Wireless - Como driblar a segurança!

2007-08-13 16:10:41

Todos temos lido, visto e ouvido muita “propaganda” sobre insegurança nas redes Wireless. Quem não teve já contacto com redes desprotegidas? E os que se protegem sabem se estão seguros dessa forma?

É um “clichê” dizer que “nada é 100% seguro”, é verdade, nada é 100% seguro. Estou mesmo convencido que se alguém com certos e determinados conhecimentos se aplicar a explorar vulnerabilidades na segurança do Wireless, conseguirá frutos em quantidade industrial.

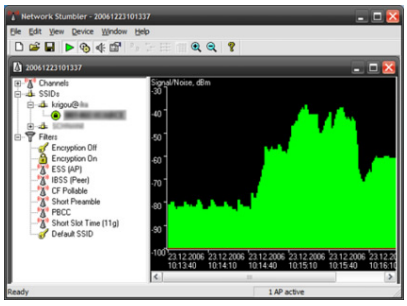
Quem estiver mal intencionado pode, com as ferramentas certas, descobrir redes desprotegidas e de alguma forma prejudicar quem se sente seguro por trás do seu PC ligado ao mundo da Internet.

Felizmente ou infelizmente a Internet é um berço para estas ferramentas gratuita, ferramentas que nos fornecem dados importantes sobre redes Wireless, neste caso deveremos usar esta mala de ferramentas para testar a nossa própria segurança.

Descobrir Redes Wireless

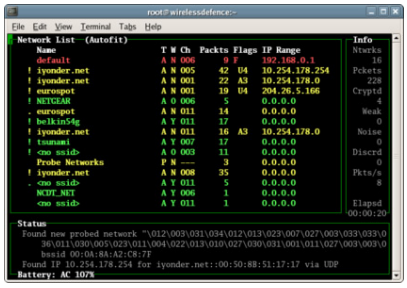
Localizar a rede Wireless é o primeiro passo para explorar, existem para esse fim duas ferramentas que serão certamente do vosso conhecimento:

Network Stumbler a.k.a NetStumbler – Esta ferramenta para o Windows facilmente encontra o sinal Wireless difundido das redondezas, é uma fantástica aplicação. Uso-a para em casos de dificuldade de captação de sinal determinar a força e o ruído existente no sinal enviado. existem empresas que para instalar os seus hotspots recorrem a esta aplicação determinando com mais exactidão as características do terreno envolvente tendo em conta a qualidade do sinal difundido.



Licença: Freeware | Download: NetStumbler 0.4.0 [1.26MB]

Kismet - Esta ferramenta vem completar a ferramenta apresentada anteriormente o NetStumbler, pois este não consegue detectar as redes Wireless que escondem o SSID. Portanto esta ferramenta além de detectar as redes difundidas de forma visível, consegue identificar quais as que estão camufladas, podendo mesmo identificar tentativas de acesso ao seu ponto Wireless.



Licença: Freeware | Download: Kismet 2007-01-R1b [4.58MB]

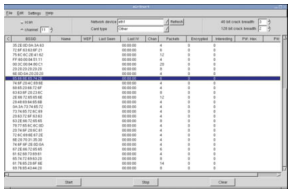
Anexar ligação às redes descobertas

Agora que descobriu as redes Wireless passe para o nível seguinte, ligar-se a essas redes.

Se a(s) rede(s) não está a usar qualquer tipo de autenticação ou encriptação de segurança então pode simplesmente ligar-se ao SSID. Se o SSID não está a ser difundido o utilizador pode criar um perfil com o nome do SSID pois esse nome não estará a ser difundido, mas claro que o utilizador já o sabe pois usou o Kismet, certo? Mas e se a rede wireless solicitar autenticação? Bem nesse caso teremos que passar para um nível mais a cima nesta pirâmide de recursos.

Airsnort – Bem esta é a ferramenta que irá "cheirar" e quebrar a protecção das chaves WEP que normalmente usamos para "proteger" as nossas ligações. É muito simples de usar. Temos já referido aqui no Peopleware em artigos anteriores dedicados às protecções Wireless que a chave WEP é muito fraca, com este tipo de aplicações usar uma chave WEP é o mesmo que não usar nada.

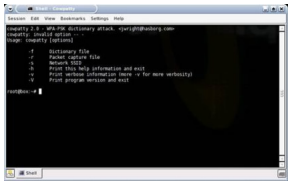
Ao usar esta ferramenta descobrirá formas e estratégias para mais rapidamente descobrir as chaves WEP, ferramentas adicionais podem melhorar a técnica e simplificar o processo, essas ferramentas não estão anexas ao Airsnort. O processo não é rápido o que descobrir as chaves, serão precisas várias tentativas a cheirar os pacotes de chaves para "crackar" as chave WEP, mas descobri que até se consegue.



