ACME!
Computer Security Research

Redes sem Fio: Solução ou Ameaça?

Luiz Otávio Duarte
ACME! Researcher

Marcelo Carvalho Sacchetin
ACME! Researcher

Prof. Dr. Adriano Mauro Cansian
ACME! Coordinator

Maio – 2003

Contato:

Luiz Otávio Duarte
ACME! – Computer Security Research
lod@acmesecurity.org

Marcelo Carvalho Sacchetin
ACME! – Computer Security Research
sacchet@acmesecurity.org

Adriano Mauro Cansian
ACME! - Coordinator
adriano@acmesecurity.org / adriano@unesp.br

UNESP - Universidade Estadual Paulista
Campus de São José do Rio Preto

Depto. de Ciência da Computação e Estatística
Laboratório ACME! de Pesquisa em Segurança de Computadores e Redes

Endereço:
R. Cristóvão Colombo, 2265 - Jd. Nazareth
15055-000 * São José do Rio Preto, SP.
Tel. (17) 221-2475 (laboratório) / 221-2201 (secretaria)
http://www.acmesecurity.org/

Prefácio

Este material é uma coleção dos *slides* da palestra **"Rede sem Fio: Solução ou Ameaça?",** ministrado a convite da comissão organizadora do II Encontro de Evangelização e Informática, promovido pela CNBB – Confederação Nacional dos Bispos do Brasil (Regional Sul 1) realizado na Faculdade e Colégio Claretianos, na cidade de Rio Claro - SP, de 16 a 18 de maio de 2003.

A principal função destes *slides* e notas de aula é facilitar a realização das anotações dos tópicos mais importantes discutidos durante a apresentação. Sugestões e apontamentos de falhas podem ser enviadas diretamente aos autores, em lod@acmesecurity.org ou sacchet@acmesecurity.org. A versão revisada destas notas de aula, e outros eventuais materiais complementares, estão disponíveis em **http://www.acmesecurity.org/cnbb2003**

São José do Rio Preto, 06 de maio de 2003.

Luiz Otávio Duarte

Marcelo Carvalho Sacchetin

ACME! STANDARD DISCLAIMER

Please, read carefully.

