GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

The Evolution of War Flying

GSEC Practical Assessment v4.1b
Ramsey Williams
October 2002

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Table of Contents

Introduction_____ 3

War Dialing……...3

War Driving……...3

802.11 and WEP (Wired Equivalency Privacy)……..4

How the pieces involved work together……5

War Chalking……...6

War Flying……6

Tools……..7

Recommendations……..11

Conclusions_____ 12

Works Cited……..……...13

Tools Cited……..…….……14

Reference Sources……..……..15

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Introduction

This paper begins by defining time through the actions of the technical community as they move their way through the evolution of those who are called War Flyers. I describe the different protocols, standards, and tools used throughout in an in-depth overview of several closely related subjects. All while maintaining my objective to express this paper in terms anyone could understand along with my recommendations to help you protect your own wireless networks.

Discovering wireless networks is acceptable. Anything else is not. Do not attempt to access a network you do not own--that is illegal. Someone is going to find that out the hard way, I am sure!

War Dialing

War Dialing involves using a software application to dial blocks of sequential numbers in order to look for a modem backdoor into a network. War Dialing became known to the world after the release of the movie War Games. In the movie, a child computer genius sets up his computer to call every phone number in a state until he reaches another modem, from which he can then crack into the systems.

War Driving

War Driving (wôr dri'vin) is a verb coined by Pete Shipley. War Driving involves looking for unsecured wireless networks, while driving around in your vehicle mapping out their local areas. For example, if you were to drive around with your laptop and a wireless NIC (Network Interface Card) in promiscuous mode, writing down the location of wireless networks as you come across them, then you would be War Driving.

The graphic below is the result of a War Driver. The network locations are gathered, and then shared. This is so common that you should be able to find a map of your local area on the Internet.

California Los Angeles

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.





http://www.socalwug.org/wlan-security/img10.html

802.11 and WEP (Wired Equivalency Privacy)

802.11 standard designates the wireless standard. There are several variations of the standard, usually specified with a letter appended to the end of 802.11 such as in 802.11a. Standards are designed to require many vendors to make products that will be compatible. NOTE: Standards do not always work; however, multi-vendor systems achieve the great success when using standards. For example, the Orinoco wireless NIC will work with a Linksys access point, because the two hardware devices use the same standard. Standards also help consumers to select a product. If a consumer needs a particular function, and only that function is contained on one variation of a standard, then the standard allows the consumers to narrow their search to products that conform to that standard.

802.11 started off as the standard for home or small WLAN (wireless local area networks), but has since moved into the realm of enterprise scalable WLAN for corporate use. This change has caused some systems to use more bandwidth and tighter security, thereby creating several variations of the standard. Here are some standard variations:

- 802.11a provides around 25Mbps and up to 54Mbps on a 5GHz unlicensed band. This is considered high speed for wireless local area networks.

- 802.11b is the most popular wireless standard, but is unsecure due to WEP. With this standard the user receives 11Mbps up to 150 feet, then 1 or 2Mbps up to 400 feet with the 2.4GHz unlicensed band. “The Wired Equivalency Privacy (WEP) system is the encryption standard used by 802.11b wireless networks. However, WEP is undermined by common mistakes, including the failure to activate it entirely or engage WEP with

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

the encryption key set to the default value." (Miller) 802.11b should be upgraded to 802.11i standard when available.

- 802.11g combines the high speed of 802.11b and the higher range of the 2.4 GHz unlicensed band for the best of both worlds. Also backwards compatible with 802.11.b.

- 802.11e gives a wireless standard quality of service, which then allows you to use VOIP (voice over IP). This would be your digital phone system running over the IP (Internet Protocols) with an emphasis on voice quality, which is beyond the scope of this paper.

- 802.11i – This standard was created to replace WEP (Wired Equivalency Privacy) with TKIP (Temporal Key Integrity Protocol).

How the pieces involved work together

Laptop or PDA, Wireless NIC, Software, a way to get around and GPS. Here are a few examples:

- Pocket PC 2002 (Operating System)
- Compaq iPaq Model 3765 (Handheld Device)
- Lucent WaveLan PCMCIA card (Orinoco gold) (NIC)
- Compaq Single slot PCMCIA adapter sleeve
- Sniffer program "Mini-Stumbler" (Software)

- Windows 2K (Operating System)
- Panasonic C-48 (Handheld)
- Orinoco Sliver PCMCIA card (NIC)
- Netstumbler (Software)
- Garmin eTrex GPS

- Linux RedHat 7.3 (Operating System)
- Kismet 2.4 or most current development (Software)
- AirSnort (Software)
- PCMCIA reworked for RFMON mode for Aironet 350
- Orinoco Sliver PCMCIA card (NIC)
- Garmin eTrex GPS

Using what you already have is the obvious choice when setting a new system up for use. Orinoco's gold and silver NICs (Network Interface Cards) seems to be extremely popular among War Driving wireless systems. Also, you only need a GPS system is if you wish to keep track of the networks you find.

