From MacHacking.net Knowledge Base
http://kb.machacking.net

Wardriving, An Introduction By Zelda. V3.6

Background:

Many of you may have heard of wireless networking. It's basically where data packets are sent using air to travel and not physical wires. Many people think that wireless networking is quite a new concept and technology this is not true, wireless networking has been here for over 70 years (With the development of the radio spectrum) and only has recently been adopted for computers for less than 9 years. But the early wireless networks were expensive, unreliable and slow. With the new development of new Universal technologies like Bluetooth or WiFi these have made wireless networking more affordable and a reliable data link over a network of computers.

Why Do We Want/Need It:

The idea behind such wireless data transmissions was that you could do two things at once or just the freedom to move without wires. Mobility without restrictions and the ability to send something over the air with special radio waves carrying data packets and information. Imagine a workstation that was wireless either with keyboards or actual Internet connections.

Types Of Wireless Networks:

There are many different types of Wireless networks some have been described here:

Infrared

Infrared is the form of using Infrared light to send data. You use this technology in everyday life (For Example Televisions and Remote controls). Infrared can be further divided into two subdivisions.

- Direct Infrared Transmission:

Is where you need a direct line of sight to transmit data (Imagine a remote control to a Television you need to point it at the TV). Direct Infrared Transmission is the most secure because it is harder to intercept the signal unless within the line to sight (10m). But one of the major drawbacks of any infrared technology is that you cannot get more than 10 metres away from the target without noticing a considerable depletion in signal strength.

- Indirect Infrared Transmission

Is the technology that was designed to compensate for the drawbacks of direct transmission. This is where the infrared light bounces of walls, people, dogs and furniture (almost anything really) this being its advantage as well as its weakness because the data packets could just *bounce* out the door into a Wardriver waiting over the road and this could be a problem because many new devices have this to carry important information.

Radio:

Discovered in 1902, Radio was and still is a breakthrough used by oscillating at certain frequencies in the radio spectrum. Radio is used everywhere from walkie talkies, To TV and finally mobile phones (though TV radio broadcasts and plain Radio have different modulation of the data packets but they both have the same principle).

Wireless Technologies:

These are the technologies designed as universal brands for the different types of wireless networks some include:

Bluetooth:

Is now the standard for short distance Infrared transmission. It was a breakthrough because in the beginning there were many devices and incompatibility in the 1990's. Bluetooth transmits at 2.4 GHz and can transfer a whopping 751 kb/s but its major drawback is that most bluetooth devices can only transmit over a 10m distance.

802.11 a.k.a WiFi:

Is a very good choice for a wireless technology because it covers both physical layer as well as media access layer based on the IEEE's specifications for networks. 802.11 operates at 2.4 Ghz and up to 2.8 Ghz. 802.11 works much like cellular phones because 802.11 uses Basic Service Sets (BSS) this enables devices to leave and join the node. There are currently three versions of 802.11 and one in development (802.11b, 802.11a, 802.11g and 802.11i is in development.) Before you go into the field check the compatibility your card has with the varying versions of 802.11 because there is some compatibility problems with some of these versions transmitting to each other. Also the Universally known brand name for 802.11 (all versions) is WiFi, which stands for Wireless Fidelity.

Security Threats:

The security threats of wireless devices were quickly recognised and with that a form of hacking was created called “Wardriving” and it was the art of intercepting, editing and injection packets to your discretion. With this, development of WEP (Wired Encryption Privacy) was formed. WEP encrypts data with a 128-bit key and makes any data that is intercepted, encrypted beyond cracking form (or so they thought :P). WEP made many devices more secure and with basic authentication. WEP is not the only encryption available many different forms are used but WEP is the most common form and is fast and efficient. WEP, although secure is known for its weak keys and reverse engineering flaws

Software:

There is much software available that enables you to scan for Wireless networks access points some include:

Windows:
NetStumbler (http://www.stumbler.net)

Palm OS:
Ministumbler (http://home.pacbell.ney/mariusm)

Macintosh:
KisMac (http://binaervarianz.de/projekte/programmieren/kismac/)
iStumbler (http://www.istumbler.com/)

Linux:
Kismet (http://www.kismetwireless.net)
Note: Kismet is one of my favourites because its scanning is completely passive and doesn’t send out probe requests which means it can detect the wireless networks that are known as cloaked (When the person disables probe requests on the node).

