AUDITORIA WI-FI BASEADA EM ESP32

POR: AUGUSTO DALEFFE & JOÃO PAVAN

OBJETIVO DO PROJETO

O projeto teve como intuito desenvolver um auditor para redes sem fio, a fim de trazer à tona vulnerabilidades comuns dentro do meio. Para isso, foram utilizados exclusivamente um conjunto de ESP32, componentes responsáveis pela simulação de uma rede sem fio e seus usuários.

Durante o desenvolvimento foram implementados alguns ataques comuns a redes wifi, nosso objetivo foi mostrar como é possível identificar e neutralizar esses ataques com dispositivos de baixo custo e sem muito poder computacional.

ARQUITETURA GERAL DO SISTEMA

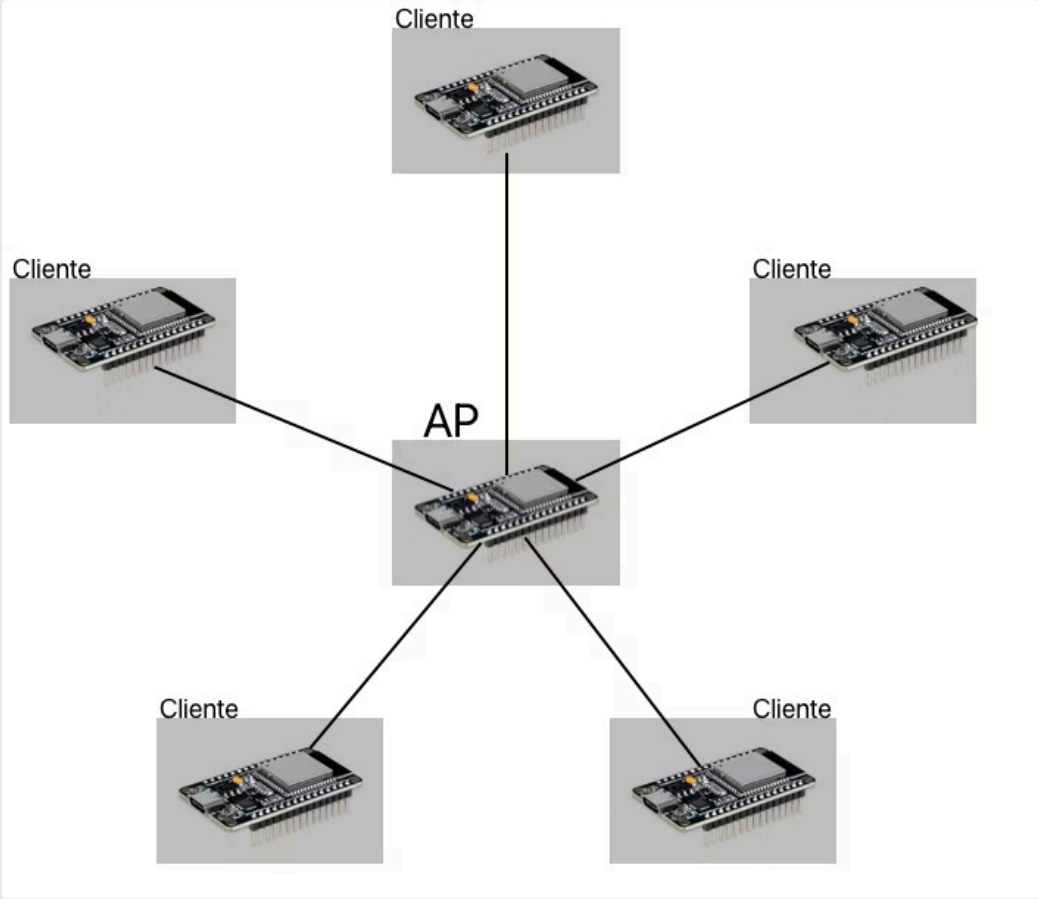
Topologia Escolhida:

- **Topologia Estrela:** Apenas um AP para N clientes

Componentes principais:

- **ESP32 Auditor/AP:** Ponto de acesso e monitor da rede Wi-Fi
- **Clientes legítimos:** Dispositivos simulando uso normal
- **Clientes maliciosos:** Dispositivos injetando ataques de flooding

A comunicação é totalmente embarcada, sem dependência de ferramentas externas, garantindo integração eficiente e autossuficiente.

