Artigo

O MÉTODO BRUTE FORCE PARA INVASÃO DE REDES SEM FIO

Alter Breitenbach [1]

Vinicius Possamai[2]

RESUMO

O aumento de dispositivos sem fio de acesso à internet e a crescente demanda por acesso à rede mundial de computadores (internet) são alvos de criminosos que, para se utilizarem de privilégios de usuário, realizam tentativas de invasão de redes e computadores por tentativa e erro. Desta forma, evidenciaremos a utilização do método brute force e métodos de evitar ataques deste tipo em computadores, contas privadas em sites, e-mail, entre outros e como o usuário deve garantir e proteger sua privacidade.

Palavras-chave: Brute force. Internet. Usuários. Computadores. Invasão.

1. Aluno do Curso técnico em redes de computadores – Faculdade e Escola técnica Alcides Maya. alterbreitenbach@gmail.com
2 Professor do Curso técnico em redes de computadores – Faculdade e Escola técnica Alcides Maya. vinicius_possamai@alcidesmaya.edu.br

1 Introdução

O presente trabalho visa apresentar uma visão geral do método de ataque force brute a redes sem fio (wireless), padrões de criptografia e indicar algumas soluções práticas que devem ser utilizadas para evitar tal tipo de ataque.

De antemão, podemos afirmar que o método de ataque não pode ser eliminado totalmente, visto que o ataque parte de invasores ou criminosos em busca de dinheiro, prestígio, motivações ideológicas, entre outros motivos.

2 O método de ataque force brute

Resumidamente podemos dizer que o ataque por force brute consiste “em que o atacante objetiva adivinhar, por tentativa e erro, *logins* e senhas de acesso de usuários legítimos” (DIORIO et al., 2019) com a utilização de listas de palavras e senhas as quais há dezenas espalhadas pela internet. Complementando, SOARES explica em seu artigo que:

> O ataque consiste em três etapas: a preparação das *wordlists*, a etapa de captura das redes e ataque WPS e por último, a execução dos ataques de dicionário e força bruta com os arquivos de capturas obtidos na segunda etapa e as listas de palavras obtidas na primeira etapa. (SOARES, s.d.)

Como observamos, a tentativa de invasão é relativamente simples, entretanto, as redes sem fio se utilizam de padrões de criptografia para impedir estas invasões, são eles: WEP, WPA e WPA2.

2.1 Padrões de criptografia

2.1.1 WEP (Wired Equivalent Privacy)

Lançado em 1997, foi o pioneiro no assunto proteção a redes sem fio. Utiliza um algoritmo de criptografia RC4, apontado como seu principal ponto fraco. Por outro lado “continua sendo amplamente utilizado em residências de todo o mundo, reflexo da falta de informação dos usuários de redes sem fio e da insistência de fabricantes de pontos de acesso em permitir que ele seja um dos padrões de segurança” (PAIM, s.d.). Basicamente o padrão WEP funciona em duas partes: autenticação e encriptação/decriptação de mensagens, na camada 2 do modelo OSI, ou de enlace.

2.1.2 WPA (Wi-Fi Protected Access)

Criado em 2002 pela WFA (Wi-Fi Alliance) e durante sua concepção foi “dado um enfoque maior na correção das falhas de segurança encontradas neste protocolo” (PAIM, s.d.), como forma de remediar e aprimorar o algoritmo RC4.

Utilizando-se do protocolo TKIP (Temporal Key Integrity Protocol), que, como o WEP, se utiliza do algoritmo RC4, entretanto “mas algumas precauções para evitar ataques, como não enviar a chave secreta “em claro” e trabalhar com uma política de vetores de inicialização mais inteligente” (PAIM, s.d.). Tornando, assim, o processo de encriptação/decriptação mais complexo e menos sujeito a invasão pelo método force brute.

2.1.3 WPA2

O padrão WPA2 é um avanço do WPA, também com avanços no processo de encriptação/decriptação e com a utilização de outro protocolo, neste caso o CCMP e abandonar a utilização do algoritmo RC4. Neste caso, a mensagem é anteriormente codificada para, após, ser enviada o que garante maior dificuldade de invasão.

SOARES (s.d.), em seu experimento, verificou que a maior parte das invasões decorre da falta de senhas fortes ou não triviais. Deste modo, o processo de criptografia e as proteções à rede sem fio, somente através da aprimoração de protocolos de segurança, tornam-se inúteis.

2.2 Métodos de defesa

Os principais métodos de defesa para os ataques de force brute recaem no usuário final ou ao administrador de rede. A eles cabe gerenciar e manter senhas de difícil compreensão, por exemplo: We$g3908$Cab3#Zhafsjkfhjk$&. Por outro lado, uma senha de fácil compreensão: @1ice1990, em que o nome do usuário (alice) fica “disfarçado” junto com o ano de, provavelmente, seu nascimento. Note-se que, neste caso, as simples substituições de algumas letras por símbolos semelhantes, muitas vezes, é algo óbvio. Por exemplo: a=@; o=0 (zero); l(éle)=1; s=5; entre outros.

Some-se a isto o fato dos usuários finais, em sua grande maioria, serem leigos no que diz respeito ao tema segurança. Todavia, há na internet diversos sites que tratam sobre segurança, como exemplo, cito o www.cert.br e recomendo a leitura da cartilha de segurança. SOARES (s.d.) acrescenta que “outro fato importante e positivo é a preocupação dos fabricantes em disponibilizar correções para vulnerabilidades recentes.” E, por fim, PAIM (s.d.) apresenta outro problema “existe uma resistência por parte dos fabricantes em retirar o protocolo WEP dos pontos de acesso, o que faz com que ele continue sendo usado, causando vulnerabilidade em milhares, senão milhões, de redes espalhadas pelo mundo”.

3 Conclusão

Após analisarmos os padrões de encriptação/decriptação de mensagens por redes sem fio e o método do ataque por force brute, podemos deduzir que o tipo de ataque não pode ser eliminado em sua totalidade, entretanto, é possível evitá-lo.

Por conseguinte, cabe reforçar aos usuários a constante necessidade de mudança de senhas fortes, normalmente a cada 15 dias ou menos, dependendo da utilização da rede e da confidencialidade dos dados e boas práticas no quesito segurança. Além disso, utilizar o padrão de encriptação/decriptação WPA2.

Este trabalho ainda fica longe de ser conclusivo, entretanto para uma melhor análise estatística e dos padrões descritos, necessita de testes práticos mais elaborados.

Referências bibliográficas

DIORIO, Rafael Fernando *et al.*; **Ataques de Força Bruta: Um Estudo Prático**. Departamento de Informática. Instituto Federal de Educação, Ciência e Tecnologia de São Paulo (IFSP). Capivari – SP.

FERRAZ, João Henrique; TORRES, Claudines Taveira. **Análise e Teste de Vulnerabilidade do Protocolo SMTP (Correio Eletrônico)**. Curso de Tecnologia em Redes de Computadores - Faculdade de Tecnologia de Bauru. Bauru – SP

PAIM, Rodrigo R.; **WEP, WPA e EAP**. In: https://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2011_2/rodrigo_paim/downloads/trabalho.pdf. Acesso em 11/04/2020.

SOARES, Leonardo F.; MORAES, Igor M. **Uma avaliação de vulnerabilidades em protocolos de autenticação para redes sem fio IEEE 802.11**. Instituto de Computação – Universidade Federal Fluminense. Niterói – RJ

WRIGHTSON, Tyler. **Segurança de redes sem fio: guia do iniciante**. Porto Alegre, Bookman, 20