REDTEAM32 COMO UMA FERRAMENTA DE BAIXO CUSTO MEDIADA POR INTELIGÊNCIA ARTIFICIAL PARA O ENSINO DE SEGURANÇA EM REDES DE COMPUTADORES NA ENGENHARIA

Pedro Cézar Silva Ferreira[1], Dr. Carlos Galvão Pinheiro Júnior[2]

[1]Escola de Engenharia Elétrica, Mecânica e de Computação, Universidade Federal de Goiás,Goiânia, Brazil (pedrocezar@discente.ufg.br)
[2]Escola de Engenharia Elétrica, Mecânica e de Computação, Universidade Federal de Goiás, Goiânia, Brazil

Resumo: O RedTeam32 apoia o ensino de segurança em redes na engenharia por meio de um aplicativo móvel que integra o microcontrolador ESP32 com a API Gemini, configurada como tutora especializada do firmware Marauder. A ferramenta auxilia estudantes na interpretação de saídas do terminal e na execução de comandos sem substituir sua agência cognitiva, mobilizando competências previstas pelas DCNs de Engenharia de 2019.

Palavras-chave: Aprendizagem ativa; Educação em Engenharia; ESP32 Marauder; IA generativa; Segurança de redes sem fio.

INTRODUÇÃO

As Diretrizes Curriculares Nacionais (DCN) para os cursos de Engenharia, estabelecidas pela Resolução CNE/CES n.º 2/2019, impuseram uma reorientação significativa do ensino: o egresso deve ser formado por competências e não apenas por conteúdos, com ênfase em aprendizagem ativa, resolução de problemas reais e capacidade de utilizar ferramentas modernas. No contexto das disciplinas de redes de computadores e segurança da informação, essa exigência colide com uma realidade recorrente: as ferramentas móveis de testes de penetração (pentest) disponíveis para experimentação prática ou exigem modificações profundas nos sistemas

operacionais dos dispositivos, ou apresentam custo de aquisição proibitivo para muitas instituições, ou impõem curvas de aprendizado que inviabilizam seu uso em laboratórios com tempo limitado.

Este trabalho apresenta a ferramenta RedTeam32 como uma estratégia pedagógica inserida no contexto das metodologias ativas e da educação mediada por tecnologia. RedTeam32 é um aplicativo móvel de código aberto, desenvolvido em Flutter, que estabelece comunicação serial entre dispositivos Android e o microcontrolador ESP32 (embarcado com o firmware Marauder) via cabo USB OTG. Como diferencial pedagógico central, o aplicativo integra a API Gemini do Google por meio de injeção de prompt de contexto especializado, oferecendo ao estudante um assistente de inteligência artificial condicionado a atuar como tutor do firmware: interpretando saídas do terminal, sugerindo próximos comandos e traduzindo dados técnicos em linguagem acessível, sem substituir a agência do aprendiz.

O trabalho discute como essa combinação de hardware de baixo custo, software livre e assistência por IA especializada pode ser empregada como estratégia de aprendizagem ativa em laboratórios de segurança de redes, quais competências ela mobiliza segundo as DCN de Engenharia e quais limitações técnicas e pedagógicas precisam ser gerenciadas pelo docente.

Vale destacar que o uso de ferramentas de segurança ofensiva em ambientes educacionais exige uma abordagem ética e juridicamente responsável. Embora recursos como análise de tráfego, captura de pacotes e testes de redes sem fio sejam importantes para a formação técnica em segurança da informação, sua utilização deve ocorrer exclusivamente em ambientes controlados, autorizados e destinados ao ensino ou pesquisa. No contexto brasileiro, a Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, tipifica a invasão de dispositivos informáticos sem autorização, reforçando a necessidade de conscientização dos estudantes sobre limites legais, privacidade e boas práticas profissionais durante a realização de atividades práticas relacionadas à segurança da informação.

FUNDAMENTAÇÃO TEÓRICA

2.1 METODOLOGIAS ATIVAS E APRENDIZAGEM BASEADA EM PROBLEMAS REAIS

A literatura em educação em engenharia é consistente ao apontar que a aprendizagem ativa, estratégias em que os estudantes se engajam na construção do conhecimento por meio de fazer, explorar e resolver problemas, produz resultados superiores às abordagens expositivas tradicionais, especialmente no desenvolvimento de competências técnicas complexas (Felder e Brent, 2016). No ensino de segurança de redes, isso se traduz em laboratórios que permitam ao estudante executar ataques e defesas em ambientes controlados, observando na prática comportamentos de protocolos que, de outra forma, permanecem abstratos no slide ou no quadro.

