada à porta 22 do TCP, obteve uma graduação CVSS de 4.3, sendo considerada média. A varredura detectou que o algoritmo de criptografia associado ao SSH utiliza a cifra de fluxo Arcfour com chaves de 128 bits, compatível com o RC4. O Arcfour e o RC4 têm problemas quanto ao uso de chaves de criptografia fracas e não devem mais ser usados. O parâmetro "*none*" especifica que nenhuma criptografia deve ser realizada. Observa-se que esse método não oferece proteção de confidencialidade e o seu uso não é recomendado. Também foi detectada a existência de vulnerabilidades nas mensagens SSH que empregam o modo de cifra de bloco CBC. Esse tipo de cifra permite que um invasor recupere um texto pleno a partir de um bloco de texto cifrado;

b) A vulnerabilidade, Telnet *Unencrypted Cleartext Login*, associada à porta 23 do TCP, obteve uma graduação CVSS de 4.8, considerada média. A ferramenta detectou que o *host* remoto (concentrador) está executando um serviço Telnet que permite *logins* utilizando texto não criptografado em conexões não criptografadas. Um atacante pode descobrir nomes e senhas de *logon* acessando o serviço Telnet. Para minimizar o problema, recomenda-se a utilização de um protocolo que usa conexões encriptadas, como por exemplo, o SSH;

c) O teste NVT do tipo e a SSH Weak MAC *Algorithms Supported* aplicado à porta 22 do TCP, obteve uma graduação CVSS de 2.6, considerada baixa. O resultado da detecção indica que os algoritmos MAC, hmac-md5 e hmac-sha1-96, que são suportados pelo serviço remoto, são considerados fracos. Esses algoritmos podem ser configurados tanto para a comunicação de cliente para servidor como de servidor para cliente. A ferramenta indica a desativação desse algoritmo para mitigar essa vulnerabilidade.

4.2 Resultados da ferramenta Nessus

O relatório de varredura do Nessus apresenta um total de 27 ocorrências de vulnerabilidades, das quais seis foram consideradas significativas, distribuídas em duas ocorrências com severidade baixa, duas com severidade média, uma com severidade alta e uma com vulnerabilidade crítica. A Figura 6 ilustra um fragmento do relatório das vulnerabilidades encontradas. A ferramenta Nessus utiliza um sistema de *plugin* que referencia o detalhamento das vulnerabilidades em seu site. O detalhamento das vulnerabilidades encontradas é listado e discutido:

a) A vulnerabilidade, Dropbear SSH Server 2016.72 Multiple Vulnerabilities, associado à porta 22 do TCP, obteve uma graduação de CVSS 10, considerada crítica. O relatório de varredura indica que, de acordo com a versão referenciada em seu *banner*, o Dropbear SSH em execução no *host* remoto é anterior à versão 2016.74 e é afetado por várias vulnerabilidades conforme listadas:

– Existe uma falha na *string* de formato devido ao manuseio inadequado de especificadores de formato de *string* (por exemplo, %s e %x) nos nomes de usuário e argumentos do *host*. Um invasor remoto não autenticado pode explorar esse fato para executar código arbitrário com privilégios de *root*. (CVE-2016-7406);

