9ª Jornada Científica e Tecnológica do IFSULDEMINAS
6º Simpósio da Pós-Graduação

PROXY LINUX GERANDO *LOGS* PARA POSSÍVEIS BUSCAS EM RELAÇÃO AO MARCO CIVIL DA INTERNET

ANDRADE; Jadeir de[1]; CASTRO, Marcelo R. de[2]

RESUMO

Este artigo descreve a idealização e construção de um servidor com Linux utilizando Squid, Lightsquid, SquidGuard e Sarg para gravação de logs de usuários em possíveis buscas para o Marco Civil da Internet. Para tal implementação foi utilizado o Sistema Operacional Linux Debian, e nele foram instalados e configurados os seguintes serviços necessários para seu funcionamento. Posteriormente é apresentado os resultados do estudo e são apresentadas a maneira como são gerados os relatórios de acessos dos usuários e a forma proposta por esse trabalho visando a segurança da informação e a proteção do usuário.

Palavras-chave: Servidores *Linux; Proxy;* Marco Civil da Internet; Segurança da informação

1. INTRODUÇÃO

A Internet pode ser definida como uma rede de computadores destinada à troca de informações, podendo ser configurada em qualquer escala, com qualquer número de computadores, desde que haja uma comunicação (KUROSE, 2009).

No Brasil, a utilização da Internet se desenvolveu através das universidades e da iniciativa privada, estando disponível até o ano de 1995, apenas para esses dois setores da nação. Mas a partir daí o número de provedores, a qualidade e a tecnologia empregada aumentaram a cada ano. Atualmente, o que impõe a Lei à Internet no Brasil são as normas do Marco Civil da Internet, que, segundo seu projeto de lei sancionado pela ex-presidente da república Dilma Rousseff no dia 23 de abril de 2014 e está em vigor desde o dia 24 de junho de 2014[3], estabelece princípios, garantias, direitos e deveres para o uso da Internet, tanto para usuários, quanto para Provedores de Internet.

O Provedor de Internet oferece os serviços de Internet através dos servidores, que são computadores com sistemas específicos implementados que fornecem serviços a uma rede de computadores (TANEMBAUM, 1997). Segundo Morimoto(2008) um servidor de *proxy* administra a Internet de uma determinada empresa ou provedor tornando-a mais rápida.

O *proxy* é o elo entre o servidor e o usuário, e, dentro deste elo é que ficam guardadas todas as regras de uso, ou seja, cabe a ele, intermediar a solicitação de endereço entre o

[1] - IFSULDEMINAS- Campus Muzambinho; jadeir_crc@hotmail.com
[2] - IFSULDEMINAS- Campus Passos; marcelo.castro@ifsuldeminas.edu.br
[3] - Lei 12.965 de 23 de Abril de 2014: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

usuário e o servidor. Um servidor de *proxy* pode ser configurado utilizando o Sistema Operacional *Linux*, onde se utiliza o *Squid* (MORIMOTO, 2008).

O *Squid* embora seja definido como um *software*, nada mais é que um conjunto de normas estabelecidas através de linhas de comandos dentro do servidor *Linux* pelo administrador deste servidor, onde este as organiza da melhor forma a permitir ou bloquear o acesso à determinados conteúdos. O *Lightsquid* é um pacote desenvolvido em linguagem *Perl,* para o *Squid*, que gera os relatórios que contém os dados dos usuários que acessaram os serviços de Internet do servidor em questão. Já o *Sarg*, conforme cita Morimoto (2008), é um interpretador de *logs* para o *Squid* que sempre que executado cria um conjunto de páginas divididas por dia, com uma lista de todas as páginas que foram acessadas, a partir de que máquina da rede veio cada acesso (OGAWA, 2012).

Considerando o Marco Civil da Internet no seu Capítulo III (Da Provisão de Conexão e de Aplicações de Internet), na Seção II (Da Guarda de Registro), o Artigo 10 diz que:

> A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de Internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.

E no parágrafo primeiro:

> O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no *caput*, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7°.

Assim, é proposto a implementação de um servidor *proxy* utilizando *Squid*, as listas do *SquidGuard* e os relatórios do *Lightsquid e Sarg*, para registrar as informações (*logs*) dos usuários e no caso de possíveis ordens judiciais, disponibilizar, de forma segura, tais informações através de buscas realizadas dentro do servidor.

2. MATERIAL E MÉTODOS

Foram realizadas atividades iniciais de implementação virtual (laboratório). O modelo virtual procedeu-se em um único computador para simulação das instalações, configurações do servidor e testes. O equipamento utilizado foi um notebook com processador de 2 núcleos, 2 *gigabytes* de memória *RAM* e *HD* de 500*GB*, onde foram emulados 4 computadores virtuais

que receberam o sistema operacional *Linux*.

