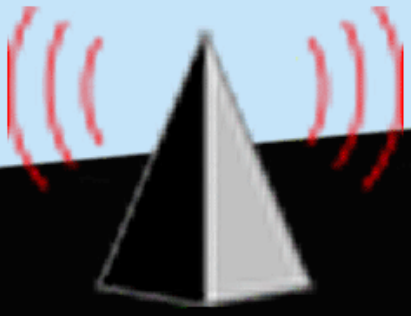


Das HowTo für WARdriver

MaxMatter 2003

Wireless Access Revolution

Wardriving für Dummies

Dies ist nicht als Anleitung zum Eindringen in fremde Netzwerke gedacht sondern als kleiner Newbie Guide für Leute die sich für Ihr privates Wlan interessieren und es verstehen möchten. Dazu gilt es erst einmal zu verstehen wie man in das Wlan gelangt, wie sensibel die Benutzung eines Wlan`s ist und wie man es letztendlich sicherer machen kann. Den meisten Leuten ist oft nicht richtig bewusst dass das eigene WLAN nicht an der Wand endet, sondern oft noch viele Meter nach außen in die Realität dringt.
Dieser Aspekt kann Unternehmen oft teuer zu stehen kommen, da sensible Daten für jedermann frei zugänglich sind.
Oft werden Wardriver in den Medien als „Kriminelle" oder „Verbrecher" dargestellt aber Schuld ist immer eine Frage der Perspektive. Ist nicht jede Information frei, solange sie nicht als „Verschlusssache" deklariert ist? In Wahrheit sind es Industriespione und unliebsame Konkurrenz die eine potentielle Gefahr für jedes WLAN darstellt. Die Gefahr geht nicht von irgendwelchen Wardrivern, sondern von der Unwissenheit der Gefahr aus und wir möchten erreichen dass man die Netze öffnen kann ohne Angst zu haben, dass dieses Privileg von ein paar „Schwarzen Schafen" ausgenutzt wird. Deshalb scannen wir unsere Umgebung und geben Tipps und Tricks weiter. Wir müssen uns Anfangs mit dem Prinzip der Ursache und Wirkung auseinandersetzen. Jede Aktion ruft immer auch eine Reaktion auf.
WAR steht nicht etwa für Krieg gegen die Gesellschaft, WAR steht für Wireless Access Revolution einem miteinander in einer in einem neuen Raum welche überall und jederzeit zugegen ist. Wir leben bereits in dieser vierten Dimension und leben das Digital welches für uns nicht mehr aufzuhalten scheint.

Respektiert den § 202a Ausspähen von Daten

(1) Wer unbefugt Daten, die nicht für ihn bestimmt **und die gegen unberechtigten Zugang besonders gesichert sind**, sich oder einem anderen verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

Dies erfordert aber, dass die Daten gegen unberechtigten Zugang besonders gesichert sind. Eine unverschlüsselte Mail oder ein ungesichertes WLAN fällt also nicht in den Schutzbereich des § 202a StGB. Wird die Mail oder das Netzwerk hingegen verschlüsselt, ist eine Strafbarkeit nach § 202a StGB gegeben, wenn diese unberechtigterweise gelesen bzw. genutzt werden.

Genauso wie Sonderfunk (Polizeifunk) ist nach der letzten Änderung des TKG (Telekommunikationsgesetz) das Mithören nicht strafbar. Lediglich die Weitergabe und / oder Veröffentlichung des Gehörten wird bestraft. (Das vorsätzliche Ausspionieren einer Firma bzw. eines geschütztes Netzwerk oder Firmendaten ist natürlich immer unter Strafe gestellt.)

Im ersten Teil möchte ich veranschaulichen wie das einloggen in das Wlan funktioniert und innerhalb welchen Umkreises das WLAN noch funktioniert. Ich nehme bewusst Tools aus dem Free- und Shareware Bereich, da diese im Gegensatz wie NAI Sniffer für jedermann erhältlich sind.
Da die meisten mit Windows-XP arbeiten möchte ich auf diese Variante näher eingehen. Die Möglichkeiten unter Linux sind bei weitem Umfangreicher als unter Windows.

