12º Simpósio de Ensino de Graduação

DETECÇÃO E PREVENÇÃO DE INTRUSÕES, ATAQUES E VULNERABILIDADES

Autor(es)

FELIPE AUGUSTO PALMA
RODRIGO FABRICIO

Orientador(es)

JOSÉ LUIS ZEM

Resumo Simplificado

É comum definir o protocolo ARP (Address Resolution Protocol) como um protocolo da camada de Enlace de Dados (modelo ISO/OSI), porém o mesmo acompanha os protocolos da arquitetura TCP/IP estando localizado na camada de Rede. Seu funcionamento é bastante simplificado e seu objetivo é o de atuar apenas no contexto de uma rede local (LAN - Local Area Network) oferecendo uma maneira de descobrir o endereço fisico (MAC - Media Access Control) da interface de rede de um determinado computador a partir do endereço IP do mesmo. Seu funcionamento baseia-se em encaminhar quadros com característica de difusão (broadcast) contendo o endereço IP do computador de destino e, ao atingir o mesmo haverá uma resposta informando o seu respectivo endereço MAC. A modalidade de ataque “ARP Poisoning” consiste em enviar respostas falsas a partir de requisições ARP feitas pelos computadores de uma rede. Estes computadores começam a encaminhar quadros à máquina do atacante que, por sua vez, estará configurada para capturar as transmissões. Dessa forma, o atacante tem a possibilidade de capturar e produzir registros de todo o tráfego usando para isso um software de captura de pacotes conhecido com sniffer. Já na modalidade conhecida por “MAC Flooding”, o objetivo é o de atacar o switch da rede. Ela consiste em encaminhar um grande número de quadros com endereços MAC falsos e, dessa forma, levando ao estouro da tabela de armazenamento de endereços MAC e fazendo com que o switch passe a operar como um HUB, encaminhando as transmissões para todas as portas, assim o atacante consegue capturar todas as transmissões realizadas na rede. Os ataques às redes de computadores podem ter simplesmente o objetivo de causar anomalias, ou então, algo mais sério, como o roubo ou a manipulação de informação. Para detectar estas modalidades de ataque é possível usar ferramentas livres, como por exemplo, o arpwatch, e o wireshark, este último utilizando a técnica de spanning. No protocolo IPv4, o ARP é o responsável pela resolução de endereços MAC já no protocolo IPv6, o responsável pela descoberta de computadores vizinhos é o NDP (Neighbor Discovery Protocol), que funciona a partir do protocolo ICMPv6, mantendo uma tabela de vizinhança, correspondente à tabela ARP no IPv4. Os objetivos desse artigo são o de apresentar o protocolo ARP, descrevendo brevemente o seu funcionamento, e algumas de suas vulnerabilidades, bem como, formas de detecção e prevenção de ataques que possam ocorrer em redes de computadores. A metodologia empregada neste estudo foi a de levantamento realizado em livros, artigos e materiais coletados diretamente da Internet. Como resultado desse estudo, torna-se importante, em um ambiente de rede de computadores, entender o funcionamento das partes individuais e técnicas empregadas para que se possa propor alternativas que viabilizem a construção de um ambiente mais seguro. Concluindo, o protocolo ARP possui funcionamento simples e não possui sistema de verificação de autenticidade, por isso torna-se alvo de ataques. Para o administrador de rede é essencial conhecer o funcionamento dos protocolos da rede de computadores para que seja possível detectar e isolar os problemas.