UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
CURSO DE ESPECIALIZAÇÃO EM CONFIGURAÇÃO E GERENCIAMENTO DE SERVIDORES E EQUIPAMENTOS DE REDE

DANILO RENATO DE ASSIS

ANALISADOR DE REDE WIRELESS COM RASPBERRY PI

MONOGRAFIA DE ESPECIALIZAÇÃO

CURITIBA
2015

DANILO RENATO DE ASSIS

ANALISADOR DE REDE WIRELESS COM RASPBERRY PI

Monografia apresentada como requisito para a obtenção do grau de Especialista em Configuração e Gerenciamento de Servidores e Equipamentos de Rede, do Programa de Pós-Graduação em Tecnologia. Universidade Tecnológica Federal do Paraná. Área de Concentração: Redes de Computadores Orientador: Prof. MSc. Lincoln Herbert Teixeira.

CURITIBA
2015

RESUMO

ASSIS, Danilo R. **Analisador de Rede Wireless com Raspberry PI.** 2015. 48 folhas. Monografia (Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes). Universidade Tecnológica Federal do Paraná. Curitiba, 2015.

A presente monografia visa a implementação de um analisador de rede sem fio, visando identificar os pacotes que trafegam na rede. Isso facilita a identificação de possíveis invasões em uma rede pelo administrador. Devido ao seu tamanho reduzido, facilita da mobilidade dentro de uma empresa ou instituição para verificar as vulnerabilidades. O ambiente utilizado para teste é uma rede doméstica e a ferramenta utilizada para análise de pacotes é o TCPDUMP.

Palavras-chave: Raspberry. WIFI. Auditoria de Redes. Mobilidade. Embarcado. Wireless.

ABSTRACT

Assis, Danilo R. **Wireless Network Analyzer with Raspberry PI**. 2015. 48 pages. Monograph (Specialization in Configuration and Management of Servers and Network Equipment's). Federal Technological University of Paraná. Curitiba, 2015.

This monograph aims to implement a wireless network analyzer, to identify packets that travel over the network. This facilitates the identification of possible intrusions on a network administrator. Because of their small size facilitates mobility within a company or institution to verify the vulnerabilities. The environment is used to test a home network and the tool used for packet analysis is TCPDUMP.

Keywords: Raspberry. WIFI. Network audit. Mobility. Shipped. Wireless

LISTA DE SIGLAS

API - Application Programming Interface

BIT - Binary Digit

CSS - Cascading Style Sheets

DHCP - Dynamic Host Configuration Protocol

DNS - Domain Name Server

FTP - File Transfer Protocol

GB - Gigabytes

HTML - Hypertext Markup Language

HTTP - Hypertext Transfer Protocol

ICMP - Internet Control Message Protocol

IEEE - Institute of Electrical and Electronics Engineers

IP - Internet Protocol

ISO - International Organization for Standardization

ISP - Internet Service Provider

LAN - Local Area Network

MAN - Metropolitan Area Network

MB - Megabytes

Mbit/s - Megabits por Segundo

Network - Rede

OSI - Open Systems Interconnection

PHP - Hypertext Pre processor

POE - Power Over Ethernet

POP3 - Post Office Protocol Version 3

RAM - Random Access Memory

RFC - Request for Comments

SMTP - Simple Mail Transfer Protocol

SFTP - Secure File Transfer Protocol

SSH - Secure Shell

USB - Universal Serial Bus

TCP - Transmission Control Protocol

UDP - User Datagram Protocol

UTFPR - Universidade Tecnológica Federal do Paraná

WAN - Wide Area Network

WEB - World Wide Web

WIFI - Wireless Fidelity

WLAN – Wireless Local Area Network

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

A mobilidade de dispositivos tem se tornado um tema recorrente nas últimas décadas. Principalmente pelo fato da indústria eletrônica ter um fator de crescimento acelerado, o que contribuiu para dispositivos cada vez menores, e de baixo custo, sejam criados com múltiplos recursos. Aliado a esse raciocínio, o presente trabalho visa desenvolver um sistema mínimo utilizando as ferramentas de análise de redes sem fio em um equipamento de baixo custo. Otimizando, por consequência, o trabalho e agilizando o processo de identificação de eventos adversos na rede wireless.

1.1 TEMA

As redes de computadores têm se tornado, cada vez mais, parte integrante da sociedade digital, seja cabeada ou sem fio. Por isso é de suma importância que se tenha controle, cada vez melhor, dos dados que trafegam em uma LAN, bem como ter o controle dos eventos adversos que visam prejudicar o tráfego como um todo. Para isso acontecer, é necessário que seja realizado uma análise dos dados que circulam pelo ambiente digital seja ele corporativa ou pessoal.

A análise de tráfego é um assunto essencial para administradores de redes de computadores. Fazendo a análise, um administrador realmente dominará a sua rede. Muitas vezes, administradores não conhecem os conceitos básicos sobre protocolos de redes e terminam não resolvendo, conscientemente, os problemas técnicos encontrados. Isso sem mencionar os problemas que existem, mas nunca foram vistos ou notados (MOTA FILHO, 2013, p 37).

1.2 OBJETIVOS

Implementar um dispositivo mínimo embarcado com suporte a análise de pacotes de redes sem fio.

1.2.1 OBJETIVO GERAL

O principal objetivo deste projeto é implementar a ferramenta TCPDUMP, para fazer as análises dos pacotes, em um Raspberry PI, com uma interface WEB desenvolvida em PHP e com APACHE 2.

1.2.2 OBJETIVOS ESPECÍFICOS

São objetivos específicos deste trabalho:

- Criação de uma interface gráfica para apresentação dos resultados da execução da ferramenta de análise de pacotes em PHP;
- Integração com display de 3.5'' de LCD no Raspberry PI, para visualização das informações por parte do operador;

1.3 JUSTIFICATIVA

A análise de redes sem fio é feita utilizando equipamentos como notebook, programas como Wireshark® e a ferramenta de análise TCPDUMP, o que torna o processo lento devido à dimensão dos equipamentos e a dificuldade de manuseio em locais onde a rede sofre com obstáculos, bem como transporte dos mesmos até a rede em questão ou em deslocamento a um determinado campus ou empresa.

Além disso, as soluções do mercado como o AirCheck®, da Fluke Networks®, possuem um alto custo de aquisição e necessitam de treinamento prévio para utilização do equipamento.

A proposta deste projeto é a criação de uma ferramenta de fácil manipulação e, portanto, com baixo custo de implementação e manutenção em comparação com as soluções do mercado.

O Raspberry PI vem de encontro com o problema levantado por se tratar de computador em tamanho reduzido, de baixo custo e grande poder de processamento.

Algumas palavras surgem repetidamente quando as pessoas falam sobre o Raspberry Pi: pequeno, barato, hackeável, educacional. (RICHARDSON, 2013).

Com estes benefícios fica claro que a utilização, em projetos, por se tratar de um *hardware* reduzido, mas também sua grande capacidade de integração a outros projetos eletrônicos.

1.4 METODOLOGIA DA PESQUISA

Este trabalho foi desenvolvido com estudo da ferramenta TCPDUMP, de análise de tráfego, PHP e Apache 2, de cunho bibliográfico, por meio de consulta a livros, sites e palestras e proporcionou embasamento teórico e prático para implantação da plataforma de análise de pacotes em um sistema embarcado.

Para desenvolver tal recurso, foi utilizado o modelo “B+” do Raspberry Pi, com 512 MB de memória RAM, 2 portas USB 2.0, conforme a Figura 1 e cartão de memória de 16 GB.

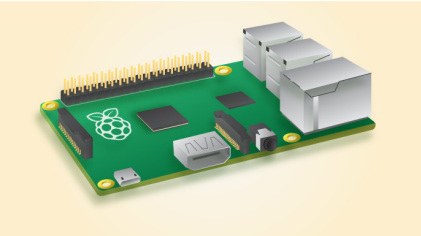

Figura 1 - Raspberry Pi B+
Fonte: raspberrypi.org. 2015.

Além de um mini adaptador USB wireless TP LINK 802.11n com velocidade 150 Mbit/s (Figura 2). Aliado ao hardware utilizado foi integrado um Display de LCD de 3.5 polegadas próprio para o Raspberry PI.

Figura 2 - USB Wireless
Fonte: Ali Express. 2015.

A versão da ferramenta de análise testada foi a versão 4.7.4, lançada em 22 de abril de 2015. Com relação a linguagem de programação PHP, a versão instalada foi a 5.6.9, com lançamento efetuado em 14 de maio de 2015. Seguindo, a instalação das ferramentas de análise e programação foi feita a partir de um sistema operacional customizado para Raspberry PI: O Raspbian, baseado em Linux Debian 7.3 Wheezy.

Em consonância com testes, foi analisado os requisitos mínimos para execução do projeto para determinar o equipamento necessário para um desempenho favorável.

Com o equipamento em operação, seguiu para etapa de coleta dos dados e processamento, no Raspberry PI, para análise das informações geradas pelo equipamento.

2 REFERENCIAL TEÓRICO

2.1 BREVE HISTÓRICO DAS REDES SEM FIO

A comunicação digital sem fios não é uma ideia nova. Em 1901, o físico italiano Guglielmo Marconi (Figura 3) demonstrou como funcionava um telégrafo sem fio que transmitia informações de um navio para o litoral por meio de código Morse. Os modernos sistemas digitais sem fios têm um desempenho melhor, mas a ideia básica é a mesma (TANEMBAUM, 2003).

