Vulnerabilidades em redes sem fio

Ataques à criptografia do padrão IEEE 802.11, Explorando o WEP, WPA/WPA2, WPS ataques de deauth e exploits de roteadores.

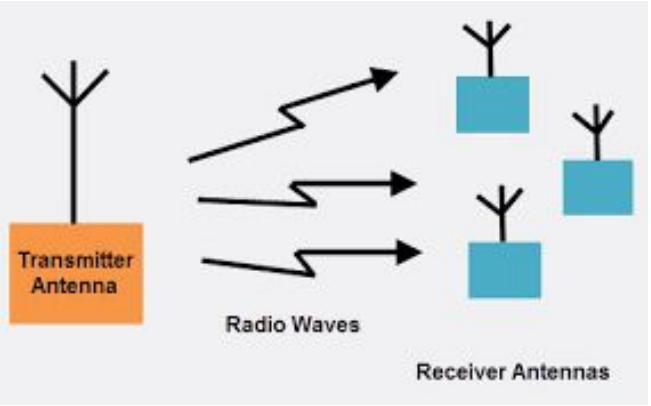
Vitor de Oliveira Fernandez Araujo

José Luiz Negreira Castro de Oliveira

GRIS - DCC/UFRJ

Como uma rede sem fio funciona?

Comunicação através de ondas eletromagnéticas omnidirecionais, em frequências pré-determinadas (conhecidas como canais)

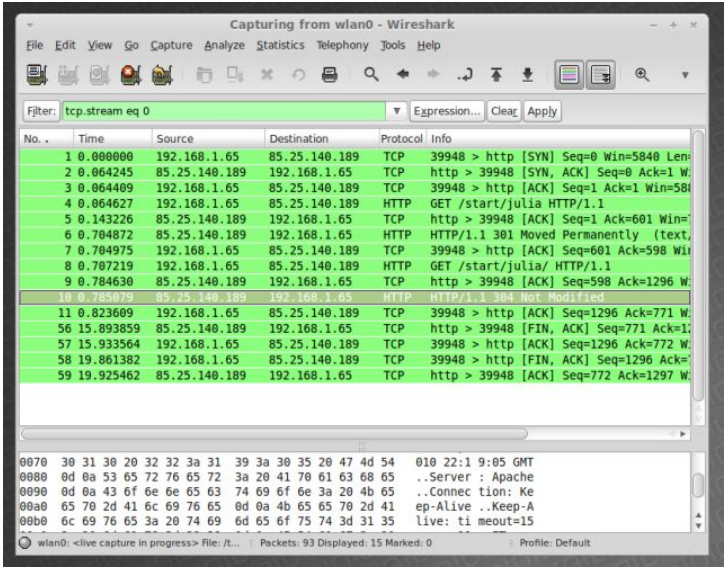


Problemas

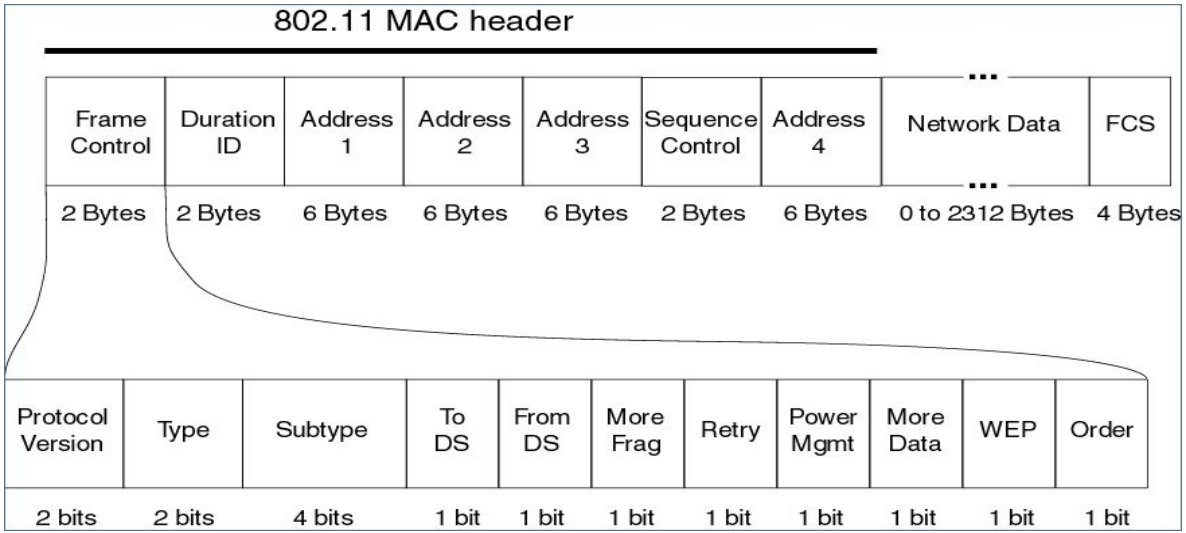
- Dispositivos com antenas que operem no padrão 802.11 podem “ver” os dados trafegando pelo ar;
- Dispositivos podem se passar uns pelos outros, manipulando cabeçalhos de dados;