Benötigte Hardware:

1. **Notebook**
2. **Karte mit Lucent Chipsatz (Orinocco Karten)**
   Als SSID im ClientManager „**any**"(ohne Klammern) eingeben
3. **evtl. Antenne zum verstärken (z.B. Huber&Suhner +5db)**

Wer mit der Auswahl der Hardware sicher gehen möchte, kann entsprechendes Equipment bei http://www.freebird-solutions.com bestellen.

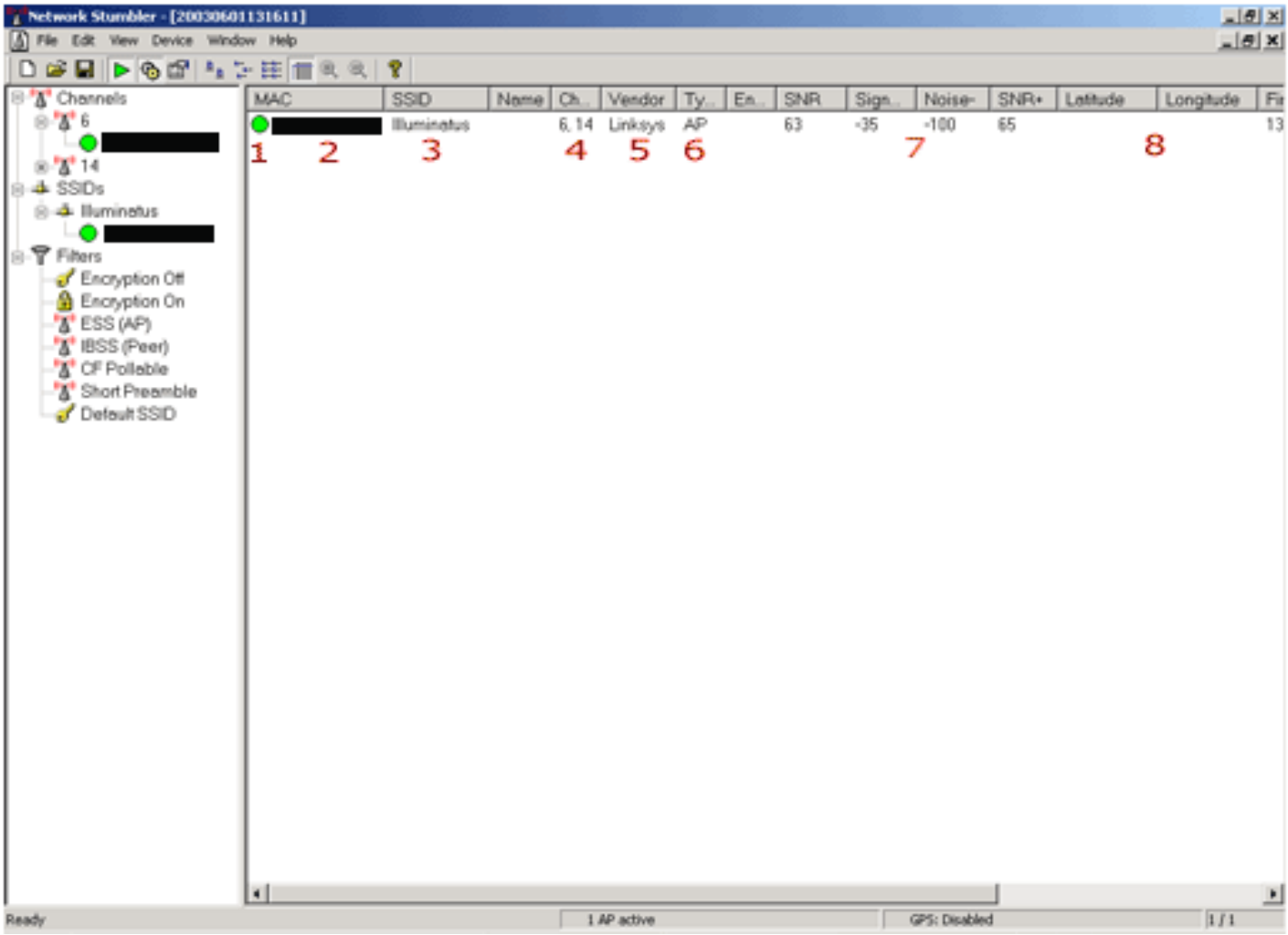
Benötigte Programme:

