INSTITUTO FEDERAL DO TRIÂNGULO MINEIRO - CAMPUS PARACATU
INFORMÁTICA

Análise das utilizações dos Sniffers de Redes

Isabelle Nascimento Falcão e Lucas Guimarães Mendes

Paracatu-MG
2017

Isabelle Nascimento Falcão e Lucas Guimarães Mendes

Análise das utilizações dos Sniffers de Redes

Pré-projeto de Trabalho científico de pesquisa apresentado no Instituto Federal do Triângulo Mineiro - Campus Paracatu como requisito básico para a conclusão da matéria de Metodologia do Trabalho Científico e Oficinas Integradas.
Orientador: Flávio Alves

Paracatu-MG
2017

SUMÁRIO

Resumo

O *sniffer* é uma espécie de ferramenta que possibilita e favorece o monitoramento da transferência de dados e pacotes pela rede. Esta, utilizada de diversas formas, por administradores de redes e, também, por *crackers*.
Para que haja maior abrangência ao que se refere ao estudo dos diferentes temas alcançados pela utilização dos *sniffers* de redes, os objetivos do presente trabalho integram o estudo das vantagens e desvantagens da utilização dos *sniffers* de redes, juntamente com a análise do aplicativo escolhido para a captura de pacotes, o *Wireshark*, e a compreensão das duas utilizações dos *sniffers*, pelos administradores de redes e pelos crackers.
O *Wireshark*, é um dos analisadores mais utilizados, sua característica gratuita é uma das vantagens que mais favorece sua utilização.
Os experimentos da pesquisa são estabelecidos e executados a partir das características dos usuários analisados. Juntamente com a implementação de uma rede teste para a execução de experimentos comprobatórios e exemplificadores dos dados recolhidos durante a pesquisa.

1.Introdução

Existem diversas ferramentas que auxiliam a administração da rede favorecendo o monitoramento e segurança do tráfego de dados, porém, essas mesmas ferramentas podem ser de grande utilidade para criminosos conseguirem informações sigilosas, e de valor elevado para o proprietário. Uma dessas ferramentas é o *sniffer* de rede, esta ferramenta possibilita o acesso às informações dos pacotes transmitidos na rede de computadores.

Um *packet sniffer* (farejador de pacotes) é um tipo de programa que captura os pacotes que estão trafegando na rede cabeada ou wireless. Esses pacotes são exibidos na tela através de aplicativos como *Wireshark*, *NTOP (Network Traffic Generator)*, *rootnet,* entre outros e também podem ser armazenados no HD para uma análise posterior.

2.Justificativa

Hoje, com a grande expansão da internet, principalmente a do tipo *wireless* (rede sem fio) muito se discute sobre a segurança dos dados que estão trafegando na rede. Muitas empresas investem altos valores para manterem os seus dados seguros, pois o que está contido na rede certamente vale muito mais do que tudo o que é vendido ou oferecido como serviço, e qualquer vazamento de dados pode acarretar sérios prejuízos.

Segundo (Oppennheimer 1999), a diversidade e complexidade das redes de computadores têm tornado o seu gerenciamento uma atividade cada vez mais complexa. Neste contexto, uma atividade de fundamental importância é a análise do tráfego da rede, a qual permite compreender quantitativamente o comportamento do objeto de pesquisa.O conhecimento aprofundado das características deste tráfego permite ao administrador adotar medidas para otimizar a operação da rede analisada.

O *sniffer* é uma ferramenta que permite identificar as informações de controle dos protocolos necessárias para eles realizarem as funções essenciais na comunicação como, por exemplo, o número da porta definido pelo protocolo da camada transporte, a qual endereça os dados do pacote recebido para a aplicação específica no computador (*Web*: Porta 80, FTP: Portas 20 e 21, etc).

Além disso, esta ferramenta possibilita a realização de experimentos práticos para melhor entendimento das teorias estudadas no decorrer do curso técnico, ou seja, o funcionamento dos protocolos de rede.

Sendo assim, este trabalho tem importante relevância para obtermos informações com o intuito de saber como é o funcionamento do *sniffer* de rede, e como ele pode ser utilizado tanto para segurança quanto para obtenção de dados.

3.Objetivos

Na busca por um melhor conhecimento na área de *sniffer*, este estudo tem como objetivo geral conhecer as diversas utilizações dos *sniffers* de rede. Para alcançar tal objetivo, foram delineados os seguintes objetivos específicos:

- estudar as vantagens e desvantagens da utilização de *sniffers* de rede;
- analisar como se utiliza o aplicativo de *sniffer* de rede escolhido para estudo, o *wireshark*;
- compreender as funcionalidades dos *sniffers* para administradores de rede e *crackers*;

4.Materiais e métodos

Neste presente trabalho a escolha do aplicativo para estudo foi feita de acordo com suas utilizações, funcionalidades e acessibilidades. O material escolhido foi o *Wireshark*, um analisador de pacotes que atende a necessidade de estudar os protocolos de rede.