Figura 3 - Guglielmo Marconi, 1901
Fonte: Ramo Estudantil – UEL, 2015.

Esse anseio de mobilidade teve um crescimento acentuado ao longo dos anos, e consequentemente o desejo de velocidade de transmissão cada vez maior. Com o passar o tempo, as redes sem fio foram padronizadas pelo IEEE com o nome de padrão 802.11, na década de 90, e suas derivações ao logo dos anos como: 802.11b, 802.11a, 802.11g, 802.11n, 802.11ac (Figura 4).

Figura 4 - Padrões IEEE802.11
Fonte: ENTELCO TELECOM, 2015.

2.2 A RAZÃO DE UTILIZAR AS REDES SEM FIO

As redes sem fio estão cada vez mais presentes tanto nas redes corporativas quanto nas redes pessoais, devido a sua mobilidade entre os espaços tanto interno como externo de uma residência como de um departamento empresarial. Ainda aliado a isso, a rede cabeada dependendo do ambiente, não é a melhor opção devido a limitação física. É nesse sentido que as redes sem fio se tornam a melhor solução tanto em mobilidade quanto em atendimento aos requisitos do local.

Uma outra vantagem das redes sem fio é o custo da implantação e operação ser menor em comparação com a rede cabeada, garantindo melhor desempenho e eficiência com menores custos em um tempo relativamente menor que rede entregue via cabo.

Com esses fatores positivos, as redes sem fio têm se popularizado em grande escala e faz necessário um maior controle dos eventos adversos da rede, afim de controlar e otimizar a LAN de acordo com o uso definido.

2.3 ANÁLISE DE TRÁFEGO DE REDE

A análise tráfego de dados nos permite detectar, rapidamente, quais problemas estão ocorrendo em uma rede e onde eles estão. (MOTA FILHO, 2013).

Para que isto seja possível é necessário conhecimento da topologia da rede, a fim de isolar com maior rapidez segmento comprometido.

Ao analisar os dados que trafegam na rede é possível constatar algumas possibilidades:

- Pode-se encontrar pontos de obstrução na rede;
- Detectar eventos adversos na rede;
- Identificar os equipamentos ou estruturas defeituosas;
- Analisar informações não visíveis ao usuário, como mensagens de retorno dos protocolos;

Para realizar a análise de trafego da rede é de suma importância ter conhecimento sobre os protocolos em questão e do modelo de referência da ISO, chamado Modelo OSI além da ferramenta de análise de pacotes.

O software de análise de pacotes está disponível em sites da internet e em produtos comerciais. Professores que ministram um curso de redes passam exercícios que envolvem a composição de um programa de reconstrução de dados de da camada de aplicação e um programa analisador de pacotes. (KUROSE; ROSS, 2013)

2.4 MODELO OSI

O modelo de referência Open Systems Interconection (OSI) foi desenvolvido pela ISO como um modelo para a arquitetura de um protocolo de comunicação de dados entre dois computadores (TELECO, 2007)

Com essa proposta de padronização é possível realizar a interoperabilidade, compatibilidade, portabilidade e ainda escalabilidade nas redes. O modelo é estruturado em níveis ou camadas em que cada camada possui serviços específicos e são oferecidos a camada imediatamente superior e inferior. A Figura 5 mostra a estrutura dos níveis do modelo de referência com seus respectivos serviços.

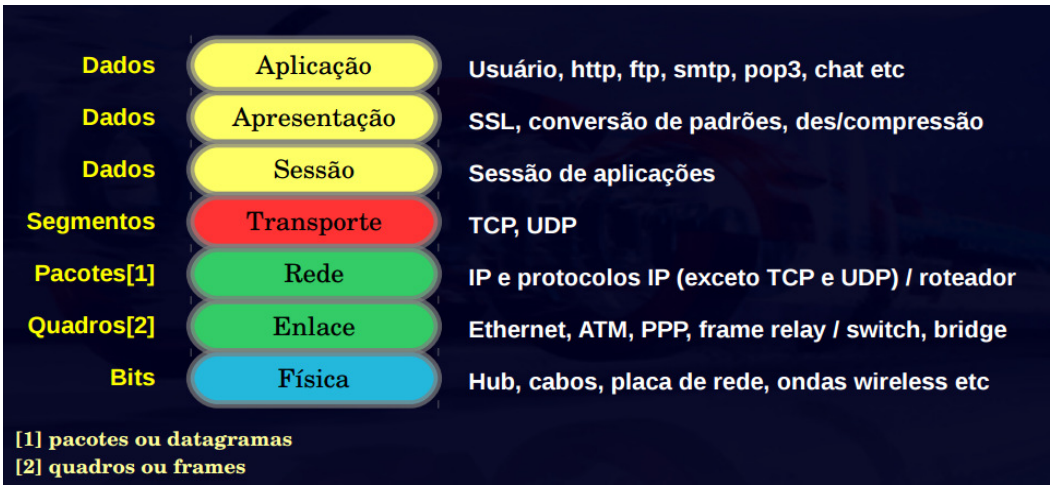

Figura 5 - Modelo OSI
Fonte: MOTA FILHO, 2013.

2.4.1 CAMADA APLICAÇÃO

A camada de aplicação é o nível mais próximo do usuário. É nessa camada que estão os serviços e protocolos que compõem os nossos aplicativos. É aqui que encontramos: TELNET, FTP, SMTP e outros protocolos. (TAVARES C ALEXEI, 2011).

2.4.2 CAMADA APRESENTAÇÃO

A camada de apresentação faz o tratamento dos dados de origem, da camada sessão, de forma que os mesmos sejam entendidos pela camada de aplicação. Os serviços oferecidos por esta camada são: compressão de dados e criptografia.

2.4.3 CAMADA SESSÃO

A camada de sessão é responsável pelo início e fim de uma conexão de rede. Essa camada dispõe de serviços de transferência eficiente de dados para as camadas superiores imediatamente superiores.

2.4.4 CAMADA TRANSPORTE

É nessa camada que ocorre o estabelecimento da sessão TCP, segmentando os dados e enviando-os através da rede até o destino, onde dados são remontados. Os protocolos presentes nesta camada são: TCP e UDP.

2.4.5 CAMADA DE REDE

A camada de rede ou camada 3 é uma das camadas mais nobres, pois estabelece a rede. É nela que encontraremos o IP e todos os seus protocolos, exceto TCP e UDP. Também é nela que ocorre o roteamento. (MOTA FILHO, 2013).

Além do roteamento, a camada 3 trata os problemas encontrados tanto nas rotas como na verificação do fluxo e erros de endereçamento.

2.4.6 CAMADA ENLACE

A principal tarefa da camada de enlace de dados é transformar um canal de transmissão bruta em uma linha que pareça livre de erros de transmissão não detectados para a camada de rede. Para executar essa tarefa, a camada de enlace de dados faz com que o transmissor divida os dados de entrada em quadros de dados (que, em geral, têm algumas centenas ou alguns milhares de bytes), e transmita os quadros sequencialmente. Se o serviço for confiável, o receptor confirmará a recepção correta de cada quadro, enviando de volta um quadro de confirmação. (TANENBAUM, ANDREW S., 2003, p.46)

2.4.7 CAMADA FÍSICA

Nessa camada encontramos tudo o que é físico. Nela estão elementos como cabos de rede, placas eletrônicas, ondas eletromagnéticas de dispositivos wireless entre outros. (MOTA FILHO, 2013, p 271)

Os dados trafegam através do cabeamento via eletricidade ou luz, representados por bits (1 ou 0).

2.5 PROTOCOLOS

Um acordo que especifica o formato e o significado da troca de mensagens entre computadores é conhecido como protocolo de comunicação. Os programas aplicativos que usam a rede não interagem diretamente com hardware de rede. Em vez disso, um aplicativo interage com o software de protocolo que segue as regras de um determinado protocolo quando da comunicação. (COMER, DOUGLAS S., 2009. p 246)

Os protocolos são um conjunto de regras que regem a forma como comunicação entre os sistemas e programas acontecem. Eles podem ser classificados quanto a sua procedência em proprietários ou abertos.

Além de reger a comunicação, os protocolos podem fornecer informações sobre a rede tais como performance, erros e endereçamento.

A seguir será descrito a função dos protocolos usados neste projeto como: ICMP, POP3, SMTP, HTTP, TELNET, FTP, DHCP E DNS.

2.5.1 ICMP

O protocolo ICMP (Internet Control Message Protocol), comumente conhecido como “ping”, faz parte da família de protocolos TCP/IP, fornece relatórios de erros e estados para o agente solicitante e é referenciado pela RFC 792 de setembro de 1981.

O cabeçalho do ICMP possui no total 32 bits de largura, com campos como *Type* e *Code* de 8 bits cada, variando de 0 a 255 e contem respectivamente o tipo de ping e código do mesmo. A figura 6 ilustra o cabeçalho do protocolo ICMP de forma básica, com os campos *Type*, *Code* e *Checksum*.

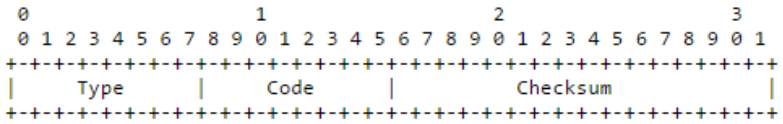

Figura 6 - Cabeçalho básico do ICMP
Fonte: RFC 792.