1. **Languard (www.gfisoftware.de)**
2. **Netstumbler (www.netstumbler.com)**

Nachdem wir die entsprechende Software installiert haben können wir beginnen. Ich gehe mal davon aus, dass Ihr die Programme zum laufen bekommen habt, sollte ja nicht schwer sein. Ansonsten schaut mal aufs Board: http://www.wardriving-forum.de.

1.Schritt:

Starten des Netstumblers:



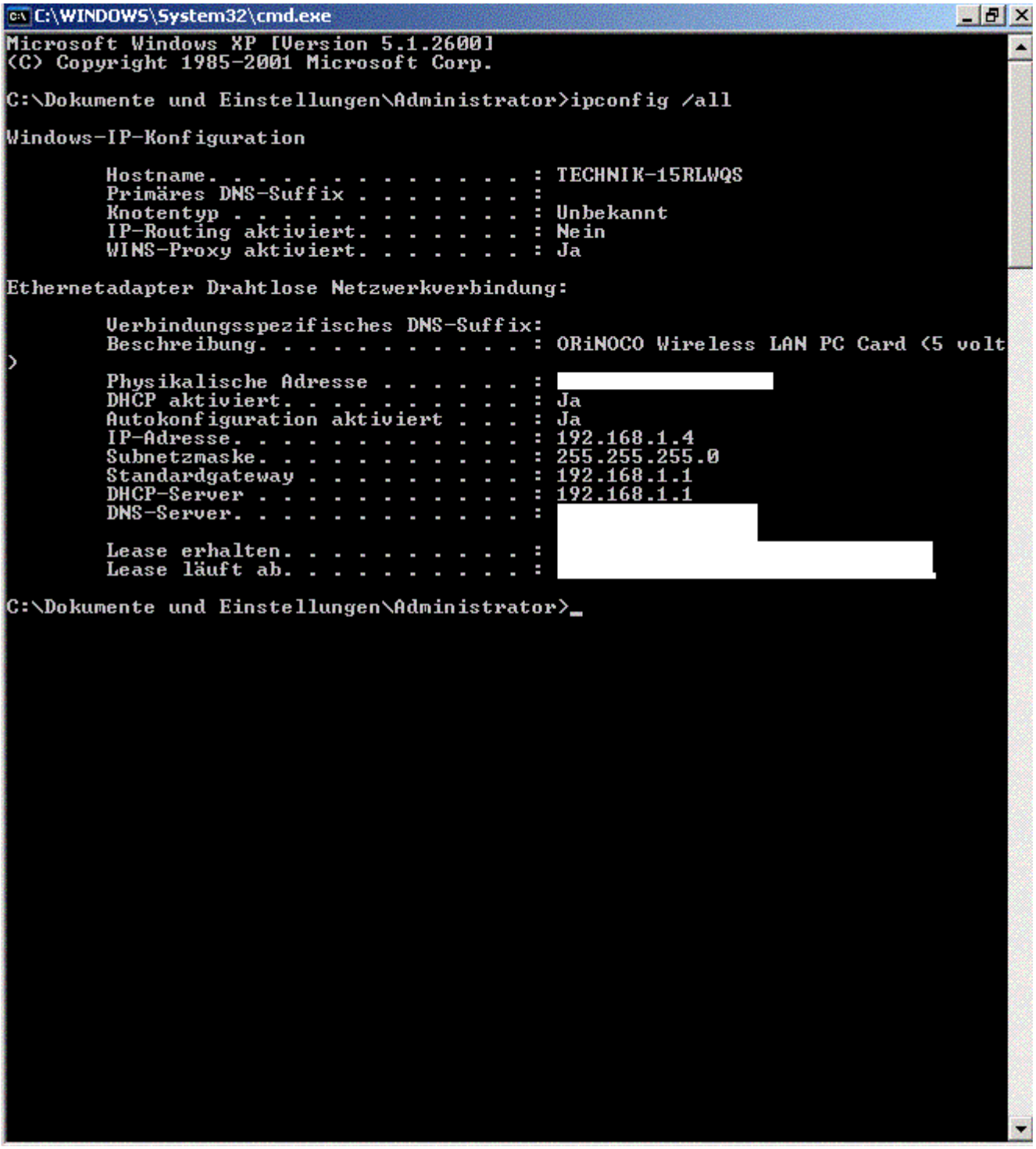
Habt Ihr jetzt euer Netz gefunden? Ihr seht auf der rechten Seite folgendes:

