Quebra de senhas com aircrack-ng

Juan Felipe Serafim dos Santos

[1] Centro de Informática
Universidade Federal de Pernambuco (UFPE) – Recife, PE – Brazil

jfss@cin.ufpe.br

Resumo. *A quebra de senhas refere-se ao processo de descobrir ou decifrar senhas com o objetivo de obter acesso não autorizado a sistemas, contas ou dados protegidos, utilizando métodos diversos como: ataque de força bruta, ataque de dicionaŕio, interceptação do tráfego de rede, engenharia social, entre outras técnicas. No contexto de redes Wi-Fi, diz respeito ao processo de obtenção de acesso não autorizado a uma rede sem fio protegida por senha. Essa prática pode ser realizada de várias formas, dependendo da complexidade da senha, do sistema de autenticação adotado, do nível de proteção implementado ou se o alvo detém alguma vulnerabilidade inerente.*

1. Objetivo

Nessa atividade, iremos utilizar o software aircrack-ng para invadir uma rede WEP. As redes WEP, sigla para *Wired Equivalent Privacy*, foi uma das primeiras medidas de segurança em acessos à redes *wireless*. Com o passar do tempo, vulnerabilidades foram detectadas e exploradas em seu algoritmo de encriptação, de tal forma que a segurança de rede foi completamente extinguida.

2. Como a ferramenta funciona

De acordo com a documentação do aircrack: “O Aircrack-ng pode recuperar a chave WEP assim que pacotes criptografados suficientes forem capturados com o airodump-ng. Esta parte do pacote aircrack-ng determina a chave WEP usando dois métodos fundamentais. O primeiro método é por meio da abordagem PTW (Pyshkin, Tews, Weinmann).

[...] O outro método, mais antigo, é o FMS/KoreK. O método FMS/KoreK incorpora vários ataques estatísticos para descobrir a chave WEP e os utiliza em combinação com força bruta. Ele requer mais pacotes que o PTW, mas, por outro lado, é capaz de recuperar a senha quando o PTW às vezes falha.”

Então, vamos utilizar o pacote de ferramentas aircrack-ng. A tela inicial dele mostra um pouco dos parâmetros que serão utilizados.

Figura 1. Tela de ajuda do aircrack-ng

Para o objetivo da quebra de senha, será necessário capturar uma quantidade considerável de pacotes que trafegarão entre o ponto de acesso e um determinado dispositivo final. Ainda assim, caso nenhum dispositivo esteja conectado a rede, é possível forçar um tráfego de pacotes entre o ponto de acesso e a máquina atacante, para assim capturar os pacotes necessários.

Para armazenar os pacotes, utilizaremos a ferramenta airodump, incluída no pacote aircrack-ng.

Figura 2. Tela de ajuda do airodump-ng

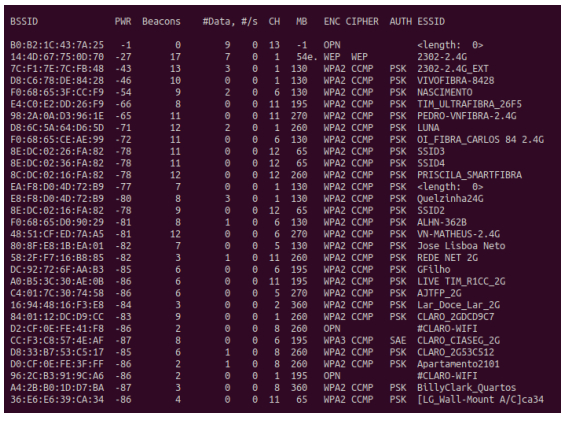

Figura 3. Funcionamento do airodump-ng

A configuração atual da rede vulnerável é a seguinte:

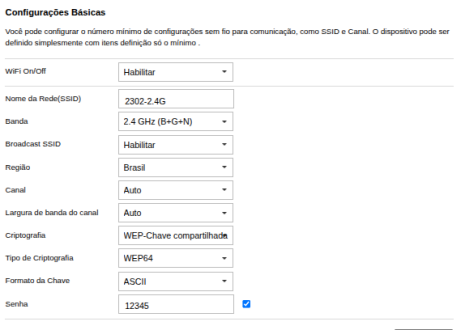

Figura 4. Parâmetros da rede Wi-Fi a ser atacada

Será feita a captura de pacotes da rede vulnerável via airodump-ng com os seguintes parâmetros: –channel 1 –ivs –bssid 14:4D:67:75:0D:70 -w wep wlp1s0mon

