DESENVOLVIMENTO DE ARQUITETURA DE TESTES DE PENETRAÇÃO EM REDES INDUSTRIAIS BASE ETHERNET

Jorge Augusto Pessatto Mondadori[1], Wesley Candido da Silva[2]

RESUMO

A crescente digitalização de sistemas industriais e a adoção de redes baseadas em Ethernet têm ampliado a superfície de ataque das infraestruturas críticas, exigindo novas abordagens para avaliação de segurança. Este trabalho propõe o desenvolvimento de uma bancada de testes de penetração (*testbed*) voltada para redes industriais, com foco nos protocolos Modbus/TCP, Ethernet/IP, S7comm e Profinet. A metodologia envolveu a montagem de uma arquitetura híbrida composta por controladores lógicos programáveis (CLPs), interfaces homem-máquina (IHMs), roteadores e softwares de coleta e análise de dados, como Node-RED e Kali Linux. Foram utilizados diversos scanners e analisadores de tráfego, como Nmap, Wireshark, Tcpdump, ArpWatch e Bettercap, para avaliar a resposta dos protocolos a diferentes tipos de testes. Os resultados demonstraram que os protocolos apresentam comportamentos distintos frente às ferramentas de penetração, sendo os protocolos baseados em TCP/IP mais suscetíveis à detecção e interferência. Já os protocolos industriais com comunicação em tempo real, como Profinet e Ethernet/IP, mostraram-se mais resilientes, embora com limitações na análise por ferramentas convencionais. Conclui-se que a bancada proposta é eficaz para simular cenários realistas de ataque e defesa, sendo uma ferramenta útil para ensino, pesquisa e desenvolvimento de estratégias de segurança em redes industriais.

Palavras-chave: redes industriais; segurança cibernética; protocolos industriais; testes de penetração; Ethernet.

PENETRATION TEST ARCHITECTURE DEVELOPMENT FOR ETHERNET BASED INDUSTRIAL NETWORKS

ABSTRACT

The increasing digitalization of industrial systems and the adoption of Ethernet-based networks have expanded the attack surface of critical infrastructures, demanding new approaches for security assessment. This work proposes the development of a penetration testing bench (testbed) focused on industrial networks, with emphasis on the Modbus/TCP, Ethernet/IP, S7comm, and Profinet protocols. The methodology involved assembling a hybrid architecture composed of programmable logic controllers (PLCs), human-machine interfaces (HMIs), routers, and data collection and analysis software such as Node-RED and Kali Linux. Several scanners and traffic analyzers, including Nmap, Wireshark, Tcpdump, ArpWatch, and Bettercap, were used to evaluate the response of the protocols to different types of tests. The results showed that the protocols behave differently when subjected to penetration tools, with TCP/IP-based protocols being more susceptible to detection and interference. On the other

[1] UniSenaiPR londrina; e-mail: jorge.mondadori@sistemafiep.org.br
[2] UniSenaiPR londrina; e-mail: wesley.candido@sistemafiep.org.br

hand, industrial protocols with real-time communication, such as Profinet and Ethernet/IP, proved to be more resilient, although with limitations in analysis by conventional tools. It is concluded that the proposed testbed is effective in simulating realistic attack and defense scenarios, serving as a useful tool for education, research, and the development of security strategies in industrial networks.

Key words: industrial networks; cybersecurity; industrial protocols; penetration testing; Ethernet.

1 INTRODUÇÃO

A crescente digitalização de sistemas industriais, impulsionada pela convergência entre Tecnologias da Informação (TI) e Tecnologias Operacionais (TO), tem ampliado significativamente a superfície de ataque das infraestruturas críticas. Redes industriais baseadas em Ethernet, amplamente utilizadas em Sistemas de Controle Industrial (ICS), como SCADA (Supervisory Control and Data Acquisition – Controle Supervisório e Aquisição de Dados) e CLP (Controladores Lógicos Programáveis), tornaram-se alvos recorrentes de ciberataques, conforme evidenciado por incidentes como Stuxnet e os ataques à infraestrutura elétrica da Ucrânia. A natureza crítica desses sistemas, aliada à sua operação contínua e à presença de dispositivos legados, impõe severas restrições à aplicação de testes de segurança diretamente em ambientes produtivos.