1. **Runder Button:** Anzeige des Empfangs (grün=gut/ gelb=schlecht/ rot=gar nicht)
   Anm: Ist noch ein Schloss zu sehen ist WEP aktiviert
2. MAC: zeigt die Macadresse des gefundenen AP`s an
3. **SSID:** Das ist der Name eures AP`s
4. Die Kanäle auf dem der AP sendet/empfängt
5. Marke des AP`s (Hierbei kann man oft Rückschlüsse auf die Standartpasswörter bekommen. Das Passwort also auf jeden Fall bei einer Installation ändern)
6. Zeigt hier an dass es sich um einen AP handelt
7. Nur interessant bei Verwendung einer Richtantenne
8. GPS Koordinaten falls ihr einen GPS-Empfänger verwendet

Wichtig ist für euch erst einmal der runde farbige Button. Ist ein Schloss zu sehen dann vergesst es wenn Ihr euren WEP-Key vergessen habt. Ihr könntet Ihn zwar errechnen, aber das dauert bestenfalls 4-6 Stunden und benötigt eine Menge Know How. Wenn kaum Daten laufen kann es Monate dauern….

So wie oben abgebildet (runder grüner Button) ist schon mal nicht schlecht, da machen wir weiter. Schließt euren Netstumbler jetzt und geht in eure DOS-Box (Win98: Start-ausführen-[command] (ohne Klammern) und Enter // WinXP: Start-ausführen-[**cmd**] ohne Klammern) und Enter

Jetzt gebt mal hinter C:…>**ipconfig /all** ein und schaut ob Ihr eine IP-Adresse bekommen habt.



Hier haben wir jetzt unsere IP hier 192.168.1.4 und den DHCP Server mit 192.168.1.1

Wir erinnern uns an das kleine 1x1 eines Netzwerkes:

192.168.1.**1** - 192.168.1.**255** (Netzwerkbereich)
Ihr habt keine IP bekommen?!