O campo *Type* são tipos de mensagem de retorno do ICMP através da rede e o campo *Code* é uma mensagem informativa que mostra o significado do retorno do *ping*.

A tabela 1 mostra as principais variações dos campos *Type* e *Code* e o significado de cada resposta.

Tabela 1 - Type e Code do ICMP corriqueiros

Type	Code	Significado
0 – *echo reply*	0 – *ping echo reply*	Resposta de *ping*.
3 – *destination unreachable*	0 – *network unreachable*	A rede de destino não foi encontrada.
	1 – *host unreachable*	A máquina de destino não foi encontrada.
	2 – *protocol unreachable*	O protocolo de destino não foi encontrado.
	3 – *port unreachable*	A porta de destino não foi encontrada.
	4 – *Fragmentation needed and DF was set*	Um roteador existente no itinerário precisa realizar a fragmentação, mas a *flag don´t fragment* está ativada. Então, a máquina de origem deverá fazer tal fragmentação ou construir pacotes menores.
	5 – source route failed	Falha na rota de origem.
	6 – *destination host unknown*	A máquina de destino é desconhecida.
	7 – *destination network unknown*	A rede de destino é desconhecida.
8 – *echo request*	0 –*ping echo request*	Envio de um *ping*.
11- *time exceeded*	1 – *fragment reassembly time exceeded*	Tempo excedido ao remontar o fragmento.

Fonte: Adaptado de João Eriberto Mota Filho. (2013 p 210)

2.5.2 POP3

O protocolo POP3 ou *Post Office Protocol*, na sua versão 3, é o protocolo com a função de recuperação das mensagens de e-mail através do controle da conexão entre um cliente de e-mail e um servidor de e-mail e é regulamentado pela RFC 1939 em maio de 1996.

O POP3 começa quando o usuário inicia o leitor de correio. O leitor de correio chama o ISP (a menos que já exista uma conexão) e estabelece uma conexão TCP com o agente de transferência de mensagens na porta 110. (TANENBAUM, ANDREW S., 2003, p.458)

2.5.3 SMTP

A função do protocolo *SMTP, Simple Mail Transfer Protocol*, é transferir e-mails de forma confiável e eficiente. A primeira versão foi referenciada pela RFC 788 de novembro de 1981 e sofreu atualizações das *RFC´s* posteriores.

Em sua concepção, o protocolo SMTP é independente do sistema operativo utilizado pelo usuário destinatário quanto pelo emissor, conduzindo os e-mails pela internet sem problemas de compatibilidade com sistema operacional utilizado no dispositivo do usuário.

2.5.4 HTTP

Em princípio, HTTP é simples: permite a um navegador solicitar um item específico, que o servidor então retorna. (COMER, DOUGLAS S., 2009. p 485)

O funcionamento do protocolo HTTP pode ser resumido em:

- O cliente digita o endereço no navegador;
- O servidor encontra o arquivo solicitado;
- O servidor lê o arquivo e devolve ao requisitante;
- O navegador requisitante exibe a página solicitada;

A figura 7 mostra o acesso a um servidor HTTP através do nome “exemplo.com.br”.

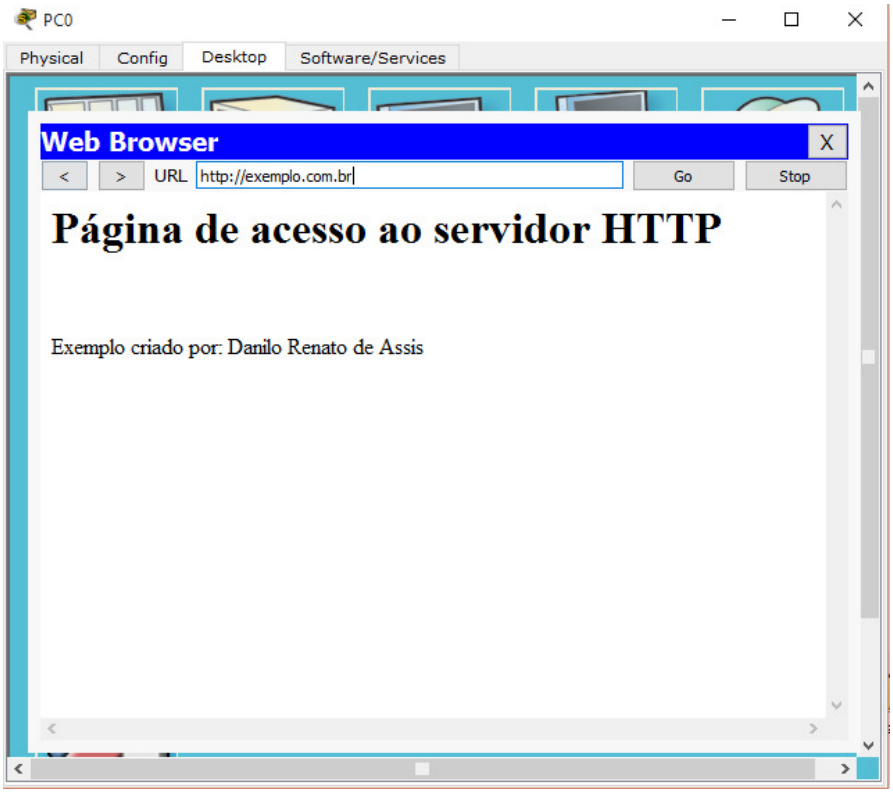

Figura 7 - Exemplo de acesso HTTP
Fonte: Autoria própria.

2.5.5 TELNET

O TELNET é um protocolo, cliente – servidor, de camada 7 do modelo OSI, e permite acesso remoto às interfaces de entrada e saída de uma máquina. Este protocolo foi um dos primeiros protocolos de acesso remoto criado e embora seja superado por outros mais confiáveis.

O TELNET ainda resiste devido ao fato de ter sido protocolo padrão instalado nos equipamentos antigos e que ainda estão em operação. Esse protocolo tornou-se obsoleto devido a total falta de segurança significando que os dados trafegam com formato de texto plano sendo de fácil interceptação e, consequentemente, identificação das informações como usuário e senha. Com essa vulnerabilidade,

surgiu outros protocolos como SSH que criptografa os dados que trafegam entre as sessões.

O TELNET foi regulamentado em maio de 1983 pela RFC 854 e posteriormente em março de 2008, atualizado pela RFC 5198 e estabelece uma conexão TCP através da porta 23 onde é possível enviar e receber bytes em forma de protocolo de aplicação como HTTP.

A figura 8 mostra o acesso via TELNET a um roteador Cisco 2621XM® na ferramenta de simulação *Cisco Packet Tracer®.*

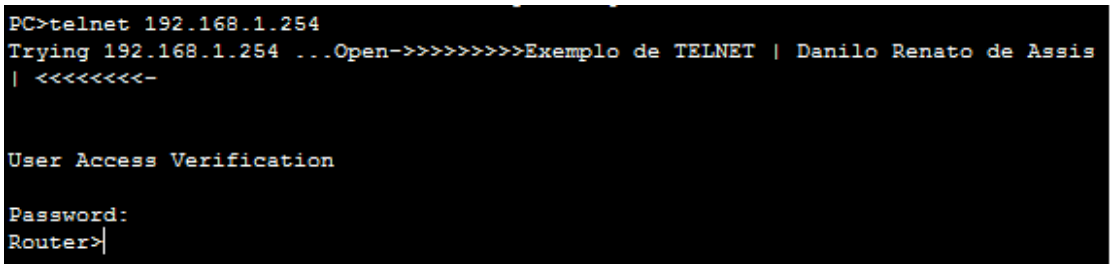

Figura 8 - Exemplo de TELNET
Fonte: Autoria própria.

2.5.6 FTP

Este protocolo atua na camada 7 do modelo OSI e é responsável pelo serviço de transferência de arquivos entre computadores. O FTP está entre os protocolos de aplicativos mais antigos ainda em uso na internet e é invocado pelos navegadores quando um usuário requer um *download* de arquivo. (COMER, DOUGLAS S., 2009. p 466)

A figura 9 demostra o acesso via FTP na porta 21, utilizada para transferência de dados de controle, e a porta 22, para conexão de dados entre dos dois computadores.

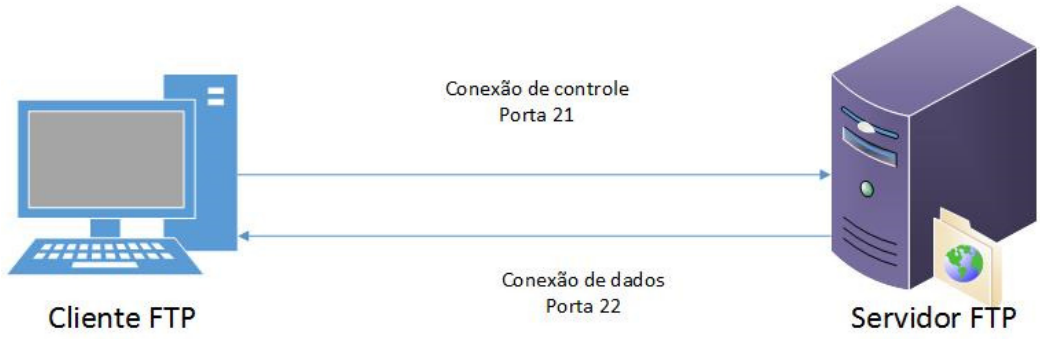

Figura 9 - Acesso via FTP
Fonte: Autoria própria.