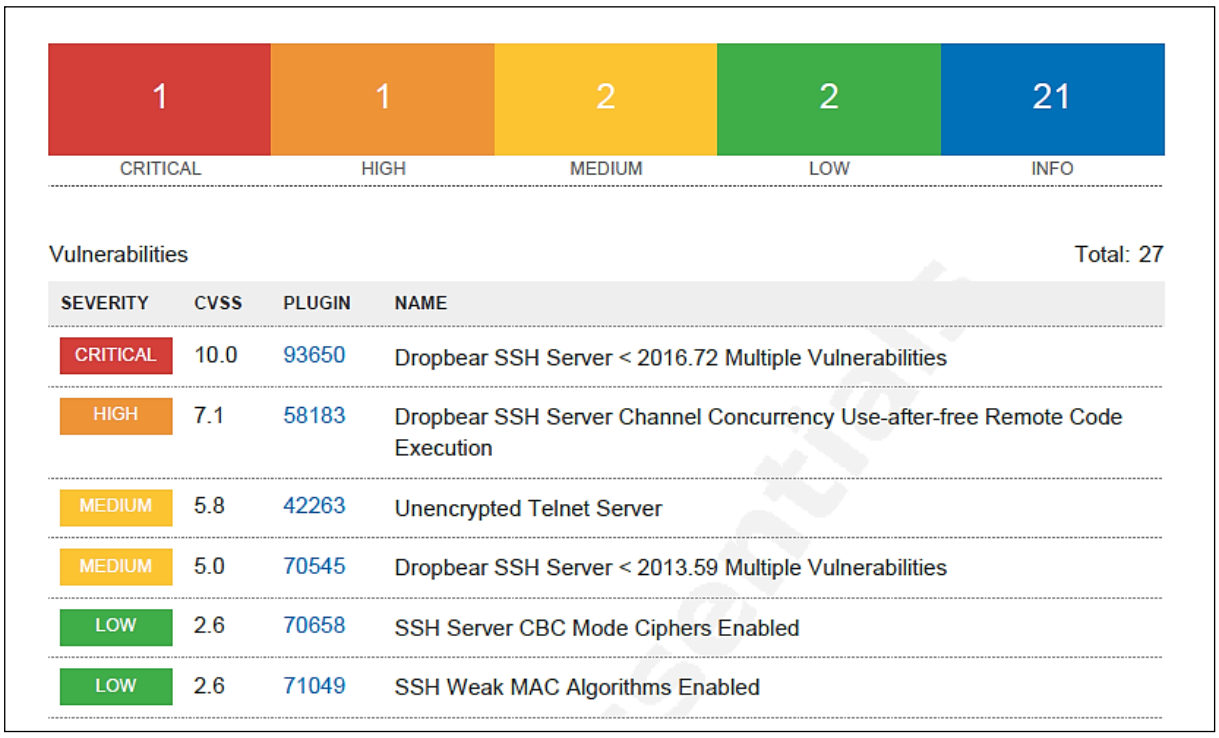
– Existe uma falha no *dropbearconvert* devido ao manuseio inadequado de arquivos-chave OpenSSH especialmente criados. Um invasor remoto não autenticado pode explorar esse fato para executar código maliciosos. (CVE-2016-7407).

– Existe uma falha no *dbclient* ao manipular os argumentos -m ou -c nos *scripts*. Um invasor remoto não autenticado pode explorar isso, por meio de um *script* especialmente criado, para executar código malicioso (CVE-2016-7408);

– Existe uma falha no servidor *dbclient* ou *dropbear*, caso haja compilação com a opção *DEBUG_TRACE* e, em seguida, executados usando a opção -v. Um invasor local pode explorar isso para divulgar a memória do processo. (CVE-2016-7409). O relatório da ferramenta sugere como solução, a atualização do SSH do *host* remoto (concentrador) para a versão igual ou superior a 2016.74.

b) A vulnerabilidade *Dropbear SSH Server Channel Concurrency Use-after-free Remote Code Execution*, também associada à porta 23, obteve uma graduação de severidade CVSS de 7.1, sendo considerada crítica. Conforme o seu *banner* autorrelatado, o concentrador está executando uma versão do *Dropbear SSH* anterior à versão 2012.55. Como tal, ele contém uma falha que pode permitir que um invasor possa executar código arbitrário no concentrador com privilégios de *root* se ele for autenticado usando uma chave pública e se a restrição de comandos for aplicada. Observe que a ferramenta Nessus não tentou explorar essa vulnerabilidade, mas confiou apenas na versão do serviço obtida através do *banner* do serviço que foi apresentado. Como solução, o relatório apresenta a atualização do SSH para uma versão do *Dropbear* SSH igual ou superior a 2012.55;

Figura 6 – Fração do relatório de vulnerabilidade do Nessus para concentrador AMI



Fonte: Resultados da pesquisa.

c) A vulnerabilidade, *Unencrypted* Telnet Server, associada à porta 23 do TCP, apresentou uma severidade CVSS de 5.8, considerada média. O relatório indica que o servidor Telnet remoto transmite o tráfego em texto não criptografado. O uso do Telnet em um canal não criptografado não é recomendado, uma vez que *logons*, senhas e comandos são transferidos em texto pleno. Isso permite que um

invasor remoto, entre os dois terminais, interaja com uma sessão Telnet para obter credenciais ou outras informações confidenciais, permitindo a modificação do tráfego trocado entre um cliente e um servidor. O relatório recomenda o uso do SSH, pois protege as credenciais da interceptação e pode encapsular fluxos de dados adicionais;

d) A vulnerabilidade, *Dropbear* SSH Server 2013.59 *Multiple Vulnerabilities*, associada à porta 22, obteve uma graduação de severidade CVSS de 5.0, classificada como de vulnerabilidade média. O relatório indica, baseado no *banner* autorrelatado, que a versão do *Dropbear* SSH em execução nessa porta é anterior à 2013.59, afetada por várias vulnerabilidades conforme listadas:

– Uma vulnerabilidade de negação de serviço causada pela forma como a função "*buf_decompress* ()" lida com arquivos compactados (CVE-2013-4421);

