Professor
Massaki

Soluções Integradas com IoT

Tema: Segurança Cibernética

SENAI

A importância do Monitoramento na Segurança Cibernética

Hoje exploraremos a importância do monitoramento em redes de computadores, focando na ferramenta Wireshark, que fornece popssibilidade de diagnóstico e segurança, com exemplos e telas demonstrativas, que ilustrarão o poder do Wireshark no fortalecimento da sua postura de segurança cibernética. permitindo a detecção de anomalias e tráfego malicioso.

A importância do Monitoramento na Segurança Cibernética

A segurança cibernética é um campo em constante evolução, onde o monitoramento de redes desempenha um papel fundamental na proteção contra ameaças. O monitoramento proativo permite a detecção precoce de atividades suspeitas, minimizando o impacto de ataques. A resposta à incidentes, com a geração de alertas em tempo real e a automação de respostas, é crucial para mitigar ataques e isolar dispositivos comprometidos.

No entanto, o monitoramento de redes enfrenta desafios como a escalabilidade em redes grandes, a criptografia que impacta a visibilidade e a ocorrência de falsos positivos e negativos em alertas. Ameaças cibernéticas atuais, como ransomware, phishing e DDoS, ressaltam a necessidade de uma defesa proativa, garantindo a conformidade com regulamentações como a LGPD e protegendo contra o impacto financeiro e reputacional de incidentes.

Monitoramento Proativo

Identificação precoce de atividades suspeitas

Resposta a Incidentes

Geração de alertas em tempo real

Conformidade Regulatória

Atendimento a normas como a LGPD

O que é o Wireshark?

O Wireshark é um analisador de protocolos de rede de código aberto, disponível para Linux, Windows e macOS. Permite a captura e análise de pacotes em tempo real, oferecendo uma visão detalhada do tráfego de rede. A ferramenta é utilizada para analisar micro detalhes de um fluxo de dados.

O Wireshark foi criado por Gerald Combs no final dos anos 90 e originalmente chamado de Ethereal, foi rebatizado para Wireshark devido a problemas de marca registrada. Sua história de desenvolvimento é marcada por uma comunidade ativa que contribui continuamente para aprimorar suas funcionalidades e suportar novos protocolos. O Wireshark se tornou uma ferramenta indispensável para profissionais de redes, segurança cibernética e desenvolvedores de software.

Código Aberto

Disponível para todos

Multiplataforma

Compatível com Linux, Windows e macOS

Captura em Tempo Real

Análise imediata do tráfego

Principais Características do Wireshark

O Wireshark oferece uma ampla gama de recursos para análise de redes. A captura de pacotes em diversas interfaces de rede permite monitorar o tráfego em diferentes pontos da rede. Os filtros de captura e visualização, como tcp.port == 80, facilitam a análise de tráfego específico.

A ferramenta suporta a análise de diversos protocolos, como TCP, UDP, HTTP e DNS, e fornece estatísticas detalhadas de rede, incluindo tráfego e protocolos utilizados. Além disso, o Wireshark permite a decriptação de tráfego SSL/TLS e WEP/WPA, quando possível e legal, oferecendo uma visão clara do conteúdo dos pacotes.

Filtros

Captura e visualização seletiva

Análise de Protocolos

Suporte para TCP, UDP, HTTP, DNS

Decriptação

SSL/TLS e WEP/WPA (quando possível)

Aplicações do Wireshark na Prática

O Wireshark é amplamente utilizado para solucionar problemas de rede, como lentidão e falhas, permitindo a identificação de gargalos e a análise de pacotes perdidos. Na análise de tráfego HTTP, o Wireshark possibilita inspecionar requisições, respostas e cookies, auxiliando no diagnóstico de problemas de aplicações web.

A ferramenta é essencial na investigação de incidentes de segurança, auxiliando na identificação de malware e ataques, bem como na análise de tráfego de VoIP para avaliar a qualidade de chamadas e codecs utilizados. Engenheiros de redes e desenvolvedores de sistemas usam a ferramenta para análise de protocolos.

Troubleshooting

Identificação de gargalos e falhas

Análise HTTP

Inspeção de requisições e respostas

Investigação de Segurança

Identificação de malware e ataques

Wireshark em Cybersecurity: Detecção de Anomalias

No campo da segurança cibernética, o Wireshark é uma ferramenta poderosa para a detecção de anomalias em redes. A identificação de tráfego incomum, como portas ou destinos inesperados, é facilitada pela análise detalhada dos pacotes capturados. A análise de payloads suspeitos, incluindo a busca por strings ou padrões específicos, pode revelar a presença de malware ou atividades maliciosas.
O Wireshark também auxilia na detecção de exfiltração de dados, identificando transferências volumosas de informações para destinos desconhecidos. Filtros específicos podem ser utilizados para identificar potenciais ataques, como SYN flood, permitindo uma resposta rápida e eficaz.