Onde:

- channel: número do canal em que a rede vulnerável se encontra.
- bssid: endereço MAC da rede alvo
- w: escrever em um arquivo
- ivs: flag para indicar que seja salvo no arquivo somente os *Vetores de inicialização*

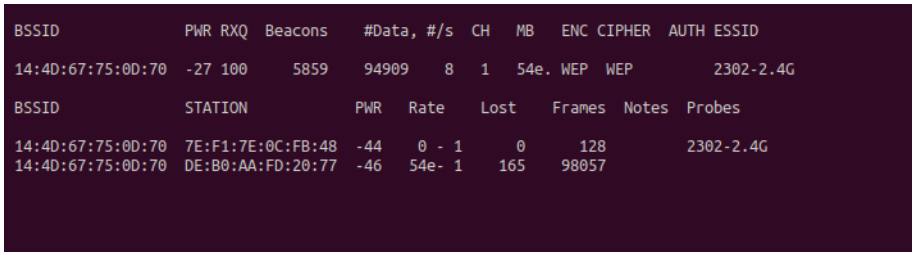

Figura 5. Capturando pacotes da rede Wi-Fi a ser atacada

Nesse momento, os IVs estão sendo salvos no armazenamento interno do dispositivo atacante e, enquanto o armazenamento ocorre, é possível verificar se, com a quantidade de IVs disponíveis, qual valor da senha da rede Wi-Fi.

Executando o aircrack com os parâmetros -b 14:4D:67:75:0D:70 wep-01.ivs Onde:

- b: BSSID da rede alvo.
- wep-01.ivs: arquivo com os vetores de inicialização.

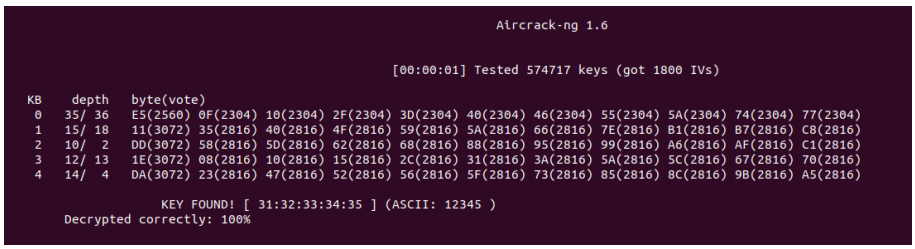

Figura 6. Ataque concluído e recuperação completa de senha

3. Análise da vulnerabilidade

A vulnerabilidade das redes WEP é principalmente relacionada ao seu algoritmo de encriptação, o RC4. A segurança da rede utiliza a cifra citada anteriormente, combinado com uma chave estática (de 40 ou 104 bits) e um vetor de inicialização (IV) de apenas 24 bits. O problema é que o tamanho reduzido do IV faz com que ele se repita rapidamente, especialmente em redes com muito tráfego. Como o IV é transmitido em *plaintext* nos pacotes, um atacante pode capturar milhares ou milhões de pacotes para analisar os padrões de repetição dos IVs com os métodos FMS e/ou PTW.

4. Sugestão de defesa

Alterar imediatamente o protocolo de encriptação da rede para um dos mais recentes como o WPA2 e WPA3. Tais cifras tem procedimentos distintos aos da rede WEP e (ainda) não foram descobertas vulnerabilidades latentes.

Referências

(2019). Documentação aircrack-ng. https://www.aircrack-ng.org/doku.php?id=aircrack-ng.

Erik Tews, A. P. and Weinmann, R.-P. (2007). aircrack-ptw. https://web.archive.org/web/20070714194826/http://www.cdc.informatik.tu-darmstadt.de/aircrack-ptw/.

Stubblefield, A. Ioannidis, J. e. R. A. (2001). Using the fluhrer, mantin, and shamir attack to break wep. https://download.aircrack-ng.org/wiki-files/doc/using_FMS_attack.pdf.