2.5.7 DHCP

O *Dynamic Host Configuration Protocol* (DHCP) é a delegação automática e dinâmica dos dados de uma rede para que o solicitante possa participar da mesma rede. O DHCP fornece, basicamente, os dados abaixo:

- Endereço IP;
- Máscara de rede;
- Gateway;
- DNS primário e secundários;
- Data e hora atualizadas;

O DHCP atende pela porta 67 UDP na rede e a máquina configurada para receber de forma automática e dinâmica os endereços da rede, faz uso da porta 68 UDP para enviar uma mensagem de *broadcast* em IPV4 e *multicast* em IPV6 solicitando resposta para pedido dos dados da rede caracterizando esta ação com o nome de DCHP DISCOVERY em forma de *broadcast.*

Por sua vez, o servidor DHCP envia um *unicast* de DHCP OFFER, ofertando alguns parâmetros da rede. A seguir o cliente envia um pedido por meio de um

broadcast de DHCP REQUEST requisitando que seja arrendado o IP para a máquina solicitante. Quando o servidor recebe o pedido do cliente, envia um DHCP ACKNOWLEDGE iniciando a fase de configuração dos parâmetros de IP da máquina solicitante.

A figura 10 esboça a conversação DHCP entre um cliente e servidor de forma sucinta.

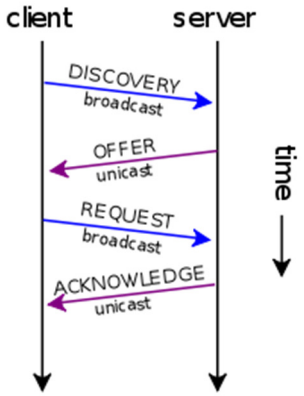

Figura 10 - Funcionamento do DHCP
Fonte: PARAPPAZOS. 2012.

2.5.8 DNS

Segundo MOTA FILHO (2013, p. 82), o *Domain Name System* (DNS) é um serviço que realiza conversões de nomes de máquinas para IP ou de IP para nomes. Este serviço, em sua essência, faz a consulta em uma tabela para analisar a associação correta e direta entre o nome e um endereço IP (Figura 11). Caso a consulta seja fornecido o endereço IP, a associação é de forma reversa, entregando ao cliente o nome da máquina.

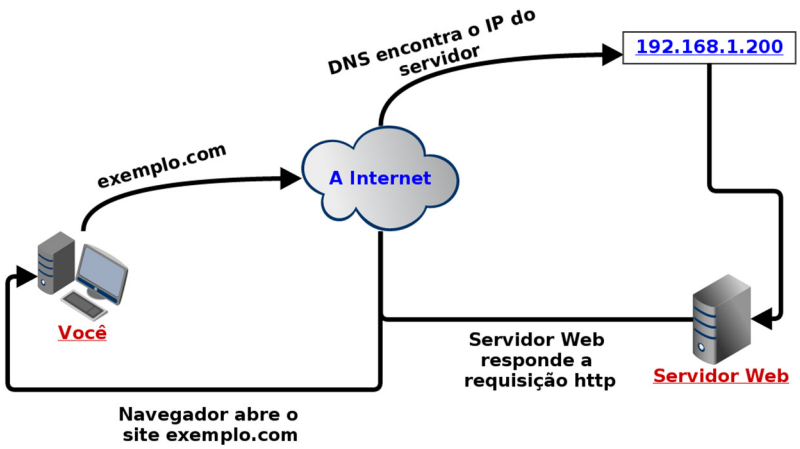

Figura 11 - Exemplo de DNS Direto
Fonte: Marcelo Fox. 2014.

2.6 RASPBERRY PI

O Raspberry PI é um microcomputador compatível com sistemas operacionais baseados na arquitetura ARMv6, e, portanto, qualquer linguagem que possa ser compilada nessa arquitetura pode ser usada para o desenvolvimento de softwares. Em virtude disso, o Raspberry PI pode ser aplicado a inúmeras finalidades a citar: projetos de eletrônica, reprodução de vídeos de alta definição e diversas atividades que o computador convencional executa como planilhas, processamento de textos e jogos. (RASPEBERRY PI FOUNDATION, 2014)

Por se tratar de um sistema embarcado com alto processamento em um sistema do tamanho de um cartão de crédito, o Raspberry PI tem se popularizado em todo mundo devido ao seu baixo custo e sua alta aplicabilidade em projetos distintos.

Com essa tecnologia é possível conectar discos rígidos USB além de editar documentos de textos, navegar na internet e ainda desenvolver projetos de automação residencial ou industrial.

2.7 RAPBIAN

O Raspberry PI suporta diversos sistemas operacionais baseados em Linux e o mais novo modelo, na versão 2, contém o suporte ao *Microsoft Windows* 10®.

Para o projeto em questão, o sistema escolhido para desenvolvimento da interface WEB foi o *Raspbian*. Esse sistema operacional é baseado em Debian e foi otimizado para ser utilizado no Raspberry PI.

A figura 12 mostra o *Raspbian* com uma instalação padrão com programas e utilitários básicos para melhor performance com hardware dedicado.

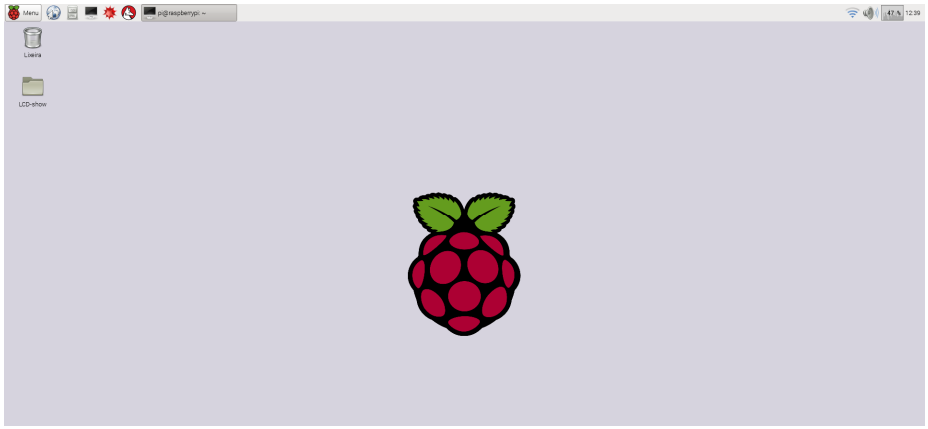

Figura 12 - Raspbian
Fonte: Autoria própria.

2.8 PHP

Para o desenvolvimento do sistema, foi utilizando a linguagem de programação para WEB denominada PHP (acrônimo recurso de *Hypertext Preprocessor*) por se tratar de uma linguagem gratuita e que atende amplamente o escopo do projeto. Possui a característica de ser *serve-side*, ou seja, é executada no servidor e não no cliente, diminuindo a necessidade de o cliente ter máquina robusta para fazer acesso ao sistema.

PHP é uma linguagem de programação que pode fazer todo o tipo de coisas: avaliar dados de formulários enviados por um navegador, criar conteúdo web personalizado para o navegador, conversar com um banco de dados, e até mesmo enviar e receber cookies. (CODECADEMY, 2014).

2.9 APACHE 2

Ao acessar um site, é feita uma requisição ao servidor que hospeda a página e por sua vez, o servidor WEB faz o processamento baseado nestas requisições e fornece a resposta ao cliente através de uma página HTML. A figura 13 demostra o acesso a página e a resposta do servidor.

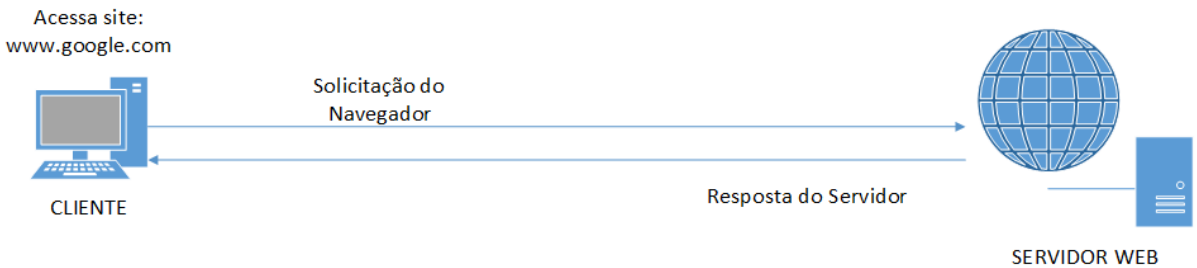

Figura 13 - Serviço WEB
Fonte: Autoria própria.

Este servidor faz uso de uma aplicação chamada de APACHE 2 que é um servidor WEB popular, livre, usado principalmente em sistemas operacionais baseados em Linux, além de possuir versão para a plataforma Windows.

O Apache HTTP Server Project, foi desenvolvido com o objetivo de manter um servidor Web que fosse livre (*open-source*), seguro, eficiente, rápido, flexível e que estivesse em sincronia com os padrões HTTP. (Apache, 2011).

