ATIVIDADE DE LABORATÓRIO I - ARP POISONING

Victor Dallagnol Bento
Universidade Federal de Santa Maria
Santa Maria - RS, Brasil
victor.bento@ecomp.ufsm.br

I. INTRODUÇÃO

A disciplina de Segurança de Rede tem como objetivo compreender os conceitos e princípios fundamentais de segurança de rede. Assim como conhecer os tópicos básicos de segurança, incluindo criptografia de chave pública e simétrica, assinaturas digitais, funções hash criptográficas e protocolos de segurança de rede. Também tem como objetivo configurar serviços básicos de segurança.

II. DESENVOLVIMENTO TEÓRICO

O Address Resolution Protocol (ARP) é um protocolo de camada que é responsável pela resolução de endereços IP e MAC. Quando acontece o envio de um pacote de um host para outro, o endereço MAC deve ser indicado no cabeçalho, que é um identificador fixo e exclusivo atribuído a cada placa de rede.

Para a comunicação entre aplicativos de uma rede, é necessário utilizar o protocolo IP para identificar a máquina de destino. Pelo fato de que os endereços IPs podem variar, é essencial associá-los aos endereços MACs.

O protocolo ARP é usado para verificar se o endereço MAC que está indicado no cabeçalho do pacote que chega na máquina coincida com o seu, se os endereços não coincidirem o pacote é ignorado.

Todos os dados associados aos endereços IP e MAC podem ser vistos em uma tabela ARP. Isso pode ser o caso de um aplicativo que queira enviar um pacote para um IP que não esteja nessa tabela. Neste caso, é necessário perguntar quem tem o IP desejado e, para isso, o ARP também é usado atraveś da função Request.

Todas as máquinas da rede receberão esse pacote, que será lido e atualizado em suas tabelas IP e MAC com as novas informações, e não apenas a máquina que fez a pergunta. Desta forma, todas as tabelas das máquinas serão atualizadas com essa nova informação maliciosa. Fazendo com que toda vez que alguém enviar um pacote através do roteador, o mesmo não será apanhado pelo roteador, mas pela máquina atacante, uma vez que é direcionado para o seu endereço MAC. O mesmo acontecerá todas as vezes que o roteador ou outro equipamento enviar um pacote para a vítima.

Como a máquina do cibercriminoso sabe que “está envenenando o protocolo ARP”, ele conhecerá os endereços MAC reais de todas as suas vítimas, podendo assim configurá-los para encaminhar esses

pacotes ao seu verdadeiro destinatário, de modo que ninguém perceba que foram interceptados no caminho.

III. DESENVOLVIMENTO EXPERIMENTAL

No experimento ministrado em aula em primeiro momento foi feita a instalação e configuração do Windows Server 2003, onde a máquina de cada aluno recebeu um IP específico.

Através do Prompt de Comando do Windows efetuou-se o comando ping seguido do endereço IP de cada máquina para que todos os dados (endereço IP e endereço MAC) estejam presentes na Tabela ARP. Efetuada essa comunicação entre as máquinas, o próximo passo seria fazer com que uma delas desse um ping contínuo (se comunica-se continuamente - comando Request) em outra.

Neste meio tempo entre a comunicação entre as duas máquinas, uma terceira máquina seria a invasora, interceptando os pacotes enviados para o destino (enviando o comando arp replay). Para verificar a comunicação entre as máquinas foi utilizado o programa WireShark que analisa o tráfego de uma rede e monitora a entrada e saída de dados do computador, em diferentes protocolos, ou da rede à qual o computador está ligado.

Após a verificação da comunicação, utilizou o software Karat, onde possibilitou através de algumas configurações enviar uma pergunta (como explicado na parte teórica) fazendo com que a tabela ARP fosse atualizada para que o IP destino fosse associado com o MAC da máquina invasora, fazendo com que o invasor recebesse os dados que seriam para a máquina destino.

IV. CONCLUSÕES

Neste experimento de laboratório aprendeu-se sobre o funcionamento do protocolo ARP, assim como o funcionamento do envio de pacotes entre máquinas e a associação do endereço IP com o endereço MAC de cada uma delas, pela tabela ARP.

REFERÊNCIAS

[1] **Ementario Segurança de Rede**, https://portal.ufsm.br/ementario/disciplina.html?idDisciplina=99759 acessado em 26.03.2019.

[2] **ARP spoofing: ataque às redes locais**, https://www.welivesecurity.com/br/2017/11/07/arp-spoofing-ataque-as-redes-locais/ acessado em 26.03.2019

[3] **Wireshark**, https://pt.wikipedia.org/wiki/Wireshark acessado em 26.03.2019