Tráfego Incomum

Identificação de portas e destinos atípicos

Payloads Suspeitos

Análise de strings e padrões maliciosos

Exfiltração de Dados

Detecção de transferências volumosas

Wireshark em Cybersecurity: Análise de Malware

A análise de malware é uma das aplicações cruciais do Wireshark na área de segurança cibernética. A ferramenta permite identificar a comunicação com servidores de C&C (Command & Control), revelando a presença de malware na rede. A análise de tráfego DNS pode detectar domínios maliciosos, utilizados para disseminar malware ou realizar ataques de phishing.

O Wireshark também permite a detecção de malware baseado em assinatura, identificando strings conhecidas associadas a determinados tipos de malware. Um exemplo prático é a análise de um arquivo PCAP com tráfego malicioso, onde o Wireshark exibe o tráfego e os filtros utilizados para identificar a atividade maliciosa.

Servidores C&C

Identificação de comunicação com servidores de controle

Tráfego DNS

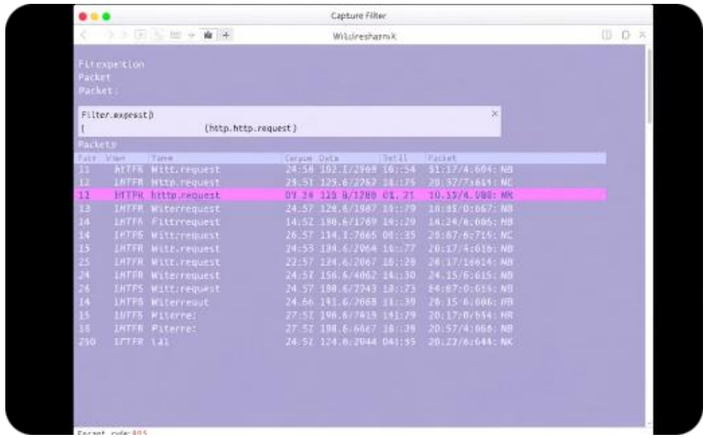
Detecção de domínios maliciosos

Assinaturas

Detecção de strings conhecidas de malware

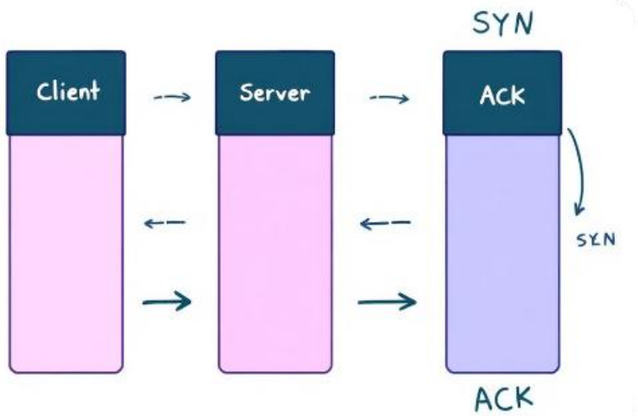
Exemplos Práticos com Wireshark

Para ilustrar o uso do Wireshark, apresentamos alguns exemplos práticos.
A demonstração de filtros de captura, como **ip.addr == 192.168.1.100**, mostra como focar em tráfego específico. A análise de um handshake TCP (SYN, SYN-ACK, ACK) revela o estabelecimento de uma conexão.
A visualização do conteúdo de um pacote HTTP (GET request) permite inspecionar os dados transmitidos em uma requisição web.
A análise de um pacote DNS (query e response) mostra como o Wireshark pode ser utilizado, por exemplo, para monitorar a resolução de nomes de domínio.