2.10 TCPDUMP

O TCPDUMP é o melhor analisador de tráfego em modo texto que existe. Ele é baseado na *libcap*, uma poderosa API para a captura de pacotes de redes durante seu tráfego. (MOTA FILHO, 2013, p 37)

TCPDUMP mostra uma descrição do conteúdo de pacotes em uma interface de rede que corresponde a uma expressão booleana; a descrição é precedida por uma janela de tempo, impresso, por padrão, como horas, minutos, segundos e frações de segundos. (TCPDUMP/LIBCAP, 2014)

Por este motivo e pela facilidade em instalar utilização foi escolhida como ferramenta base na análise de tráfego deste projeto.

3 RESULTADOS

3.1 O SISTEMA TCPDUMP

O sistema está baseando em um arquivo de funções denominado “funcao.php”, contendo as rotinas executadas pelo sistema em si. A seguir tem-se uma página principal chamada “index.php”, onde são chamadas as rotinas do sistema. Além disso, possui pasta denomina “img” com as imagens pertinentes ao *site*. Também possui

uma pasta com a rotina “jquery.js” responsável pelas atualizações das informações sobre a rede. Do mesmo modo, possui uma folha de estilos denominada “estilo.css” com as definições de CSS do sistema presente na pasta “css”.

A figura 14 faz a ilustração da arquitetura estrutural do site.

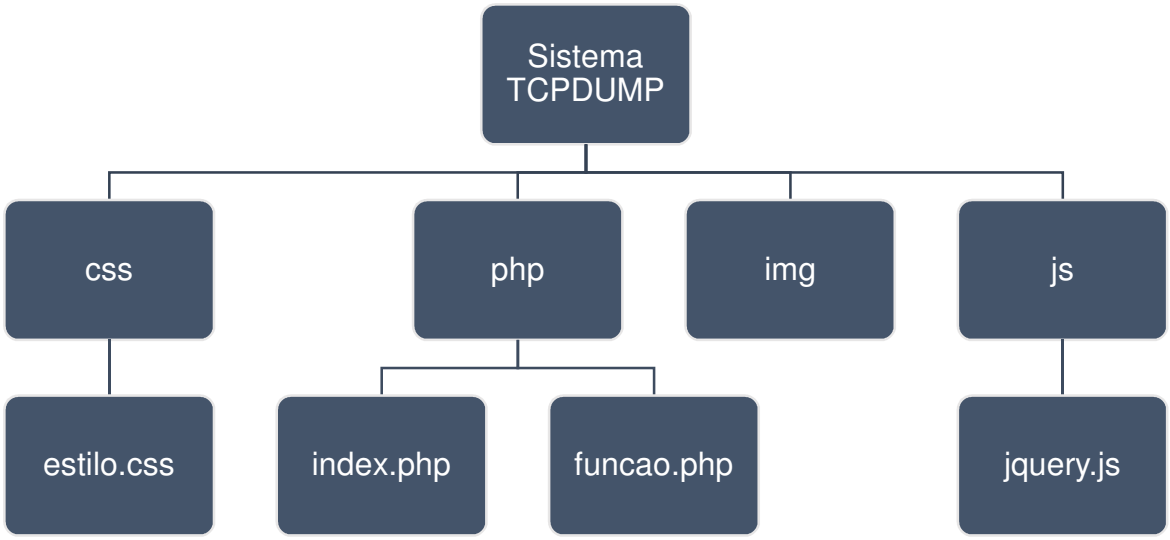

Figura 14 - Diagrama estrutural do sistema
Fonte: Autoria própria.

O site foi desenvolvido com a linguagem de programação PHP 5 e diagramado em CSS e HTML 5. Ao ligar o equipamento, após carregamento do sistema operacional *Raspbian*, o sistema TCPDUMP informará o número de IP definido, devido ao fato do conjunto Raspberry PI e sistema TCPDUMP estarem configurados desta forma.

Com o endereço IP, basta abrir o navegador em qualquer máquina da rede e acessar, como a figura 15 demostra, com o número de IP, acrescido de "\tcpdump".

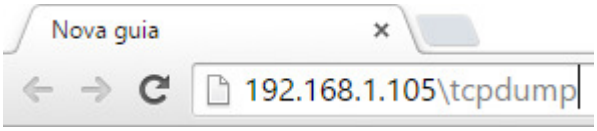

Figura 15 - Acesso ao sistema
Fonte: Autoria própria.

Ao acessar o sistema, a tela será carregada com a interface como mostra a figura 16. Nesta tela é possível observar o grupo "Status" com a função de listar os eventos que ocorreram no sistema como: Desligar, reiniciar e backup.

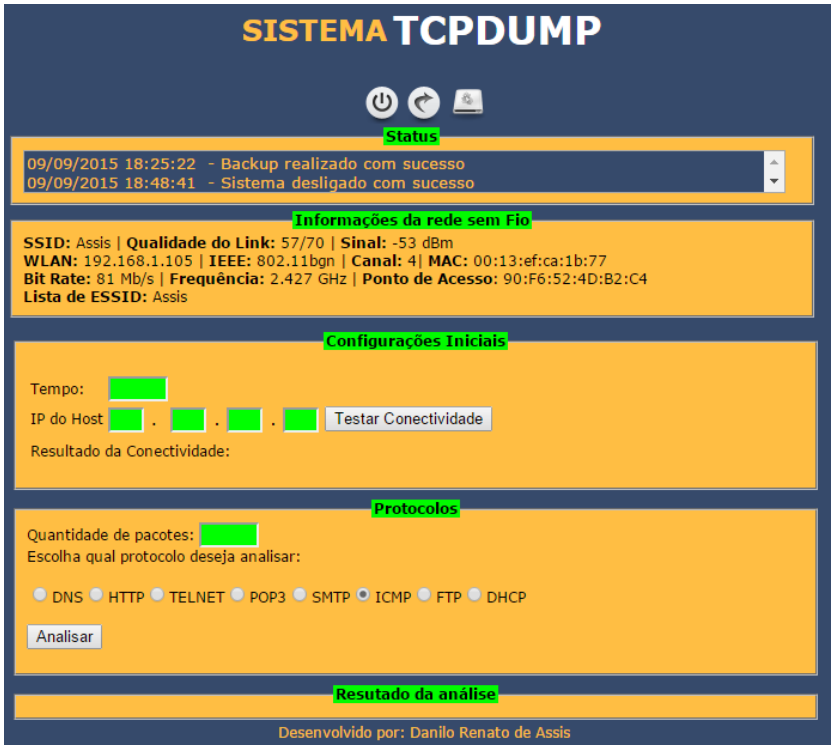

Figura 16 - Sistema TCPDUMP
Fonte: Autoria própria.

O grupo “Informações de rede sem fio” mostra as informações referentes a rede *wireless* do local analisado. Já o grupo “Configurações Iniciais” mostra a interação com usuário para realizar “*ping*” em algum equipamento com endereçamento IP na versão 4.

Ao final, o grupo “Protocolos” permite que seja determinado quantidade de pacotes e também escolhido o tipo de protocolo que será analisado.

3.2 ANALISANDO O TRÁFEGO DE UMA REDE SEM FIO

A análise de tráfego foi feita com base na topologia da figura 17 onde o RAPBERRY PI escuta o tráfego da WLAN e faz a captura dos pacotes de acordo com a escolha do usuário. Esta topologia é um desenho lógico de uma rede local doméstica.

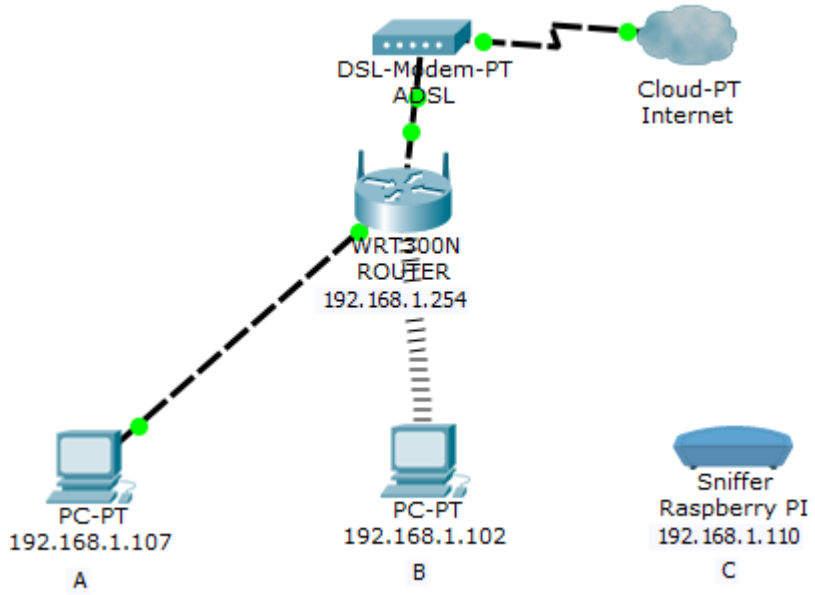

Figura 17 - Topologia da rede sem fio
Fonte: Autoria própria.

As capturas realizadas visam demonstrar o resultado da execução do sistema TCPDUMP através do uso do navegador. A quantidade de pacotes por amostragem abordada foi fixada em 10 pacotes, em alguns casos, para rápida demonstração do sistema.

Ao finalizar a captura dos pacotes, o arquivo contendo o resultado da captura será enviado para o e-mail do operador.

