AVALIAÇÃO DE VULNERABILIDADES EM ELEMENTOS DE AUTOMAÇÃO DE SUBESTAÇÃO

AZEVEDO, Huliano F. M. de [1]
SOUZA, Ronaldo Rocha de [2]
LIMA, José A. G. de[3]

RESUMO

A segurança cibernética nas instalações de geração, transmissão e distribuição de energia elétrica tem constituído um desafio contínuo de todas as empresas destes setores, considerando a necessidade de cada vez mais compartilharem informações operacionais entre si e o crescente fluxo de dados entre redes e equipamentos diferentes, conduz a cenários de mais exposição e vulnerabilidades. Os sistemas de proteção e automação de subestações (SAS), no seu início, caracterizavam-se pela sua arquitetura fechada com protocolos de comunicação proprietários separados de outros sistemas. Atualmente, os SAS migraram em sua grande parte, para arquiteturas abertas com redes quase que totalmente integradas com a infraestrutura de TI. Este trabalho justifica-se pela particularidade e importância das subestações inteligentes em toda a vida produtiva nacional, sendo as ameaças que enfrentam mais direcionadas e destrutivas. Para o desenvolvimento deste artigo, inicialmente foi feita uma pesquisa bibliográfica dos principais guias das certificações voltadas para segurança cibernética. A literatura consultada subsidiou a pesquisa e avaliação de vulnerabilidades baseada nas ferramentas *open source* Nmap *(Network Mapper)* e OpenVAS *(Open Vulnerability Assessment System)* em uma rede montada em laboratório. Por fim, os testes de vulnerabilidades realizados, classificamos as ameaças de acordo com os critérios de impacto definidos pelo scanner e avaliamos os riscos de maior severidade identificados no ambiente de testes.

Palavras-chave: Cibersegurança, Automação, Nmap, OpenVAS, CVSS.

[1] Graduando em Engenharia Elétrica pelo Centro Universitário UNINTER.
[2] Graduando em Engenharia Elétrica pelo Centro Universitário UNINTER.
[3] Especialista em Inovações no Ensino de Matemática, Especialista em Engenharia de Produção, Licenciatura Plena em Matemática, Bacharel em Engenharia Elétrica. Orientador de TCC no Centro Universitário UNINTER, Professor na rede pública de ensino, Professor corretor de provas discursivas EAD no Centro Universitário UNINTER.

1 INTRODUÇÃO

A automação das subestações coopera decisivamente na mitigação dos erros causados pela operação humana e também melhora a eficiência da interação de informações e controle dos equipamentos, o que desenvolve muito a segurança e a confiabilidade na operação de todo o Sistema Elétrico de Potência. Entretanto, com a escalada de aplicações em rede, fragilidades comuns no meio cibernético são reveladas. O tema pesquisado justifica-se pela questão das crescentes ameaças de segurança cibernética em sistemas de automação de subestações e com base nisso, justificou a pesquisa teórica que embasou a realização de testes de vulnerabilidades com base em ferramentas *open source*.

Este artigo tem como objetivo geral destacar os principais conceitos relacionados ao setor elétrico e a área de cibersegurança e também, apresentar o experimento realizado em um ambiente de testes.

Dentro deste contexto, o artigo tem como objetivos específicos apresentar algumas ferramentas *open source* para avaliação de vulnerabilidades, descrever seu funcionamento e aplicação no ambiente de testes e coletar os dados gerados para diagnóstico dos elementos de rede. O estudo limitou-se a não incluir demais testes que de que integram o *penetration test* e o *ethical hacking*.

Durante a revisão bibliográfica foi encontrado um grande acervo acadêmico (artigos, teses e dissertações) referentes a segurança da informação e automação. Dentre os trabalhos relacionados consultados para este estudo, destaca-se o trabalho de Barbosa *et al.* (2020) na implementação de uma metodologia de avaliação dos riscos em uma planta industrial, com utilização de uma ferramenta *open source* para avaliação. Já Yongiun *et al.* (2020) desenvolveu um sistema de escaneamento de vulnerabilidades aplicado a um sistema de automação de subestação.

O artigo está organizado da seguinte forma: no Capítulo 2, para fundamentação teórica, são apresentados conceitos do sistema elétrico, sistema de proteção e automação de subestações e de cibersegurança. Em seguida, o Capítulo 3 apresenta a metodologia adotada, infraestrutura e ferramentas computacionais utilizadas. No Capítulo 4 são apresentados os resultados obtidos, bem como a análise acerca dos

mesmos. Por fim, o Capítulo 5 conclui o artigo, ressaltando os resultados alcançados e também trabalhos futuros que podem ser desenvolvidos.

2 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo apresentam-se os principais conceitos relacionados ao setor elétrico e a área de cibersegurança, com objetivo de contextualizar o trabalho produzido e justificar o estudo.

