

Tecnologia da Informação

**Segurança e Auditoria**

SALVADOR

2019

Vitor Lopes

Gabriel Vasconcelos

Rafael Azevedo

Albano Souza

Moises Santos

Gidevaldo Chaves

**Segurança e Auditoria**

Trabalho apresentado no curso de Tecnologia da Informação (TI) do Centro Universitário UniRuy (Wyden).

Orientador(a): Talita Rocha Pinheiro

SALVADOR

2019

SUMÁRIO

1. **INTRODUÇÃO** ............................................................................................................. 04
2. **WIRESHARK** ............................................................................................................... 05

2.1. Características e Funcionalidades ................................................................. 05

2.2. Funcionamento ............................................................................................... 06

**3. CONCLUSÃO** ............................................................................................................... 13

**4. REFERÊNCIAS BIBLIOGRÁFICAS** ............................................................................ 14

1. **INTRODUÇÃO**

Esse trabalho tem o intuito de demonstrar as funcionalidades bem como a implementação e operacionalização da ferramenta Wireshark. No qual seria um software analisador de pacotes, conhecido como Sniffer, essas ferramentas do tipo Sniffer além de permitir analisar pacotes, permitem ainda captura-los e caso seja necessário decodifica os dados brutos do pacote, mostrando os valores de vários campos no pacote. Porém softwares do tipo Sniffer podem ser utilizados de forma maliciosa em uma rede, pegando os pacotes que trafegam na mesma e obtendo as informações como por exemplo login e senha dos usuários que utilizam aquela rede. A ferramenta Wireshark escolhida como tema do relatório a seguir é utilizada pelos administradores da rede para detectar problemas ou conexões suspeitas e além disso, testar se as senhas usadas na rede estão realmente sendo criptografadas, podendo ainda ser utilizada em diversas outras atividades envolvendo segurança no trafego dos pacotes em uma rede.

1. **WIRESHARK**

Wireshark é um analisador de protocolo que permite que você capture os pacotes e navegue interativamente no tráfego de uma rede de computadores em tempo de execução usando a interface de rede do computador. Este tipo de software, também chamado de Sniffer (ou farejador, em português), é bastante usado por administradores de rede para detectar problemas ou conexões suspeitas, testar se as senhas usadas na rede estão realmente sendo criptografadas e realizar uma série de outras atividades relacionadas à segurança. A grande lista de funcionalidades e recursos presente no Wireshark é, sem dúvida alguma, o fator que explicado toda a sua popularidade, essa fermenta permite uma grande compatibilidade com arquivos do tcpdum, quando se analisa ela mais profundamente, é difícil pensar em algum formato não suportado, sem contar que ela está disponível para plataformas Windows ou Linux.

**2.1. Características e Funcionalidades**

Além da fácil visualização do usuário por meio da interface gráfica a grande quantidade de funcionalidades foi um importante fator que acabou impulsionando a popularidade do Wireshark no mercado. O Wireshark possui compatibilidade com arquivos gerados por outra ferramenta como por exemplo o tcpdump que possui funcionalidades bastante semelhantes ao próprio Wireshark, alguns dos diversos formatos suportados pela ferramenta são:

* Catapult DCT2000;
* Cisco Secure IDS iplog;
* Novell LANalyzer;
* Microsoft Network Monitor;
* Network General Sniffer®;

Outa funcionalidade do Wireshark seria a possibilidade de visualizar em tempo real o conteúdo dos pacotes enviados ou recebidos pelo servidor tornando as ações caso ocorra algum problema com os pacotes na rede mais eficientes e eficazes, pois seria possível tomar medidas rápidas após a visualização do problema em tempo real.

**2.2. Funcionamento**

Para escolher a interface de rede que deseja usar, clique no menu “Capture” em “options”, ou utilize o atalho “ctr + K” (fig.1).

Uma imagem contendo captura de tela

Descrição gerada automaticamente

*Figura 1*

Na aba input, selecione a interface de rede que deseja usar e habilite a opção “Enable promiscuous mode on all interface”, permitindo que o programa capture todos os pacotes da rede atual (fig. 2).