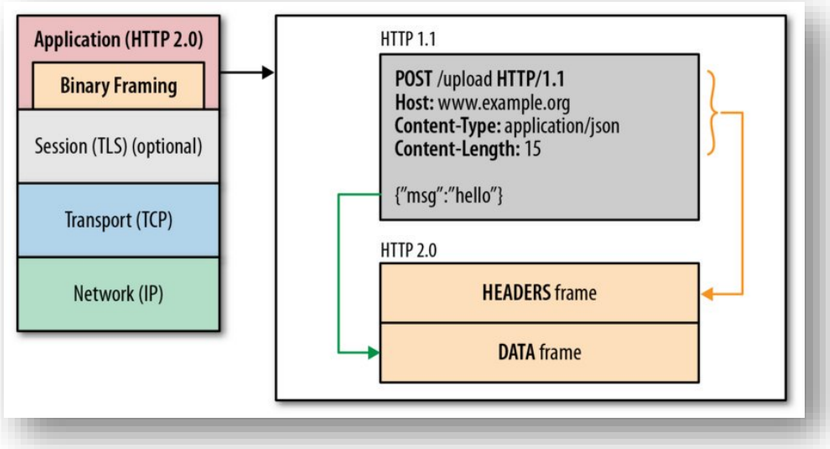
Filtros de Captura

Captura de tráfego específico



Handshake TCP

Análise da conexão TCP

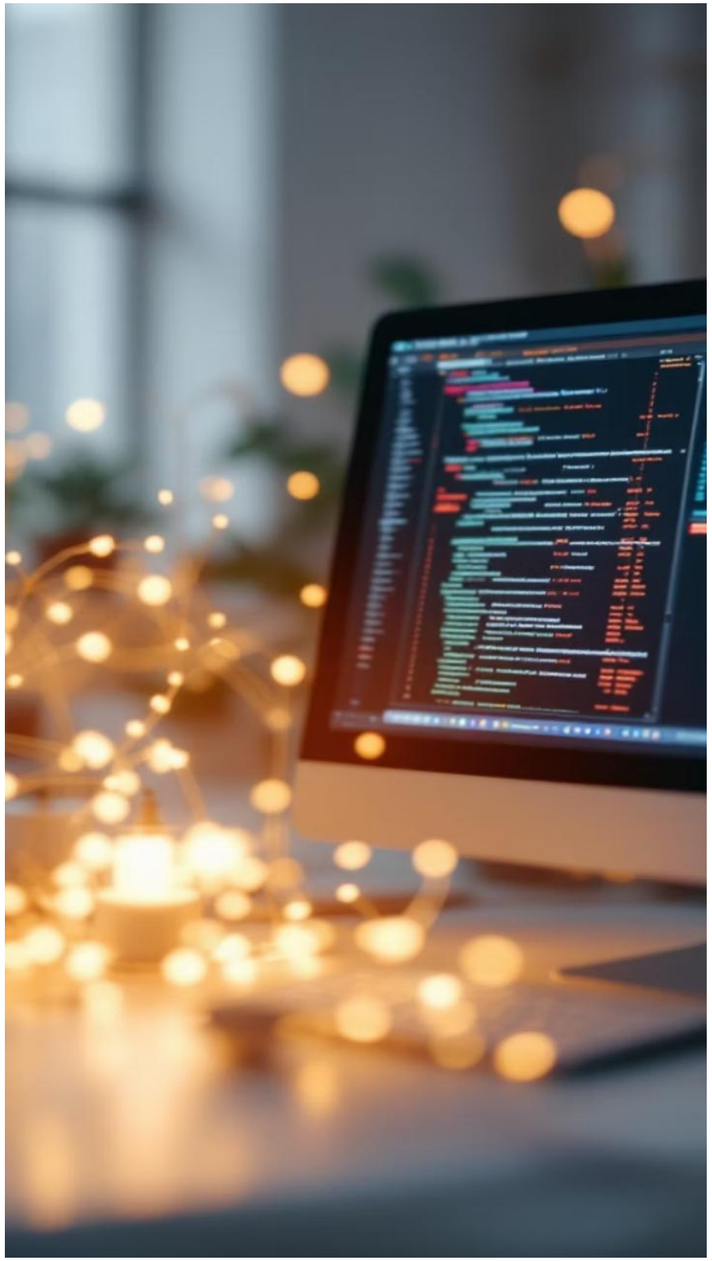


Pacote HTTP

Visualização do conteúdo HTTP

Estudo de Caso: Análise de Rede com Wireshark e ESP32

Neste estudo de caso prático faremos uma breve análise da rede utilizando o Wireshark e o microcontrolador ESP32. Examinaremos como o Wireshark pode ser usado para monitorar dados trocados entre um terminal de acesso IP e um servidor web hospedado em uma placa ESP32. Além disso, discutiremos a importância da segurança de rede, com foco na implementação de Access Control Lists (ACLs) para proteger as comunicações.



Wireshark: Ferramenta para Análise de Tráfego de Rede

Análise Detalhada de Pacotes

O Wireshark é uma poderosa ferramenta de análise de tráfego de rede que permite capturar pacotes em tempo real. Ele oferece recursos avançados para diagnóstico e segurança, ajudando a identificar e solucionar problemas de rede. É uma ferramenta indispensável para qualquer administrador de rede.

Filtros Avançados para Análise Específica

Com seus filtros avançados, o Wireshark possibilita a análise específica de tráfego, permitindo que você se concentre nos dados relevantes. Seja para identificar gargalos na rede ou investigar possíveis ataques, o Wireshark oferece as ferramentas necessárias para uma análise completa.

Filtros básicos para Ips no Wireshark

- `ip.addr == <endereço_ip>`: Filtra todos os pacotes onde o IP especificado é a origem ou o destino.

- `ip.src == <endereço_ip>`: Mostra apenas os pacotes enviados do endereço IP de origem especificado.

