FACULDADES INTEGRADAS SANTA CRUZ DE CURITIBA

MONITORAMENTO - WIRESHARK

CURITIBA

2016

AUGUSTO MONTOVANI
DUANN G. PLISKIEVISKI
EDERLO RODRIGO
MARCOS V. HERMAN
SMAYLESON DE LIMA

MONITORAMENTO - WIRESHARK

Trabalho apresentado para disciplina Software Livre do curso de Bacharelado em Sistemas de Informação das Faculdades Integradas Santa Cruz de Curitiba

Orientador: Prof. Titulação Francisco Aparecido da Silva

RESUMO

Uma ferramenta bastante utilizada por gerentes de rede para monitorar o tráfego de rede como o Wireshark. Este trabalho apresenta esta ferramenta e sua aplicação de monitoramento e suas funcionalidades.

Palavras Chave: Wireshark, Análise de Tráfego.

SUMÁRIO

1. INTRODUÇÃO

Nos últimos anos houve um grande aumento do número de usuários que utilizam a Internet para diversos fins, paralelamente a isto vem surgindo milhares de aplicações web que são disponibilizadas na grande rede. Estas possuem serviços variados e uma série de requisitos como interface web, protocolos de comunicação, protocolos de transporte entre outros que as tornam muito utilizadas. No entanto, aplicações web são vulneráveis a falhas de segurança facilmente encontradas nos navegadores de internet, mensageiros instantâneos etc. Avaliar e caracterizar o tráfego que uma aplicação web gera na rede, portanto, é essencial para se ter o conhecimento do que esta envia para os usuários (clientes) a fim de evitar, por exemplo, possíveis invasões de arquivos maliciosos nas estações dos clientes.

Este trabalho tem como objetivo caracterizar o tráfego gerado por uma aplicação web para uma estação cliente, utilizando um protocolo totalmente livre chamado Wireshark.

2. INTRODUÇÃO AO TEMA

Existem diversossoftwares que fazem o monitoramento de redes de computadores, esses programas são conhecidos como sniffers, analisadores de redes ou alisadores de protocolo e são ferramentas desenvolvidas para interceptar e registrar o trafego de redes de computadores. A técnica de Sniffing pode ser usada tanto para o bem, tanto a para o mal dependendo apenas dos propósitos de quem opera a ferramenta.

Agora iremos citar brevemente algumas ferramentas e abordaremos o Wireshark um pouco mais a fundo, pois é um dos melhores e mais conhecidos sniffers de rede.

2.1 - NETWORKS MINER

É uma ferramenta de análise forense network para Windows, Linux e MAC OS X. Usa-se como uma ferramenta de captura de rede sniffer, afim de detectar sistemas operacionais, sessões, nomes de host, portas abertas e etc. Tudo isso sem ocupar o trafego da rede. O Network Miner torna a execução mais fácil no analise de trafego, a forma como os dados são apresentados torna a análise mais simples e economiza muito tempo. Sua primeira versão foi lançada em 2007. (NETWORKMINER, 2015)

2.2 – SNIFFERPASS

É um software de monitoramento de senha pequeno que escuta a sua rede, para capturar as senhas que passam pelo seu adaptador de rede e exibi-los na tela instantaneamente. Sniffpass pode capturar senhas dos seguintes protocolos: POP3, IMAP4, SMTP, FTP e HTTP (senhas de autenticação básica). Pode-se usar também para recuperar senhas da Web / FTP / E-mail perdidos. (SNIFFPASS, 2012)

3. WIRESHARK

O Wireshark é uma ferramenta desenvolvida para realizar análise de pacotes que trafegam pela rede. É um software de código livre, (WIRESHARK, 2016) sob a licença GNU GPLv2 que dentre outras normas já difundidas entre os softwares livres, garante que o mesmo permaneça sempre com seu código-fonte aberto. (VIEIRA, 2011)

O Wireshark é suportado por uma enorme quantidade de plataformas como o UNIX, Linux, Solaris, FreeBSD, MAC OS X, Windows e outros sistemas, ou seja, praticamente qualquer computador pode utilizar o Wireshark.

Como já mencionado, o Wireshark analisa e também pode ser usado para monitorar o trafego de dados em uma única máquina ou em uma rede com vários computadores.