Modos de placas de rede do 802.11 & Sniffing

- Managed
- Promiscuous
- Monitor



Estrutura de Cabeçalho

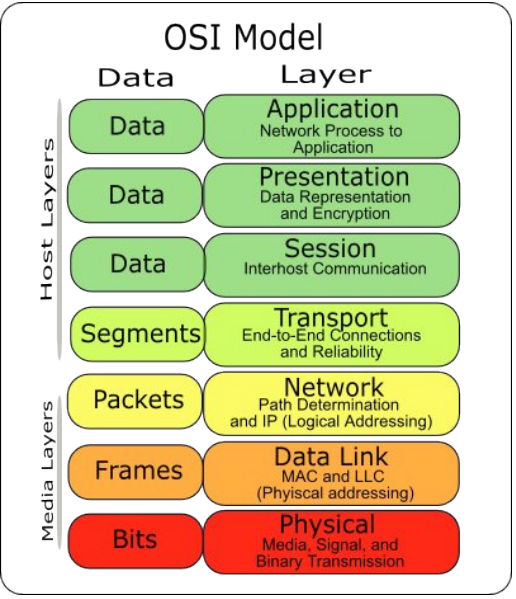


Segurança da Informação

No contexto de Segurança da Informação, gostaríamos de manter 3 propriedades básicas em nosso sistema:

- Confidencialidade
- Integridade
- Disponibilidade

DOS – negação de serviço



- Embaralhadores de sinal (Jammers)
- Funcionam via emissão de onda (camada 1)

- Ataques de Desautenticação
- Operam dentro do Protocol de Ethernet (camada 2)
- “Injetam” Management Frames forjados na rede alvo

Dos – Management Frames

- unidade de dados da camada de enlace
- Podem ser:

1. Beacon
2. Probe Request
3. Probe Response
4. Association request
5. Association response
6. Authentication
7. Deauthentication

- Problema, esses quadros não sao criptografados.

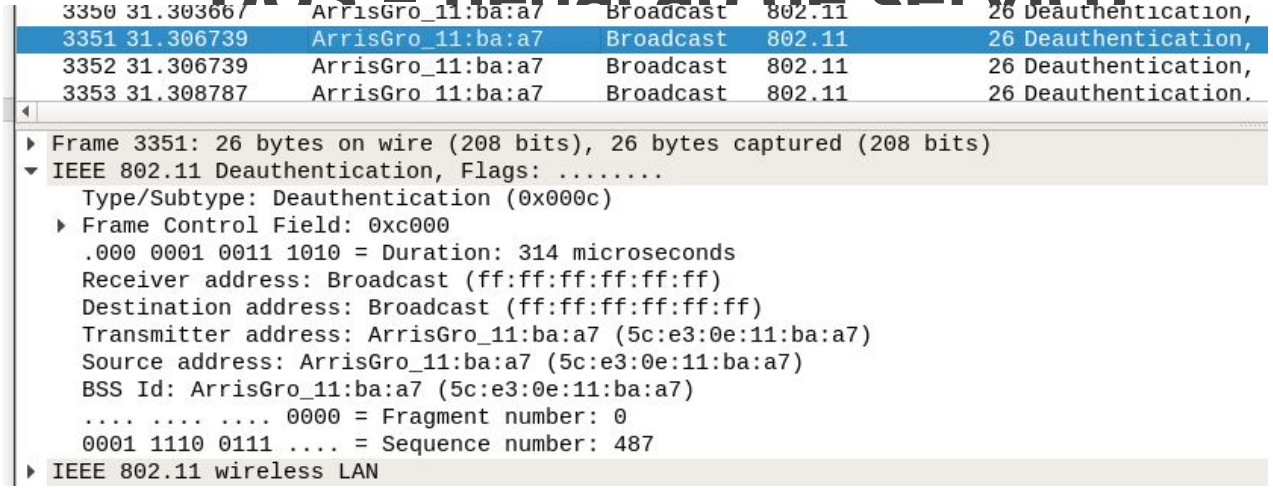
DOS exemplo pratico:

- Entrem nessa rede

SSID: EuUsoWep

Senha: Gris2018

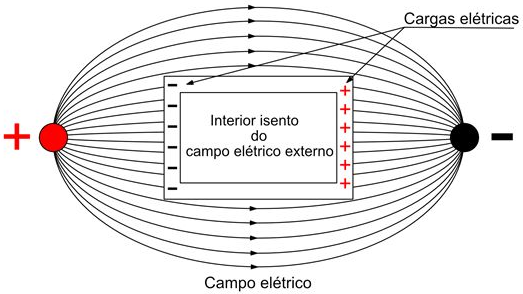
DOS – negação de serviço



- # aireplay-ng --deauth 0 –a BSSID <iface>
- O Quadro todo é forjado.
- Como Evitar?
- Como descobrir quem foi?

DOS – Soluções

- É preciso q o atacante não tenha acesso ao MAC do seu Roteador ou não possa transmitir pra ele.
- Opção 1: Por todos os seus dispositivos dentro de uma gaiola de faraday.
- Opção 2: Mudar o roteador de lugar, talvez pro centro da residencia
- Opção 3: Mudar de 2,4 para 5ghz
- Opção 3: Chamar a polícia. Talvez Com uma antenna direcional ou um sistema de triangulação seja possivel estimar de onde vem o ataque
- Opção 4: Frame Management Protection - 802.11W.



Como proteger?

Podemos ocultar, através de criptografia, os dados que vão trafegar entre os dispositivos e o ponto de acesso (AP).

Até os dias de hoje, 3 padrões de criptografia foram implementados no 802.11:

- WEP
- WPA
- WPA2

WEP (Wired Equivalent Privacy)

Definido junto com o padrão 802.11 em 1999, o WEP foi o primeiro e mais simples mecanismo de proteção aplicado à comunicação por Wi-Fi. É considerado ultrapassado pelo IEEE desde 2004, tendo inúmeros ataques conhecidos que quebram sua segurança.

- Oferece criptografia e compressão
- Opera com chaves compartilhadas de 40 ou 104 bits
- Utiliza o algoritmo criptográfico RC4
- Implementa controle de integridade através do algoritmo CRC-32

WEP (Wired Equivalent Privacy)

Tem dois modos de autenticação:

- Open System Authentication
- Shared Key Authentication

WEP - Open System Authentication

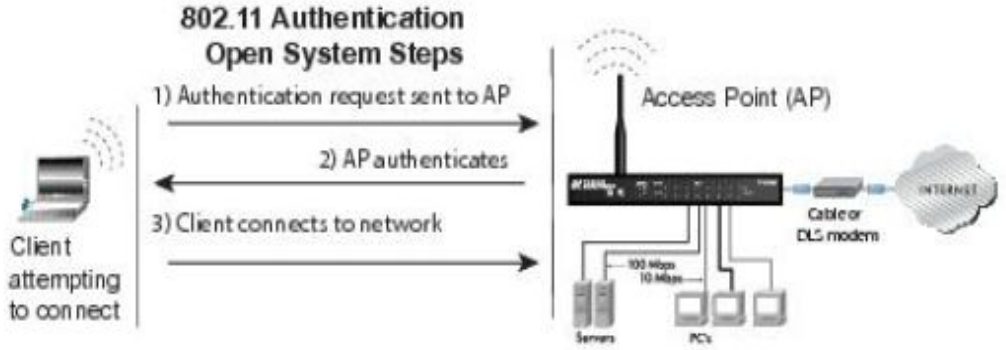
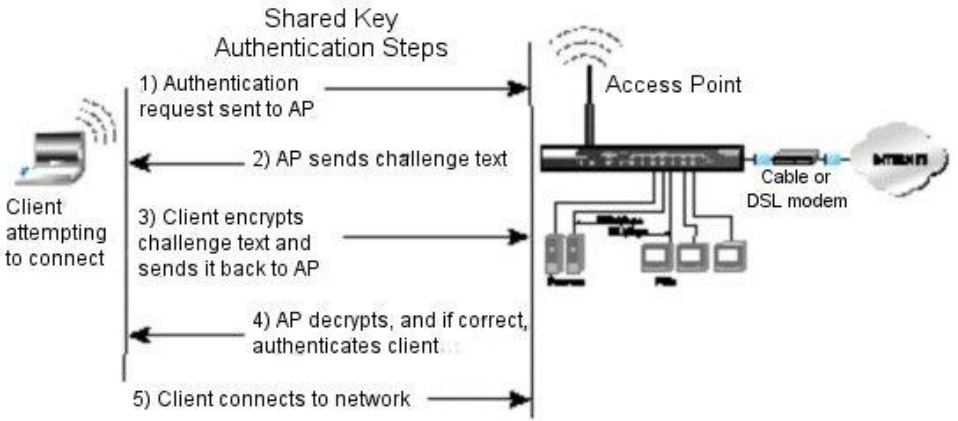