- `ip.dst == <endereço_ip>`: Exibe apenas os pacotes enviados para o endereço IP de destino especificado.

ESP32 como Servidor Web: Uma Solução IoT Versátil

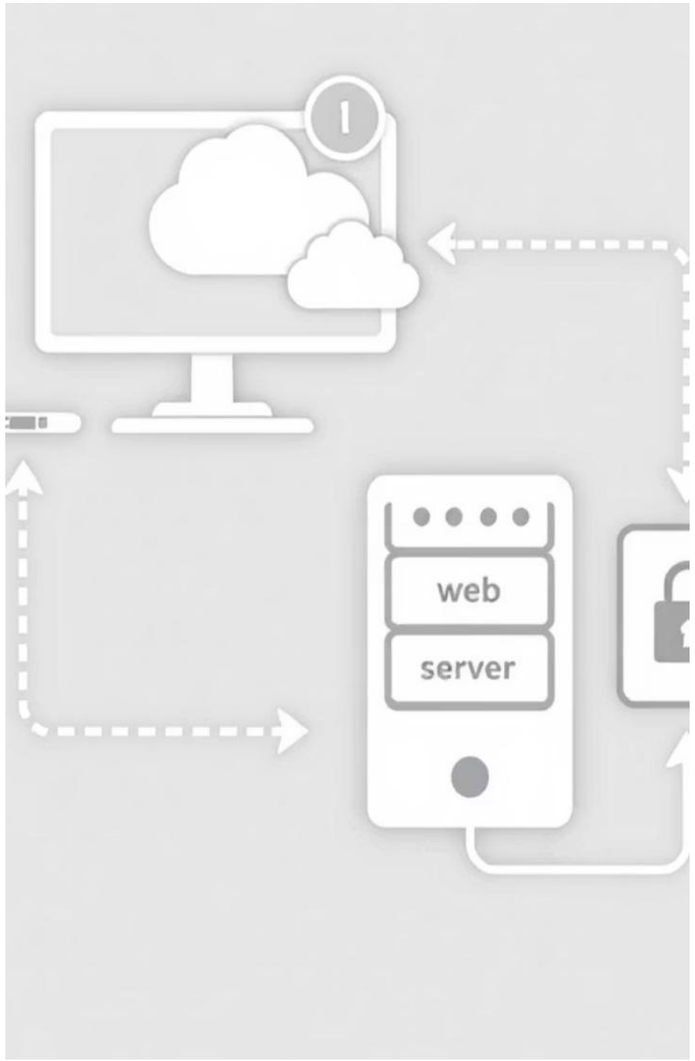
Microcontrolador Programável

O ESP32 é um microcontrolador programável ideal para aplicações de Internet das Coisas (IoT). Sua capacidade de hospedar páginas web e monitorar dados de sensores o torna uma escolha popular para projetos de automação e monitoramento remoto.

Comunicação HTTP

A comunicação entre o cliente e o servidor ESP32 ocorre via HTTP, o protocolo padrão da web. Essa comunicação permite que os dispositivos interajam e troquem dados de forma eficiente, abrindo portas para diversas aplicações inovadoras.

Cenário do Estudo de Caso: Monitorando a Comunicação ESP32



Comunicação Terminal IP e ESP32

Nosso estudo de caso se concentra na comunicação entre um terminal IP e um ESP32 configurado como servidor web. Utilizaremos o Wireshark para monitorar os dados trocados na rede e identificar possíveis vulnerabilidades.

Avaliação de Vulnerabilidades

O objetivo principal é avaliar as vulnerabilidades presentes na comunicação entre o terminal IP e o servidor web ESP32. Buscaremos identificar brechas de segurança que possam comprometer a integridade dos dados.

Análise Detalhada com Wireshark

A ferramenta Wireshark será nossa principal aliada para analisar o tráfego de rede, permitindo-nos inspecionar os pacotes de dados e identificar informações sensíveis sendo transmitidas sem criptografia.