Foram realizadas as instalações de todos os softwares necessários como *DHCP, BIND, Apache, Squid, SquidGuard, Lightsquid, Sarg e SSH Server*, que foram utilizados para a configuração e comunicação em rede dos computadores virtuais. O *software* para virtualização foi o *VirtualBox* da empresa *Oracle*. Todos os softwares utilizados na implementação foram obtidos gratuitamente na internet.

3. RESULTADOS E DISCUSSÕES

Nos relatórios gerados pelo servidor da forma que foi proposta por este trabalho, visando a Segurança da Informação e atender às normas do Marco Civil da Internet, o administrador do servidor ao ter a busca judicial solicitada, vai digitar o seguinte comando no *Sarg* para gerar o relatório do usuário em questão: **sarg -d 'data-data' -u 'usuário'**

Ao acessar o endereço 'http://192.168.10.100/squid-reports' o *Sarg* pede-se *login* e senha ao usuário como na Figura 1, dados estes que apenas um usuário permitido pela justiça deve ter acesso.

Geralmente os administradores de servidores executam os comandos para gerar o relatório e vão em um navegador de um dos computadores conectados na rede do servidor, digitam o IP do servidor e acessam os relatórios. Para gerar relatórios no *Sarg* os administradores executam o comando 'sarg' no servidor, vão a um navegador de um computador na rede e digitam: 'http://''Ip''/' 'squid-reports' e acessam os relatórios gerados (Figura 2). Neste caso o endereço do *Sarg* ficou: **http://192.168.10.100/squid-reports**

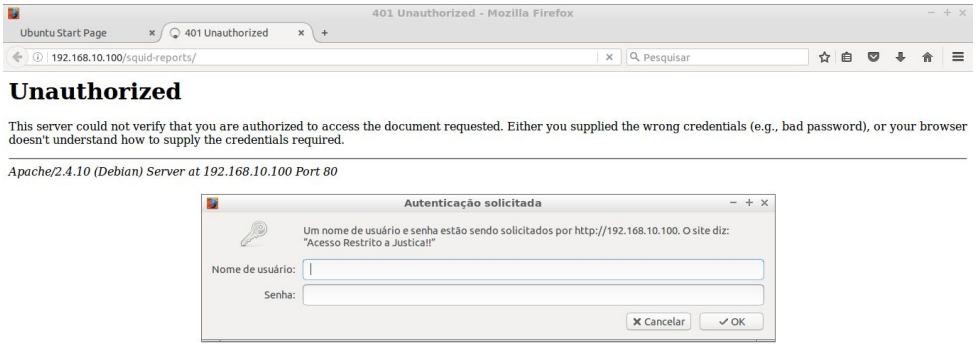

Figura 1 - Pedido de credenciais para acessar os relatórios

Figura 2 - Relatórios gerados com *Squid, SquidGuard, Lightsquid e Sarg*. Nesse relatório pode-se verificar: qual usuário, quando, onde e o que o usuário acessou; dados esses que uma eventual busca judicial pode requisitar.

3. CONCLUSÕES

Este trabalho teve como objetivo geral propor e mostrar a implementação de um servidor *proxy* de modo que, com segurança, pudesse gravar os *logs* de usuários que acessarem os serviços fornecidos por tal servidor, afim de possíveis buscas de acordo com as necessidades do Marco Civil da Internet.

De forma mais específica, esperava-se com a realização deste trabalho mostrar que é possível obedecer o que impõe o Marco Civil da Internet, sem ferir a confidencialidade, integridade e disponibilidade das informações dos usuários, além de mostrar como agir no caso de alguma solicitação de busca judicial.

REFERÊNCIAS

KUROSE, James F.; ROSS, Keith W.. **Redes de Computadores e a Internet Uma abordagem top-down**. 3. ed. São Paulo: Pearson Education, 2009.

MORIMOTO, Carlos E.. **Servidores Linux: Guia Prático**. Porto Alegre: Gdh Press e Sul Editores, 2008. 736 p. Disponível em: <http://www.hardware.com.br/livros/servidores-linux/>. Acesso em: 15 abr. 2015.

OGAWA, Takanori. **Análise e Implementação de Nova Solução de Firewall.** 2012. 70 f. Monografia (Especialização) - Curso de Tecnologia em Análise e Desenvolvimento de Sistemas, Centro de Ciências Tecnológias - Cct, Instituto Federal Catarinense de Educação, Ciência e Tecnologia – Campus Araquari, Joinville, 2012. Disponível em: <http://www.pergamum.udesc.br/dados-bu/000000/000000000016/0000164D.pdf>. Acesso em: 11 abr. 2015.

TANENBAUM,Andrew S.. **Redes de Computadores**. 4ª ed. São Paulo: Campus, 2010.