Avaliação do Protocolo WEP na Segurança de Redes IEEE 802.11

Atrícia Sabino[1], Samy Soares[2]

[1]Estudante de Redes de Computadores/Bolsista Integrante PET – Conexões de Saberes – Universidade Federal do Ceará (UFC)

[2]Docente/Pesquisador/Tutor PET – Conexões de Saberes – Universidade Federal do Ceará (UFC)

atricia@alu.ufc.br, samysoares@gmail.com

Abstract. *This paper describes an evaluation of key protocol (WEP), used in IEEE 802.11 networks. Based on an article replicated experiments to discover if the complexity of a key may influence the security of the protocol. Has Executed another type of methodology and approach to check if the protocol is influenced by the keys.*

Resumo. *Este artigo descreve uma avaliação das chaves do protocolo (WEP), usado em redes IEEE 802.11. Com base em um artigo foram replicados experimentos para descobrir se a complexidade de uma chave pode influenciar na segurança do protocolo. Executou-se um outro tipo de metodologia e abordagem para verificar se o protocolo é influenciável pelas chaves.*

1. Introdução

Atualmente as redes sem fio vêm se tornando cada vez mais presentes nos ambientes corporativos, fazendo com que, os requisitos de segurança sejam considerados fatores de suma importância para proteção dos dados em trânsito.

Utilizando-se da prática de experimentos, este artigo tem como objetivo avaliar se a complexidade de senhas configuradas em redes 802.11 usando a criptografia WEP, pode influenciar na segurança do protocolo. Em princípio a ideia é replicar um experimento que já foi executado e validado os resultados. O artigo tomado como referência foi "Segurança em Redes IEEE 802.11: Um Estudo de Caso". Porém passou-se a usar uma outra abordagem e metodologia diferente do experimente em questão, para comparar as complexidades das senhas.

2. Conceitos

O protocolo WEP foi criado em 1999 visando preencher na época a lacuna existente nas redes IEEE 802.11[ANSI/IEEE 802.11]. O objetivo inicial era tentar simular a segurança de redes cabeadas, no entanto ocorreu muitas falhas visto que o pessoal responsável pelo desenvolvimento não era especializado [FLUHRER et al. 2001].

O padrão IEEE 802.11 é um padrão usado em redes locais sem fio que inclui mecanismos de controle de acesso, dentre eles a confidencialidade e integridade. Esse padrão utiliza um atributo para identificar a rede no qual é conhecido por SSID (*Service Set IDentifier*), este por sua vez é transmitido por *broadcast*, em texto plano o que permite que qualquer cliente facilmente capture pacotes dessa rede, ou seja, o SSID não é considerado um mecanismo eficaz de segurança.

Os ataques a redes sem fio estão cada vez mais comuns, sem contar na facilidade para a realização desses ataques, sendo possível até atacar redes que não fazem *broadcast* do SSID. A ideia por trás de um ataque a rede sem fio não é apenas comprometer ou invadir a rede, mas também encontrar uma maneira de comprometer a rede cabeada podendo assim comprometer todos recursos e serviços da rede como um todo.

3. Procedimentos Metodológicos

Para a realização desse trabalho foi necessário criar um cenário de experimentos a fim de realizar os testes. Para avaliação desse trabalho foi utilizados os seguintes equipamentos: 1) Um AP (*Acess Point*) D-Link para a criação da rede 802.11. 2) Um PC rodando o sistema operacional Linux conectado ao AP através da rede wifi.

3) Um PC rodando o sistema operacional Linux conectado ao AP via rede cabeada.

4) Um PC usando o sistema operacional Linux responsável pelo ataque. A figura 1 apresenta o cenário do experimento.

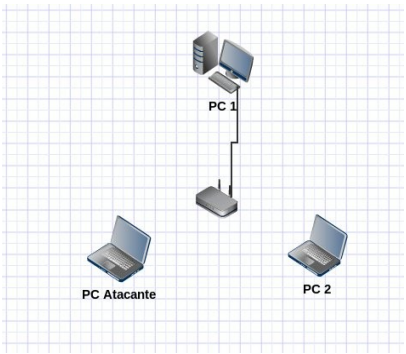

Figura 1 – Cenário dos experimentos

Para esse experimento o tráfego foi gerado pelas próprias máquinas, simulando portanto um funcionamento de uma rede normal, duas máquinas foram conectadas uma através da rede *wifi* e outra via rede cabeada, enquanto que a terceira máquina era responsável pelo ataque. Os ataques para recuperação de senhas foram feitos usando a ferramenta *Aircrack-ng*, ferramenta que permite analisar redes sem fios 802.1. Usando o método PWD (Pyshkin, Tews, Weinmann) no qual são necessários poucos pacotes de dados para que seja quebrado uma chave WEP. Para os testes iniciais foram utilizadas apenas duas chaves WEP: 1) Chave 1: APIAP (Apenas Maiúscula) e APIAP@(Acrescentando um caractere especial). Com a rede em funcionamento usou-

se da ferramenta *airodump-ng* integrante do *Aircrack-ng* para capturar os pacotes criptografados. Com um PC atacante em modo monitor é possível capturar pacotes de uma conexão que trafegam pela rede. O artigo no qual tentou-se replicar o mesmo experimento, tomou como base uma outra abordagem e outra metodologia, optaram por usar um script que ficasse capturando e comparando as senhas até encontrar sucesso e fracasso.

4. Resultados Parciais

A execução dos experimentos consistiu em realizar ataques ao AP configurado com as senhas WEP, e rapidamente com uma quantidade de pacotes pequenas capturadas pela ferramenta *airodump-ng* foi possível identificar as senhas configuradas. Em menos de 10 minutos já estava concluída toda a ação. Como atividades futuras, pretende-se testar os mais variado tipos de chaves, como por exemplo apenas números, números e caracteres especiais, apenas caracteres especiais, letras e caracteres, letras, números e caracteres.

5. Considerações Finais

Baseado no experimento inicial e nos resultados parciais obtidos nota-se que o protocolo tende a ser vulnerável a ataques, independente das chaves, visto que ambas levaram o mesmo tempo para serem quebrada. Ou seja, basta uma pessoa ter conhecimento sobre ferramentas e estar dispostos a atacar uma rede sem fio. Outra coisa importante é que não é necessário saber como funciona todo o processo do ataque, basta apenas executar a ferramenta e seguir os passos indicados.

6. Agradecimentos

Agradecemos ao professor João Marcelo pelo fornecimento de alguns equipamentos físicos necessários ao experimento e ao aluno Edigleison Barbosa pela participação na realização dos experimentos.

Referências

IEEE 802.11 WG, 1999. “Part11: Wireless LAN Medium Access Control (MAC) and Physical Layer Specification”. IEEE Computer Society.

Fluhrer, S., Mantin, I. e Shamir, A., 2001. “Weaknesses in the key scheduling algorithm of RC4”. Eighth Annual Workshop on Selected Areas in Cryptography.

D'Ambrosio, G. Bruno. e Gonçalves, da Silva. Paulo André. 2008. “Segurança em Redes IEEE 802.11: Um Estudo de Caso”. Congresso de Iniciação Científica da UFPE.