Nesse contexto, *testbeds* — bancadas de testes que simulam ambientes industriais — emergem como ferramentas essenciais para a realização de testes de penetração, avaliação de vulnerabilidades e validação de contramedidas. No entanto, a literatura aponta diversas limitações nos *testbeds* existentes: muitos são proprietários, de alto custo, pouco escaláveis e com baixa reprodutibilidade. Além disso, há uma carência de plataformas que integrem componentes físicos e virtuais de forma modular, permitindo a simulação realista de cenários de ataque e a análise de protocolos industriais como Modbus/TCP, S7Comm, Profinet e Ethernet/IP.

Estudos recentes, como o SCASS (2025), demonstram a viabilidade de arquiteturas híbridas e de código aberto para simular ambientes industriais com alta fidelidade. Outros trabalhos, como os de Martín-Liras et al. (2017) e Robles-Durazno et al. (2019), reforçam a importância de mecanismos de detecção e resposta a

ataques em CLP, bem como a necessidade de *testbeds* que permitam a análise forense e a replicação de ataques em memória. Além disso, a proposta de emuladores autônomos para cenários de IoE (Ruiz-Villafranca et al., 2025) amplia as possibilidades de simulação de dispositivos e protocolos em ambientes industriais complexos.

Diante dessas lacunas, este trabalho propõe o desenvolvimento de uma arquitetura de bancada de testes de penetração voltada para redes industriais baseadas em Ethernet. A proposta visa oferecer uma plataforma modular, acessível e reprodutível, capaz de integrar componentes físicos e virtuais, suportar múltiplos protocolos industriais e permitir a simulação de cenários realistas de ataque e defesa. Tem-se como objetivos específicos: investigar as principais vulnerabilidades associadas a protocolos industriais baseados em Ethernet, como Modbus/TCP, S7Comm, Profinet e Ethernet/IP, com base na literatura e em experimentos controlados; projetar e implementar uma bancada de testes híbrida (física e virtual) que permita a simulação de redes industriais com diferentes topologias, dispositivos e protocolos; integrar mecanismos de ataque e defesa na bancada, incluindo ferramentas para execução de testes de penetração, injeção de pacotes, manipulação de memória de CLP e coleta de evidências; e documentar a arquitetura, os componentes e os procedimentos da bancada de forma a permitir sua replicação por outros pesquisadores ou instituições de ensino.

Este trabalho é organizado da seguinte maneira: nesta primeira seção apresentou-se a introdução, motivação e objetivo do trabalho, na próxima seção apresenta-se a fundamentação teórica para o desenvolvimento, na terceira seção apresenta-se a metodologia utilizada, bem como equipamentos e materiais, na quarta seção discute-se o resultado da montagem da bancada de testes, por fim conclui-se com considerações finais e proposição de trabalhos futuros.

2 FUNDAMENTAÇÃO TEÓRICA

Nesta seção apresenta-se a fundamentação teórica baseada em livros, artigos normas e documentação técnica para estrutura do desenvolvimento.

2.1 Redes de computadores

Segundo Tanenbaum e Wetherall (2011), uma rede de computadores é uma ligação física e lógica, por meio de equipamentos (hardwares) e programas (softwares) capazes de transmitir dados seguindo um conjunto de regras de comunicação em comum (protocolo). Os equipamentos são comumente computadores, comutadores (switches), concentradores (hubs), cabos e conectores. Em nível de programas, tem-se as aplicações, drivers e softwares de gerenciamento dos hardwares.

Kurose e Ross (2009) apresentam dois modelos de camadas de redes de computadores, uma é aplicada a internet, composta de cinco camadas (Aplicação, Transporte, Rede, Enlace e Físico) e o modelo tradicional proposto pela ISO (International Standard Organization) que é composto de sete camadas, generalizando comunicações além da internet tradicional, que são: Aplicação, Apresentação, Sessão, Transporte, Rede, Enlace e Físico. Ainda afirmam que um determinado protocolo de comunicação pode ou não implementar por norma as camadas conforme modelo ISO.