This ACME! product is meant for educational purposes only. Any resemblance to real persons, living or dead is purely coincidental. Void where prohibited. Some assembly required. List each check separately by bank number. Batteries not included. Contents may settle during shipment. Use only as directed. No other warranty expressed or implied. Do not use ACME! while operating a motor vehicle or heavy equipment. Postage will be paid by addressee. Subject to CAB approval. This is not an offer to sell securities. Apply only to affected area. ACME! may be too intense for some viewers. Do not stamp. Use other side for additional listings. For recreational use only. Do not disturb. All models over 18 years of age. If condition persists, consult your physician. No user-serviceable parts inside. Freshest if eaten before date on carton. Subject to change without notice. Times approximate. Simulated picture. No postage necessary if mailed in the United States. Breaking seal constitutes acceptance of agreement. For off-road use only. As seen on TV. One size fits all. Many suitcases look alike. Contains a substantial amount of non-tobacco ingredients. Colors may, in time, fade. We have sent the forms which seem right for you. Slippery when wet. For office use only. ACME! Research is not affiliated with the American Red Cross. Drop in any mailbox. Edited for television. Keep cool. process promptly. Post office will not deliver without postage. List was current at time of printing. Return to sender, no forwarding order on file, unable to forward. ACME! is not responsible for direct, indirect, incidental or consequential damages resulting from any defect, error or failure to perform. At participating locations only. Not the Beatles. Penalty for private use. See label for sequence. Substantial penalty for early withdrawal. Do not write below this line. Falling rock. Lost ticket pays maximum rate. Your canceled check is your receipt. Add toner. Place stamp here. Avoid contact with skin. Sanitized for your protection. Be sure each item is properly endorsed. Sign here without admitting guilt. Slightly higher west of the Mississippi. Employees and their families are not eligible. Beware of dog. Contestants have been briefed on some questions before the show. Limited time offer, call now to ensure prompt delivery. You must be present to win. No passes accepted for this engagement. No purchase ecessary. Processed at location stamped in code at top of carton. Shading within a garment may occur. Use only in a well-ventilated are. Keep ACME! away from fire or flames. Replace with same type. Approved for veterans. Booths for two or more. Check here if tax deductible. Some equipment shown is optional. Price does not include taxes. No Canadian coins. Not recommended for children. Prerecorded for this time zone. Reproduction strictly prohibited. No solicitors. No alcohol, dogs or horses. No anchovies unless otherwise specified. Restaurant package, not for resale. List at least two alternate dates. First pull up, then pull down. Call ACME! toll free before digging. Driver does not carry cash. Some of the trademarks mentioned in this product appear for identification purposes only. Record additional transactions on back of previous stub. Unix is a registered trademark of AT&T. Do not fold, spindle or mutilate. No transfers issued until the bus comes to a complete stop. Package sold by weight, not volume. Your mileage may vary. This article does not reflect the thoughts or opinions of either myself, my company, my friends, or my cat. Don't quote me on that. Don't quote me on anything. All rights reserved. You may distribute this article freely but you may not take a profit from it. Terms are subject to change without notice. Illustrations are slightly enlarged to show detail. Any resemblance to actual persons, living or dead, is unintentional and purely coincidental. Do not remove this disclaimer under penalty of law. Hand wash only, tumble dry on low heat. Do not bend, fold, mutilate, or spindle. No substitutions allowed. For a limited time only. This ACME! article is void where prohibited, taxed, or otherwise restricted. Caveat emptor. Article is provided "as is" without any warranties. Reader assumes full responsibility. An equal opportunity article. No shoes, no shirt, no articles. Quantities are limited while supplies last. If any defects are discovered, do not attempt to read them yourself, but return to an authorized service center. Read at your own risk. Parental advisory - explicit lyrics. Text may contain explicit materials some readers may find objectionable, parental guidance is advised. Keep away from sunlight. Keep away from pets and small children. Limit one-per-family please. No money down. No purchase necessary. You need not be present to win. Some assembly required. Batteries not included. Instructions are included. Action figures sold separately. No preservatives added. Slippery when wet. Safety goggles may be required during use. Sealed for your protection, do not read if safety seal is broken. Call before you dig. Not liable for damages arising from use or misuse. For external use only. If rash, irritation, redness, or swelling develops, discontinue reading. Read only with proper ventilation. Avoid extreme temperatures and store in a cool dry place. Keep away from open flames. Avoid contact with eyes and skin and avoid inhaling fumes. Do not puncture, incinerate, or store above 120 degrees Fahrenheit. Do not place near a flammable or magnetic source. Smoking this article could be hazardous to your health. The best safeguard, second only to abstinence, is the use of a condom. No salt, MSG, artificial color or flavoring added. If ingested, do not induce vomiting, and if symptoms persist,consult a physician. Warning: Pregnant women, the elderly, and children should avoid prolonged exposure to ACME! Caution: ACME! may suddenly accelerate to dangerous speeds. ACME! contains a liquid core, which if exposed due to rupture should not be touched, inhaled, or looked at. Do not use ACME! on concrete. Discontinute use of ACME! if any of the following occurs: Itching, Vertigo, Dizziness, Tingling in extremities, Loss of balance or coordination, Slurred speech, Temporary blindness, Profuse Sweating, or Heart palpitations. If ACME! begins to smoke, get away immediately. Seek shelter and cover head. ACME! may stick to certain types of skin. When not in use, ACME! should be returned to its special container and kept under refrigeration. Failure to do so relieves the makers of ACME! , ACME! Products Incorporated, and it's parent company, ACME! Chemical Unlimited, of any and all liability. Ingredients of ACME! include an unknown glowing substance which fell to Earth, presumably from outer space. ACME! has been shipped to troops in Saudi Arabia and is also being dropped by warplanes on Iraq. Do not taunt ACME! May cause any of the aforementioned effects and/or death. Articles are ribbed for your pleasure. Possible penalties for early withdrawal. Offer valid only at participating sites. Slightly higher west of the Rockies. Allow four to six weeks for delivery. Must be 18 to read. Disclaimer does not cover misuse, accident, lightning, flood, tornado, tsunami, volcanic eruption, earthquake, hurricanes and other Acts of God, neglect, damage from improper reading, incorrect line voltage, improper or unauthorized reading, broken antenna or marred cabinet, missing or altered serial numbers, electromagnetic radiation from nuclear blasts, sonic boom vibrations, customer adjustments that are not covered in this list, and incidents owing to an airplane crash, ship sinking or taking on water, motor vehicle crashing, dropping the item, falling rocks, leaky roof, broken glass, mud slides, forest fire, or projectile (which can include, put not be limited to, arrows, bullets, shot, BB's, shrapnel, lasers, napalm, torpedoes, or emissions of X-rays, Alpha, Beta and Gamma rays, knives, stones, etc.). ***Other restrictions may apply. This supersedes all previous notices. The ACME! Computer Security Research.***

"Nós trabalhamos no escuro. Fazemos o possível para combater o mal, que do contrário nos destruiria. Mas se o caráter de um homem é seu destino, a luta não é uma escolha, mas uma vocação."