O grande obstáculo para a adoção dessas práticas é a barreira de acesso às ferramentas. Plataformas como o Kali NetHunter requerem desbloqueio de bootloader e instalação de kernels customizados, procedimentos incompatíveis com as políticas de TI da maioria das instituições de ensino. Dispositivos como o Flipper Zero apresentam custo elevado e interface de controle móvel limitada. Aplicativos como o Terminal Serial USB, embora acessível, restringe à comunicação textual básica, sem oferecer suporte didático, interpretação contextual de comandos ou integração com ferramentas de apoio educacional. O RedTeam32 foi concebido para preencher essa lacuna: um laboratório portátil de segurança de redes sem fio, operável a partir de um smartphone Android comum, sem root, com custo de hardware inferior a R$ 50,00.

2.2 IA GENERATIVA COMO SUPORTE PEDAGÓGICO

A integração de assistentes de inteligência artificial em ferramentas educacionais tem sido investigada como estratégia para reduzir a curva de aprendizado em domínios técnicos de alta complexidade. A abordagem adotada no RedTeam32, injeção de prompt de contexto antes da inicialização da sessão, condiciona o modelo Gemini 2.5 Flash a atuar exclusivamente como especialista no firmware Marauder. Diferentemente de um assistente de

propósito geral, que tenderia a fornecer respostas genéricas sobre segurança de redes, o assistente configurado interpreta saídas brutas do terminal, incluindo dumps hexadecimais de pacotes capturados, e as traduz em linguagem acessível, além de sugerir proativamente o próximo comando adequado ao fluxo de operação em curso. Esse comportamento se aproxima do papel de um tutor especializado que guia o estudante sem realizar a tarefa por ele, princípio central das abordagens de aprendizagem scaffolded (Vygotsky, 1978).

2.3 O MICROCONTROLADOR ESP32 E O FIRMWARE MARAUDER

O ESP32, desenvolvido pela Espressif Systems, reúne em um único chip de baixo custo processador dual-core Xtensa LX6, conectividade Wi-Fi 802.11 b/g/n e Bluetooth 4.2/BLE nativos. O firmware Marauder, desenvolvido especificamente para o ESP32, consolida em uma suíte de código aberto um conjunto abrangente de ferramentas de auditoria de redes sem fio, explorando diretamente o hardware de rádio do chip. Isso permite operações como varredura ativa e passiva de pontos de acesso, captura de beacons, análise de handshakes WPA e monitoramento de dispositivos Bluetooth, operações que ilustram concretamente conceitos das camadas física, de enlace e de rede do modelo OSI, frequentemente abordados apenas de forma teórica nas disciplinas de redes.

DESCRIÇÃO DO REDTEAM32

3.1 ARQUITETURA E IMPLEMENTAÇÃO

O RedTeam32 adota uma arquitetura modular organizada em camadas funcionais: telas (screens), serviços (services), componentes visuais (widgets) e sistema de temas (theme). A comunicação serial com o ESP32 ocorre via protocolo UART configurado em 115200 8N1, padrão amplamente adotado em sistemas embarcados. O modelo de concorrência do framework Flutter, baseado em isolates e programação assíncrona, permite que a leitura contínua do stream serial ocorra sem bloqueio da interface gráfica, garantindo

responsividade ao terminal mesmo sob alto volume de saídas do microcontrolador. Todo o fluxo de dados seriais permanece exclusivamente no dispositivo, sem hospedagem em servidores externos, assegurando a privacidade das sessões de laboratório. O projeto é de código aberto e está disponível no GitHub (Ferreira, 2026).

3.2 O ASSISTENTE DE IA E A INJEÇÃO DE CONTEXTO

Antes de qualquer interação com o estudante, a sessão é inicializada com um prompt de sistema fixo em português que instrui o modelo Gemini 2.5 Flash a: (i) sugerir comandos do firmware Marauder em resposta a objetivos expressos em linguagem natural; (ii) interpretar saídas brutas do terminal e traduzi-las em explicações acessíveis; e (iii) manter respostas concisas, de no máximo três a quatro frases por resposta. A cada interação, a última saída do ESP32 é injetada como contexto serial atualizado antes do envio da mensagem do usuário, com limite de 500 caracteres por resposta. Os parâmetros de geração, temperature 0,7, topK 40 e topP 0,95, limitam respostas excessivamente criativas e mantêm o assistente aderente à sintaxe específica do firmware.