War Chalking

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

During the Great Depression hobos drew signs to let the next hobo know where one could get a meal, and this is where Matt Jones got his ideal. Matt Jones coined the term War Chalker. Like War Driving, wireless security experts, in an attempt to educate the technically ignorant public, recently took up the act of War Chalking. War Chalking is the action of physically marking a wireless access point with chalk in a visible location. There are different symbols used to indicate whether a wireless network is open, closed or encrypted with WEP.



http://www.doc-x.de/cgi-bin/wiki.pl?WarChalking

The bandwidth is written under the symbol and the network's SSID (Service Set ID) is written above as you can see in the graphic above.

"Some people have asked why not use stickers or paint," said Matt Jones. "But the idea of chalk means that people have to go around and renew the symbols to the network is constantly revalidating itself and checking its own integrity. Also, using chalk won't piss too many people off." (Jones)

This is so common that, "the FBI is now telling companies that, if they see the chalk marks outside their offices, they should check the security of wireless networks and ensure they remain closed to outsiders."(BBC) The FBI has a right to be concerned; however, I think War Chalkers should be allowed to exploit un-secure wireless networks with chalk to help educate the ignorant by embarrassment. When a corporation is publicly humiliated they do not forget it and this is one of the best educational techniques, because it will affect everyone that hears the story too.

War-Flying

WAR Driving extremists have taken it to a new level with WAR-Flying. War Flying has added a whole new element to strategically placing Wireless Access Points. Before when you had your own building, your main concern was to deny access

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

to the street and adjacent buildings. Now if you were to deploy wireless access point with a range of 100 feet in a two-story building, you are left wide open from above. The first documented case was in Perth, Australia.

Tracy Reed's story was the first glimpse into War Flying in the United States of America and it is amazing as explained in the next paragraph "The first apparent case in the United States of warflying was achieved by Tracy Reed, a system administrator for MP3.com. Besides being a Wi-Fi enthusiast, he's also an amateur pilot."(Stevenson)



Tracy Reed mapped out all of the access points he located on his first flight with his friends. You can make out his flight path. "The entire flight lasted about 1.5 hours and during that time we detected 437access points."(Reed) Not to say that all 437 access points are un secure; however, it is very unlikely that all 437 are secure.

Tools

Some tools used by War Drivers, War Chalkers and War Flyers are listed below. Due to rapid development and additions of features I have include the links to the products homepage if I have them or other well known sources, so in weeks to come you can get the most up to date product information.

AirJack for Linux

When AirJack is used correctly it will let the user take over a connection to a wireless LAN. First you DOS (Denial of Service) the access point by bombarding

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

it with forged packets causing it to crash. Then when the access point comes back to life it automatically starts looking for a new access point. When the access point searches for another access point it will recognize you as one, making you the middleman between the two access points giving you access to the network.
http://802.11ninja.net/

AiroPeek for Windows 98, ME, 2000, XP

"AiroPeek is a comprehensive packet analyzer for IEEE 802.11b wireless LAN, supporting all higher-level network protocols such as TCP/IP, AppleTalk, NetBEUI and IPX. AiroPeek contains the entire network troubleshooting features familiar to EtherPeek. In addition, AiroPeek quickly isolates security problems, fully decodes 802.11b wireless local area networks (WLAN) protocols, and analyzes wireless network performance with accurate identification of signal strength, channel and data rates."
http://www.wildpackets.com/products/airopeek

AirSnort for Linux

AirSnort is primarily for cracking WEP (Wired Equivalency Privacy), not discovering wireless networks. AirSnort is a tool provided by The Shmoo Group (www.shmoo.com). If you use AirSnort on a network that is not yours, you are certainly breaking the law. "AirSnort is a WLAN tool that recovers encryption keys. AirSnort operates by passively monitoring transmissions, computing the encryption key when enough packets have been gathered." AirSnort can guess your encryption key in microseconds.
http://airsnort.shmoo.com/