2.1 SISTEMA ELÉTRICO DE POTÊNCIA (SEP)

O SEP possui como objetivo principal fornecer energia aos consumidores finais e que este fornecimento é realizado através dos processos de geração, transmissão e distribuição de energia elétrica. (LOPES, 2013). No Brasil, o SEP possui uma divisão bastante clara e hierarquizada entre sistemas e é conhecido como Sistema Interligado Nacional (SIN) e o seu coordenador e controlador, o Operador Nacional do Sistema (ONS, 2021) define como:

> Sistema de produção e transmissão de energia elétrica do Brasil é um sistema hidro-termo-eólico de grande porte, com predominância de usinas hidrelétricas e com múltiplos proprietários. O Sistema Interligado Nacional é constituído por quatro subsistemas: Sul, Sudeste/Centro-Oeste, Nordeste e a maior parte da região Norte (ONS, 2021).

Dentro destes sistemas, os elementos de maior importância são:

- Geração: Na geração, as usinas são classificadas conforme os recursos que utilizam, podendo ser hidroelétricas, termoelétricas, eólicas, nucleares, fotovoltaicas, etc. Ocorre nesta etapa, a conversão de um tipo de energia (cinética, térmica) em energia elétrica.
- Transmissão e Distribuição: Lopes (2013, p. 9) descreve esses sistemas como condução da energia elétrica das usinas de geração até os

consumidores. Após gerada, a tensão é elevada a altos níveis de tensão, para que se minimize as perdas e otimize o transporte de grandes blocos de potência, normalmente por longas distâncias entre os centros de geração e os centros de consumo.

- Subestação: Subestações são instalações responsáveis por aumentar ou diminuir os níveis de tensão na transmissão e na distribuição. Lopes (2013, p. 9) cita que seu funcionamento é autônomo, normalmente suportados por sistemas tipo SCADA *(Supervisory Control and Data Acquisition)* para controle e supervisão remotos. Internamente, a subestação também desempenha funções de comutação, proteção e controle.

2.1.1 Sistema de Proteção e Automação de Subestações (SAS)

As concessionárias dos sistemas de energia apresentam, como uma das principais metas, garantir economicamente a qualidade do serviço e assegurar uma vida razoável às instalações e equipamentos elétricos, entretanto estas empresas enfrentam perturbações e anomalias na operação que afetam as redes elétricas e seus dispositivos de controle. (COURY, 2007).

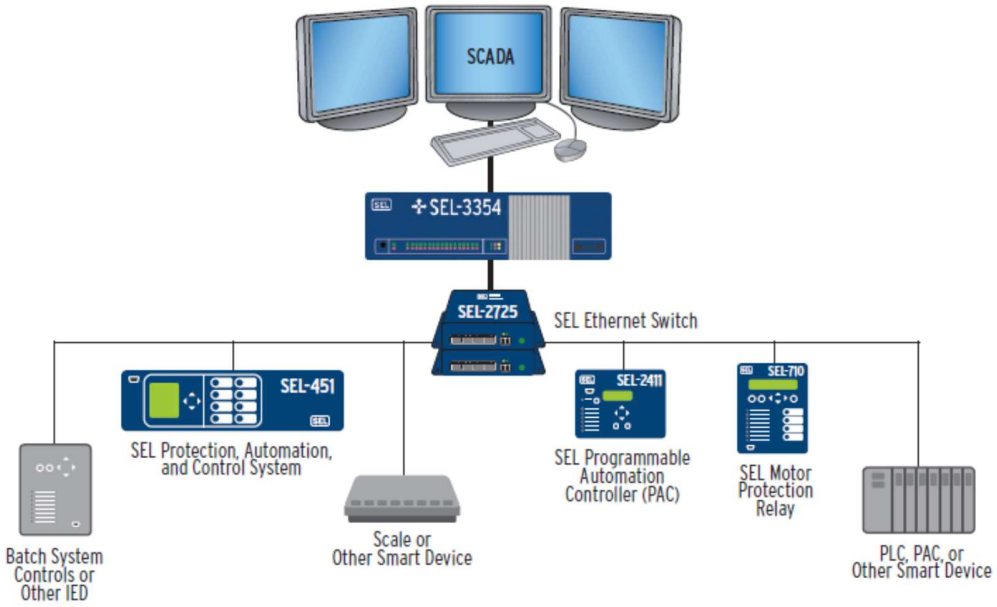
Logo, para atenuar os efeitos das perturbações ou condições anormais, Coury (2007, p. 21) explica que o sistema de proteção deve assegurar, o melhor possível, a continuidade de dos consumidores, bem como salvaguardar o material e as instalações da rede. Neste sentido, o sistema de proteção deve tanto alertar os operadores em caso de perigo não imediato como retirar de serviço a instalação se há, por exemplo, um curto-circuito que arriscaria danificar um equipamento ou afetar toda a rede.

Coury (2007, p. 21) ainda explica que embora o sistema de proteção seja usualmente associado aos relés de proteção, este consiste de muito subsistemas que atuam no processo de remoção da falta, controle e supervisão do sistema elétrico. Com o desenvolvimento dos relés de proteção, que advieram a ter características microprocessadas, o SAS vem mudando para se adaptar a esse novo cenário. Lopes

(2013, p. 11) explica que os relés passaram a ter funções adicionais e, além da proteção, passam a controlar e registrar eventos, medidas, etc.