Ainda sobre redes de computadores, os autores apresentam o modelo de referência para o TCP/IP (Transfer Control Protocol/Internet Protocol), no qual implementa-se as camadas de aplicação, Transporte, Internet e Enlace, não apresentando a camada de rede de forma tradicional e sendo genérica quanto ao meio físico, deixando para que outras normas definam. Esta ausência de definição entre camadas pode deixar lacunas na operação, embora seja um dos protocolos mais utilizados para comunicação mundial entre dispositivos. O protocolo internet em sua versão 4, atribui um endereço para cada dispositivo que não ocorre de forma física, formando apenas um laço lógico entre os endereços. Como isto é feito via software, identifica-se uma possível vulnerabilidade nas aplicações, objetivo de pesquisa deste trabalho.

2.2 Redes Industriais

Em uma publicação técnica de atualização tecnológica, o Senai (Serviço Nacional de Aprendizagem Industrial, 2014) define uma rede industrial como equipamentos e dispositivos agrupados em nível hierárquico que se comunicam por

meio de um conjunto de regras pré-estabelecidas (protocolo industrial): Supervisão, Controle, Campo e Processo; e Entradas e Saídas.

Albuquerque e Alexandria (2009) concordam com Senai e dividem os protocolos de rede industriais em dois grandes grupos. Os barramentos de campo (que podem ser cabeados ou sem fio) mas que a estrutura lógica principal se dá por meio de um barramento de informações compartilhadas, mesmo que em topologias físicas distintas, como árvore, anel ou estrela. O outro tipo são os protocolos industriais derivados do barramento de campo que utilizam o padrão IEEE 802.3 também chamado de ethernet. Estes possuem características de barramentos de campo, implementam algumas camadas do modelo ISO/OSI, porém são de tecnologia similar as redes locais e de longa distância, compartilhando meio físico com as redes convencionais, como cabeamento, roteadores, comutadores, concentradores e conectores.

O modelo tradicional de barramento de campo para comunicação industrial preconiza um ou mais dispositivos conectados na rede que definem a ordem e tráfego de informações, chamados mestres (SENAI, 2014). Outros dispositivos de rede, que responde às solicitações dos mestres são chamados dispositivos remotos.

2.3 Redes Industriais em base Ethernet

Em protocolos base ethernet para redes industriais, o modelo escravo-remota se diferencia pela ótica da aplicação, sendo o mestre chamado de cliente, que solicita as informações enquanto os dispositivos remotos são chamados de servidores (ALBUQUERQUE E ALEXANDRIA, 2009). Esta forma de entendimento entra em conflito com o conceito cliente servidor para sistemas de informática, onde geralmente temos um dispositivo central chamado de servidor e diversos dispositivos clientes solicitando informações. Portanto, ainda que em base ethernet, o modelo mestre-remota ainda é utilizado para redes industriais.

O guia de implementação para protocolo MODBUS/TCP (Modbus Organization, 2006) define o protocolo como uma variação do Modbus RTU, que utiliza o padrão Ethernet com implementação sobre o protocolo TCP/IP. Isso implica na necessidade de endereçamento de IP para os dispositivos, além do endereço do dispositivo para o protocolo Modbus. Padronizado pela norma IEC 61158 para redes

de comunicação de CLP, utiliza a porta 502 como padrão, não utiliza algoritmo de Checksum na mensagem e é utilizado por mais de 400 fabricantes ao redor do mundo.

Com tráfego de informações similar ao protocolo Profibus, o protocolo Profinet poderia ser chamado como sua versão base Ethernet (PROFINET, 2017). Diferente do protocolo Profibus, esses opera em três principais canais de comunicação:

- Padrão TCP/IP: precisa de endereçamento de IP e é utilizado em comunicações não determinísticas, como configuração de dispositivos e trafego de dados com sistemas de Tecnologia da Informação (TI).
- Tempo real (Real Time – RT): neste canal as camadas TCP/IP são ignoradas, e direto da camada de rede para a aplicação os dados trafegam. É utilizado para aplicações determinísticas, com faixa de intervalo de tempo de 1 a 10 ms.
- Tempo real Isócrono: para aplicações com o mínimo possível de variação temporal, dentro da faixa de microssegundos, com ciclos abaixo de 1ms. Depende de interface de comunicação dedicada e exclusiva para operação.