Fox Mulder – *Grotesque*

II – Encontro de Evangelização e Informática
CNBB – Sul 1

Rio Claro - 2003

Rede sem fio: Solução ou Ameaça?!

Luiz Otávio Duarte
ACME! Researcher

Marcelo Carvalho Sacchetin
ACME! Researcher

Prof. Dr. Adriano Mauro Cansian
ACME! Coordinator

Redes sem fio, necessidade

- Nas últimas décadas as LANs sofreram um crescimento explosivo.
  - As LANs cabeadas se tornaram ingrediente indispensável para o mundo dos negócios.
- Surge uma indústria multi-bilionária para suprir a necessidade das LANs cabeadas
- Necessidades de redes sem fio:
  - Computadores pessoais;
  - Necessidade do homem de se manter em movimento;
  - Barateamento de equipamentos de tecnologia celular.
- Redes sem fio podem ser obtidas via rádio freqüência, IrDA ou laser.

LANs nas Empresas (1/2)

- LANs (Local Area Network) : presente na infra-estrutura interna das empresas;
- Crescimento acelerado lembra a internet no início dos anos 90;
- Indispensável para o funcionamento das empresas;
- Alto custo da infra-estrutura cabeada para interconectar pontos da rede;
- Solução: não usar cabos -> WLANs (Wireless Local Area Network) ;

LANs nas Empresas (2/2)

- WLANs são mais baratas e com desempenho comparável às redes cabeadas;
- Tecnologia spread spectrum nas WLANs por rádio frequência (RF) visando diminuir interferências;
- Assim como no início da internet: problemas com segurança devido à falta de preocupação efetiva por parte das empresas.

Desenvolvimento de redes wireless

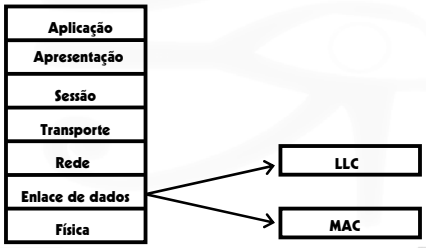
- A tecnologia wireless cresce ao longo dos anos
  - Crescimento devido ao ganho de performance dos semicontutores, o barateamento da tecnologia e também pela necessidade de maiores taxas de transferência, bem como, de bandas com poucos ruídos.
- As 4 gerações de produtos Wireless:
  - 1ª. Opera na banda ISM (Industrial Scientifc and Medical) que abrange de 902 a 928 MHz. Consegue taxas de 500 Kbps
  - 2ª. Opera na ISM que abrange de 2.40 a 2.48 GHz. Consegue taxas de 2 Mbps.
  - 3ª. Opera na ISM de 2.4 GHz. Conseguindo taxas de 11Mbps
  - 4ª. Opera na ISM que abrange de 5.775 a 5.850 GHz. Conseguindo 10 Mbps de início.

Padrões para redes sem fio

- **IEEE 802.11 – É o padrão utilizado para redes sem fio.**
  - Este padrão inclui suporte para WEP para proteger as mensagens trocadas entre os hosts.
- **IEEE 802.11b – É a terceira geração das redes wireless.**
  - Opera em 2.4 GHz provendo 11 Mbps. É o padrão mais utilizado também conhecido com o WiFi.
- **IEEE 802.1x – Processo de autenticação para IEEE 802.11.**
  - O processo de autenticação é feita criando chaves "dinâmicas" para o WEP.
- **IEEE 802.11g – Padrão com 54 Mbps em 2.4 GHz.**
  - Este, ganhou aprovação do grupo de trabalho da IEEE 802.11.