Hardware:

Exploiting Wireless networks requires alot of Equipment some of it is available over the counter and some you can/must buy off the net. I will try and have an explanation of the equipment when possible.
A brief list for the field kit includes:

1x Laptop or Handheld computer (PDA). One with long battery life. (Laptop must have wireless card functionality and generally is the first piece of equipment you need.)

1x PCMICA Wireless card based on the Hermes or PRISM2 chip set this is the (vital) piece of equipment that allows you to join/connect with the wireless network. A card with antenna connectivity would also be preferable.

1x 2.4 Ghz External Omni-Directional Antenna (An antenna for a wide area of mapping [much like the function of a radio Ariel] this antenna does not rely on a direct line of sight.)

1x 2.4 Ghz External Directional antenna also known as an cantenna (This piece of equipment is used to aim at specific locations generally into an office block or apartment because it directs the waves in a direct line).

1x Camera Tripod (to mount the directional antenna/cantenna). Optional.

1x GPS with a Computer interface. (Note: This is entirely optional but recommended because you can note exact location and co-ordinates as well as a few good GUI's allow you to map and pinpoint.)

1x Amplifier (good if you dislike signal loss or are in a remote area or just want to boost the performance of a card) (available from 1-50 watts Note: These are not cheap and I have opted into NOT getting one generally because of $$$)

1x Smart ID WiFi Detector Used for determining signal strength without the correspondence of your computer. This piece of equipment is Useful and recommended.

Misc:

Legal:

Many different states and cities have varying rules and guidelines for wireless communications. It is understood that you research these laws and find out yourself what these laws are in your state and area and the appropriate precautions to make while Wardriving. This may include a variety of stories that you may need to make up before you set out to covering up evidence, number plate switching, Abiding speeding laws and other things. It is also good to create a checklist before you go on a wardriving ride or you may end up riding in the back of a police car with your equipment confiscated. It has happened to me so be careful.

Mapping:

Many maps are available on the net where they have been uploaded by wardrivers that may have been in your location before and may provide you with a small (but useful) bit of information that may help you with your wardriving/walking. Two web sites that have downloadable maps include:

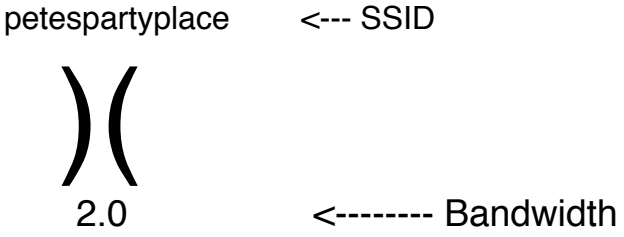
WiFi Maps (http://www.wifimaps.com)
Map Server (http://mapserver.zhrodague.net)

And if you want to make maps yourself, you may want to try out StumbVerter (http://www.sonar-security.com) Windows.
But generally Mapping is an essential part of wardriving for you to keep track of all the different nodes. I personally use a normal map and a simple marking system that involves pooling all the information into one big map in my room and using different coloured tacks to determine where the access points are. Also note taking is your best

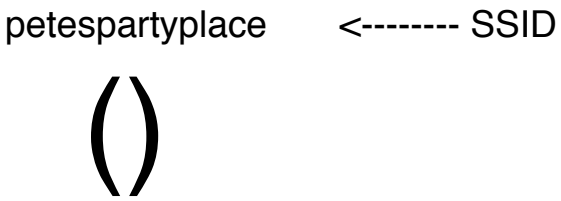
friend (Direct Address, SSID, Bandwidth and Users and passes where applicable)

Warchalking:

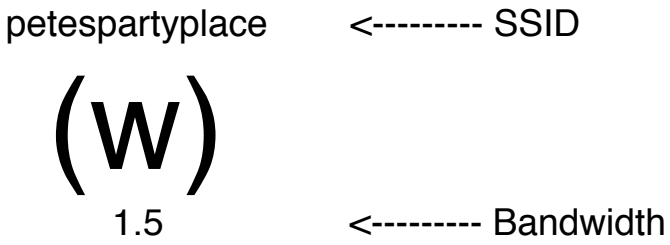
Warchalking is used by wardrivers around the world. It involves chalking buildings, roads and footpaths with different symbols that represent different things in the field of Wardriving where nodes are, are they open/closed, signal strength etc. For example here is a common sign that you may find on a footpath.