Seguindo os preceitos de protocolos abertos, a ODVA (2024) apresenta o protocolo Ethernet/IP como uma tecnologia baseada em IEEE 802.3 para Protocolo Industrial Comum (CIP – Common Industrial Protocol). Opera de forma similar ao protocolo DeviceNet porém garante interoperabilidade com diversos protocolos de internet como HTTP, FTP e DHCP. De forma diferente do protocolo Profinet, o Ethernet/IP utiliza o protcolo UDP para transferência de dados em tempo real, ou seja, ainda trafega dados sobre protocolo IP.

O protocolo S7comm é uma forma de comunicação proprietária da Siemens para seus controladores da linha S7-300 e superior (Siemens, 2019). Este protocolo é de fácil implementação, tornando o CLP um servidor HTTP sobre TCP/IP permitindo comandos convencionais como PUT e GET, por meio da porta 102. Utiliza a própria interface profinet do dispositivo como uma porta ethernet e permite que diversos softwares de supervisão, e equipamentos industriais consumam e forneçam dados dos controladores S7. A estrutura de rede profinet RT fica apartada da comunicação S7, sendo necessário desenvolvimento de código para o acesso das variáveis de rede.

2.4 Segurança cibernética

Tanenbaum e Wetherall (2011) estabelecem que uma comunicação segura, que é o objetivo de uma rede entre dispositivos, deve conter quatro fatores:

1. Confidencialidade: capacidade da rede entregar informações aos pontos garantindo que não haja o escape das informações;
2. Autenticação: verificação da veracidade da presença do equipamento ou usuário na rede;
3. Integridade da mensagem: garantia de o pacote de informações recebido ser exatamente o enviado;
4. Segurança operacional: garantir a segurança de forma global aos usuários da rede sem comprometer acesso e informação a usuários externos.

A preocupação contra invasão de rede é que usuários não intencionados possam monitorar mensagens; monitorar, inserir ou eliminar informações; ou incapacitar a rede de operar normalmente.

Em cenário que a maioria das empresas e instituições estão com suas redes interconectadas na rede, o estudo de segurança cibernética se faz cada vez mais necessário.

2.5 Distribuição Kali Linux

Almeida Junior (2021) apresenta o Kali Linux como uma ferramenta comum para testes de penetração em ambientes reais e simulados. O Kali Linux é uma distribuição do sistema operacional Linux, primariamente baseada em Debian. As ferramentas para teste já estão pré-instaladas para execução de tarefas de segurança ofensivas. Também é recomendada o uso de máquinas virtuais ou utilizar um computador dedicado para não haver compartilhamento de dados em disco sem isolamento adequado.

Diversas ferramentas são disponibilizadas na distribuição Kali Linux. A seguir apresentasse as mais comuns para testes de penetração em rede com uma breve descrição.

- Nmap ou Network mapper: identifica dispositivos na rede, seus endereços, portas e protocolos em uso;
- Masscan: mapear portas IP para grandes redes, ao contrário do Nmap que é focado para dispositivos específicos;
- Unicornscan: monitora trafego de dados TCP/IP com potenciais vulnerabilidades pelo protocolo e retorna análise de resultados;
- Wireshark: permite monitorar diversos protocolos de rede e retornar os pacotes trafegados. Também permite exibição do conteúdo dos pacotes exceto os criptografados;
- Tcpdump: registra todos os dados trafegados na rede sobre o protocolo TCP/IP gerando logs para posterior análise;
- Metasploit: explora vulnerabilidades conhecidas e documentadas, bem como a injeção de código malicioso para teste de penetração e alteração de informações;
- Aircrack-ng: decodificador de redes sem fio, permitindo análise de dados que trafegam criptografados para quebrar senhas, criar túneis entre pontos de rede e penetração de rede;
- Bettercap: reconhecer e atacar redes por meio de captura de pacotes, realização de ataques man-in-the-middle e falsificação de ARP, DNS, DHCP em redes IPv4 ou IPv6. Também pode ser utilizado para ocupar a rede e impedir que outros dispositivos utilizem o meio;
- Arpwatch: monitoramento de tráfego para redes Ethernet e ARP, mantendo um banco de dados de relação entre MAC e IP;
- Netcat: verificação de portas de rede e permite gerar solicitações aleatórias a aplicações para coleta de informações;

Nesta seção apresentou-se a fundamentação teórica para atingir os objetivos do trabalho. A próxima seção apresenta a metodologia utilizada para a montagem da bancada de testes de penetração de rede industrial.