Ethernet X Wireless

- **Redes sem fio são compatíveis com redes cabeadas.**
  - Tipicamente as únicas mudanças para produtos wireless repousa sobre as duas primeiras camadas do modelo OSI. Mais especificamente na camada física e metade inferior da camada de enlace de dados, conhecida como MAC (Media Access Control)



Definições para redes sem fio

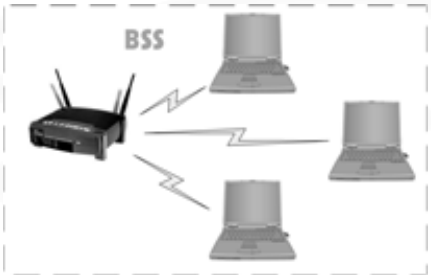
- **AP – Access Point.**
  - É um hub/bridge/switch/roteador que provê o controle na camada sem fio e provê o acesso à rede cabeada.
- **STA – Wireless Station.**
  - Qualquer estação de trabalho que possua dispositivo wireless.
- **WLAN – Wireless Local Area Network.**
  - Rede local de computadores interligados por uma infra-estrutura sem fio.
- **Modos de operação de uma rede sem fio:**
  - Independente;
  - Básicamente infra-estruturado;
  - Infra-estruturado.

Configurações de Redes Wireless (1/3)

- **Redes Independentes (Ad Hoc)**
  - São redes que possuem somente STAs que se comunicam mutuamente. Todas possuem o mesmo BSSID (identificador de BSS). O termo mais correto para redes Ad Hoc seria IBSS (Independent BSS).

Configurações de Redes Wireless (2/3)

- **Redes de Infra-estrutura básica (BSS)**
  - Um conjunto de STAs controlados por um AP. Toda conexão é realizada através deste AP. O termo mais correto para uma rede de infra-estrutura básica é BSS.



Configurações de Redes Wireless (3/3)

- **Rede infra-estruturada (ESS)**
  - Um número de BSSs conectadas com a finalidade de que as STAs aparentem estar em uma rede única. Este esquema é tecnicamente chamado de ESS (Extended Service Set)

Autenticação em redes sem fio

- Quando um cliente pretende entrar em uma rede sem fio específica ele precisa se autenticar.
- Esta autenticação pode ser feita de duas formas, na camada 2 ou na camada 3 do modelo OSI.
  - A autenticação e privacidade na camada 3 seria baseado em endereços IPs um exemplo comum seria o uso de Rede Privada Virtual (VPN – Virtual Privated Network) com servidores RADIUS.
- O padrão IEEE 802.11-1997, apenas define o WEP (Wired Equivalend Privacity) como opção de segurança, feita em camada 2.
- O grupo de trabalho do IEEE 802.11, bem como a aliança WiFi estudam formas de autenticação e privacidade alternativas ao WEP.

Configurações de autenticação de APs

- Quando se configura um AP, existem três formas de autenticação:
  - Open Authentication (Autenticação Aberta) – Qualquer estação wireless pode se associar ao access point e obter acesso a rede.
  - Shared Authentication (Autenticação Compartilhada) – Onde chaves WEP são previamente compartilhadas. Estas são utilizadas para autenticar uma estação wireless a um access point.
  - Network-EAP – Baseado em algoritmos EAP (Extensible Authorization Protocol) que rodam sobre o padrão IEEE-802.1x

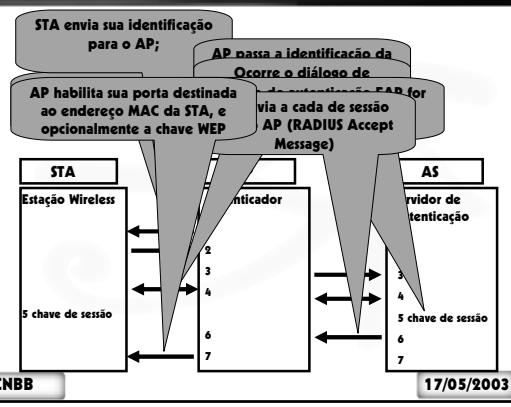
WEP (Wired Equivalent Privacity)

- Nas redes IEEE 802.11b o tráfego é criptografado utilizando-se o WEP.
  - Este algoritmo é simétrico e as chaves são compartilhadas.
- As chaves WEP possuem vulnerabilidades.
  - Os tamanhos das chaves criptográficas variam de 64-128 bits.
  - Quando foi proposto, este algoritmo se tornou alvo de estudos e uma série de vulnerabilidades foram encontrados.
- Ataques ao WEP
  - Já existem ferramentas que conseguem quebrar facilmente este tipo de criptografia.
  - Uma forma de se prevenir destes ataques é fazer a troca da chave de criptografia periodicamente, como de 10 em 10 minutos. Isto não é implementado no IEEE 802.11b.