AirTraf for Linux

"AirTraf is a package with many features. On a basic level, it performs packet capture/decode in the 802.11b wireless level. It gathers and organizes packets captured over the air based on the type of traffic (management, control, data), according to the dynamically detected access points (in case there are multiple in a given area), and performs bandwidth calculation as well as signal strength information on a per wireless node basis. It determines the SSID of access points, the channel it is operating under, the number of wireless nodes connected to the access point of interest, the overall load on the access point, as well as the bandwidth utilized by all connected wireless nodes. And as of AirTraf-0.3-1beta, AirTraf is database-aware, meaning that multiple sniffers can be polled via a central polling server periodically to gather up2date information, and saving the information for long-term load analysis over periods of days, weeks, months, and even years. The other feature of AirTraf includes tracking of access related activity generated in the area, it tracks all probe/authentication/association requests made to a given access point, and by observing access point's reaction,

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

make a judgment as to the nature of activity, and determine whether the activity is hostile or friendly. (Currently fairly unstable, and being worked on)"
http://airtraf.sourceforge.net/index.php

BSD-AirTools for FreeBSD 4.4, OpenBSD 2.9/3.0, NetBSD 1.5.1+

"BSD-AirTools is a package that provides a complete toolset for wireless 802.11b auditing. Namely, it currently contains a BSD-based WEP cracking application, called Dweputils (as well as kernel patches for NetBSD, OpenBSD, and FreeBSD). It also contains a curses based access point detection application similar to Netstumbler (Dstumbler) that can be used to detect wireless access points and connected nodes, view signal to noise graphs, and interactively scroll through scanned AP's and view statistics for each. It also includes a couple other tools to provide a complete toolset for making use of all 14 of the prism2 debug modes as well as do basic analysis of the hardware-based link-layer protocols provided by prism2's monitor debug mode."
http://www.dachb0den.com/projects/bsd-airtools.html

Kismit for Linux

Kismet is an 802.11b sniffer capable of sniffing using almost any wireless card supported in Linux.
http://www.kismetwireless.net

Mognet for Linux

Mognet open source wireless ethernet sniffer/analyzer. It is licensed under the GNU General Public License. It was designed for PDAs (Personal Digital Assistant), but will run just as well on everything else running Linux.
http://chocobospore.org/projects/mognet/

Netstumbler for Windows 2000, 9X, ME, XP, Pocket PC

Netstumbler has a user friendly GUI and is the most popular wireless discovery tool out there. Netstumbler uses your wireless network card to detect WLANs. It will return the SSIDs (Service Set Identifier), channel and signal strength. Netstumbler will determine if the WLAN is using WEP or not.
http://www.netstumbler.com

PrismStumbler for Linux

PrismStumbler scans for beacon frames from access points. PrismStumbler monitors any frames received on the currently selected channel as it switches through them one by one.
http://prismstumbler.sourceforge.net/

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

SSID Sniff for Linux

SSID Sniff is a tool use when looking to discover access points and save the captured traffic like a sniffer. It comes with a configure script and supports Cisco's Aironet and prism2 based cards.
http://www.bastard.net/~kos/wifi/

Stumbverter for Windows 2000, 9X, ME, XP

Stumbverter is used to import Netstumbler's summary files into Microsoft's MapPoint 2002. "The logged WAPs (wireless access points) will be shown with small icons, their color and shape relating to WEP mode and signal strength." You can also add information to each mapped icon.
http://www.sonar-security.com/

THC-RUT for Linux

"THC (The Hackers Choice) RUT (aRe yoU There) is a local network discovery tool developed to brute force its way into WLAN access points. It offers APR (Address Resolution Protocol) request on IP (Internet Protocol) ranges and identifies the vendor of the NIC, spoofed DHCP (Dynamic Host Configuration Protocol), BOOTP (Bootstrap Protocol) and RARP (Reverse Address Resolution Protocol) requests, ICMP (Internet Control Messaging Protocol) address mask request and router discovery techniques." Because this is a brute force network discovery tool it used first when a new network is discovered.
http://www.thehackerschoice.com

THC-WarDrive -for Linux

"THC-WarDrive is a tool for mapping your city for wavelan networks with a GPS device while you are driving a car or walking through the streets. It is effective and flexible, a "must-download" for all wavelan nerds."
http://www.thehackerschoice.com

WarLinux

WarLinux is a distribution specifically for War Drivers. It main intended use was for the auditing and evaluation of wireless network installations.
https://sourceforge.net/projects/warlinux/