3 METODOLOGIA

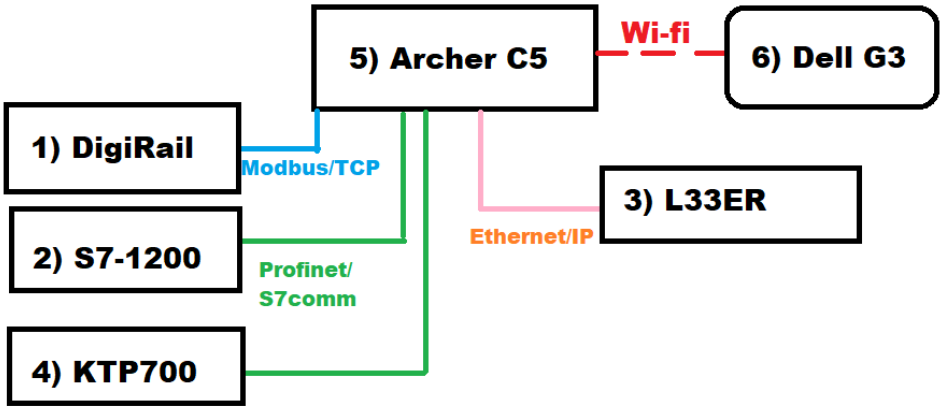
Primeiramente define-se a arquitetura de rede industrial a ser utilizada para montagem da bancada de testes para testes de penetração aplicada. Os protocolos de comunicação industriais são os seguintes: Modbus/TCP, Ethernet/IP, S7comm e Profinet.

Escolheram se os seguintes equipamentos para montagem da estrutura:

1) Coletor de dados industriais DigiRail OEE Novus, com protocolo Modbus/TCP, porta ethernet 10/100.
2) CLP S7-1200 1214/DC/DC/DC Siemens com 1 porta ethernet.
3) CLP 1769-L33ER CompactLogix Allen-Bradley com duas portas ethernet.
4) IHM KTP700 Siemens com 1 porta ethernet.
5) Roteador Archer C50 Tp-Link com função de comutador de rede para 4 portas ethernet e wifi.
6) Notebook Dell G3 com conectividade Ethernet wifi.

A montagem física dos equipamentos é representada pela figura 1. Do item 1 ao 4, todos foram conectados via cabo par trançado Cat5, sem blindagem ou malha, e conectores plásticos RJ45 sem aterramento.

Figura 1 – Arquitetura de rede proposta



Fonte: Elaborado pelo autor (2025)

Como o objetivo não é testar desempenho de redes, estabeleceu-se o intervalo de um segundo para coleta de dados pelo computador. Um software desenvolvido em Node-red coleta os dados de variáveis internas dos controladores.

O código dos CLP S7-1200 e L33ER possuem uma instrução para incrementar uma memória interna a cada 1s e armazenar na posição de memória que será lida pela rede. Para o caso do DigiRail OEE, o registrador a ser lido é o timestamp em UTC, pois ele não permite programação.

Por meio do protocolo Profinet, a IHM KTP700 receberá um valor de memória do CLP para apresentar em uma tela.

Além de receber os dados por meio da programação em node-red, o computador armazena o log de cada um dos protocolos: Ethernet/IP, S7comm e Modbus/TCP. O protocolo profinet para ser implementado no computador precisaria de um sistema com driver de comunicação adequado ou uma porta capaz de implementar protocolos Real Time, indisponível no modelo Dell G3.

No computador Dell G3, além da coleta de dados também é executada uma máquina virtual com sistema Kali Linux. Dentre as ferramentas disponíveis, para desenvolver os testes nesta bancada, busca-se aquelas que tenham capacidade de interferir tanto em procolo TCP/IP como padrão Ethernet, na camada de endereçamento MAC. Para tal, utiliza-se: Nmap, WireShark, Tcpdump ArpWatch e Bettercap.

4 APRESENTAÇÃO E DISCUSSÃO DOS RESULTADOS

O desenvolvimento da bancada de testes permite testes e interoperabilidade entre protocolos distintos. Esta seção busca estruturar a experiência do desenvolvimento e por consequência seus resultados preliminares.