Padrão 802.1x

- Um padrão mais robusto que utilizaremos para ilustrar o processo de autenticação de acesso entre uma estação cliente e um ponto de acesso é o 802.1x;
- Um servidor RADIUS é utilizado para prover esta autenticação;
- O diálogo de autenticação entre a estação e o servidor RADIUS é feita através de frames EAP (Extensible Authentication Protocol);

Padrão 802.11x exemplo



Riscos de segurança das WLANs (1/3)

- Além de todos os problemas das redes cabeadas, as redes sem fio possuem riscos inerentes da própria tecnologia.
- Qualquer access point conectado a uma rede sem fio essencialmente faz um broadcast de uma conexão ethernet.
- Muitas empresas cometem o erro de não se preocuparem sobre segurança de redes sem fio.
  - Muitas empresas acreditam que só devem se preocupar com suas redes sem fio se estas estiverem rodando serviços de missão crítica.

Riscos de segurança das WLANs (2/3)

- Entretanto poucas redes trabalham como LANs isoladas;
- O nível de segurança de uma instituição que deixa em aberto a questão da sua rede sem fio, pode ser comparada à construção de uma casa com uma porta de ferro bem reforçada, mas com paredes de vidro;
- Dessa forma um intruso terá facilidade em explorar as vulnerabilidades da rede sem fio para lançar seu ataque sem precisar "driblar" um bom firewall por exemplo;

Riscos de segurança das WLANs (3/3)

- **Vulnerabilidades Internas.**
  - São vulnerabilidades que ocorrem devido a má configuração de equipamentos. Não dependem de um potencial atacante externo.
  - Fazem parte destas vulnerabilidades:
    - WLANs Grampeáveis / Rouge WLANs;
    - Configuração inseguras de rede;
    - Associação acidental.
- **Riscos Externos.**
  - São aqueles em que um atacante externo explora vulnerabilidades bem conhecidas de redes sem fio.
  - Fazem parte destas vulnerabilidades:
    - Eavesdropping & Espionage;
    - Roubo de identidade;
    - Ataques emergentes.

Vulnerabilidades Internas (1/3)

- **WLANs Grampeáveis/ Rogue WLANs**
  - São redes sem fio onde ocorrem acesso não autorizado.
    - Access points conectados em redes corporativas são utilizados como ponto de acesso externo sem o aval da empresa.
    - Estações de trabalho setadas para trabalhar em modo Ad Hoc. Ou seja, estas estações estão abertas a ataques externos.
  - Rogue Acess Points podem ser escondidos bastando duplicar o MAC de uma máquina legítima.
  - Em 2001 estimava-se que 20% das redes corporativas dos EUA possuíam rogue WLANs.

Vulnerabilidades Internas (2/3)

- **Configuração de rede Insegura.**
  - Muitas empresas fazem a segurança de suas redes sem fio com a utilização de VPNs e cometem o erro de achar que suas redes são a prova de bala.
  - Este tipo de abordagem faz com que as demais configurações permanecam padrões.
    - Isto faz com que passwords fiquem padrões;
    - Broadcasts de SSIDs;
    - Criptografia fraca ou ausente.
  - Técnicas mais sofisticadas conseguem atacar VPNs, mas a opção mais simples seria atacar o próprio access point.

Vulnerabilidades Internas (3/3)

- **Associação Acidental**
  - Ocorre quando um access point "a" emite um forte sinal RF que faz com que o sinal pareça melhor do que a de uma rede wireless vizinha "b".
  - O que ocorre então é que estações de "b" se associam a "a"
  - O Windows XP se associa automaticamente a estas redes sem o consentimento do usuário ou da rede vizinha.
  - Um outro problema grave pode ocorrer se os dois access points de associarem gerando uma ESS. Ou seja, fazendo com que duas redes distintas aparentassem ser uma única rede.

Vulnerabilidades Externas (1/3)

- **Eavesdropping & Espionage.**
  - É a escuta das ondas de rádio com a finalidade de se obter informações valiosas sobre a rede.
  - Mensagens encriptadas com WEP podem ser facilmente decriptadas com um pouco de tempo e a utilização de ferramentas hackers.
  - É importante ressaltar que é um trabalho difícil identificar atacantes que se utilizam dessas técnicas.
  - Uma forma de se identificar este tipo de técnica é através da utilização de uma armadilha, em que pacotes forjados são enviados para a rádio freqüência.