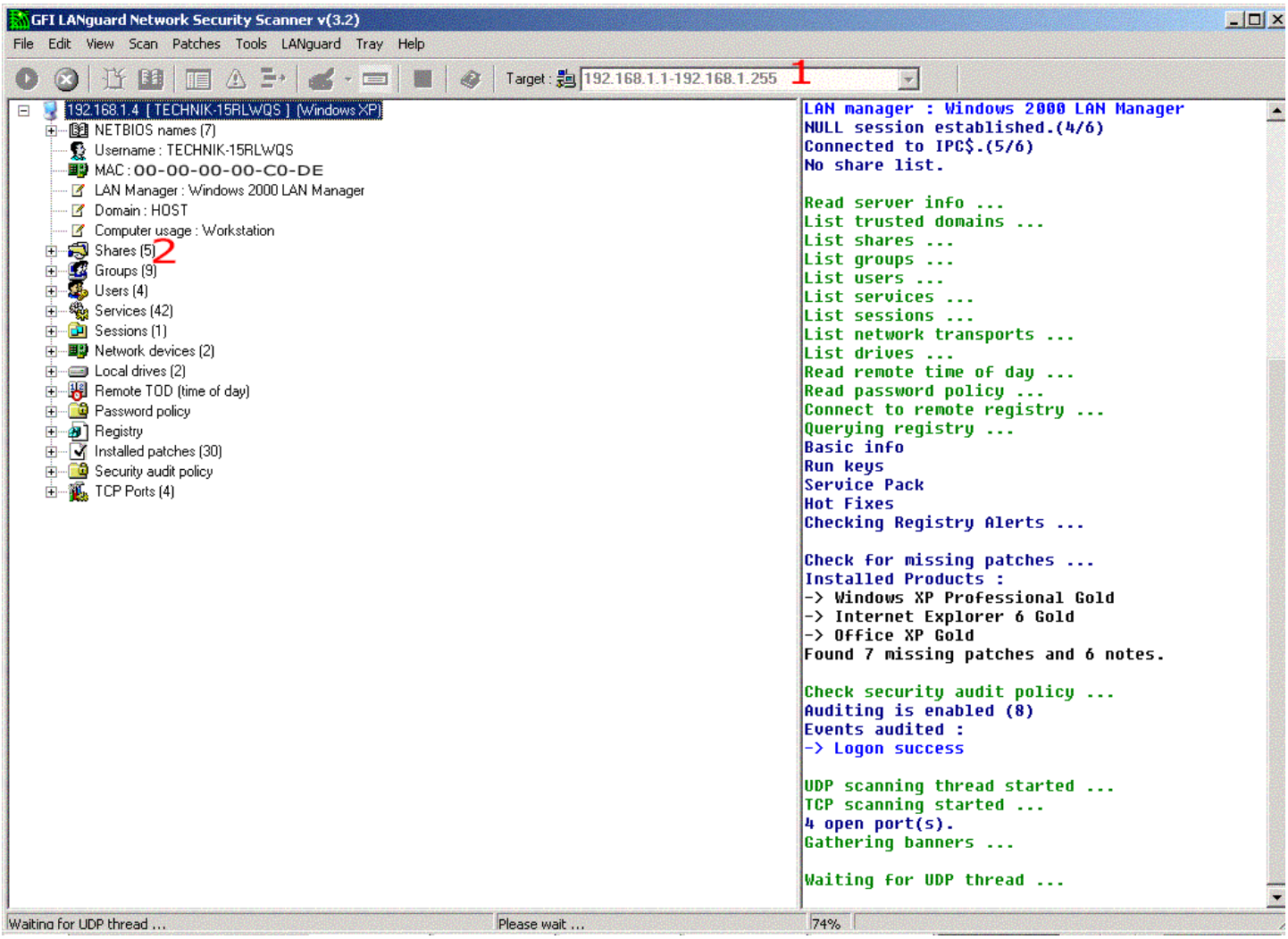
Dann ist wahrscheinlich DHCP deaktiviert. Versucht euch mal eine IP zuzuweisen. Dazu geht in eure Netzwerkeinstellungen unter Eigenschaften. Hier auf Internetprotokoll (TCP/IP) und auf Eigenschaften. Tragt die IP-Adresse (z.B. 192.186.1.4) oder eine andere ein und den Standartgateway (hier 192.168.1.1).

Jetzt noch mal in die DOS-Box und Ipconfig /renew eingeben. IP bekommen?! Super !

Geht es immer noch nicht könnte zusätzlich ein MAC Filter laufen, da geh ich jetzt mal nicht näher darauf ein...

So jetzt wir es interessant. Wir kennen unseren Adressbereich des Netzwerkes und wollen uns mal umschauen. Jetzt kommt der Languard ins Spiel:

Programm starten, den Adressbereich (1 .)eingeben und Start drücken.
Hier ist jetzt nur ein Rechner im Netz. Interessant sind die Shares (2.)



Klickt die Shares mal an, wartet einen Moment und schaut was passiert. Ist die Festplatte freigeben könnte jeder im Funknetz theoretisch auf die Daten zugreifen.

!! Gebt auch mal die gefundenen IP`s in euren Browser ein und schaut was passiert Mit etwas Übung solltet Ihr den euren Router schnell gefunden haben!!!