ANALISANDO AS APLICAÇÕES DO PROXY

Aprendemos que o servidor proxy trabalha para manter a autenticação em redes de computadores, a fim de limitar o acesso de usuários conforme suas permissões, o que promove uma maior segurança dentro de determinada rede. Assim, o proxy funciona graças à aplicação de filtros pelos administradores de redes, que filtram requisições baseadas no endereço IP do cliente, domínios, redes, localização (URL) do arquivo requisitado, bloqueando assim requisições inapropriadas.

Contudo, muitos usuários, chamados de crackers, utilizam o proxy para realizar ações ilegais que iludem sistemas de proteção, para acessar a deep web, entre outros. Desse modo, é possível que crackers montem um servidor proxy falso, mas que se passa por confiável, através da instalação de um software malicioso no computador. Com isso, o computador infectado funciona como um proxy que recebe instruções de um servidor controlado pelos crackers. Esse e outros artifícios são úteis para que invasões sejam realizadas inclusive em roteadores, como relatado recentemente em Marchetti (2018).

Quando crackers têm acesso ao seu roteador, ele pode ter acesso a todos os dispositivos conectados na rede, isto é, uma vez que roteadores são infectados, toda uma rede fica vulnerável. Nesse caso, os crackers conseguiram alterar o endereço do servidor DNS utilizado pelos roteadores, o que possibilitava que eles direcionassem você a um site falso, mas que você pensa que é oficial, como, por exemplo, qualquer página que exija login. Eles podem, então, obter senhas que você digitou pensando estar em um site oficial e seguro, desde redes sociais até sistemas de bancos. Além disso, o vírus instalado nos roteadores também tinha a capacidade de transformar o dispositivo do usuário conectado a rede em proxies. Em Malware (2015), você pode entender o que acontece quando um computador em um proxy.

Independentemente do tipo de invasão, é algo que agride a privacidade das pessoas e empresas e pode incorrer como um crime. A intenção é ter o conhecimento sobre o que é possível fazer na configuração dos proxies em uma organização para tirar vantagens de sua utilização. As aplicações são em prol de:

Redução do tráfego externo;

Redução da latência;

Possibilidade de acesso;

Impedir o acesso indevido;

Redução de carga dos servidores.

Referências

COMER, D. E. Redes de computadores e internet. 6. ed. Porto Alegre: Bookman, 2016.

MALWARE transforma computador infectado em proxy de internet. Canaltech. 29 dez. 2015. Disponível em: <https://canaltech.com.br/seguranca/malware-transforma-computador-infectado-em-proxy-de-internet-55257/>. Acesso em: 15 jul. 2019.

MARCHETTI, B. Quadrilha de hackers fez a festa ao invadir roteadores de brasileiros. Vice, 27 abr. 2018. Disponível em: <https://www.vice.com/pt\_br/article/wj733z/hackers-virus-roteadores>. Acesso em: 15 jul. 2019.

SCHMITT, M. A. R. Rede de computadores: nível de aplicação e instalação de serviços. Porto Alegre: Bookman, 2013.

Vamos praticar

Você viu um exemplo de possibilidade de acesso indevido a dispositivos em uma rede de computadores conectada à internet. Isso pode ocasionar diversos problemas. Embora esse seja um exemplo de aplicação do proxy, ele não foi criado para isso e sim para tirar vantagens de sua utilização, como citado acima.

Portanto, escolha uma vantagem, dentre as cinco citadas na contextualização acima, explique como ela funciona e dê um exemplo de aplicação. Pesquise e responda em até uma página.

Não se esqueça de disponibilizar suas conclusões no fórum da seção “Compartilhe”.

Aplicação do *proxy* para impedir acessos indevidos

Iuri de Carvalho Salgado

Tentativas de acesso indevido podem ocorrer de forma interna ou externa a uma rede, sendo elas quando um usuário cliente busca acessar alguma página ou url que estejam fora da política de uso da rede em questão ou quando algum individuo mal intencionado tenta acessar os servidores desta rede.