Quando o Wireshark é iniciado, a primeira coisa que deve ser feita é selecionar uma placa de rede instalada na máquina utilizada, a partir daí a ferramenta analisa todo o trafego, e sua interface gráfica exibe os dados capturados na tela com base nos protocolos que transmitem ou recebem esses mesmos dados. É possível aplicar inúmeros filtros, que são absolutamente necessários, devido à grande quantidade de pacotes capturados durante um pequeno período no qual o software esteja ativo. (UFPR, 2016)

O Wireshark também é capaz de criar diversos gráficos que mostram o trafego de redes conforme o protocolo utilizado, como medição do nível de broadcast em uma rede ou o trafego destinado a uma determinada porta dentre tantas outras possibilidades possíveis (UFPR, 2016)

Como observado o software apresentado pode ser utilizado para diversas tarefas, tanto para o bem, tanto para o mal. Pode ajudar administradores de redes a controlar o trafego de rede e encontrar problemas, como também podem ser usados por pessoas mal-intencionadas, realizando diversas formas de ataque como:

Clonagem de MAC –Onde o atacante clona o endereço MAC da vítima, se passando por ela, dessa forma recebendo todos os pacotes destinados a mesma. Este tipo de ataque pode ser usado em redes que utilizam o controle de acesso por MAC. (ALVES et al., 2010)

- Escuta do Tráfego com ARP Spoofing - é um tipo de ataque no qual uma falsa resposta ARP é enviada à uma requisição ARP original. Confundida pelo ataque a Estação A envia pacotes para a Estação B

pensando que ela é o gateway da rede, e a Estação B captura a transmissão e redireciona os dados para o endereço correto sem que o tráfego da rede seja interrompido. (IMASTERS, 2010)

- Deve ser ressaltado que os ataques mencionados acima não são tão simples de serem executados e também existem outras camadas de segurança que podem impedir ou dificultar ainda mais o ataque. Essas possibilidades foram expostas de forma extremamente simplificada, com o intuito de mostrar as inúmeras possibilidades que o Wireshark traz e podem ser exploradas, junto com outras ferramentas, por qualquer pessoa que tenha interesse e vontade de aprender e explorar.

4. CONSIDERAÇÕES FINAIS

Durante o desenvolvimento deste trabalho foi mostrado a utilidade e eficiência da utilização do Wireshark para se avaliar o tráfego em uma rede de computadores, permitindo assim apresentar um resultado do tráfego capturado durante um período de execução de várias formas, facilitando sua caracterização. Aprendeu-se, portanto, que em qualquer rede de computadores, com qualquer plataforma, podemos monitorar e avaliar todo o tráfego gerado por uma aplicação web através do uso de algum programa analisador de protocolos.

5. REFERÊNCIAS

WIRESHARK (Ed.). **Wireshark Frequently Asked Questions.** 2016. Disponível em: <https://www.wireshark.org/faq.html>. Acesso em: 13 nov. 2016.

VIEIRA, Vinícius. **Entenda as diferenças entre a GPLv2 e GPLv3.** 2011. Disponível em: <http://sejalivre.org/entenda-as-diferencas-entre-a-gplv2-e-gplv3/>. Acesso em: 13 nov. 2016.

UTFPR - Campo Mourão (Ed.). **Wireshark - Analisador de Tráfego de Rede.** 2014. Disponível em: <http://wiki.cm.utfpr.edu.br/index.php/Wireshark_-_Analisador_de_Tráfego_de_Rede>. Acesso em: 13 nov. 2016.

ALVES, Francinildo Ramos et al. **Redes Sem Fio II: Análise de Vulnerabilidade.** 2010. Disponível em: <http://www.teleco.com.br/tutoriais/tutorialredesemfio2/pagina_3.asp>. Acesso em: 13 nov. 2016.

IMASTERS (Ed.). **Arp Poisoning.** 2010. Disponível em: <http://imasters.uol.com.br/artigo/10117/seguranca/arp_poisoning/>. Acesso em: 25 maio 2010.Acessado em 25/05/2010.

NETWORKMINER (Ed.). **NetworkMiner.** 2015. Disponível em: <http://www.netresec.com/?page=NetworkMiner>. Acesso em: 13 nov. 2016.

SNIFFPASS (Ed.). **SniffPass.** 2012. Disponível em: <http://www.nirsoft.net/utils/password_sniffer.html>. Acesso em: 13 nov. 2016.