Wavemon for Linux

"wavemon is a ncurses-based monitoring application for wireless network devices. It currently works under Linux with the Lucent Orinoco cards."
http://www.jm-music.de/projects.html

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

WaveStumbler for Linux

"WaveStumbler is console based 802.11 network mapper for Linux." WaveStumbler is used for gathering basic information from the access point like channel, WEP, ESSID (Extended Service Set Identifier), MAC etc. While still and like most Linux tools always in development it tends to be stable.
http://www.cqure.net/tools08.html

WEPCrack for Linux

WEPCrack is a tool used for breaking 802.11 WEP secret keys. "This tool is an implementation of the attack described by Fluhrer, Mantin, and Shamir in the paper "Weaknesses in the Key Scheduling Algorithm of RC4"." WEPCrack was the first available open source code that demonstrated the breaking of secret keys.
http://wepcrack.sourceforge.net/

WSA for Linux on an iPaq

"WSA (Wireless Security Auditor) is an IBM research prototype of an 802.11 wireless LAN security auditor, running Linux on an iPAQ PDA." WSA automated the security audit process of wireless network, to help network administrators find and remove any vulnerability before someone tries to use the vulnerability to gain access to the network.
http://researchweb.watson.ibm.com/gsal/wsa/

Recommendations

Wireless network security is a topic onto its self and near impossible to cover in its entirety. When you consider no two networks are identical and most are not even similar. I have written this paper to help educate the community in regards to common wireless threats. After all you are responsible for the network. Now that you know what you are up against you can do something about it.

You may want to download some of the tools above for testing; however, a few of them are more than capable of damaging your network. Your best bet is an off site lab, because your test lab could in fact link with your production environment, not to mention a destructive tool acting up.

One way to help secure your network is the use of a tool named Fake AP. Fake AP (Access Point) is a tool that generates thousands of counterfeit 802.11b access points. "Hide in plain sight amongst Fake AP's cacophony of beacon frames. As part of a honey pot or as an instrument of your site security plan, Fake AP confuses War Drivers, Netstumbler, Script Kiddies, and other undesirables." (Fake AP) I think it a good idea for at home, but you should rely on more secure system at the enterprise level.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Fake AP has also just recently got a lot of negative press too. The consumption of your networks bandwidth was the first released problem with the product; however, this was disproved by several simulated testing environment setup specifically to push the bandwidth thresholds. Another issue that has arisen recently is that you can identify the real access points with a port scan. Fake AP basically broadcasts fake SIDs created with a dictionary of venders MAC address. Fake AP is simple, and easily bypassed, but it will keep the inexperienced War Drivers out.

Strategically placing your access points is critical, and the best way to protect your self. Securing your network is made simple by deploying more access points with a smaller range to avoid War Driving and War Flying. Less range or overlapping access points is necessary to keep the limits of you WLAN contained. Once implemented, test the outer limits of your access points, do not take the manufactures word on the actual range. Now what are you going to do about your employee's PDAs? You could lock them out of the building or implement virtual offices. Right, you will need a WDMZ (Wireless Demilitarize Zone).

Implementing a WDMZ is something to consider when constructing a WLAN. It is one way to keep a possible disgruntle employee out of your critical systems. WLAN must be designed to meet your network security configuration requirements; however, implementation of a WDMZ is as simple as segregation using a VLAN (Virtual LAN) and dedicating a DHCP server to the WDMZ.

"Wireless users should be authenticated and authorization received every time they connect to the WDMZ. Some legacy systems will not have support. In order to achieve data confidentiality, a VPN should perform authentication tasks. Windows XP will support this…and this is an ideal method for user authentication and authorization." (Enteraysys Networks)

Conclusions

This paper explores War Flying and the main technically historical stepping-stones if its invention. I describe the tools used in today's environment with many different standards and protocols. Projecting the knowledge of harmful entities in hopes to educate the community. This paper was written to give the reader in-depth insight into a world known to few, enabling one to protect themselves. I hope you enjoyed reading this paper as much as I enjoyed writing it.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Works Cited

BBC "FBI warns about wireless craze" BBC News World Edition. 16 August 2002. UK http://news.bbc.co.uk/2/hi/technology/2197252.stm (10 September 2002)

Enterasys Networks "Wireless DeMilitarized Zone (WDMZ)" – Enterasys Networks' Best Practices Approach to an Interoperable WLAN Security Solution http://www.enterasys.com/products/whitepapers/wLANDMZBestPractices.pdf (14 September 2002)