Na Figura 1 temos uma arquitetura de um SAS típico, do fabricante *Schweitzer Engineering Laboratories, Inc.* (SEL).

Figura 1. Arquitetura de um SCADA típico



Fonte: SEL, 2011

2.1.2 Sistemas SCADA

Sistemas supervisórios são sistemas digitais de monitoração e operação de plantas que gerenciam variáveis de processo. Estas são atualizadas continuamente e podem ser armazenadas em bancos de dados locais ou remotos para fins de registro histórico. (AZEVEDO, 2010). O Centro de Pesquisas de Energia Elétrica (CEPEL)[4], desenvolvedor do Sistema Aberto de Gerenciamento de Energia (SAGE), o supervisório mais utilizado no sistema elétrico brasileiro define:

[4] O Centro de Pesquisas de Energia Elétrica - CEPEL tem por objetivo principal e permanente preservar a capacidade em pesquisa, desenvolvimento, inovação, qualificação e capacitação na área de sistemas elétricos e disciplinas correlatas. A ELETROBRAS e suas empresas subsidiárias são os associados fundadores da instituição.

> O SAGE é um SCADA/EMS robusto, modular e expansível, aplicável na supervisão e controle de subestações, usinas, centros regionais e centrais, sistemas de distribuição e em redes de centros de controle. Possui capacidade de aquisição e distribuição através de grande biblioteca de protocolos nativos. Inclui, ainda, funções avançadas de Análise de Redes elétricas em tempo real, modo de simulação para estudos elétricos, previsão de cargas, automação de manobras e funções de concentrador de dados sincrofasoriais. (CEPEL, 2022).

O SEP depende, em sua totalidade, dos recursos disponibilizados pelos softwares SCADA para supervisão e controle das instalações de geração, transmissão e distribuição de energia. O SAGE foi o software SCADA utilizado em nosso laboratório, com a versão 2014-27 em plataforma Linux CentOS 6.8.

2.2 CIBERSEGURANÇA

Qualquer dispositivo conectado a uma rede está exposto e precisa de segurança cibernética. Isso compreende os computadores e todos os demais equipamentos que compõem a infraestrutura crítica do SEP. Santos (2021, p. 52) descreve que o objetivo da cibersegurança é:

> Proteger cada um de nós, nossa economia, nossas infraestruturas críticas e qualquer outra organização dos danos que podem resultar de uso inadvertido ou intencional, comprometimento ou destruição de informações e sistemas de informação (SANTOS, 2021, p. 52).

Os cibercriminosos têm o *know-how* e os instrumentos necessários para interferir nas infraestruturas críticas e sistemas. Os ativos devem ser identificados e protegidos. Johnson (2020, p. 285) recomenda que as vulnerabilidades devem ser abordadas antes que se tornem ameaças e as técnicas de mitigação são necessárias antes, durante e depois de um ataque. (JOHNSON, 2020).

Os ativos estão sujeitos a diversos eventos e potencialidades prejudiciais à sua segurança, divididos em três categorias: ameaças, vulnerabilidades e incidentes, os quais compõem e caracterizam os riscos. (AZEVEDO, 2010).

2.2.1 A tríade da CIA

Confidencialidade, integridade e disponibilidade são comumente chamadas de tríade da CIA. Este modelo foi criado para definir políticas de segurança e o conceito é que a confidencialidade, integridade e disponibilidade devem ser garantidos em qualquer sistema que seja considerado.

- Confidencialidade: Barbosa e Reis (2020, p. 2) conceitua que confidencialidade é a obrigação de proteger os segredos das pessoas ou de uma organização. Na prática, garante a privacidade dos dados, restringindo o acesso através das políticas e garantindo que apenas os indivíduos autorizados visualizam esses dados.
- Integridade: Você também precisa garantir que os dados não sejam alterados incorretamente. A criptografia ajuda a garantir a integridade dos dados em repouso, mas não é a melhor opção para dados em movimento. Em vez disso, o *hash* é normalmente aplicado (SVIDERGOL, 2021).
- Disponibilidade: Refere-se a garantir alta disponibilidade de serviços e dados, podendo utilizar técnicas como resiliência de site, *failover* automático, balanceamento de carga, redundância de componentes de hardware e software e tolerância a falhas (SVIDERGOL, 2021).

2.2.2 Ameaças, Vulnerabilidades e Explorações

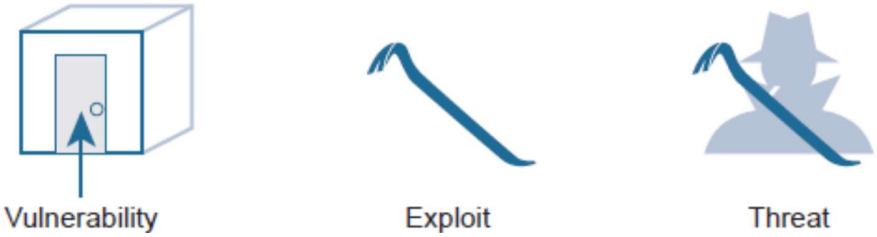
Existe uma terminologia específica que é usada para descrever suas ferramentas e ataques (JOHNSON, 2020). A seguir, descreveremos os principais termos de segurança:

- Ativos: Qualquer coisa de valor para a organização, incluindo pessoas, equipamentos, recursos e dados.
- Vulnerabilidade: Uma fraqueza no sistema ou em seu design que pode ser explorada por uma ameaça.