A priori, os eventos serão capturados entre a interação dos computadores “A” e “B” e o roteador “ROUTER”.

3.2.1 CAPTURA DO PROTOCOLO ICMP

A captura do trafego da WLAN, para protocolo ICMP, foi realizada mediante ao "*ping*" do computador "A" para o roteador "ROUTER" e gerou o resultado ilustrado na figura 18.

Nessa análise é possível observar o campo TYPE sendo mostrado com tipo 8, ou seja, houve um "echo request" - que significa que destino foi encontrado - entre *ping* enviado do computador "A" para "ROUTER".

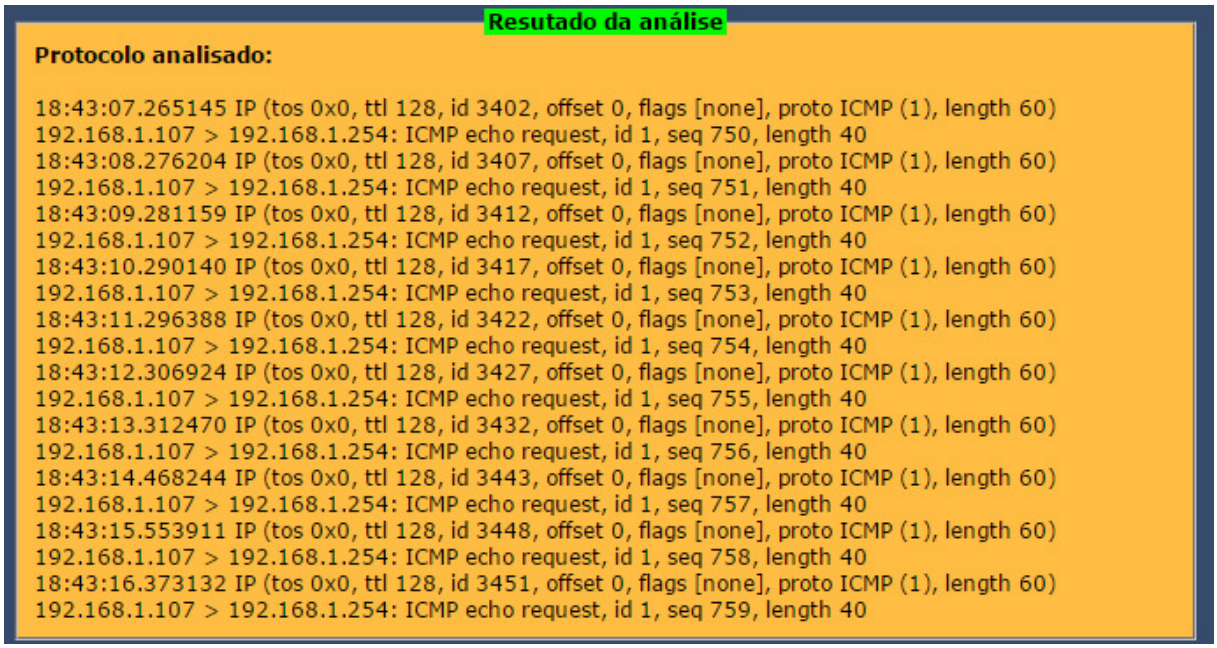

Figura 18 - Captura ICMP
Fonte: Autoria própria.

Além das informações do número de IP de origem e destino, é possível analisar o número de sequência de cada pacote não segue uma ordem, devido ao fato de existirem outros protocolos de comunicação na rede, como DHCP, DNS.

3.2.2 CAPTURA DO PROTOCOLO FTP

O acesso ao FTP foi feito pelo computador “A”, através da linha de comando do terminal do *Linux*, como o objetivo de acessar os diretórios do computador “B”.

A figura 19 mostra o protocolo FTP sendo analisado, por parte do sistema, e demonstra a captura do usuário e senha do acesso via terminal ao computador “B”, denotando a vulnerabilidade do protocolo devido ao fato de não existir criptografia para esconder os dados do acesso.

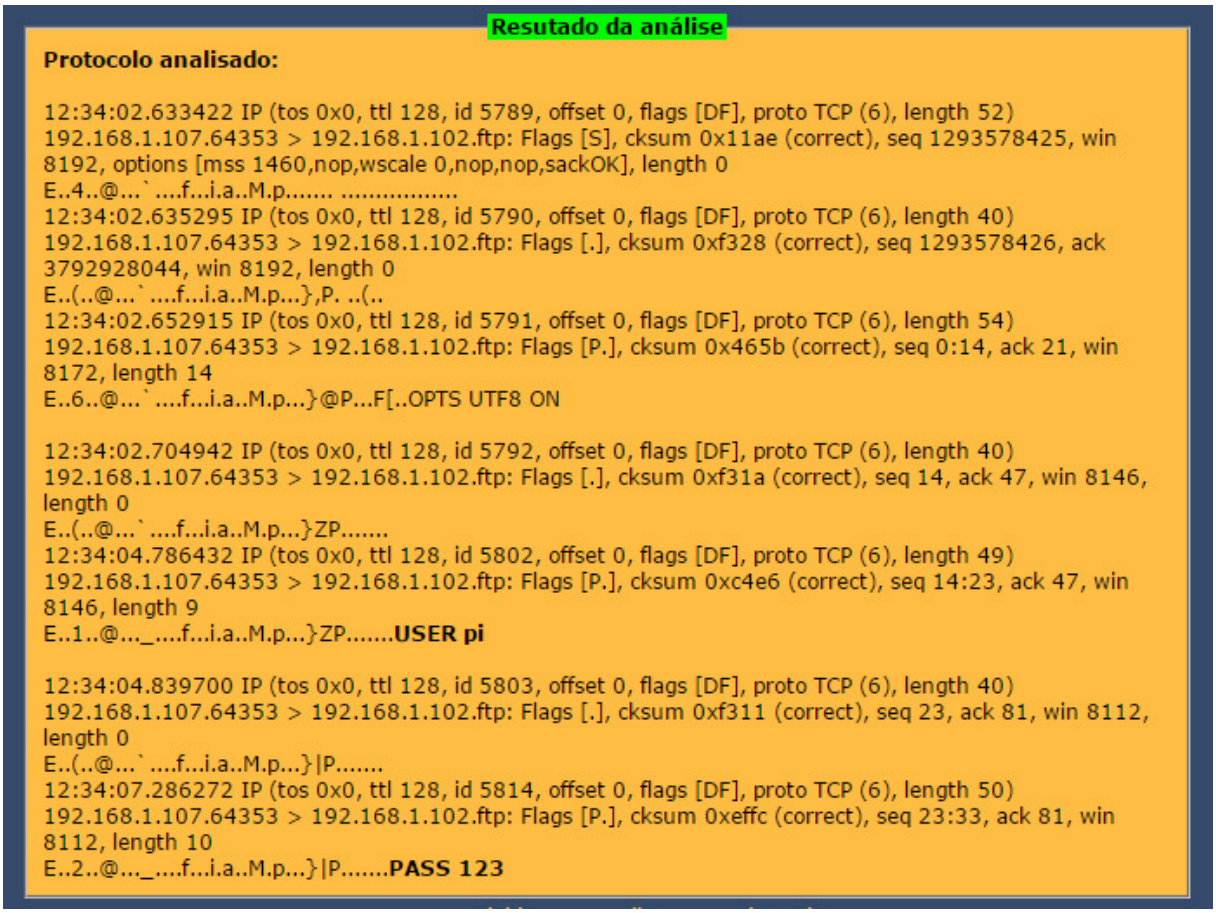

Figura 19 - Captura FTP
Fonte: Autoria própria.

3.2.3 CAPTURA DO PROTOCOLO HTTP

A captura do HTTP foi feita mediante requisição por parte do computador “A” (cliente), acessando o serviço, via navegador, do computador “B” (servidor). Nesta captura ilustrada na figura 20, pode-se notar que o navegador do cliente solicitante foi capturado que, no exemplo abaixo, é o Google Chrome, na versão 45.0 e outros parâmetros do navegador.

Figura 20 - Captura HTTP
Fonte: Autoria própria.

3.2.4 CAPTURA DO PROTOCOLO DNS

A captura do protocolo DNS foi realizada, mediante acesso do computador “B” ao site “facebook.com”. Nesta modalidade, foram empregados 05 pacotes para facilitar a ilustração da captura na figura 21.