Configuração do Experimento: Preparando o Cenário de Teste

Servidor Web no ESP32

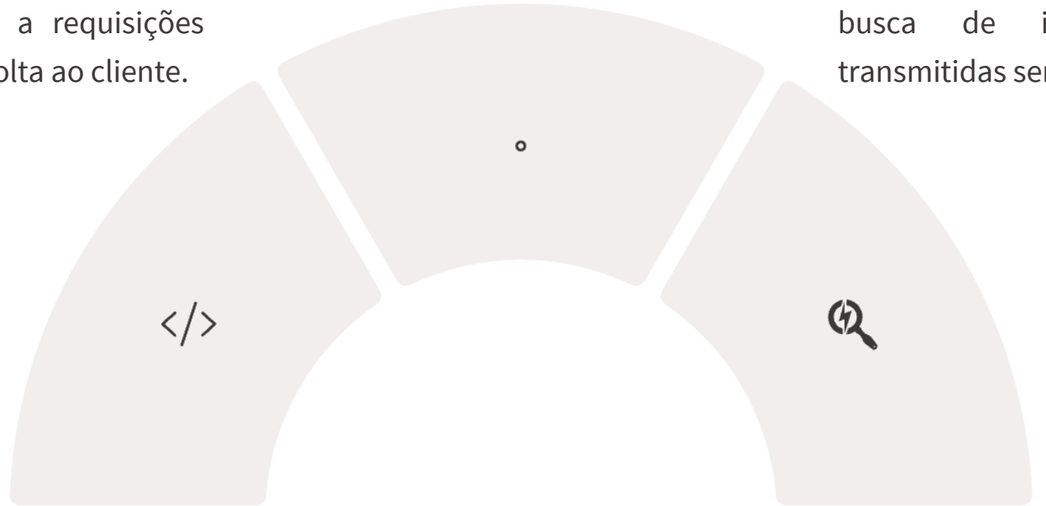
Implementamos um servidor web simples no ESP32 para simular a troca de dados com o terminal IP. Este servidor web responde a requisições HTTP e envia dados de volta ao cliente.

Conexão Wi-Fi e IP Fixo

O ESP32 é conectado à rede via Wi-Fi e configurado com um endereço IP fixo para facilitar a monitorização. Isso permite que o Wireshark identifique facilmente o tráfego entre o terminal IP e o servidor ESP32.

Análise HTTP com Wireshark

Usamos o Wireshark para analisar a comunicação HTTP entre o terminal IP e o servidor ESP32. Capturamos pacotes de dados e os analisamos em busca de informações sensíveis transmitidas sem criptografia.



Resultados da Captura: Expondo Dados Sensíveis

Pacotes HTTP Capturados

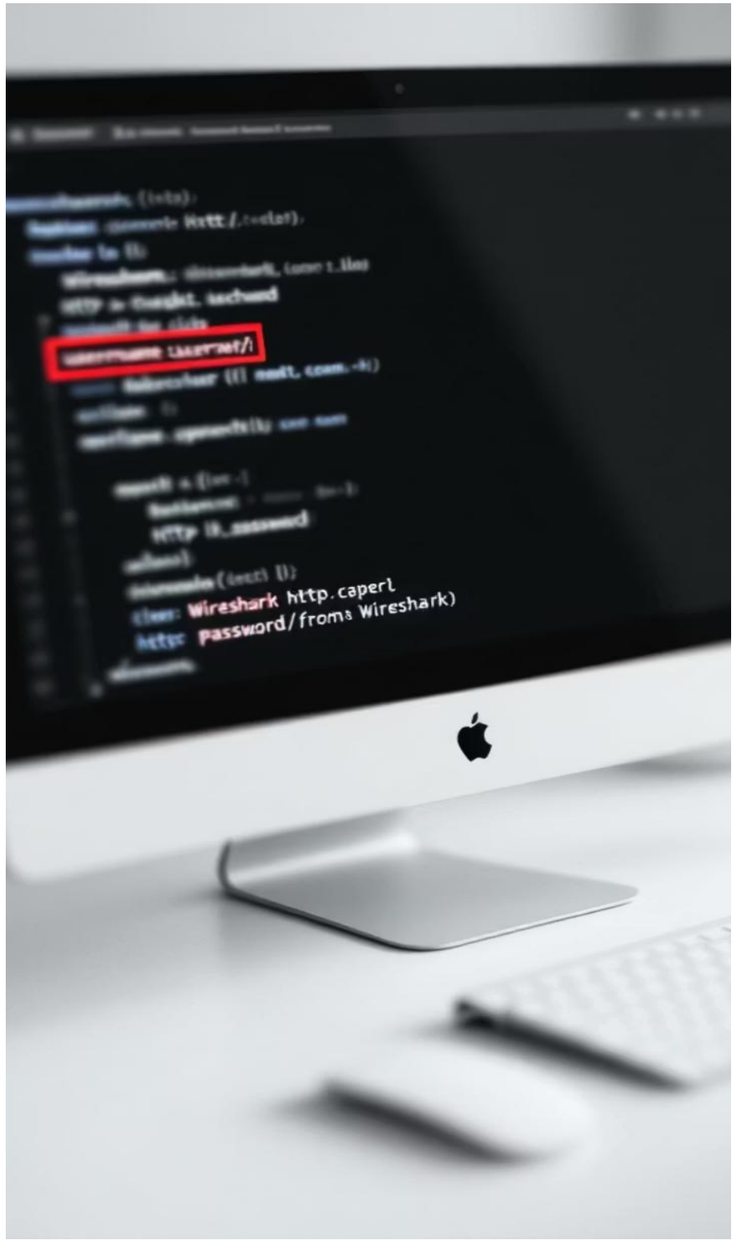
O Wireshark capturou com sucesso os pacotes HTTP trocados entre o terminal IP e o ESP32. Esses pacotes revelaram informações sobre as solicitações e respostas do servidor web.