- *Threat:* Um perigo potencial (ameaça) para os ativos, dados ou funcionalidade de rede de uma empresa.
- *Exploit:* Um mecanismo que tira proveito de uma vulnerabilidade.
- Risco: A probabilidade de uma ameaça explorar a vulnerabilidade de um ativo, com o objetivo de afetar negativamente uma organização.

Na Figura 2 é representada uma analogia entre a terminologia apresentada e uma incursão a uma propriedade.

Figura 2. Analogia entre a terminologia apresentada e uma invasão



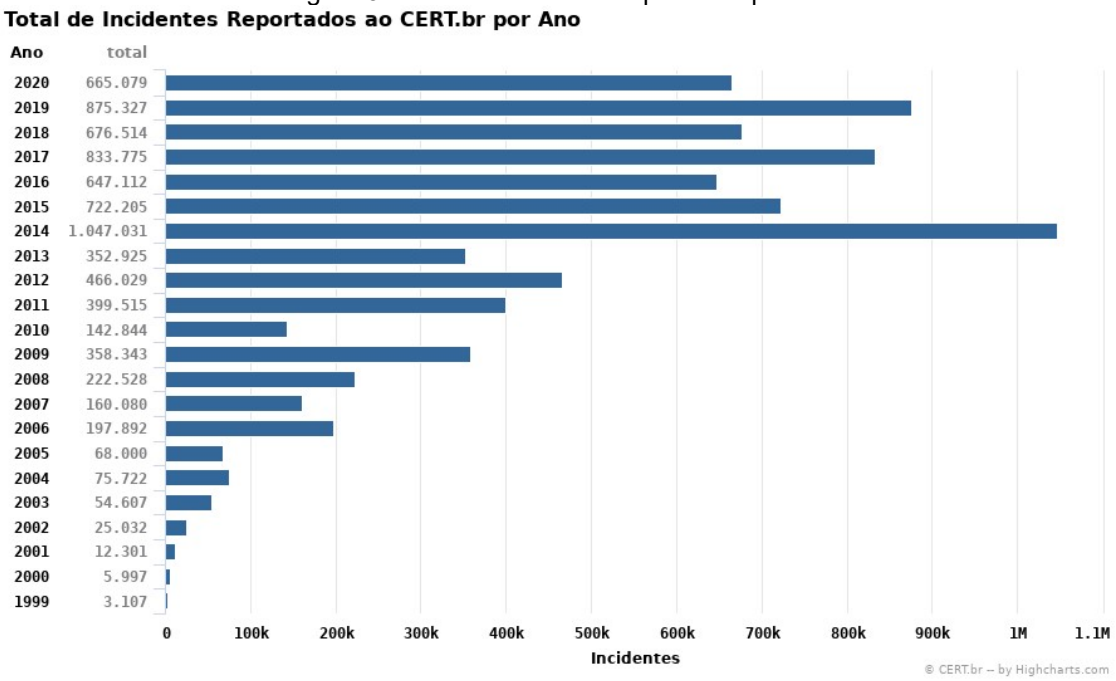
Fonte: Adaptado de (ODOM, 2019)

2.2.3 Incidentes

Azevedo (2010, p.34) esclarece que incidente é um evento que envolve uma violação que pode comprometer a confidencialidade, integridade e a disponibilidade da informação. Conforme apresentado na Figura 3, centenas de milhares de incidentes são reportados ao CERT.br[5], por ano, só no Brasil.

[5] O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) é um Grupo de Resposta a Incidentes de Segurança (CSIRT) de responsabilidade nacional, mantido pelo NIC.br, do Comitê Gestor da Internet no Brasil.

Figura 3. Total de incidentes reportados por ano



Fonte: CERT.br, 2022

3 METODOLOGIA

A metodologia adotada neste artigo foi baseada nas seguintes etapas: estudo e compreensão dos principais conceitos de segurança cibernética, através de uma pesquisa bibliográfica dos principais guias de estudo para as certificações de rede como a *Cisco Certified Network Associate (CCNA)* e de segurança, tal como a *Certified Information System Security Professional (CISSP)* e a *Cisco CyberOps Associate (CBROPS).*

Já na etapa constituída por uma pesquisa de campo, foi instalado em um notebook o sistema operacional Kali Linux, sistema este que dispos das ferramentas de testes Nmap e OpenVAS. O passo seguinte consistiu na ativação de uma rede com quatro equipamentos "alvos" e a realização dos testes de varredura de vulnerabilidades com as ferramentas seleciondas no Kali Linux. E por fim, a classificação e análise das vulnerabilidades encontradas pelo padrão CVSS.

