VI Workshop de Computação:
Profissionais do futuro
30 de Maio à 03 de Junho

SEGURANÇA DE REDES: SNIFFING

Elias de Abreu Domingos da Silva[1], Jonathan Luis Monteiro da Silva[1], Josélia Faria Pires[2]. e-mail: elias.silva@unemat.br, jonathan.eu32@gmail.com, joseliaapires@hotmail.com

[1]Universidade do Estado de Mato Grosso – UNEMAT - Campus de Cáceres/Faculdade de Ciências Exatas e Tecnológicas, Departamento de Computação

[2]Universidade do Estado de Mato Grosso – UNEMAT - Campus de Alto Araguaia /Faculdade de Letras, Ciências Sociais e Tecnológicas - FALECT, Departamento de Computação

Palavras-chave: Redes de computadores, Sniffing, Wireshark.

Resumo

Com a constante evolução da tecnologia das redes de computadores para realização de tarefas diárias, inúmeros serviços foram incorporados trazendo diversas vantagens, exemplos destas são: compras online, estudos, movimentações financeiras, troca de informações entre computadores e diversas outras. Com o crescimento da utilização de redes para transmissão de dados o tema segurança se torna muito importante. Atualmente diversas técnicas de capturas de dados estão sendo utilizadas por pessoas com intenções maliciosas visando roubar informações. A técnica de analise de pacote, denominada *Sniffing*, são umas das mais utilizadas, esta técnica consiste em capturar todo o fluxo trafegado na rede decodificando e analisando cada pacote individualmente a fim de obter informações relevantes. Existem diversos tipos de ferramentas que capturam e analisam os pacotes trafegados na rede, as mais conhecidas são o *TCPdump, Wireshark, Capsa Network Analyzer, CommView.* Qualquer pessoa que tenha um conhecimento de redes pode utilizar estas ferramentas, isto apresenta um perigo em utilizar redes não confiáveis, principalmente para realização de tarefas que envolvam trafego de dados importantes. Existem técnicas que evitam que os dados trafegados na rede sejam lidos, as mais conhecidas são a criptografia e a assinatura digital. O grande problema de identificar um *Sniffing* atuando na rede é que o mesmo atua de forma passiva, ou seja, somente lendo pacotes diferentes da técnica *man-in-the-middle* que além de analisar os pacotes também podem editá-los e excluí-los. Durante o desenvolvimento do trabalho utilizamos a ferramenta *Wireshark*para captação de pacotes em uma rede privadacom o objetivo de mostrar a fragilidade em muitas

aplicações, principalmente em sites, que não utilizam métodos que posam evitar este tipo de roubo de dados. Em apenas 24 horas capturando o trafego da rede foi possível montar um banco de dados com diversas informações importantes, entre as informações consta usuários e senhas de sites que não utilizam criptografia ou utilizam de forma incorreta, páginas acessadas dentre diversas informações. Todos os usuários da rede analisada estão cientes do trabalho que foi realizado e todas as informações serão apagadas para não causar constrangimento com os usuários desta rede de computadores.