O *Wireshark* também é um dos coletores de pacotes mais utilizado no mundo e sem fins lucrativos, um recurso livre que oferece para empresas, instituições educacionais e agências governamentais a possibilidade de gerenciar e controlar o que acontece em suas redes de forma simples e didática.

Serão realizados diversos testes com aplicativos, adequando-os aos diferentes perfis de usuários, conforme o plano padrão definido para a pesquisa. Esses dados serão analisados e estruturados para as apresentações do trabalho.

Também será feita a implementação física e lógica de uma pequena rede (com um comutador, um servidor – FTP, DHCP – e determinado número de clientes) para a realização prática dos testes e experimentos.

5.Cronograma

Meses	05/2017	06/2017	07/2017	08/2017	09/2017	10/2017	11/2017	12/2017
Escolha de tema	X							
Estudo sobre o tema	X	X	X	X				
Elaboração do trabalho		X	X	X	X	X		
Testes com aplicativos			X	X	X			
Reunião com orientador		X	X	X	X	X	X	
Elaboração do artigo		X	X	X	X	X		
Apresentação do trabalho						X	X	X

6.Análise das utilizações dos *Sniffers* de Redes

6.1.Utilização de *sniffers* para administrar redes

Os *sniffers* podem ser utilizados para diversas funções. Algumas delas são importantes para o administrador da rede, como: detecção de violações na segurança da rede, monitoramento de tráfego, além de possibilitar a realização de otimizações, o que colabora para um melhor planejamento da rede, por exemplo, identificar horários de pico de utilização da rede, e através dessa informação controlar o fluxo de computadores conectados.

6.2.Utilização de *sniffers* por *crackers*

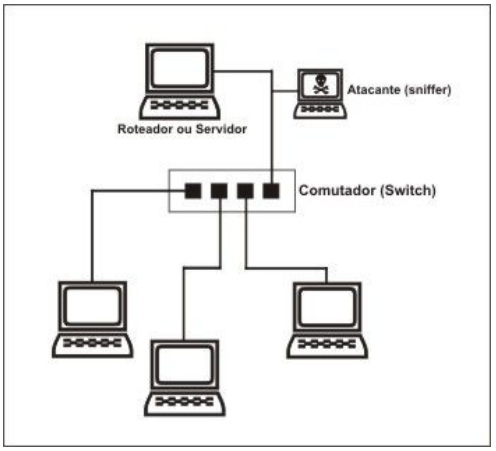
Assim como o *sniffer* é de grande importância e utilidade para a administração da rede, ele também é uma grande ferramenta para invadir e ter acesso a dados pessoais como: senhas, conversações e conteúdos particulares.

Muitos *crackers,* aproveitando-se de falhas na segurança de determinadas redes, usurpam estas informações de forma simples e rápida e, posteriormente, as utilizam de forma errônea, o que pode causar danos e transtornos aos proprietários.

Para que os *crackers* detenham essas informações, faz-se necessário que se implante o *sniffer* de acordo com o tipo de rede, por exemplo, em redes comutadas em que o meio não é compartilhado entre todas as máquinas, é de suma importância que o *sniffer* esteja em uma posição estratégica.

Uma das melhores possibilidades é a instalação de um sniffer em um servidor ou roteador, pois este pode capturar todo o tráfego, como demonstrado na Figura 1, onde o sniffer está no mesmo enlace que uma máquina importante.

Figura 1 - Ataques a redes comutadas.



Fonte: Sniffdet - Um Sistema para Detecção de *Sniffers* em Redes TCP/IP.