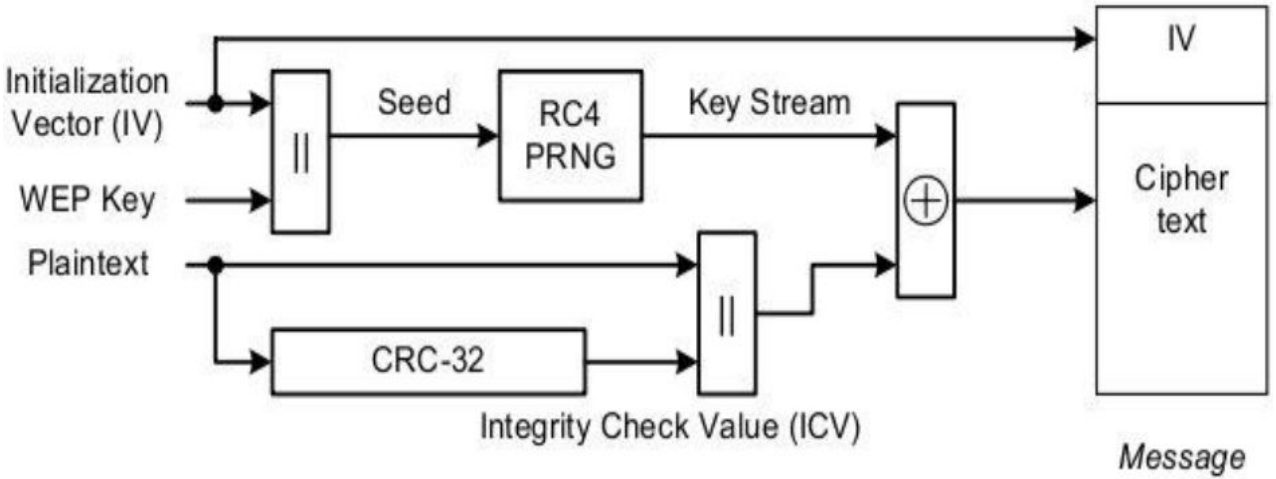
Figure 5-Open System Authentication Mode (Netgear, 2017)

WEP – Shared Key Authentication



Source: http://www.netgear.com/docs/refdocs/Wireless/wirelessBasics.htm

WEP (Wired Equivalent



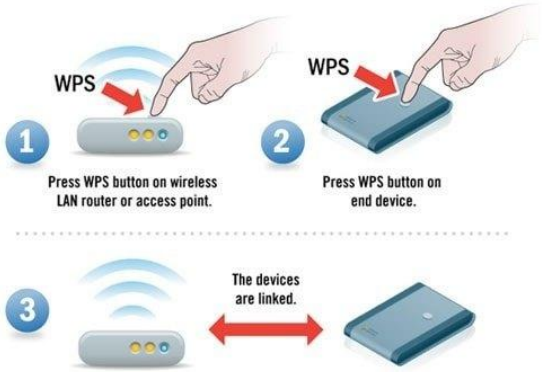
WEP - Problemas

- Chave estática e muito pequena (40 bits ou 104 bits);
- Parte aleatória (IV) da chave RC4 não é grande o suficiente para evitar repetições, além de ser transmitida sempre em texto claro;
- Quando no modo Shared Key Authentication, é possível gerar tráfego “falso” para coletar dados e descobrir a chave;
- CRC-32 é um algoritmo útil apenas para detecção de erros, não de alterações maliciosas.