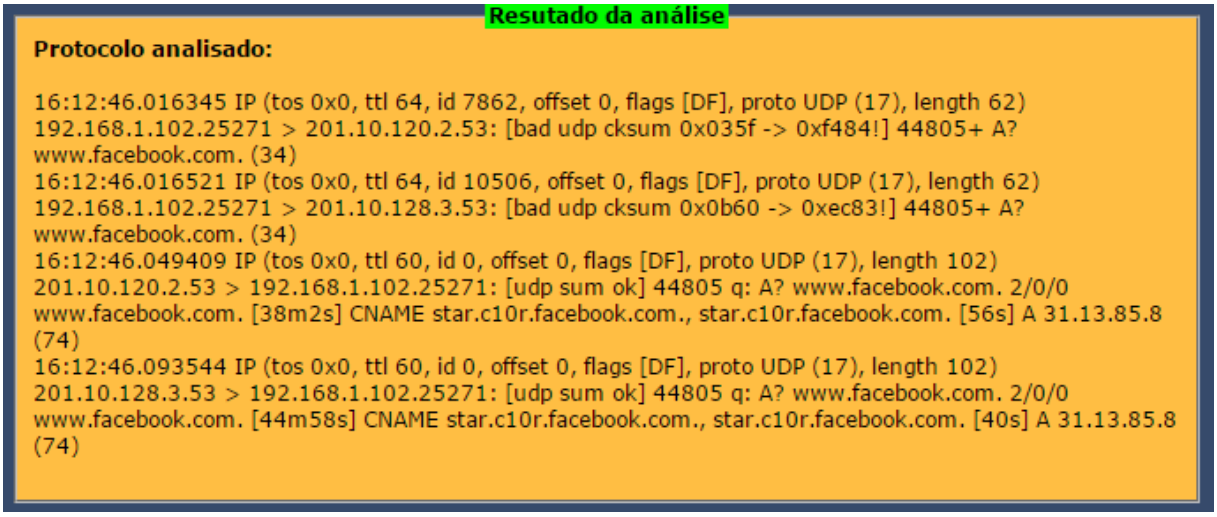

Figura 21 - Captura DNS
Fonte: Autoria própria.

3.2.5 CAPTURA DO PROTOCOLO SMTP

A captura do protocolo SMTP foi analisada através da porta 465, em que o computador “B” fez uso do programa “*Thunderbird*” para enviar um e-mail utilizando o provedor “GMAIL”.

A figura 22 mostra a captura do SMTP em que foram observados cinco pacotes para ilustrar a aquisição dos dados.

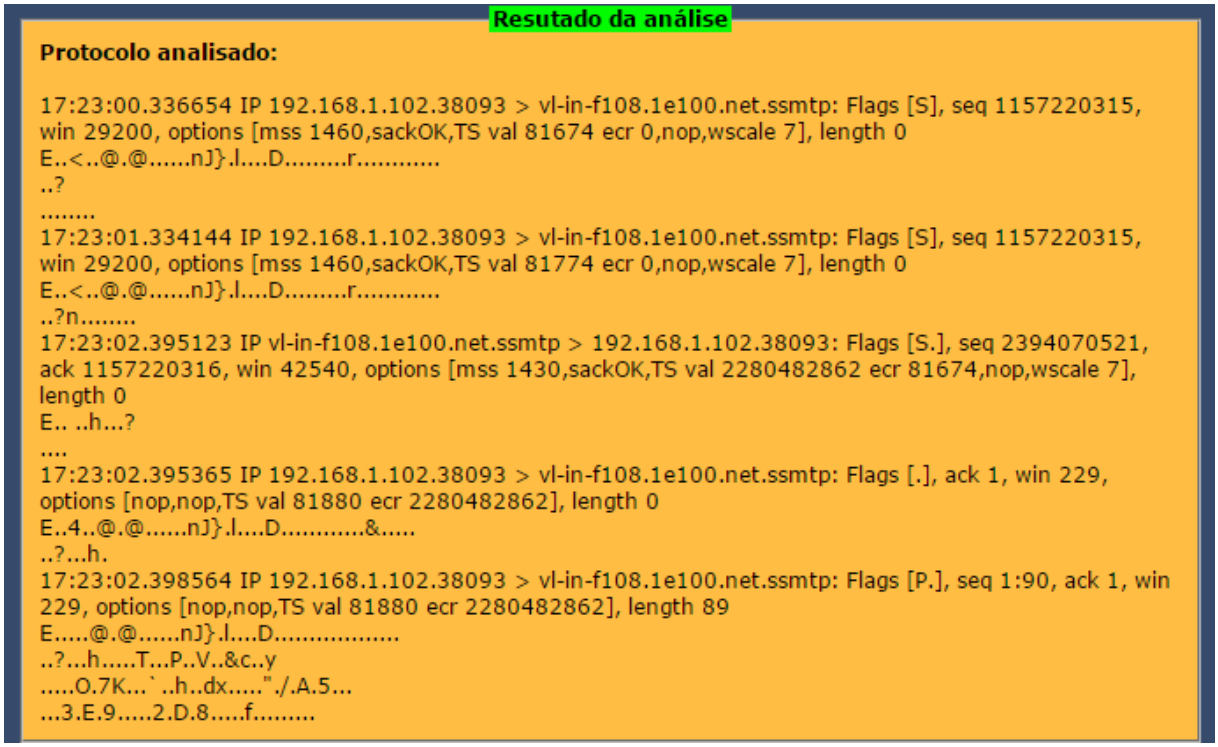

Figura 22 - Captura SMTP
Fonte: Autoria própria.

3.2.6 CAPTURA DO PROTOCOLO POP3

Para a captura do protocolo POP3, foi observado o computador “B”, com cliente de e-mail “Thunderbird” para observar o comportamento ao receber e-mail pela porta 995. A figura 23 mostra a captura feita do protocolo ao cliente receber um e-mail enviado para a conta cadastrada no cliente de e-mail.

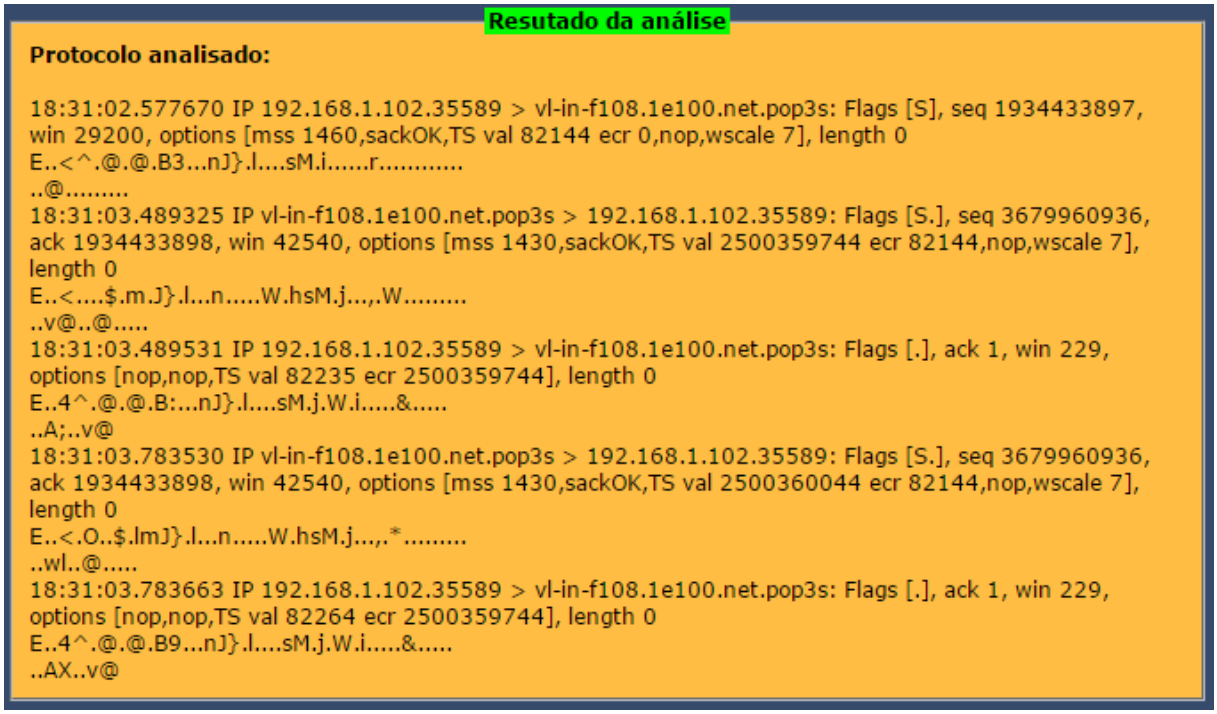

Figura 23 - Captura POP3
Fonte: Autoria própria.

3.2.7 CAPTURA DO PROTOCOLO TELNET

O computador “A” fez acesso via TELNET para computador “B” e a captura gerou uma análise de treze pacotes, conforme a figura 24.

Neste exemplo é possível observar que o usuário tentou fazer uma conexão via porta 23, mas não obteve sucesso pois retornou a mensagem “*Login incorrect”* devido ao usuário e/ou senha inválido (s).