Exposição de Dados

A análise dos pacotes revelou que dados sensíveis estavam sendo transmitidos sem criptografia. Isso inclui informações como credenciais de acesso, dados de formulários e outras informações confidenciais.

Falta de Criptografia

A ausência de criptografia SSL/TLS na comunicação HTTP permitiu que os dados fossem capturados e lidos facilmente por qualquer pessoa com acesso à rede e ao Wireshark.



Ameaças Identificadas: Riscos para a Segurança da Rede

Interceptação por Sniffers

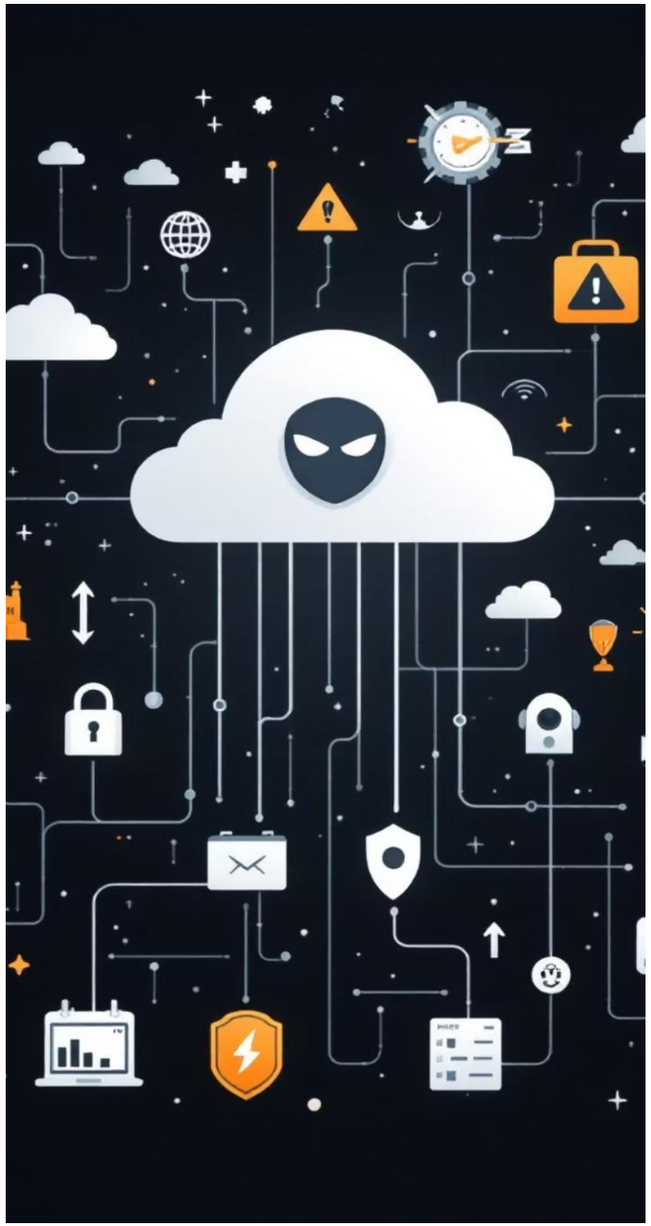
O risco de interceptação de dados por sniffers é elevado, pois qualquer pessoa na rede pode capturar o tráfego e ler os dados não criptografados.