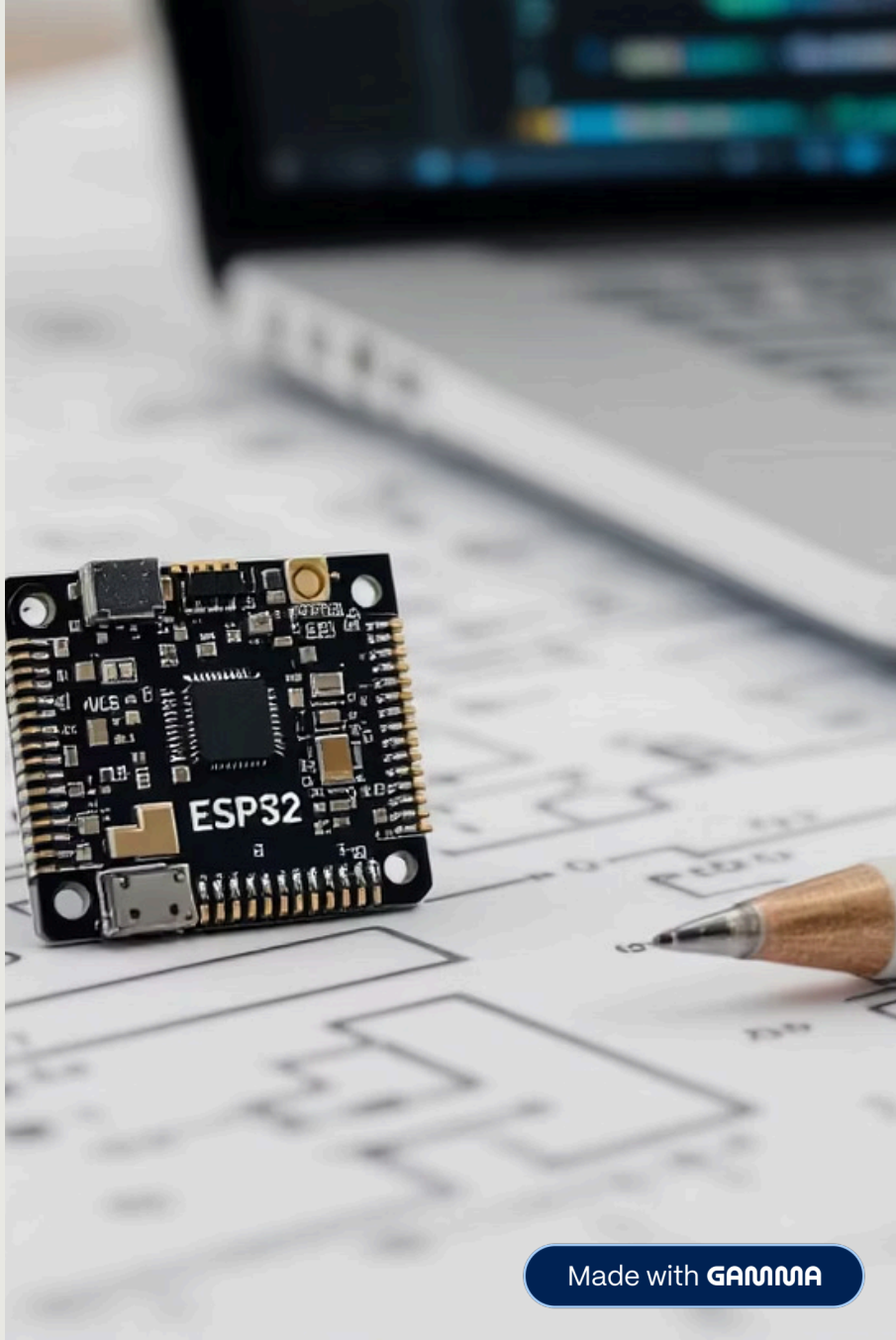


LÓGICA DO ACCESS POINT (AUDITOR)

O firmware inicializa o ESP32 como Access Point configurando nome da rede, senha, canal e limite máximo de conexões para controle rigoroso do ambiente.

Um servidor TCP na porta 3333 é criado para comunicação e debug em tempo real.

Funções internas monitoram eventos da rede, identificam padrões de ataque e acionam a função add_to_blacklist() para mitigar ameaças.



ATAQUES SIMULADOS

DEAUTH FLOOD

Envio contínuo e forçado de desconexões para desestabilizar clientes legítimos.

AUTH FLOOD

Bombardeio de tentativas de autenticação falsas para sobrecarregar o sistema.

PACKET FLOOD

Saturação do canal via envio massivo e contínuo de pacotes com MACs aleatórios.

Cada ataque é configurado com MACs randômicos, intervalos curtos entre eventos e alto número de tentativas, simulando cenários reais para testes robustos.

LÓGICA DE DETECÇÃO DOS ATAQUES

DEAUTH FLOOD

Detecta alta frequência incomum de solicitações de desconexão, típicas de ataques de negação de serviço.

AUTH FLOOD

Monitora múltiplas tentativas de autenticação rejeitadas em curto espaço de tempo.

PACKET FLOOD

Conta o número de pacotes enviados por segundo por cada endereço MAC para identificar excessos anormais.

Dispositivos identificados como ofensores são inseridos automaticamente na blacklist temporária, impedindo conexões subsequentes e protegendo a rede.

DESAFIOS TÉCNICOS ENFRENTADOS

LIMITAÇÕES AVANÇADAS

ARP Spoofing: demanda manipulação em nível de camada 2, com controle detalhado da pilha de rede não suportado no ESP32 padrão.

COMPLEXIDADE DO EVIL TWIN

Requer replicar o AP legítimo com múltiplas interfaces Wi-Fi ou soft APs simultâneos, indisponíveis no firmware nativo do ESP32.

MOTIVOS TÉCNICOS

Firmware restrito, ausência de suporte ao modo monitor + AP simultâneo e necessidade de modificações profundas no IDF da Espressif.

RESULTADO PRÁTICO

Foco confiável em ataques de flooding, ampliando conhecimento em segurança Wi-Fi embarcada e limites do hardware.

CONCLUSÃO E APRENDIZADOS

RESULTADOS DE DEFESA

Identificação e bloqueio eficaz dos ataques simulados, com preservação dos clientes legítimos.

SOLUÇÕES EMBUTIDAS

Blacklist dinâmica e lógica embarcada com recursos limitados do ESP32 mostraram-se eficientes.

POTENCIAL DIDÁTICO

O projeto oferece uma ferramenta prática para educação em segurança de redes Wi-Fi e testes em ambientes controlados.

FIM