6.3. Utilizando os *Sniffers*

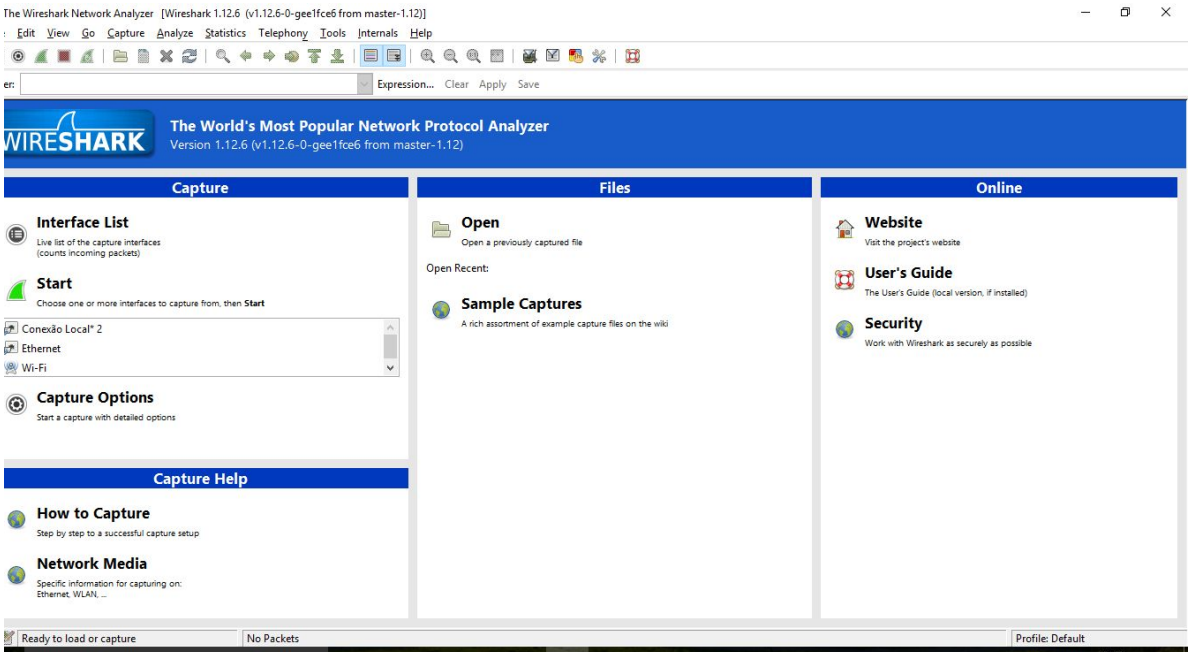
Os receptores de dados são utilizados em grande escala em todo o mundo, onde quase tudo em que se refere à segurança de redes e utilização administrativa, se encarrega de uma citação ou demonstração dos *sniffers*. O *Wireshark* e o *NTOP*, agem de forma passiva capturando dados e também, sobre os protocolos e *host* de rede.

6.4. *Wireshark*

Mostrado na Figura 2, o *Wireshark* é um dos analisadores de protocolos mais usados no mundo, um projeto iniciado em 1998, oferecendo recursos como de visualização de transferência de pacotes. Disponível para ambiente Unix e Windows, o *Wireshark* é indicado para o aprofundamento das análises de redes, que, com implementação, a *tshark,* permite a sua visualização em modo de texto.

Porém, essa ferramenta possui limitações no cenário que temos hoje, principalmente no que tange a roubo de dados pois as atuais redes de computadores transmitem seus dados de forma criptografada, ou seja, seria necessário possuir ou descobrir a chave de descriptografia para acessá-los.

Figura 2 - Visão geral do *WireShark*.



Fonte: Elaborada pelo autor.

7.Próximas Etapas

A pesquisa se encontra em período de teste com a utilização do aplicativo escolhido, o *Wireshark*, para o desenvolvimento prático do estudo estabelecido. Nesta etapa a avaliação comparativa da vulnerabilidade da transferência de dados será feita, em que poderão ser levantados aspectos favoráveis e limitações na utilização dos *sniffers* de rede. Para isso, uma rede teste será implementada no ambiente de estudo (laboratório de redes), possibilitando esta análise.

Meios para realização dos testes serão através de máquinas virtuais, que simulam de forma precisa os materiais de trabalho necessários, juntamente com a utilização de roteadores e outros equipamentos físicos contidos no laboratório.

8.Referências Bibliográficas

GARCIA, Fernando P.; SOUZA, J. N.; ANDRADE, Rossana MC. Sistemas de monitoramento passivo para RSSF–soluções existentes e uma nova proposta energeticamente eficiente. **XXXI Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC), p. 179-192, 2013.**

KUROSE, James F.; Redes de computadores e a Internet: uma abordagem top-down, 5ª edição; **São Paulo: Addison Wesley, 2010, ISBN 978-85-88639-97-3**

MANN, Cesar. "Análise Constante." **2009.**

MATIAS JR, Rivalino; GONÇALVES, Rodrigo Brasil . Uma Solução para Análise de Tráfego em Redes Comutadas Baseada em Linux Bridging e Ntop**. In: VIII Workshop de Software Livre/Fórum Internacional de Software Livre (WSL 2005), Brasil. 2005.**

MOTA FILHO, João Eriberto ; Análise de Tráfego em Redes TCP/IP: utilize tcpdump na análise de tráfegos em qualquer sistema operacional / **João Eriberto Mota Filho. São Paulo: Novatec Editora, 2013, ISBN 978-85-7522-375-8**