Vulnerabilidades HTTP

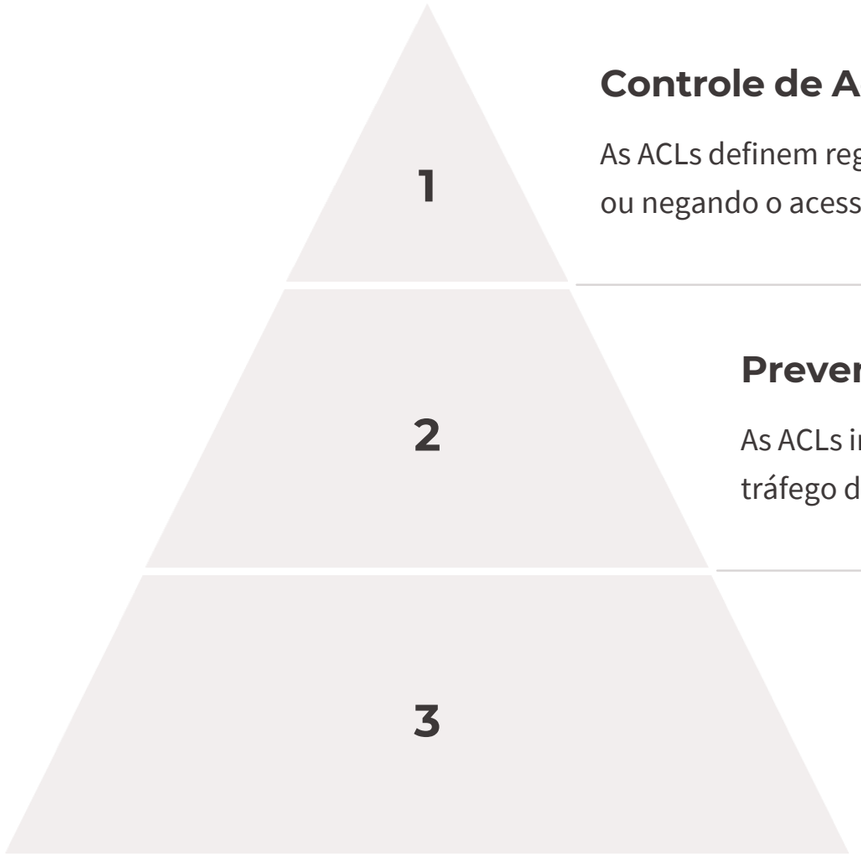
Conexões HTTP sem SSL são vulneráveis a ataques, pois não oferecem proteção contra a interceptação de dados sensíveis.

Ataques Man-in-the-Middle

A possibilidade de ataques “man-in-the-middle” é real, pois um invasor pode interceptar a comunicação e modificar os dados antes de serem entregues ao destinatário.



ACLs: A Primeira Linha de Defesa



Controle de Acesso

As ACLs definem regras para controlar o acesso ao tráfego na rede, permitindo ou negando o acesso com base em critérios específicos.

Prevenção de Acessos

As ACLs impedem acessos não autorizados à rede, bloqueando tráfego de fontes desconhecidas ou não confiáveis.

Proteção contra Espionagem

As ACLs são cruciais para prevenir a espionagem de dados, limitando o acesso a informações sensíveis apenas a dispositivos autorizados.

Implementando ACLs no ESP32: Reforçando a Segurança

Bloqueio de IPs Desconhecidos

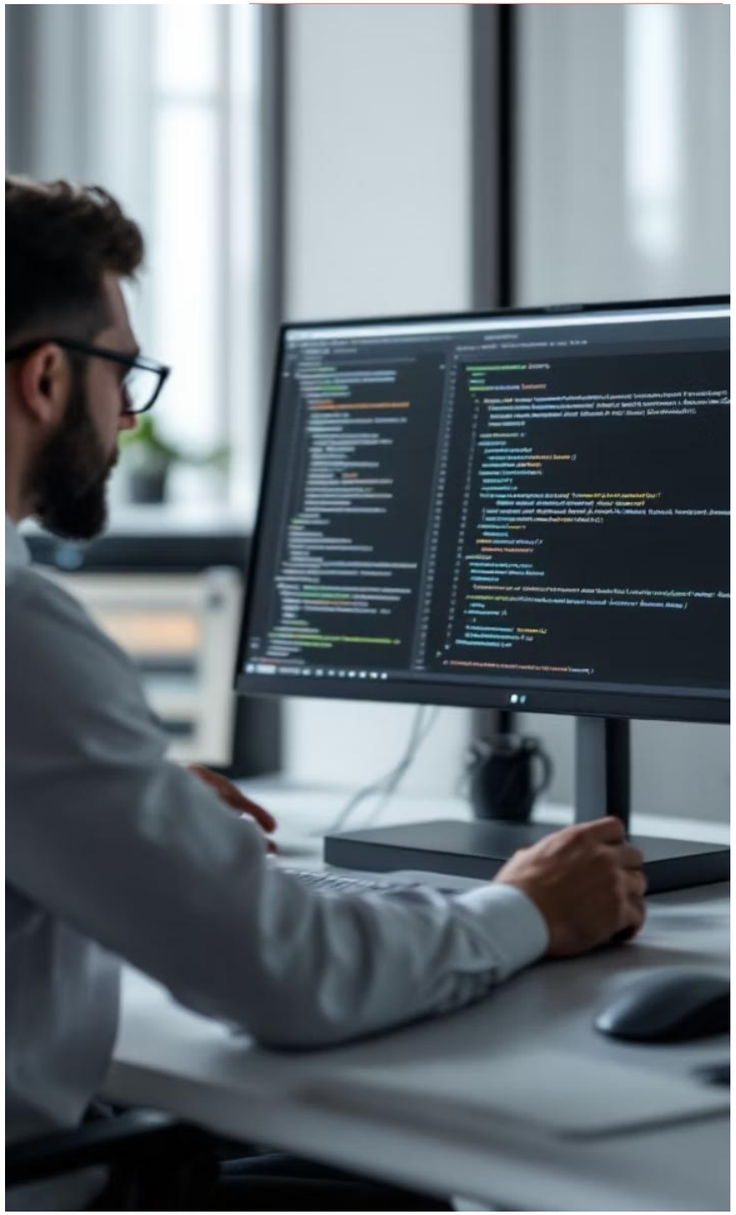
As ACLs podem ser configuradas para bloquear o tráfego de IPs desconhecidos, impedindo que dispositivos não autorizados acessem a rede.