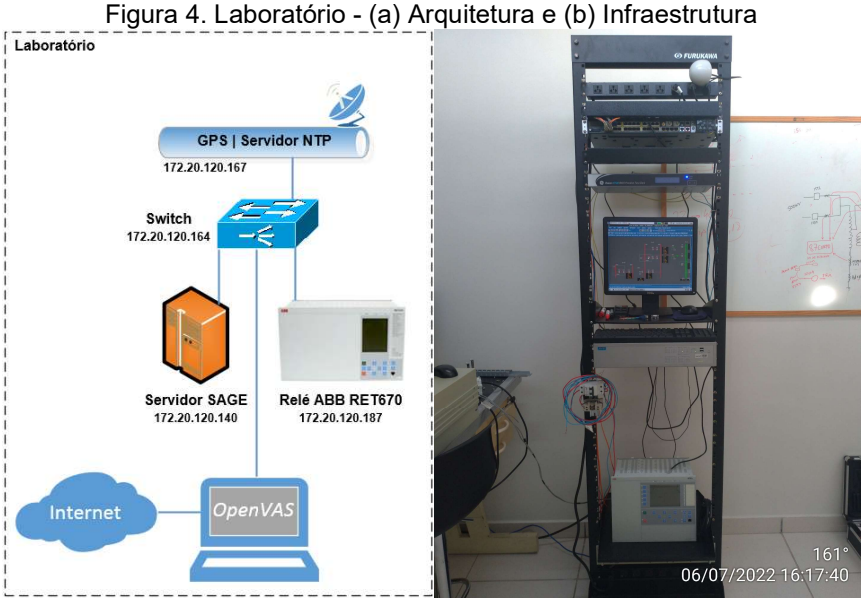
3.1 INFRAESTRUTURA DE TESTES

No ambiente de testes foi utilizado um notebook Acer Aspire V3-571-9423 com processador Intel® Core™ i7-3632QM 2.2GHz, 8 GB de memória RAM com sistema operacional Windows 10 Home, versão 21H1. Esse sistema suportou a virtualização da distribuição Kali Linux 2022.2[6] através do VMware® Workstation 8.0.3.

Como dispositivos alvos *(targets)* foram disponibilizados 04 (quatro) equipamentos:

a) **Relé ABB RET670**: *Intelligent Eletronic Device* com função de proteção para transformadores de dois a três enrolamentos, fabricado pela ABB.
b) **Servidor SAGE**: Computador industrial, fabricante ADVANTECH e com sistema SCADA SAGE.
c) **GPS | Servidor NTP**: Servidor de tempo sincronizado por satélites GPS e GLONASS, modelo RT430 e fabricado pela GE.
d) **Switch**: Switch industrial, modelo IE 5000 e fabricado pela Cisco.

Figura 4. Laboratório - (a) Arquitetura e (b) Infraestrutura



(a) (b)

Fonte: Elaborado pelo autor, 2022

[6] Kali Linux é uma distribuição Linux de código aberto, baseada em Debian, destinada a testes avançados de penetração e auditoria de segurança.

3.2 FERRAMENTAS

O Kali Linux dispõe de diversas ferramentas voltadas para várias tarefas de segurança da informação, como teste de penetração, pesquisa de segurança, computação forense e engenharia reversa (KALI, 2022). Em nossos testes, utilizamos as ferramentas *open source* Nmap *(Network Mapper)* e OpenVAS *(Open Vulnerability Assessment System).*

3.2.1 Nmap

O *Nmap* é uma ferramenta *open source* utilizada para auditoria de segurança e descoberta de rede desenvolvida e suportada pela *Nmap Software LLC*. Com esta ferramenta é possível determinar quais ativos estão em funcionamento na rede, incluindo nome, versão de aplicação, sistema operacional, portas em meio a outras informações. Utilizamos a versão 7.92 em nossos testes (ARAÚJO, 2018).

3.2.2 OpenVAS

O OpenVAS é uma ferramenta de código aberto estruturado de varredura de vulnerabilidades *(scanner)* que integra várias funções, sendo atualmente desenvolvido e suportado pela *Greenbone Networks GmbH*. Para nosso laboratório foi utilizada a versão 21.4.3.

Ele pode escanear um *host* na rede e, em seguida, analisar a ameaça do dispositivo de destino de acordo com as informações contidas na sua biblioteca de vulnerabilidades (YONGIUN, 2020).