A partir da metodologia proposta, montou-se a bancada no laboratório de Mobilidade e Energias Inteligentes do Senai de Londrina na unidade da Rua Belém. A comunicação entre o software proposto em node-red com os 3 protocolos foi realizada com sucesso e os dados puderam ser adquiridos intervalos de 1 segundo. Para a rede Profinet entre o controlador S7-1200 e a IHM KTP700, houve uma incompatibilidade da versão do software de programação, e as imagens necessárias para programar a IHM na versão do software utilizadas não foram baixadas em tempo deste trabalho.

4.1 Protocolo Modbus/TCP

A seguir apresenta-se o uso das ferramentas propostas na metodologia quanto ao protocolo Modbus/TCP:

Uso da ferramenta Nmap: foram realizados 10 testes de mapeamento de rede e nas 10 foi possível identifica a porta de comunicação bem como o IP do dispositivo.

Uso da ferramenta Wireshark: Assim como no caso do uso Nmap, foi identificada comunicação e nos 10 testes foi possível visualizar o pacote de dados do Modbus/TCP em Hexadecimal na ferramenta.

Uso da ferramenta Tcpdump: Similar ao Wireshark, foi possível visualizar o trafego de dados de requisição e resposta do Modbus/TCP.

Uso da ferramenta ArpWatch: Configurada para detectar mudança de IP, o ArpWatch não detectou nenhuma mudança de IP, conforme o esperado.

Uso da ferramenta Bettercap: Ao poluir a rede com mensagens, a ferramentaa permitiu detectar o uso da porta 502 e bloquear o acesso do Node-red e Digirail ao meio de comunicação.

4.2 Protocolo S7comm

O resultado do uso das ferramentas propostas para o protocolo de comunicação entre CLP S7 e o Node-red foi igual ao uso do protocolo Modbus/TCP. Vale ressaltar aqui que não foi utilizado nenhum tipo extra de autenticação, que pode ser feita e é recomendado pelo fabricante do controlador. A diferença base é que a porta detectada foi a 102. O protocolo base é o TCP/IP com aplicação de hipertexto (HTTP não seguro).

4.3 Protocolo Ethernet/IP

Os resultados para testes das ferramentas em Ethernet/IP começam a se diferenciar dos protocolos baseados em TCP/IP.

Uso da ferramenta Nmap: a ferramenta foi capaz de detectar o endereço MAC e o IP atribuído para o dispositivo L33ER, porém não detectou a porta de comunicação utilizada.

Uso da ferramenta Wireshark:A ferramenta detectou o IP e a presença do dispositivo na rede, porém não registrou nenhuma mensagem trafegada, mas registrou a presença do protocolo CIP.

Uso da ferramenta Tcpdump: a ferramenta não foi capaz de detectar a presença de mensagens na rede.

Uso da ferramenta ArpWatch: a ferramenta não detectou a presença do IP na rede.

Uso da ferramenta Bettercap: os resultados foram inconclusivos. Embora o retorno da ferramenta fosse que ela estava ocupando 100% da rede para tráfego de pacotes, o protocolo Ethernet/IP enviou as mensagens para o destino sem problemas. Isso deve ser investigado em cenários futuros, para entender se o cenário do uso da ferramenta se limita a algum protocolo específico.

4.4 Protocolo Profinet

O protocolo Profinet teve comportamento similar ao Ethernet/IP. Contrastando com a arquitetura proposta, para este teste foi utilizado o Software TIA Portal V17 comunicando com o S7-1200 diretamente ao invés de monitorar a comunicação entre CLP e IHM KTP700. Foi estruturada uma comunicação Profinet entre os dispositivos, porém a porta ethernet física do computador não é certificada para comunicação em tempo real.

Uso da ferramenta Nmap: a ferramenta apenas detectou o endereço MAC do dispositivo, sem detectar o IP atribuído.

Uso da ferramenta Wireshark: a ferramenta detectou o protocolo Profinet-IO, ou seja, é capaz de definir qual dos canais é utilizado, porém detectou apenas o endereço MAC, sem detectar IP ou mesmo analisar mensagem.

Uso da ferramenta Tcpdump: a ferramenta não detectou a presença de mensagens na rede.

Uso da ferramenta ArpWatch: a ferramenta não detectou presença de IP do CLP na rede.

Uso da ferramenta Bettercap: Assim como no caso do Ethernet/IP, o resultado foi inconclusivo.