Sendo assim, analisando um ataque externo, a implementação de um *proxy* reverso pode oferecer uma camada extra de proteção a esta ameaça. Uma rede sem proxy reverso pode deixar seu servidor exposto a um acesso direto dos usuários, entre eles *crackers* e *bots.* Numa rede com proxy reverso pode-se permitir apenas conexões criptografadas evitando a interceptação de dados além de esconder o endereço IP do servidor, afim de dificultar tentativas de invasão.

Se tratando de usuários internos, uma rede pode ser configurada um *proxy* que efetua o bloqueio de urls, permitindo ao administrador limitar o acesso a conteúdo. Pode ser um bloqueio de sites e filtragem de palavras ou frases sensíveis. Essa prática é aplicada em algumas organizações para evitar, entre outras coisas, o acesso a sites de conteúdo adulto, redes sociais e download de softwares duvidosos. Desta forma se implementa uma segurança maior e evita além de distrações, possíveis problemas operacionais causados por *malwares* que podem infectar toda a rede.

Referências:

DIAS, Márcio. Proxy Reverso: velocidade e segurança para seu site. **Abale**. Disponível em https://abale.com.br/proxy-reverso-velocidade-e-seguranca-para-o-seu-site/. Acessado em 23/09/2021.

Feedback:

O aluno deve explicar uma das vantagens da utilização do *proxy*e, então, demonstrar uma aplicação ou exemplo de acordo com a vantagem. A seguir, são explicados, de forma objetiva, cada vantagem citada. O aluno pode discorrer detalhadamente sobre a vantagem escolhida, o que pode variar entre um parágrafo ou uma página, dependendo da vantagem e da aplicação ou do exemplo escolhido.

 A redução do tráfego externo diz respeito à quantidade reduzida de requisições e respostas que devem trafegar na rede, de modo que o arquivo seja recuperado do servidor somente uma vez, o que reduz a quantidade de banda utilizada pelos clientes.

Nesse caso, a aplicação é do próprio *proxy* com a função de cache. O aluno deve explicar como funciona o cache em páginas HTTP.

A redução de carga dos servidores se deve à quantidade menor de requisições para o servidor *web* remoto atender. Como, por exemplo, *sites* muito congestionados quando o acesso é potencializado porque é período de *Black Friday* ou quando há divulgação de algum resultado de vestibular. O *proxy* pode auxiliar na resolução desse problema. O aluno pode explicar como funciona essa redução de carga que pode ser distribuída entre servidores e, então, dar um exemplo de problema que é resolvido.

A redução de latência se refere exatamente ao funcionamento do cache, devido ao fato dos arquivos da página *web* poderem ser acessados por meio do cache, não tendo que ser acessados pelo servidor *web* remoto. Isso explica um funcionamento mais rápido do acesso aos sites e, consequentemente, redução da latência na rede. O aluno deve explicar isso e o funcionamento do cache, nesse caso.

A possibilidade de acesso de um modo legal se refere ao fato de que se o *site* estiver inoperante por algum motivo, ou está congestionado e não pode ser acessado, se existir um armazenamento temporário no cache do servidor *proxy*, será possível acessar o *site*, porém em uma versão talvez não atualizada. O aluno deve explicar isso ou pode explicar um caso ilegal em que o *proxy* pode ser utilizado para possibilidade de acesso indevido, mas diferente do caso exemplificado na contextualização da atividade.

O impedimento do acesso indevido é possibilitado pelo *proxy* configurado para bloquear *sites* do interesse da organização. Em universidades ou escolas, por exemplo, para impedir o acesso a sites adultos ou mesmo redes sociais. Além disso, mesmo que não seja aplicado filtro para esse bloqueio, o *proxy* permite guardar o *log* de todos os acessos e então reprimir determinados usuários. O aluno deve explicar como é possível aplicar esses filtros ou ver os *logs* e dar um exemplo de aplicação, como os citados.