Licença: Open Source | Download: AirSnort 0.2.7e [4.81MB]

CowPatty – Pois é, mas o que descobriu tinha protecção WPA e agora? Agora pode usar o CowPatty, esta aplicação é usada para despoletar acções de arrombamento a chamada "brute force" para crackar WPA-PSK. Esta chave tem sido incentivada aos utilizadores como sendo a nova segurança WEP para segurança Wireless caseiras. O que faz esta aplicação? Simplesmente descarrega uns milhares de

combinações alfanuméricas de um ficheiro dicionário tentando que umas usadas coincida e permita a autenticação



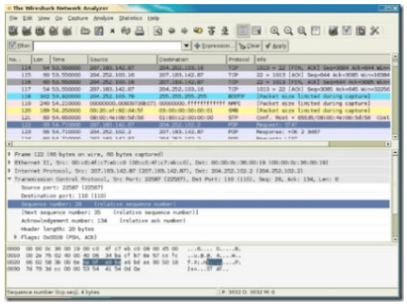
Licença: Open Source | CowPatty 2.0 [921KB]

Sniffing de dados da rede Wireless

Quer esteja directamente ligado a uma rede Wireless ou não existindo num raio de captação pacotes de dados a “voar” de um lado para o outro o utilizador poderá “vê-los” para isso precisa de uma ferramenta.

Wireshark (formerly Ethereal) – Com um sniffer, podemos monitorizar o acesso a determinados serviços de rede como por exemplo e-mail, acesso remoto (telnet, rlogin), transferência de ficheiros (FTP), etc. Permite-nos ainda identificar a existência de tráfego anormal na nossa rede. Um exemplo vulgar, é alguém mal intencionado andar pela nossa rede à procura de dados, como por exemplo passwords, para mais tarde poder usar. Imaginem que os dados que passam na nossa rede não estão encriptados? Óptimo para o hacker !!!

Os mais conhecidos para sistemas Linux são o tcpdump, ethereal. Para Windows também existe o ethereal, ou winshark que foi concebido pelos mesmos autores do ethereal. Se fizerem uma pesquisa no Google irão encontrar muitas referências a sniffers. Aqui têm uma lista com alguns deles. O processo de “sniffing” está associado a uma ou mais interfaces de rede de um determinado computador.



Licença: Freeware | Download: Wireshark 0.99.6a [17.47MB]

Como nos podemos defender?

É importante saber para que servem e como se usam estas ferramentas, este meu pequeno guia apenas tem como objectivo alertar para o que podem encontrar à disposição de pessoas mal intencionadas.
NetStumbler – Nunca permita que o seu router difunda o seu SSID. Assegure-se que a sua rede está protegida usando autenticações e encriptações avançadas.

Kismet – Aqui realmente não há muito a fazer, ele descobrirá a vossa rede, no entanto esta deverá estar protegida com as tais autenticações e encriptações avançadas existentes nos vossos routers. Se não conseguírdes fazer essas protecções o vosso ISP tem à disposição técnicos que vos podem ajudar a configurar o router.

Airsnort – Usem uma chave de encriptação a 128-bit, pois se usarem a mais baixa a 40-bit WEP de nada podeis fazer contra esta ferramenta. Não quer dizer que a chave a 128 bits não possa ser quebrada, demora é muito mais tempo que pode demover o hacker. Para estar seguro use chaves de encriptação WPA ou WPA2.

Cowpatty – Conta esta ferramenta somente o protelar para descobrir a chave WPA, para isso ude chaves longas e complexas. Quanto mais complexa for mais dificuldade cria a quem usar esta ferramenta para invadir a sua rede.

Winshark – Use encriptação, assim quem “cheirar” a sua rede terá de enfrentar uma possibilidade ínfima de conseguir recuperar quaisquer dados.

WPA2 usa encriptação de dados AES, podemos dizer que é irrisória a possibilidade de um hacker quebrar esta cifra. Mesmo o protocolo WEP poderá encriptar os dados. Quando se encontrar num hotspot publico que geralmente não oferecem protecção para dados use aplicações de terceiros para encriptar os seus dados, mesmo se usar o messenger e derivados. Para empresas a solução é usar VPN e aplicações de terceiros para proteger os dados encriptando-os.

Penso que já sabem um pouco mais sobre este assunto, caso tenha mais informação que possa completar a que aqui deixamos use os comentários para abrir novas linhas de conhecimento.