4 RESULTADOS E DISCUSSÕES

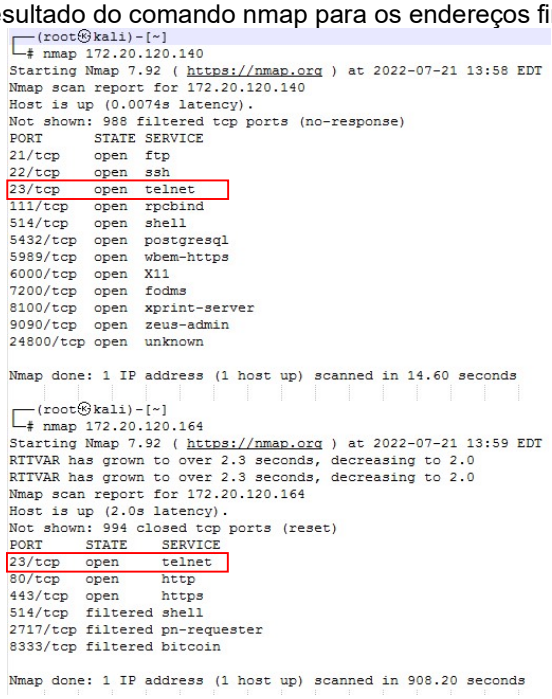
4.1 VARREDURA COM A FERRAMENTA NMAP

As simulações realizadas reproduziram algumas ações que um invasor poderia efetuar durante uma tentativa de intrusão a algum *host* especifico na rede. A comunicação entre os dispositivos na nossa infraestrutura de testes ocorre por meio de mensagens MMS sobre o protocolo TCP/IP e esta característica por si só, já é uma vulnerabilidade devido ao fato deste protocolo ser amplamente utilizado e de total domínio por *hackers*.

O *hacker* que acessa essa rede deve inicialmente, encontrar dispositivos vulneráveis, descobrir quais portas estão abertas e seu sistema operacional.

O teste foi efetuado com o comando `nmap <ip do host>`, sendo obtida a listagem das portas TCP abertas. Importante ressaltar que o Nmap dispõe de diversos outros recursos avançados, mas para nosso laboratório, esse comando atende a necessidade. Na Figura 5 pode ser conferido o resultado da varredura para os endereços 172.20.120.140 e 172.20.120.167.

Figura 5. Resultado do comando nmap para os endereços finais .140 e .164



```
┌──(root㉿kali)-[~]
└─# nmap 172.20.120.140
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-21 13:58 EDT
Nmap scan report for 172.20.120.140
Host is up (0.0074s latency).
Not shown: 988 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
111/tcp   open  rpcbind
514/tcp   open  shell
5432/tcp  open  postgresql
5989/tcp  open  wbem-https
6000/tcp  open  X11
7200/tcp  open  fodms
8100/tcp  open  xprint-server
9090/tcp  open  zeus-admin
24800/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 14.60 seconds

┌──(root㉿kali)-[~]
└─# nmap 172.20.120.164
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-21 13:59 EDT
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
Nmap scan report for 172.20.120.164
Host is up (2.0s latency).
Not shown: 994 closed tcp ports (reset)
PORT     STATE    SERVICE
23/tcp   open     telnet
80/tcp   open     http
443/tcp  open     https
514/tcp  filtered shell
2717/tcp filtered pn-requester
8333/tcp filtered bitcoin

Nmap done: 1 IP address (1 host up) scanned in 908.20 seconds
```

Fonte: Elaborado pelo autor, 2022

Em destaque, identificada abertas as portas do protocolo *Telnet* no servidor SAGE (.140) e no *switch* (.164), o que representa um risco potencial, pois todos dados que trafegam neste protocolo são enviados como texto claro, ou seja, sem nenhuma criptografia. A utilização da porta SSH e o bloqueio do *Telnet* mitiga esta vulnerabilidade.

Na Figura 6 observa-se que no GPS (.167) temos uma porta HTTPS aberta para gerência do equipamento via *browser* e no relé de proteção (.187) temos uma porta FTP aberta para o processo de atualização de *firmware* do equipamento.

Figura 6. Resultado do comando nmap para os endereços finais .167 e .187

```
┌──(root㉿kali)-[~]
└─# nmap 172.20.120.167
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-21 14:16 EDT
Nmap scan report for 172.20.120.167
Host is up (0.013s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT    STATE SERVICE
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 10.64 seconds

┌──(root㉿kali)-[~]
└─# nmap 172.20.120.187
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-21 14:16 EDT
Nmap scan report for 172.20.120.187
Host is up (0.017s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE
21/tcp open  ftp

Nmap done: 1 IP address (1 host up) scanned in 10.41 seconds
```

Fonte: Elaborado pelo autor, 2022

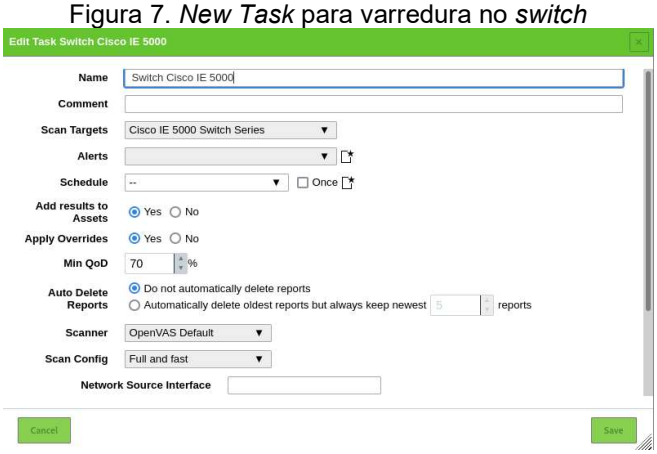
4.2 VARREDURA COM A FERRAMENTA OPENVAS

Com a ferramenta Nmap foi possível levantarmos as informações sobre portas abertas e serviços disponíveis dos *hosts* da rede. A próxima etapa consistiu na exploração destas vulnerabilidades com a ferramenta OpenVAS.