COMPETÊNCIAS MOBILIZADAS

A Tabela 1 mapeia as principais atividades práticas suportadas pelo RedTeam32 as competências que elas permitem desenvolver, em alinhamento com as DCN de Engenharia (Resolução CNE/CES n. 2/2019).

Tabela 1. Mapeamento de atividades práticas do RedTeam32 a competências das DCN de Engenharia.

Atividade prática	Recurso do RedTeam32	Competências desenvolvidas (DCN Eng. 2019)
Execução de comandos no terminal serial	CLI do firmware Marauder	Operação de sistemas embarcados; pensamento procedimental

Interpretação de saídas do firmware	Logs, dumps hexadecimais e varreduras	Análise crítica de dados técnicos; leitura de documentação
Consulta ao assistente de IA	API Gemini com injeção de contexto	Uso de IA como suporte; autonomia investigativa
Configuração do hardware ESP32	Conexão USB OTG e parâmetros UART	Integração hardware-software; prototipação de baixo custo
Compreensão de protocolos sem fio	Operações Wi-Fi 802.11 e Bluetooth/BLE	Fundamentos de redes; segurança; ética profissional

RESULTADOS E DISCUSSÕES

A confiabilidade da camada de comunicação serial foi avaliada anteriormente em Ferreira e Pinheiro Júnior (2026), onde dez sessões independentes com 1.000 pacotes cada registraram latência média de 4,61 ms (mínimo de 3,8 ms, máximo de 6,1 ms), taxa de perda inferior a 0,5% e taxa de corrupção abaixo de 0,1%, indicando que a camada de comunicação não impõe ruído técnico capaz de comprometer a experiência pedagógica em condições normais de laboratório.

Tabela 2. Resultados das medições de confiabilidade da comunicação serial.

Medição	Latência (ms)	Pacotes enviados	Perdidos	Corrompidos
1	3,8	1.000	1	0
2	4,1	1.000	0	1
3	4,5	1.000	2	0

Medição	Latência (ms)	Pacotes enviados	Perdidos	Corrompidos
1	3,8	1.000	1	0
4	3,9	1.000	1	1
5	5,2	1.000	3	0
6	4,7	1.000	1	0
7	6,1	1.000	4	1
8	4,0	1.000	0	0
9	5,5	1.000	2	1
10	4,3	1.000	1	0

RedTeam32 opera como dispositivo de aprendizagem ativa em dois eixos complementares. No primeiro, diferentemente de simuladores que abstraem o hardware, a ferramenta coloca o estudante diante de um sistema real, um microcontrolador físico, um firmware de produção e uma rede sem fio verdadeira, exigindo que ele resolva problemas concretos, interprete respostas inesperadas e construa um modelo mental do comportamento do sistema. Esse contato direto com a materialidade técnica é condição relevante para o desenvolvimento de competências como integração hardware-software e análise crítica de dados, previstas nas DCN de Engenharia. No segundo eixo, o assistente de IA configura um uso pedagogicamente sofisticado da tecnologia: não como substituto do professor, mas como tutor especializado disponível em tempo real durante a sessão prática.

Os resultados de confiabilidade da comunicação serial, latência média de 4,61 ms e taxas de perda e corrupção de pacotes inferiores a 0,5% e 0,1%, respectivamente, indicam que a camada de comunicação não impõe ruído técnico capaz de comprometer a experiência pedagógica, sustentando o uso da ferramenta em laboratórios com exigência de responsividade.

A natureza ofensiva de algumas funcionalidades do firmware Marauder exige que o docente estabeleça protocolos claros de uso ético e legal antes de qualquer atividade. Os experimentos devem ocorrer exclusivamente em redes privadas autorizadas, com ciência dos participantes, observada a vedação imposta pela Lei n.º 12.737/2012 ao acesso não autorizado a dispositivos informáticos. Esse enquadramento ético, longe de ser um obstáculo, constitui oportunidade pedagógica para o desenvolvimento da dimensão cidadã e profissional do engenheiro, em alinhamento com o perfil de egresso previsto pelas DCN.