)(Is the symbol which signifies a “open” node “free access” unencrypted and no password required access. Note:)(is also the Universal wardriving symbol.



() Is the symbol that signifies a “closed” node, one that is restricted to specific devices sometimes depending on the node you can bypass this with things like spoofing of MAC addresses or many different tings but this is only for wardrivers that want to target certain companies or offices not for your average wardriver just looking for free access.



(w) Is the symbol that symbolises a WEP encrypted node that requires authentication. Occasionally a wardriver will put the details about the authentication on the symbol but that is a rarity.

Warchalking is a universally adopted technique that will both help you and fellow wardrivers to be able to adopt knowledge about different nodes and it is essential to master if you want to carry wardriving further. My suggestion is to carry different colours of chalk on you for different coloured surfaces and textures and generally put the markings in an area where the mark was less likely to be rubbed off.

WEP Encryption Flaws:

WEP is the encryption technique described earlier on for wireless networks and involves encrypting data with a 128-bit key. Two conventional methods of cracking WEP have been made and are documented:

Brute Force:

Brute force is when only one (encrypted) packet is found and the key is found by bouncing off thousands of possible combinations to the packet. The problem with brute force attacks is that a large amount of processing power is needed and the attacks is normally ineffective unless a small amount of information is known about the origin of the key and the person setting it.

FMS attacks:

FMS attacks are conducted when large amounts of packets are collected and the keys are found by leaks in the coding algorithm that

allows parts of the secret keys to be discovered in plain text. The disadvantages of FMS attacks is that many packets need to be sniffed out and found and this is all well in good in High bandwidth wireless nodes (it can be done in a matter of hours) but in very weak bandwidth situations it can be a pain because it could take weeks to gather enough packets and so new packet injection techniques have been found: http://www.dachb0den.com/ for more information about this packet injection technique.

Programs Recommended:
AirCrack http://packetstorm.digitallinx.com/filedesc/aircrack-1.4.1.html
AirSnort http://packetstorm.digitallinx.com/wireless/airsnort-0.2.1b.tar.gz
Both do standard FMS attacks

Bluetooth Flaws:

In late 2003 a group of individuals found Bluetooth had major flaws namely, Authentication and data transfer of Bluetooth enabled phones a full discloser and list of phones vulnerable are available here:
http://www.thebunker.net/release-bluestumbler.htm

Disclosing the types of attacks as well as different titbits of information.

Resources:

This is just a place for general places to find out more and expand your knowledge on wireless networks:

Tutorials/Sites:
"Wardriving HOWTO Unofficial"
http://www.wardriving.com/doc/Wardriving-HOWTO.txt
"How to pick the right antenna"
http://www.odessaoffice.com/wireless/antenna/how_to_pick_the_right_antenna.htm
Good wardriving info resource

http://www.wardriving.com
Hyper Link
http://www.hyperlinktech.com
Good Info Resource
http://www.bitshift.org/wardriving.shtml
“Wireless Howto”
http://www.ibiblio.org/pub/Linux/docs/HOWTO/Wireless-HOWTO
“How to build a tin can Waveguide antenna”
http://www.turnpoint.net/wireless/cantennahowto.html

Books:
Maximum Wireless Security
Essential Guide to RF and Wireless
Wireless LANs
All of these books can be found at Amazon.

Conclusion:

This tutorial was based for your general knowledge of Wireless networks and how they operate and how to gain access to them through the process called wardriving. If you want more knowledge of the subjects of Wardriving, WEP, VOip or just Wireless networks in general Google it or if not there are many good tutorials out there on the net going into more depth about wireless networks. Check out the links recommended here I’m sure you will gain some valuable wealth of knowledge out of them (especially some of the books).

Disclaimer

This article is only for educational purposes only and thus I am not responsible for the malicious intent of the person reading it. Feel free to distribute this tutorial in its original form including the formatting/extension/name. Do not take snippets out of the original text

Author And General:

Zelda/Link is a Writer, Hacker, Wardriver And (apprentice) Coder from Australia.
E-mail: Zelda@undergroundmac.com
AIM: Z3lda1
Version: 3.6
Future Version Due date: v4.0b , 2004 November Somewhere

Note: Please feel free to email me to ask questions. I will answer questions where I can but you cannot expect an email straight away (also carefully ask me questions and not ones like “How do I wardrive” because my answer will always be the same). Also bugs, typos, errors, bad links and suggestions are welcome.