O primeiro passo necessário é a atualização, via internet, da base de vulnerabilidades CVEs[7] da ferramenta. Para classificar as vulnerabilidades encontradas, o OpenVAS utiliza o *Common Vulnerability Scoring System* (CVSS), que é um padrão da indústria para a classificação e avaliação de vulnerabilidades.

Concluída a atualização da base, configuramos uma *New Task* para cada *host* da rede, procedimento este necessário para inserirmos nossos alvos na *task* de varredura do software. Na Figura 7 é apresentada a tela de edição de uma *New Task*, em destaque, para o alvo no *switch*.

Figura 7. *New Task* para varredura no *switch*

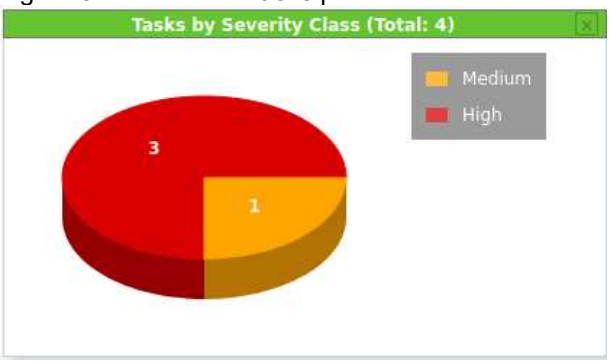


Fonte: Elaborado pelo autor, 2022

O software também apresentou uma visão geral das vulnerabilidades encontradas na rede. É destacado o gráfico da Figura 8 onde ele classifica a quantidade de *tasks* realizadas por classe de severidade. Para as 4 *tasks* realizadas, 3 detectaram pelos menos uma vulnerabilidade de classificação *High* durante o teste.

[7] CVEs (*Common Vulnerabilities Exposures*) são vulnerabilidades identificadas, em sua maioria por pesquisadores, e validadas pelo MITRE, órgão associado à Agência Nacional de Segurança Cibernética dos Estados Unidos.

Figura 8. Número de *Tasks* por classe de severidade



Fonte: Elaborado pelo autor, 2022

Para cada escaneamento, é gerado um relatório *(scan report)* com o detalhamento das vulnerabilidades detectadas e a mitigação sugerida. Ao final, obtemos os seguintes resultados:

Tabela 1. Classificação CVSS das vulnerabilidades encontradas

Host	***High***	***Medium***	***Low***	***Log***	***False Positive***
Servidor SAGE	3	10	1	50	0
Switch	1	2	0	15	0
GPS | Servidor NTP	2	7	1	27	0
Relé ABB RET670	0	4	0	17	0

Fonte: Elaborado pelo autor, 2022

Os resultados indicaram como maior severidade, o método de autenticação de usuário no serviço de base de dados PostgresSQL no servidor SAGE, sendo possível o invasor acessar e comprometer a base de dados do sistema supervisório do SAS. Como mitigação, deve ser desabilitado o método de autenticação *"trust"* e habilitado o "*secure"*.

Encontrada ainda vulnerabilidades nos métodos de conexão segura SSL/TLS do GPS por ataque SWEET32 (CVE-2016-2183).

Figura 9. Principais vulnerabilidades encontradas, classificadas pela severidade mais alta

Vulnerability	Severity ▼	QoD	Host IP	Host Name	Location	Created
PostgreSQL Trust Authentication Enabled	10.0 (High)	99 %	172.20.120.140		5432/tcp	Wed, Jul 6, 2022 4:05 PM -03
PostgreSQL no password	9.0 (High)	99 %	172.20.120.140		5432/tcp	Wed, Jul 6, 2022 4:07 PM -03
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	7.5 (High)	98 %	172.20.120.167		443/tcp	Wed, Jul 6, 2022 3:26 PM -03
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	7.5 (High)	98 %	172.20.120.140		5989/tcp	Wed, Jul 6, 2022 3:56 PM -03
HTTP Brute Force Logins With Default Credentials Reporting	7.5 (High)	95 %	172.20.120.164		80/tcp	Thu, Jul 21, 2022 3:50 PM -03
SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability	7.4 (High)	70 %	172.20.120.167		443/tcp	Wed, Jul 6, 2022 3:30 PM -03
Anonymous FTP Login Reporting	6.4 (Medium)	80 %	172.20.120.140		21/tcp	Wed, Jul 6, 2022 3:52 PM -03
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection	5.9 (Medium)	98 %	172.20.120.167		443/tcp	Wed, Jul 6, 2022 3:26 PM -03
SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits	5.3 (Medium)	80 %	172.20.120.167		443/tcp	Wed, Jul 6, 2022 3:26 PM -03
Weak Host Key Algorithm(s) (SSH)	5.3 (Medium)	80 %	172.20.120.140		22/tcp	Wed, Jul 6, 2022 3:53 PM -03

Fonte: Elaborado pelo autor, 2022

Os escaneamentos registraram também outras vulnerabilidades de média e baixa severidade, muitos relacionados as chaves SSL/TLS. Para estes casos, recomenda-se consulta junto aos fabricantes se há disponíveis versões mais atuais ou updates de *firmwares* e softwares dos dispositivos.