WPA - Wi-Fi Protected Access

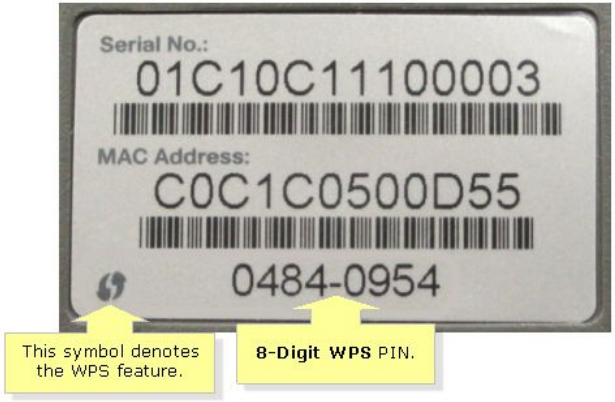
Introduzido em 2003 junto com um *draft* da revisão 802.11i, como uma resposta às diversas vulnerabilidades que vinham sendo encontradas no WEP.

WPS



- O que é?
- Para que serve?

WPS



- O que é um Pin wps:

7123 123 1

Parte 1 Parte2 checkSum

- Modos de Acesso.

1. Pin
2. Pin de outro dispositivo
3. PushButton

WPS

- Enrolee
- Registrar
- Necessidade de um protocol de autenticação mútua

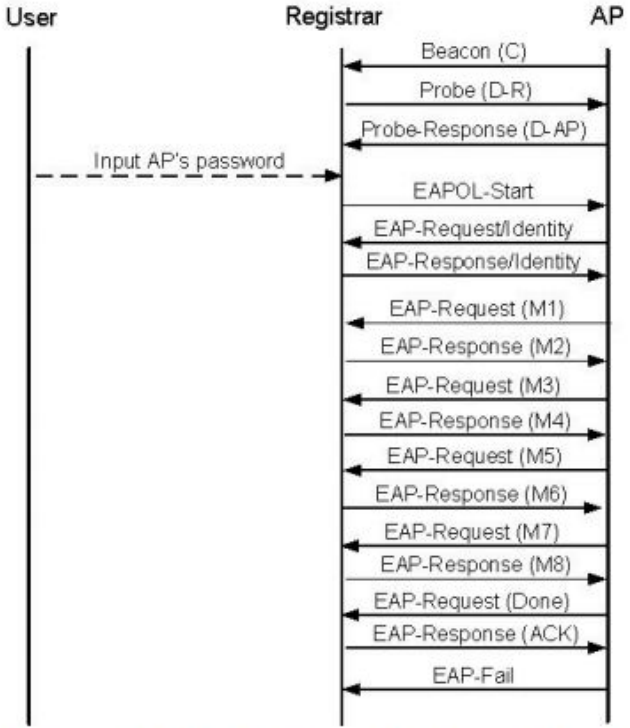


Figure 2: EAP-based Setup of an External Registrar

WPS - vunerabilidades

- “Pins Secretos”
- Brute Force = 11000 combinaçoes
- PixieDust:

```
def random( ):
    return 0;
```

IEEE 802.11/EAP Expanded Type, Vendor ID: WFA (0x372A), Vendor Type: SimpleConfig (0x01)			
M1	Enrollee → Registrar	N1 || Description || PK_E	Diffie-Hellman Key Exchange
M2	Enrollee ← Registrar	N1 || N2 || Description || PK_R || Authenticator	
M3	Enrollee → Registrar	N2 || E-Hash1 || E-Hash2 || Authenticator	
M4	Enrollee ← Registrar	N1 || R-Hash1 || R-Hash2 || $E_{KevWrapKev}$(R-S1) || Authenticator	proove posession of 1st half of PIN
M5	Enrollee → Registrar	N2 || $E_{KeyWrapKey}$(E-S1) || Authenticator	proove posession of 1st half of PIN
M6	Enrollee ← Registrar	N1 || $E_{KeyWrapKey}$(R-S2) || Authenticator	proove posession of 2nd half of PIN
M7	Enrollee → Registrar	N2 || $E_{KeyWrapKey}$(E-S2 ||ConfigData) || Authenticator	proove posession of 2nd half of PIN, send AP configuration
M8	Enrollee ← Registrar	N1 || $E_{KeyWrapKey}$(ConfigData) || Authenticator	set AP configuration

Enrollee = AP
Registrar = Supplicant = Client/Attacker

PK_E = Diffie-Hellman Public Key Enrollee
PK_R = Diffie-Hellman Public Key Registrar
Authkey and KeyWrapKey are derived from the Diffie-Hellman shared key.