Vulnerabilidades Externas (2/3)

- **Roubo de identidade**
  - **O atacante descobre o access point através de scans e a partir de então captura o tráfego da rede.**
  - **A identidade é roubada através da descoberta dos SSIDs e da descoberta de um MAC válido, de um cliente que seja válido.**
  - **O atacante seta seus SSIDs e seu MAC como sendo de um usuário válido na rede.**

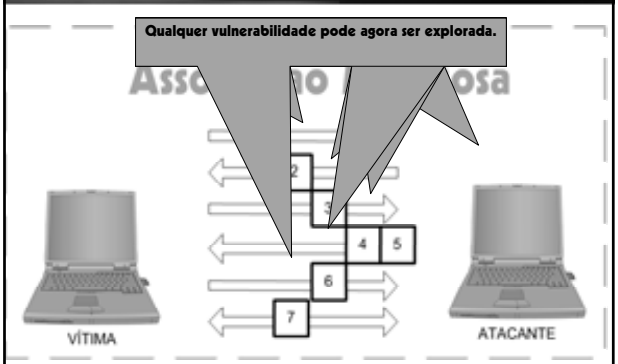
Vulnerabilidades Externas (3/3)

- **Evolving Attacks.**
  - **São ataques mais sofisticados, como Denial-of-Service e Man-in-the-Middle.**
  - **Ataques como Denial-of-Service fazem com que serviços de redes fiquem desabilitados.**
  - **Ataques como Man-in-the-Middle consequem comprometer redes privadas virtuais (VPNs).**
  - **Estes dois tipos de ataques são mais difíceis de serem efetuados, mas quando bem efetuados podem deixar a rede inteira comprometida.**

Ataques a redes sem fio

- **Alguns tipos de ataques conhecidos em redes sem fio são:**
  - **Associação maliciosa;**
  - **MAC spoofing;**
  - **Man-in-the-middle;**
  - **Denial-of-Service.**

Ataque – Associação Maliciosa



Ataque – MAC spoofing

DoS: Deny-of-Service (1/2):

- **Ataques por negativa de serviço em redes sem fio podem literalmente vir de qualquer direção;**
- **Simplesmente enviando grande quantidade de ruído na rede, um atacante pode efetuar esse tipo de ataque com sucesso;**
- **Entretanto, os criminosos eletrônicos tendem a se sofisticar cada vez mais.**

DoS: Deny-of-Service (2/2):

- **Como exemplo temos o seguinte tipo de ataque:**
  - **Com uma estação configurada como AP, ou seja, usando um SoftAP, o criminoso faz uma inundação de comandos persistentes de "desassociação";**
  - **Assim todas STAs são forçada a se desconectar da rede sem fio;**
  - **Ou então o SoftAP pode ficar enviando os comandos a cada período de 10 segundos por exemplo, assim as STAs ficarão se conectando e desconectando da rede continuamente;**

Ferramentas (1/2):

- **Tanto hackers black ou white hat, tentam identificar vulnerabilidades nos padrões assim que eles são lançados;**
- **É o que também acontece com a tecnologia wireless;**
- **Para tal, existem algumas ferramentas como por exemplo o NetStumbler e Dstumbler que são utilizadas para fazer prospecção em redes sem fio;**
- **Citando mais algumas ferramentas bem populares: Wellenreiter, WEPCrack, Kismet e Airsnort.**

Ferramentas (2/2):

- **NetStumbler (www.netstumbler.com) é uma ferramenta para Windows que por monitoramento ativo faz probes para tentar encontrar APs e levantar informações a seu respeito (SSID por exemplo);**

War Driving (1/4):

- **Utilizando-se dessas ferramentas, surge o conceito de war driving;**
- **Os hackers dirigem pela cidade tentando localizar a presença física de uma rede sem fio;**
- **Encontrando alguma rede, eles picham símbolos (warchalking) para demarcar que ali existe uma rede sem fio ativa;**
- **Existem até sites com mapas de redes wireless, tais como:**
  - **http://www.wigle.net/gpsopen/gps/GPSDB/ (Chicago);**
  - **http://www.wifinder.com/**

War Driving (2/4):

- **Wireless Geographic Logging Engine**

http://www.wigle.net/gpsopen/gpsGPSDB/ (Chicago);