– A enumeração do usuário é possível devido a um erro de tempo durante a autenticação dos usuários. (CVE-2013-4434). A recomendação da ferramenta é a atualização da versão do *Dropbear SSH* para a versão 2013.59 ou à posterior.

e) A vulnerabilidade, SSH Server CBC *Mode Ciphers Enabled*, também associada ao serviço SSH, obteve uma graduação de severidade CVSS de 2.6, considerada baixa. O relatório indica que o servidor SSH está configurado para oferecer suporte à criptografia *Cipher Block Chaining (CBC)*. Isso pode permitir que um invasor recupere a mensagem de texto claro baseado no texto cifrado. O *plug-in* verifica apenas as opções do servidor SSH e não verifica versões de software vulneráveis. O relatório apresenta como solução desativar a criptografia baseada no modo de cifra de bloco CBC e habilitar a criptografia que usa outros modos de cifra de bloco. Os modos de cifra contador (CTR) ou contador de Galois (GCM) são exemplos de tipo de cifra de bloco que podem ser utilizados nesse contexto;

f) A vulnerabilidade, SSH *Weak* MAC *Algorithms Enabled*, apresenta uma graduação de severidade CVSS de 2.6, considerada baixa. O relatório indica que o servidor SSH remoto está configurado para permitir algoritmos criptográficos MD5 ou código MAC de 96 bits, ambos considerados fracos. Esse *plug-in* verifica apenas as opções do servidor SSH e não verifica versões de software vulneráveis. A recomendação apresentada no relatório de varredura da ferramenta é o usuário contatar o fornecedor ou consultar a documentação do produto para desativar os algoritmos MD5 e o código MAC de 96 bits.

Diferentemente do ambiente de Tecnologia da Informação (TI), os recursos de segurança cibernética em ambiente de Tecnologia de Automação (TA) ou operação (TO), estão em níveis diferentes da área de TI. Isso é decorrente a fatores como dispositivos com baixo poder computacional, resposta em tempo real, e algoritmos de criptografia com elevado custo computacional e diversas tecnologias emergentes ainda não consolidadas. A tarefa de realizar a análise de vulnerabilidade em infraestrutura AMI, ainda não é usual, e os estudos dessa análise, estão em um estado embrionário. O trabalho apresenta como contribuição uma metodologia de análise de vulnerabilidade em uma plataforma que emula um sistema real de infraestrutura AMI, expondo os resultados, as dificuldades e as restrições impostas pelo contexto dos testes dessa infraestrutura.

5 Considerações Finais

Os estudos mostram que a infraestrutura de comunicações AMI está sujeita a vulnerabilidades. Essas vulnerabilidades podem ser desde modificações dos dados do medidor para obter vantagens indevidas, até interrupções no fornecimento de um usuário ou grupo de usuários. Mapear e gerenciar essas vulnerabilidades é fundamental para a operação de uma infraestrutura AMI dentro dos padrões desejados pela sociedade e pelos órgãos regulamentadores. O trabalho apresenta testes de vulnerabilidade em um concentrador de dados, componente da rede de vizinhança. Apesar do MDMS ser o coração do sistema, o concentrador foi escolhido para este estudo. Essa escolha se deu pelo fato de o MDMS estar localizado nas edificações da concessionária, com um esquema de proteção superior aos demais componentes da rede (segurança de perímetro, *firewalls*, controle de acesso).

Diferente do MDMS, o concentrador está localizado em via pública, processando uma quantidade razoável de tráfego da rede de vizinhança e sua comunicação pode ser monitorada por uma derivação implantada por um atacante. Caso o concentrador seja compromissado, é possível afetar todo o sistema de aquisição de informações da AMI.

O resultado do trabalho demonstrou a existência de vulnerabilidades em concentradores de dados da infraestrutura AMI sob estudo. Observou-se que, mesmo utilizando ferramentas de varredura de vulnerabilidades diferentes, o resultado convergiu para a identificação de vulnerabilidades semelhantes,

indicando coerência entre as ferramentas, nesse caso, vulnerabilidades múltiplas, associadas aos serviços de acesso remoto Telnet e SSH. Para evitar problemas de segurança no futuro, essas vulnerabilidades devem ser tratadas por meio de atualizações de correções.

As vulnerabilidades detectadas, obtiveram graus de severidade diversos, abrangendo desde vulnerabilidades consideradas baixas até vulnerabilidades percebidas como críticas. O trabalho, além do objetivo de avaliar o nível de segurança do concentrador, demonstra a importância do gerenciamento de vulnerabilidades que deve ser considerado, desde a fase de implantação até a operação final de um sistema AMI.