Ao término dos testes, houve o entendimento que a implementação de um *firewall* seria uma contramedida eficaz e bastante abrangente frente estas ameaças.

5 CONSIDERAÇÕES FINAIS

Para a realização deste artigo, foram realizadas pesquisas em literatura técnica especializada para redes de computadores, em específico a área de segurança cibernética. Também foi revisada a produção acadêmica voltada para testes de vulnerabilidades com ferramentas *open source*.

A montagem e configuração da plataforma de testes foram tarefas de grande complexidade, principalmente a instalação e parametrização da distribuição Kali Linux, porém desenvolveu habilidades nas competências de Linux e redes. A interação direta das ferramentas em laboratório, bem como dos próprios elementos da rede em teste permitiu ainda um maior conhecimento a respeito do funcionamento dos mesmos.

O estudo possibilitou a análise das vulnerabilidades nos dispositivos com as ferramentas propostas, detectando 31 vulnerabilidades, sendo que aproximadamente 20% dos resultados são de classificação *High*, de acordo com o padrão CVSS.

Em sequência a análise de vulnerabilidades desenvolvida, é sugerido como trabalho futuro a continuidade dos testes com técnicas de invasão *(pentest),* através de ferramentas de *exploit* e engenharia reversa disponíveis no Kali Linux.

A digitalização das subestações trouxe muitos benefícios para quem projeta, implementa, opera e mantem o SEP, entretanto a facilidade e escalabilidade de inserirmos mais dispositivos na rede abre portas para ameaças se esse processo não considerar melhores práticas de cibersegurança.

A implementação de educação e treinamento em segurança é um dever de todos, não restringindo somente as equipes de TI. A alta diretoria deve patrocinar e inclusive, participar de ações de conscientização de segurança, pois não adianta investir massivamente em tecnologia se usuário ainda continuar sendo o elo mais fraco. Além disso, ações contínuas em educação ajuda a estabelecer uma cultura de segurança nas instalações.

REFERÊNCIAS

ARAÚJO, R. S. S.;Viegas, R.. **Avaliando Sistemas de Detecção de Intrusão em uma Rede Acadêmica**. 2018. 72 p. Trabalho de Conclusão de Curso (Graduação em Ciência da Computação) - Universidade Federal do Pará, Belém, 2018.

AZEVEDO, Marcelo. **Cibersegurança em sistemas de automação em plantas de tratamento de água**. 2010. 155 p. Dissertação (Mestrado em Engenharia) - Escola Politécnica da Universidade de São Paulo, São Paulo, 2010.

BARBOSA, Ingrid Alves de Paiva; e REIS, Rafael Leme Simões; **Estudo sobre a Avaliação de Riscos Relacionados à Cibersegurança em uma Planta Industrial**. TCC (Graduação em Engenharia de Controle e Automação) - Instituto Nacional de Telecomunicações, INATEL, Santa Rita do Sapucaí. 2020.

COURY, Denis Vinicius. **Proteção digital de sistemas elétricos de potência: dos relés eletromecânicos aos microprocessadores inteligentes**. São Carlos: EESC-USP, 2007.

Estatísticas dos Incidentes Reportados ao CERT.br. **CERT.br**, 2022. Disponível em: <https://www.cert.br/stats/incidentes/>. Acesso em: 21/06/2022

JOHNSON, Allan. **31 Days Before Your CCNA Exam: A Day-By-Day Review Guide for the CCNA 200-301 Certification Exam**. Hoboken: Cisco Press, 2020.

LOPES, Yona. **SMARTFlow: sistema autoconfigurável para redes de telecomunicações IEC 61850 com arcabouço OpenFlow**. Niterói, 2013. 110 f. Dissertação (mestrado) Universidade Federal Fluminense, Departamento de Engenharia de Telecomunicações, 2013.

ODOM, Wendell. **CCNA 200-301 Official Cert Guide, Volume 2**. Hoboken: Cisco Press, 2019.

O que é o SIN. **ONS**, 2021. Disponível em: <http://www.ons.org.br/paginas/sobre-o-sin/o-que-e-o-sin>. Acesso em: 03/11/2021.

SAGE-CEPEL. **CEPEL**, 2022. Disponível em: <http://www.cepel.br/produtos/automacao-de-sistemas/sage-2/>. Acesso em: 01/07/2022.

SANTOS, Omar. **Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide**. Hoboken: Cisco Press, 2021.

SEL. **SEL-3354 Embedded Automation Computing Platform: Instruction Manual**. Pullman**:** Schweitzer Engineering Laboratories, Inc, 2011, 108 p.

SVIDERGOL, Brian. **CISSP Exam Study Guide**. Irvine: Netwrix, 2021, 93 P.

What is Kali Linux? | Kali Linux Documentation. **Kali**, 2022. Disponível em: <https://www.kali.org/docs/introduction/what-is-kali-linux/>. Acesso em 08/07/2022.

YONGIUN Xia et al. **Design and Implementation of Vulnerability Scanning Tools for Intelligent Substation Industrial Control System Based on OpenVAS**. IOP Conf. Ser.: Earth Environ. Sci. 440 042031. 2020.