Authenticator = $HMAC_{Authkey}$(last message || current message)

$E_{KeyWrapKey}$ = Stuff encrypted with KeyWrapKey (AES-CBC)

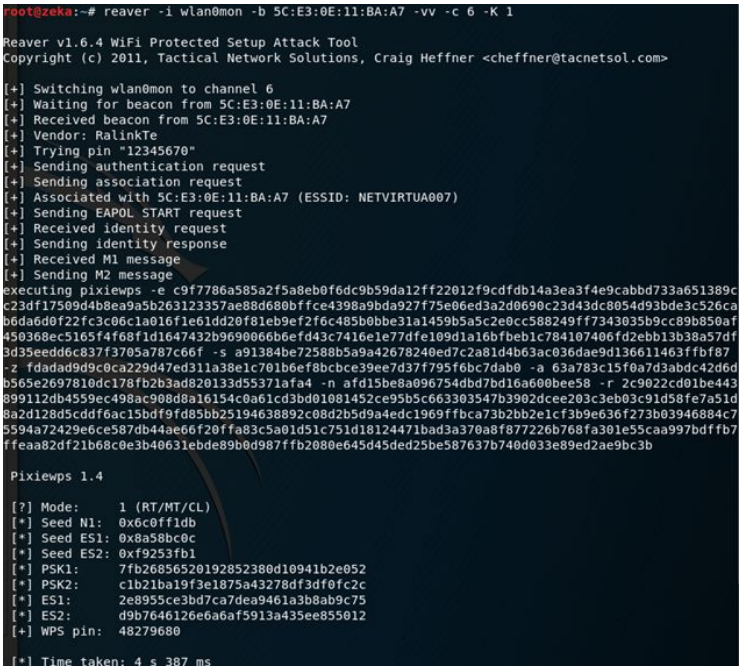
PSK1 = first 128 bits of $HMAC_{AuthKey}$(1st half of PIN)
PSK2 = first 128 bits of $HMAC_{AuthKey}$(2nd half of PIN)

E-S1 = 128 random bits
E-S2 = 128 random bits
E-Hash1 = $HMAC_{AuthKey}$(E-S1 || PSK1 || PK_E || PK_R)
E-Hash2 = $HMAC_{AuthKey}$(E-S2 || PSK2 || PK_E || PK_R)

R-S1 = 128 random bits
R-S2 = 128 random bits
R-Hash1 = $HMAC_{AuthKey}$(R-S1 || PSK1 || PK_E || PK_R)
R-Hash2 = $HMAC_{AuthKey}$(R-S2 || PSK2 || PK_E || PK_R)

1	2	3	4	5	6	7	0
1st half of PIN				2nd half of PIN			checksum

WPS-problemas de implementação



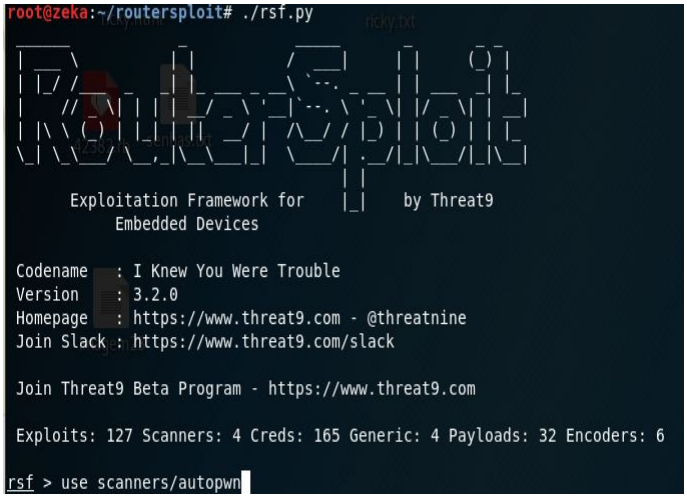
- Em aparelhos da Broadcom por exemplo, os dois nounces são gerados um após o outro, tal que E-S1=E-S2 e eles são gerados pelo mesmo PRNG que gera N1, que é enviado plano no inicio da conversa.
- A Realtek em alguns de seus modelos, utiliza E-S1=E-S2 = nounce gerado pela seed tempo

Srand(time(NULL));

- Em Alguns modelos da ralink E-S1=E-S2=0
- Pins Secretos
- Ataque:

#Reaver –I <iface> -b <Bssid> -c <canal> -K 1

ROUTERSPLOIT- metasploit para roteadores



- Ok, uma vez que temos acesso à rede, o que fazer agora?
- É a mesma interface do metasploit, porem com uma boa database de Vunerabilidades para roteadores que variam desde serviços com senhas padrão à vunerabilidades web nas paginas de login.