"Fake AP" Black Alchemy Enterprise http://www.blackalchemy.to/Projects/fakeap/fake-ap.html (27 September 2002)

Jordan, Jason "WarStorming – War Driving & Barn Storming"18 August 2002 http://www.e3.com.au/stories.php?story=02/08/18/7667279 (14 September 2002)

Miller, Sandra Kay "War Driving" Information Security Magazine. Trends 2002 Technology. November 2001 http://www.infosecuritymag.com/articles/november01/technology_wardriving.shtml (14 September 2002)

Outmesguine, Mike "These Things are Popular" TransSeller, Inc. http://www.socalwug.org/wlan-security/img10.html (10 September 2002)

Reed, Tracy. www.ultraviolet.org http://www.ultraviolet.org/treed/writings/display.php3?document=warflying (14 September 2002)

Stevenson, David "WarFling for Wi-Fi" Tech Live 4 September 2002 http://www.techtv.com/news/internet/story/0,24195,3398350,00.html (14 September 2002)

"WarChalking" 6 October 2002 http://www.doc-x.de/cgi-bin/wiki.pl?WarChalking (6 October 2002)

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Tools Cited

Abaddon “AirJacks ” Wireless Ninja http://802.11ninja.net/ (27 September 2002)

“AiroPeek” Wildpackets, Inc. http://www.wildpackets.com/products/airopeek (27 September 2002)

“AirSnort” www.shmoo.com http://airsnort.shmoo.com/ (27 September 2002)

Lee, Peter K. “AirTraf” Source Fourge http://airtraf.sourceforge.net/index.php (27 September 2002)

“bsd-airtools v2.0” Dachb0den Labs http://www.dachb0den.com/projects/bsd-airtools.html (27 September 2002)

“Kismet” www.kismetwireless.net27 September 2002 http://www.kismetwireless.net (27 September 2002)

Hyuga “mognet” chocobospore.org http://chocobospore.org/projects/mognet/ (27 September 2002)

“NetStumbler” www.netstumbler.com http://www.netstumbler.com (27 September 2002)

“PrismStumbler” Source Forge 1 June 2002 http://prismstumbler.sourceforge.net/ (27 September 2002)

“ssidsniff” www.bastard.net 23 March 2002 http://www.bastard.net/~kos/wifi/ (27 September 2002)

Puchol, Michael “StumbVerter v0.1.0 beta” Sonar Security 2002 http://www.sonar-security.com/ (27 September 2002)

THC The Hackers Choice “THC-War Drive” & “THC-RUT” http://www.thehackerschoice.com (27 September 2002)

“Project: WarLinux: Summary” SorceForge https://sourceforge.net/projects/warlinux/ (27 September 2002)

Morgenstern, Jan “WaveMon” JM Music 30 March 2002 http://www.jm-music.de/projects.html (27 September 2002)

“WaveStumbler” cqure.net http://www.cqure.net/tools08.html (27 September 2002)

Rager, Anton T. “WEPCrack” SourceForge http://wepcrack.sourceforge.net/ (27 September 2002)

“Wireless Security Auditor” Security Research. IBM http://researchweb.watson.ibm.com/gsal/wsa/ (27 September 2002)

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Background Sources

"Cisco Aironet Security Solution Provides Dynamic WEP To Address Researchers' Concerns." Cisco Systems. Product Bulletin. http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/1281_pp.pdf (14 September 2002)

Jackson, Joab. "Secure Wireless Network at Last?" Washington Technology. 5 November 2002. http://www.washingtontechnology.com/news/16_16/business/17394-1.html(14 September 2002)

Maui "Under the Hat" 8 October 2001 http://soback.kornet21.net/~maui12ro/ (10 September 2002)

Millman, Rene "Chalk symbols expose London's wireless points" VNUnet.com 27 June 2002. http://www.vnunet.com/News/1133055 (10 September 2002)

Slayer, Slayer@Kraix.com "The Definitive Guide To Wireless WarX'ing" v1.2.1 www.kraix.com 4 September 11, 200 http://www.kraix.com/downloads/TDGTW-WarXing.txt (11 September 2002)

"WAR Dialing" Wikipedia.com The Free Encyclopedia. 29 July 2002 http://www.wikipedia.com/wiki/War_dialing (10 September 2002)

"WAR Games" Wikipedia.com The Free Encyclopedia. 2 August 2002 http://www.wikipedia.org/wiki/War_Games (10 September 2002)

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.