Todas as vulnerabilidades encontradas têm *patches* de correção e, tomando-se os devidos cuidados, o sistema terá o nível de segurança adequado. As ferramentas utilizadas não consideram vulnerabilidades *zero day*, ou seja, vulnerabilidades que ainda não foram detectadas, ou até foram, mas não têm *patches* de correção dos fabricantes.

Para complementação desses estudos, os autores sugerem como trabalho futuro, a realização de estudos de vulnerabilidade envolvendo a DMZ e as portas de comunicações do concentrador que ficaram fora do escopo deste trabalho. Além disso, trabalhos podem ser realizados em relação ao uso de ferramentas que correlacionem as vulnerabilidades detectadas com os riscos para cada serviço em cada nível de aplicação. Dessa forma, ter-se-ía uma avaliação precisa dos prejuízos para os sistemas de medições inteligentes entre os consumidores e a concessionária.

AGRADECIMENTOS

Este trabalho recebeu financiamento e suporte técnico da CPFL Energia no âmbito do projeto "PA3046 - Desenvolvimento de Plataforma de Medição Inteligente com *Cybersecurity, Business Intelligence e Big Data*", que é um programa P&D regulado pela ANEEL, Brasil. Os autores também agradecem ao apoio do IATI (Instituto Avançado de Tecnologia e Inovação) e da Time Energy pelo fornecimento da infraestrutura e das informações necessárias para a realização dos ensaios.

REFERÊNCIAS

ABDULLAH, M. D. H. *et al.* Attacks, vulnerabilities and security requirements in smart metering networks. **KSII Transactions on Internet & Information Systems**, v. 9, n. 4, p. 1493-1515, 2015.

ALOUL, F. *et al.* Smart grid security: threats, vulnerabilities and solutions. **International Journal of Smart Grid and Clean Energy**, v. 1, n. 1, p. 1-6, 2012.

DUTRA, J. C. *et al.* **Redes elétricas inteligentes no Brasil**: subsídios para um plano nacional de implantação. 2. ed. Rio de Janeiro (Brasil): Synergia, 2013.

GREENBONE NETWORKS. **Greenbone security manager with Greenbone OS 6**: user manual. [s.i.], 2019. Disponível em: https://bit.ly/320ZokO. Acesso em: dez. 2019.

GUI, Y. *et al.* Security vulnerabilities of smart meters in Smart Grid. *In*: IECON 2019 – 45th ANNUAL CONFERENCE OF THE IEEE INDUSTRIAL ELECTRONICS SOCIETY, 2019, Lisbon (Portugal). p. 3018-3023.

GUNGOR, V. C. *et al.* A survey on smart grid potential applications and communication requirements. **IEEE Transactions on Industrial Informatics**, v. 9, n. 1, p. 28-42, 2012.

LIU, Y.; HU, S.; HO, T.-Y. Vulnerability assessment and defense technology for smart home cybersecurity considering pricing cyberattacks. *In*: 2014 IEEE/ACM INTERNATIONAL CONFERENCE ON COMPUTER-AIDED DESIGN (ICCAD), 2014, San Jose (United States). 2014. p. 183-190.

MELL, P. M.; SCARFONE, K. A.; ROMANOSKY, S. Complete guide to the Common Vulnerability Scoring System 2.0. National Institute of Standards and Technology (NIST), 2007.

MORENO, D. **Introdução ao Penteste**. 2. ed. São Paulo (Brasil): Novatec, 2017.

NAKAMURA, E. T.; DE GEUS, P. L. **Segurança de redes em ambientes cooperativos**. São Paulo (Brasil): Novatec, 2007.

NAMBOODIRI, V. *et al.* Toward a secure wireless-based home area network for metering in smart grids. **IEEE Systems Journal**, v. 8, n. 2, p. 509-520, 2013.

NESSUS. Welcome to Nessus 8.8.x. 2020. Disponível em: https://bit.ly/2GzssI4. Acesso em: dez. 2019.

PARK, C. H.; KIM, T. Energy theft detection in advanced metering infrastructure based on anomaly pattern detection. **Energies**, v. 13, n. 15, p. 1-13, 2020.

SKOPIK, F. *et al*. A survey on threats and vulnerabilities in smart metering infrastructures. **International Journal of Smart Grid and Clean Energy**, v. 1, n. 1, p. 22-28, 2012.

SOREBO, G. N.; ECHOLS, M. C. **Smart grid security:** an end-to-end view of security in the new electrical era. CRC Press: Boca Raton (United States), 2011.

WEIDMAN, G. **Penetration testing**: a hands-on introduction to hacking. San Francisco (United States): Starch Press, 2014.

XIAO, Y. **Security and privacy in smart grids**. CRC Press, 2013.