Entre as limitações identificadas, a mais relevante para o contexto educacional é a dependência de conectividade com a API Gemini para o funcionamento do assistente de IA, o que pode inviabilizar seu uso em laboratórios sem acesso à internet. O suporte atual restringe-se a dispositivos Android com conector USB OTG, excluindo plataformas iOS.

Como agenda de trabalhos futuros, pretende-se investigar a integração de modelos de linguagem executados localmente no dispositivo, como os da família Gemma, eliminando a dependência de conectividade externa. Também se planeja a elaboração de roteiros didáticos estruturados para uso do RedTeam32 em disciplinas de redes e segurança da informação, bem como a avaliação formal de seu impacto no aprendizado por meio de instrumentos validados, pré e pós-testes e questionários de percepção, aplicados a turmas de engenharia. A expansão do suporte a outros firmwares de pentest para ESP32 também está prevista.

CONCLUSÃO

Este trabalho apresentou o RedTeam32 como estratégia de aprendizagem ativa mediada por tecnologia para o ensino de segurança em redes sem fio na engenharia. A ferramenta combina hardware de baixo custo (ESP32, inferior a R$ 50,00), software livre (firmware Marauder e aplicativo Flutter) e assistência por inteligência artificial especializada (API Gemini com injeção de contexto),

formando um laboratório portátil que pode ser replicado por qualquer estudante com um smartphone Android e um cabo USB OTG.

Do ponto de vista pedagógico, a ferramenta mobiliza competências previstas nas DCN de Engenharia, como análise crítica, integração hardware-software, autonomia investigativa e uso ético de ferramentas modernas, e se insere naturalmente em estratégias de aprendizagem baseada em problemas. Seu caráter de código aberto favorece a adoção e a customização por instituições com diferentes perfis de infraestrutura.

Espera-se que o RedTeam32 possa contribuir para a renovação das práticas pedagógicas em disciplinas de redes e segurança da informação, aproximando o estudante de engenharia dos desafios reais de um ambiente digital em permanente evolução.

REFERÊNCIAS

BRASIL. Lei n.º 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos. Diário Oficial da União, Brasília, DF, 3 dez. 2012.

BRASIL. Resolução CNE/CES n.º 2, de 24 de abril de 2019. Institui as Diretrizes Curriculares Nacionais do Curso de Graduação em Engenharia. Diário Oficial da União, Brasília, DF, 26 abr. 2019.

ESPRESSIF SYSTEMS. ESP32 Technical Reference Manual. 2023. Disponível em: https://www.espressif.com/sites/default/files/documentation/esp32_technical_reference_manual_en.pdf. Acesso em: abr. 2026.

FELDER, R. M.; BRENT, R. Teaching and Learning STEM: A Practical Guide. San Francisco: Jossey-Bass, 2016.

FERREIRA, P. C. S. RedTeam32. 2026. Disponível em: https://github.com/pedrocsf/RedTeam32. Acesso em: abr. 2026.

FERREIRA, P. C. S.; PINHEIRO JÚNIOR, C. G. RedTeam32: aplicação móvel para teste de penetração de redes Wi-Fi e Bluetooth utilizando ESP32 com assistência por inteligência artificial. In: CONFERÊNCIA DE ESTUDOS EM ENGENHARIA ELÉTRICA (CEEL), 2026, Uberlândia. Uberlândia: UFU, 2026.

FLIPPER DEVICES INC. Flipper Zero: Portable Multi-tool Device for Geeks. 2023. Disponível em: https://flipperzero.one. Acesso em: abr. 2026.

GOOGLE LLC. Flutter Documentation. 2026. Disponível em: https://flutter.dev/docs. Acesso em: abr. 2026.

GOOGLE LLC. Gemini API Documentation. 2026. Disponível em: https://ai.google.dev. Acesso em: abr. 2026.

KOKO, J. ESP32Marauder. 2024. Disponível em: https://github.com/justcallmekoko/ESP32Marauder. Acesso em: abr. 2026.

OFFENSIVE SECURITY. Kali NetHunter Documentation. 2024. Disponível em: https://www.kali.org/docs/nethunter. Acesso em: abr. 2026.

USB IMPLEMENTERS FORUM. USB On-The-Go Supplement to the USB 2.0 Specification, Revision 1.3. Portland: USB-IF, 2006.

VYGOTSKY, L. S. Mind in Society: The Development of Higher Psychological Processes. Cambridge: Harvard University Press, 1978.