Limitação de Portas

As ACLs podem limitar as portas permitidas, como a porta 80 para HTTP, restringindo o acesso a serviços específicos apenas a dispositivos autorizados.

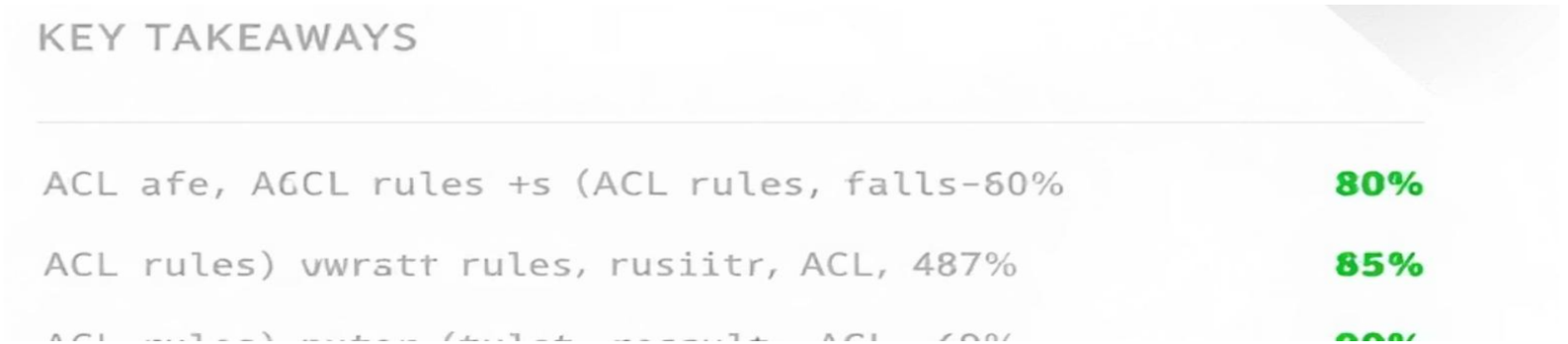
Permissão de Dispositivos Específicos

As ACLs podem permitir apenas o tráfego de dispositivos específicos, como um terminal IP autorizado, bloqueando qualquer outro acesso à rede.



Conclusões

Wireshark e ACLs como Ferramentas Essenciais



1

Diagnóstico

O Wireshark é fundamental para diagnosticar e analisar vulnerabilidades em redes, permitindo identificar brechas de segurança e dados sensíveis transmitidos sem criptografia.

2

Segurança

A segurança da comunicação no ESP32 depende de medidas como ACLs e SSL, que protegem os dados contra interceptação e acesso não autorizado.

3

Práticas

A implementação de ACLs e o uso de criptografia SSL/TLS são práticas fundamentais para proteger redes modernas contra ameaças cibernéticas.

Conclusões

O Wireshark é uma ferramenta importante devido a seus recursos poderosos para monitoramento de redes e segurança cibernética. A capacidade de capturar e analisar pacotes em tempo real permite diagnosticar problemas, detectar anomalias e investigar incidentes de segurança.

Para aprofundar o conhecimento, recomenda-se praticar com cenários reais e explorar outras ferramentas de segurança. Boas práticas e políticas de monitoramento, como a definição de KPIs e SLAs, a atualização contínua de ferramentas e políticas e o treinamento da equipe, são fundamentais para garantir a eficácia do monitoramento.

Boas Práticas
Indicadores chaves de Processo (KPIs)

Atualização
Ferramentas e políticas

Treinamento
Capacitação da equipe

ATIVIDADE

Agora, vocês precisarão se dividir **em grupo e** escolher um dos 5 temas a seguir (máximo 2 grupos por tema). Depois

Elaborar uma apresentação (mínimo 8 e máximo 10 slides) sobre 1 dos temas a seguir:

1. **Segurança cibernética**
2. **Engenharia Social**
3. **Política de Segurança da Informação - PSI**
4. **Marco Civil da Internet**
5. **Lei Geral de Proteção de Dados (LGPD)**

Nesta atividade todos estarão sendo avaliados pelas Conhecimentos

- Identificar medidas de proteção e prevenção de ataques cibernéticos.
- Conhecer para poder seguir políticas, procedimentos e legislação de segurança da informação

e capacidades:

- **Demonstrar pensamento analítico**
- **Demonstrar autonomia**