- **Piada no dia 1º de abril: Fechado pelo Departamento de Justiça (01/04/2003);**

War Driving (3/4):

- **Interface do NetStumbler no painel de um carro;**

War Driving (4/4):

- Símbolo pichado no chão, indicando a presença de uma WLAN grampeável: "até uma criança consegue se conectar";

Warchalking:
rede aberta sem mecanismo de autenticação, 2 Mbps, 802.11b
SSID: tsunami

Deixando sua WLAN mais segura (1/6)

- Existem alguns passos que podem ser seguindos para tornar uma rede sem fio mais segura:
  - Descobrimento de Rogue Access Points & vulnerabilidades;
  - Fechar seus Acess Points;
  - Criptografia e autenticação – VPN;
  - Fazer e reforçar políticas para redes sem fio;
  - Intrusion Detection & Proteção;

Deixando sua WLAN mais segura (2/6)

- Descobrindo access points grampeaveis e vulnerabilidades
  - A descoberta de access points ilegais dentro da rede pode ser feita de duas maneiras:
    - Fisicamente, caminhando pela área que contém a rede com prospectores de redes wireless;
    - Monitorando a rede com sensores remotos desenvolvidos especifiamente para este tipo de serviço. Eles monitoram toda RF das WLANs.

Deixando sua WLAN mais segura (3/6)

- Fechando seus access points:
  - Modificar os SSIDs padrões;
  - Configurar o access point para não fazer broadcasts constantes do SSID;
  - Fazer Filtragem por MAC no access point;
  - Utilizar criptografia WEP;
  - Não permitir conexões em baixa velocidade.

Deixando sua WLAN mais segura (4/6)

- Criptografia e autenticação – VPN
  - A criptografia do padrão 802.11b, WEP, é fraca. Softwares como WEPCrack podem facilmente quebrar essa criptografia.
  - Portanto, a utilização de VPN e extremamente recomendável.
  - O uso de servidores RADIUS para autenticação também é recomendável.

Deixando sua WLAN mais segura (5/6)

- Fazer e reforçar as políticas para redes sem fio
  - Não permitir uso não autorizado de access points;
  - Não permitir a má configuração de componentes wireless como Ad Hoc;
  - Não permitir accesso em baixas velocidades.
  - Etc...

Deixando sua WLAN mais segura (6/6)

- **Intrusion Detection & Proteção**
  - São ferramentas que conseguem detectar tentativas de conexões não autorizadas em redes wireless;
  - As formas mais conhecidas de ataque a redes wireless começam com probes nas RF para descoberta de SSIDs;
  - Desta maneira, combater estas ferramentas de escaneamento faz com que o número de potenciais ataques caia significadamente;
  - Para estudarmos como obter os sistemas detectores de intrusão para redes wireless (WIDS – Wireless Intrusion Detection System) precisamos estudar como as ferramentas de escaneamento funcionam.

Wireless IDS

- **Localização do detector de intrusão:**
  - O detector de intrusão deverá ser instalado na mesma área em que estão localizadas as WLANs.
- **Identificando tráfego anômalo:**
  - Para clientes localizarem WLANs para se conectarem eles a maior parte das vezes necessitam fazer requisições em broadcasts;
  - Aplicações como NetStumbler e DStumbler utilizam estas formas de scan para descobrir redes wireless.

Conclusão

- A nova tecnologia de rede sem fio, por ser ainda muito recente, contém ainda muitas vulnerabilidades e riscos na sua implementação.
- Apesar disso, uma implementação segura já é viável.
- Poucas ferramentas são capazes de analisar o tráfego da camada 2 do 802.11.
- Apesar de ser possível detectar os scanners de redes wireless, prover detectores de intrusão para esta rede ainda é uma difícil tarefa.

Refêrencias

- http://www.acmesecurity.org
- https://forum.acmesecurity.org
- http://www.airdefence.net
- http://www.cs.umd.edu/~waa
- http://www.nas.nasa.gov/Groups/Networks/Projects/Wireless/
- http://www.pluton.com.br
- http://www.ethereal.com
- http://www.netstumbler.com
- http://www.airsnort.shmoo.com
- http://hostap.epitest.fi

Thanks!

lod@acmesecurity.org
(Key id: 0x4CF4CB68)
www.acmesecurity.org/~lod

sacchet@acmesecurity.org
(Key id: 0x3264E801)
www.acmesecurity.org/~sacchet

Disclaimer