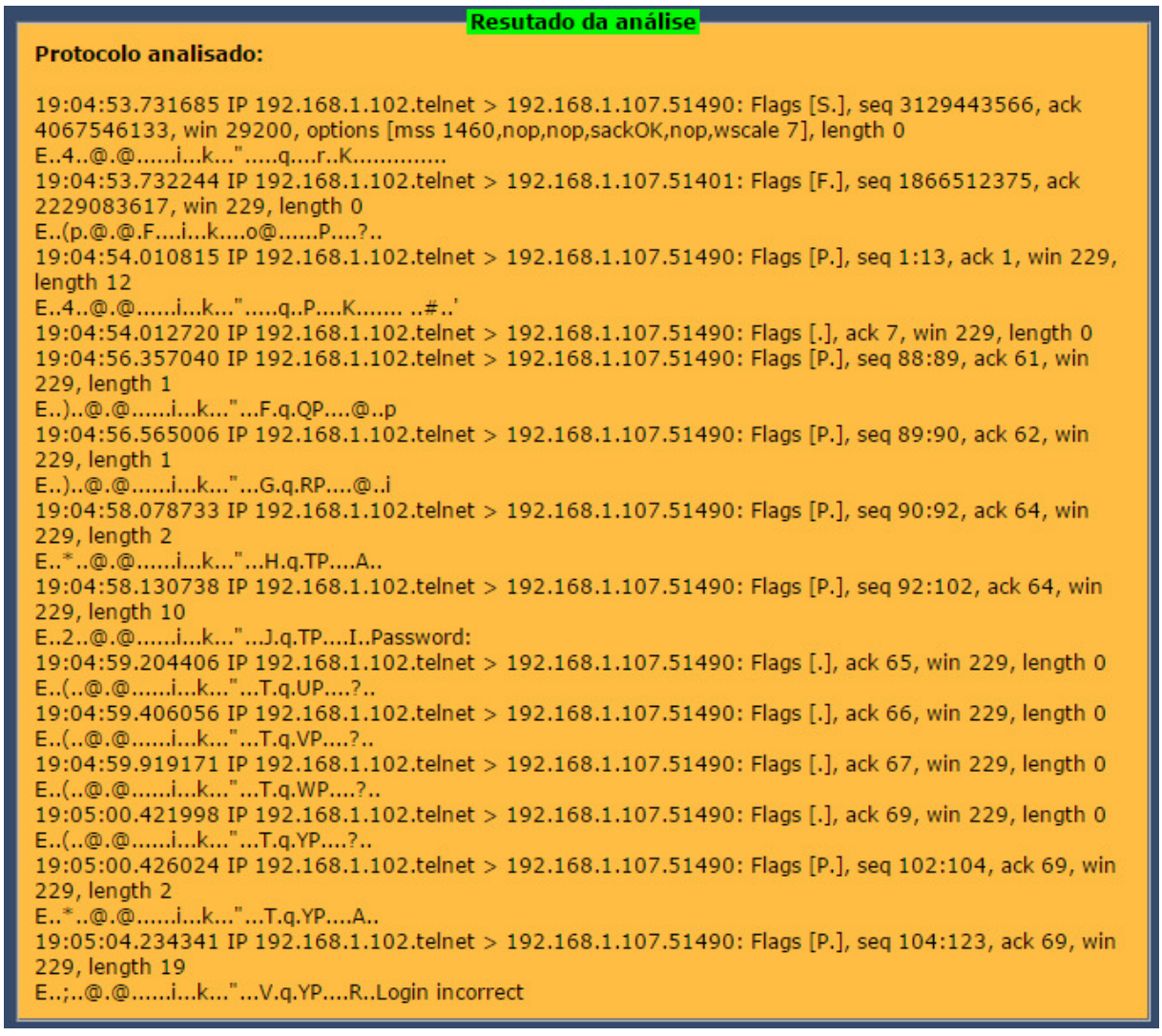

Figura 24 - Captura TELNET
Fonte: Autoria própria.

4 CONCLUSÃO

A análise de trafego de redes, seja ela cabeada ou sem fio, mostra-se como um objeto de grande valia para identificação dos eventos adversos nas redes. É nesse sentido que, cada vez mais, os administradores de rede necessitam ter um olhar crítico para os pacotes que trafegam em uma LAN e até mesmo em uma WLAN. Assim possui uma maior probabilidade de encontrar a causa do evento adverso em uma *network*.

Porém, essa análise é onerosa devido ao fato, de que, necessita de um conhecimento avançado das estruturas dos protocolos para compreender em si o que esperar de uma comunicação fim a fim.

Com isso, a aplicação da ferramenta TCPDUMP torna-se mais eficaz, uma vez que, fazendo a leitura estrutura, através das RFC´s de um protocolo, pode-se montar filtros para que a ferramenta atue especificamente na identificação do problema da rede.

Em uma rede com grandes proporções, a análise de tráfego é indispensável, pois economiza tempo e torna mais ágil a solução dos problemas da rede. Com este projeto, foi possível notar detalhes que antes passavam sem a exata noção pois viu-se apenas teorias em sala de aula e esse desenvolvimento foi vital para a implementação do analisador embarcado em um sistema mínimo.

4.1 DESAFIOS ENFRENTADOS

As dificuldades são benéficas para melhor aproveitamento da tecnologia que se tem em mãos e afinar, cada vez mais, o projeto como um todo. Nesse sentido que vários obstáculos foram surgindo e foram contornados ao longo do desenvolvimento.

Por se tratar de uma ferramenta nova, em termos de conhecimento pessoal, desprendeu-se mais tempo no estudo dela para contornar o obstáculo inicial. Outra dificuldade peculiar foi a integração do TCPDUMP com a aplicação APACHE, visto

que uma ferramenta executada em linha de comando necessita de permissão de execução através da ferramenta VISUDO, com permissão ao usuário *www-data*.

Além disso, ocorreu a corrupção dos dados do cartão utilizado, em fase inicial de 16 Gigabytes, e posterior substituição por um cartão com a metade da capacidade do projeto original. Com isso foi necessário refazer a instalação do sistema básico, com RASPIAN, PHP e APACHE 2 além de refazer a interface WEB, onde dados serão analisados e mostrados ao usuário. Para contornar essa adversidade, foi criado um sistema de backup em PHP, onde o arquivo da interface WEB é enviado por e-mail ao operador do equipamento além de criação de imagem em formato imagem de disco do sistema operacional como um todo.

Contudo, a placa USB WIRELESS inicialmente adquirida para o projeto, teve que ser substituída pois não suporta o modo de operação do tipo “monitor” cuja função é colocar a placa de rede wireless em modo de “escuta”, observando o tráfego da rede sem fio. A substituição se deu pelo modelo TP LINK TL-WN721N com suporte ao modo monitor.

Contornado esses obstáculos, o projeto seguiu seu curso normal de desenvolvimento e avaliação dos resultados obtidos.

4.2 SUGESTÕES DE PROJETOS FUTUROS

A arquitetura do Raspberry PI oferece uma gama de aplicações tanto profissionais quanto pessoais, não só pelo tamanho reduzido, mas também pela variedade de utilização que se pode agregar além de ser um dispositivo de baixo custo financeiro e consumo reduzido de energia.

Nesse sentido é possível reduzir ainda mais o consumo de energia, utilizando fontes renováveis como painéis solares, observadas as características de 5 volts de entrada e 2 Ampères de corrente elétrica. Além disso é possível ainda desenvolver um módulo *PoE*, conforme a figura 25, afim de utilizar switch que desprender dessa tecnologia, para alimentar o Raspberry PI.

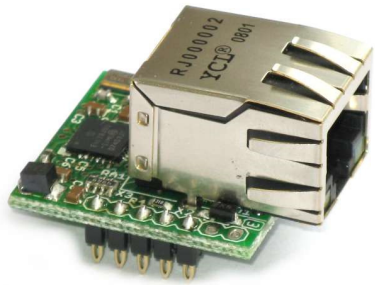

Figura 25 - Módulo PoE
Fonte: raspberrypi.stackexchange.com.

Ainda, como sugestão futura, integração com banco de dados gerenciável afim de criar um sistema de armazenamento dos eventos da rede, bem como cadastro de usuário e configurações básicas do sistema, como e-mail do operador, quantidade de pacotes e tempo de análise.

REFERÊNCIAS

COMER, Douglas E. **Redes de computadores e internet: abrange transmissão de dados, ligações Inter redes, web e aplicações**. 4. ed. Porto Alegre: Bookman, 2007, 632 p.

RICHARDSON, Matt; WALLACE, Shawn. **Primeiros passos com Raspberry Pi.** São Paulo: Novatec, 2013. 192 p.

TCPDUMP & LIBCAP. Disponível em < http://www.tcpdump.org/> Acesso em 02/06/2015, 12:39.

MOTA FILHO, João Eriberto. **Análise de tráfego em redes TCP/IP: utilize tcpdump na análise de tráfegos em qualquer sistema operacional**. 1. ed. São Paulo: Novatec, 2013. 416 p.

COMER, Douglas E**. Interligação de redes com TCP/IP**. Rio de Janeiro: Campus, 2006.

KUROSE, James F.; ROSS, Keith W. **Redes de computadores e a internet: uma abordagem top-down**. 6. ed. São Paulo, SP: Pearson Addison Wesley, 2013. xxii, 634 p.

TANENBAUM, A. S. **Sistemas operacionais modernos**. 4.ed. São Paulo: Livro Técnico, Prentice Hall, 2003.

RAMO ESTUDANTIL. 2015. Disponível em: http://sites.ieee.org/sb-uel/category/noticias/. Acessado em 25/08/2015 às 12h04min.

ENTELCO TELECOM. 2015. Disponível em: http://www.entelco.com.br/blog/mikrotik-e-o-padrao-802-11ac/. Acessado em 24/08/2015 às 10h04min.

TELECO. 2007. Disponível em: http://www.teleco.com.br/osi.asp. Acessado em 26/08/2015 às 13h:00min.

TAVARES C ALEXEI. Entendendo o modelo OSI para melhorar sua capacidade de resolver problemas em uma rede Cisco. Disponível em: http://www.dltec.com.br/blog/cisco/entendendo-o-modelo-osi-para-melhorar-sua-

capacidade-de-resolver-problemas-em-uma-rede-cisco/. Acessado em 26/08/215 às 16h00min.

MARCELO FOX. Apache | Name-Based Virtual Host Disponível em: http://marcelfox.com/blog/apache-name-based-virtual-host/. Acessado em 01/09/2015 às 12h15min.