4.5 Visão geral de multiplos protocolos

Não há uma condição inicial ou sequencial para os testes apresentados nas subseções anteriores, pois eles foram feitos de forma separada para cada protocolo. Ao testar as ferramentas com múltiplos protocolos ao mesmo tempo, o resultado foi similar aos testes individuais.

5 CONSIDERAÇÕES FINAIS

Este artigo apresentou uma revisão de protocolos de comunicação industrial de base ethernet, suas característsticas e diferenças para protocolos de internet convencional. Também estruturou um formato de bancada de teste (*testbed)*, entre software e hardware para investigar métodos de penetração em redes de comunicação.

A metodologia teve como objetivo apresentar possibilidades de aplicação de testes e ensaios de penetração utilizando diversas ferramentas. Os resultados apontam que protocolos distintos se comportam de forma distinta aos testes, apontando necessidade de investigação futura e aprofundamento no estudo das ferramentas e dos protocolos de comunicação.

As limitações deste trabalho se encontram na falta de estruturação de teste com reconhecimento de ataque e resultados, ponto que pode ser investigado em trabalhos futuros. Também o uso de um mesmo hardware para causar interpéries a rede e coletar resultados podem causar viéses de análise como os resultados inconclusivos.

Somado ao que já foi apontado, sugere-se para trabalhos futuros o estudo aprofundado de protocolos e suas vulnerabilidades de forma isolada, a inserção de um agende de monitoramento externo; o uso de cabeamento padronizado conforme normativas do fabricante; e por fim o uso de ferramentas indústriais para comutação de rede, bem como um computador com interface ethernet em tempo real.

REFERÊNCIAS

ALBUQUERQUE, Pedro Urbano B.; ALEXANDRIA, Auzuir Ripardo de. **Redes Industriais:** Aplicações em sistemas digitais de controle distribuído. 2. Ed. São Paulo: Ensino Profissional, 2009.

ALMEIDA JÚNIOR, José Augusto de. **Pentest em aplicações web:** avalie a segurança contra ataques web com testes de invasão no Kali Linux. São Paulo, SP: Casa do Código, 2021.

D'AMBROSIO, Nicola et al. SCASS: Breaking into SCADA Systems Security. **Computers & Security**, v. 151, 2025. DOI: https://doi.org/10.1016/j.cose.2025.104315.

KUROSE, James. F.; ROSS, Keith. W. **Redes de computadores e a internet:** uma abordagem top-down. 5. ed. São Paulo: Pearson, 2009.

MARTÍN-LIRAS, Luis et al. Comparative analysis of the security of configuration protocols for industrial control devices. **International Journal of Critical Infrastructure Protection**, v. 19, p. 4–15, 2017. DOI: https://doi.org/10.1016/j.ijcip.2017.10.001.

MODBUS ORGANIZATION. **Modbus messaging on TCP/IP Implementation Guide V1.0b,** 2006.

ODVA. **Ethernet/IP:** CIP on ethernet technology. Michigan, 2024.

PROFIBUS BRASIL AMÉRICA LATINA. Marco Aurélio Padovan. Leandro Torres. **PROFINET:** Descrição do Sistema – Tecnologia e Aplicação. São Paulo, 2017.

ROBLES-DURAZNO, Andres et al. PLC memory attack detection and response in a clean water supply system. **International Journal of Critical Infrastructure Protection**, v. 26, 2019. DOI: https://doi.org/10.1016/j.ijcip.2019.05.003.

RUIZ-VILLAFRANCA, Sergio et al. A self-contained emulator for the forensic examination of IoE scenarios. **Ad Hoc Networks**, v. 168, 2025. DOI: https://doi.org/10.1016/j.adhoc.2024.103718.

Senai - SERVIÇO NACIONAL DE APRENDIZAGEM INDUSTRIAL. **Redes Industriais**: Atualização Tecnológica em Mecatrônica. Porto Alegre, RS: Departamento Regional do Rio Grande do Sul, 2014.

SIEMENS. **S7 communication between Simatic S7-1200 and Simatic S7-300.** 2019.

TANENBAUM, Andrew. S.; WETHERALL, David. J. **Redes de computadores**. 5. ed. São Paulo, SP: Pearson, 2011.