Uma imagem contendo captura de tela

Descrição gerada automaticamente

*Figura 2*

Na aba output, selecione o botão “browser”, na parte “capture to a permanente file” (fig. 3).

Uma imagem contendo captura de tela

Descrição gerada automaticamente

*Figura 3*

Na janela que irá surgir, crie um diretório onde será guardado os dados da captura, nomeando o arquivo e finalizando clicando em “salvar”.

Após etapa anterior, clique em “Start”. A partir daí os programas já está capturando os pacotes que são trafegados e exibindo-os no primeiro quadro em sua janela.

Depois de feita a captura, deve-se filtrar as pesquisas destes pacotes, pois a captura está sendo feita em toda rede, e o que nos interessa são somente os destinados a esta máquina, podemos filtrá-los clicando no botão “expression” ao lado do campo do filtro (fig. 4).

Uma imagem contendo captura de tela

Descrição gerada automaticamente

*Figura 4*

Procure pelo item “IPv4 – Internet Protocol version 4″ no quadro “Field name” que fica do lado esquerdo da janela de “Filter Expression”. Depois clique no sinal de “>” ao lado do nome ” IPv4 – Internet Protocol version 4″ e selecione a opção “ip.dst”. Clique na opção “==” no campo “Relation”, no centro da tela.  No campo “Value” digite o endereço IP de seu computador. Clique em “OK” para confirmar. (fig. 5).

Uma imagem contendo captura de tela

Descrição gerada automaticamente

*Figura 5*

Percebe-se que ainda há muitos pacotes a serem exibidos aonde iremos restringir apenas para solicitações de ping, Para fazer isso, digite ” and ” (sem as aspas mas como os espaços) depois da expressão que foi criada depois do nome “Filter” na janela do programa. Agora clique novamente no botão “Expression…” (fig. 6).

Uma imagem contendo captura de tela

Descrição gerada automaticamente

*Figura 6*

Procure pelo item “ICMP – Internet Control Message Protocol” no quadro “Field name”. Depois clique no sinal de “>” ao lado do nome “ICMP – Internet Control Message Protocol” e selecione a opção “icmp.type”. Clique na opção “==” no campo “Relation” e no campo “Value” digite o número 8 (que corresponde a solicitações ping). Clique em “OK” para confirmar. A expressão completa ficará “ip.dst == 192.168.1.5 and icmp.type == 8″ e será exibida no campo “Filter” (fig. 7).

Uma imagem contendo captura de tela

Descrição gerada automaticamente

*Figura 7*

Agora só aparecerão os pacotes destinados ao seu computador que sejam solicitações do comando ping, com isso você saberá qual ou quais máquinas estão tentando se conectar a sua (fig.8).

Uma imagem contendo captura de tela

Descrição gerada automaticamente

*Figura 8*

1. **CONCLUSÃO**

Atualmente as empresas e usuários estão sempre buscando acompanhar a tecnologia mesmo que isso gere custos, ainda sim vantagens são obtidas, tornando alguns métodos viáveis. Sniffers de rede são exemplos de ferramentas que auxiliam na administração de redes, monitorando tráfego de dados e gerenciando informações da sua rede, o que se torna essencial para empresas e usuários com informações valiosas.

Administrar uma rede analisando o seu tráfego de pacotes é bastante eficiente, pois assim temos sempre controle sobre alguém que está na rede, sendo capaz de identificar possíveis ataques ou atividades suspeitas, aumentando a segurança da sua rede.

**4. REFERÊNCIAS BIBLIOGRÁFICAS**

BRITO, Edivaldo. **Como usar o Wireshark**. [*S. l.*]: Edivaldo Brito, 14 set. 2012. Disponível em: https://www.techtudo.com.br/dicas-e-tutoriais/noticia/2012/09/como-usar-o-wireshark.html. Acesso em: 1 nov. 2019.

DELFINO, Pedro. **WIRESHARK: TUDO SOBRE ESSA INCRÍVEL FERRAMENTA DE MONITORAMENTO DE TRAFEGO DE REDE** [*S.l.*]: Pedro Delfino. Disponível em: https://e-tinet.com/linux/wireshark/. Acesso em: 2 nov. 2019.