WLAN – "Hack"

Disclaimer:

Diese Anleitung soll Sie nicht dazu verleiten, kriminelle Tätigkeiten durchzuführen. Sie machen sich unter Umständen strafbar. Informieren Sie sich vorher im BDSG und TDSG und anderen relevanten Gesetzen über mögliche Verbote. Ich übernehme KEINE Verantwortung für einen Missbrauch. Die nachfolgende Beschreibung habe ich MIT Genehmigung des WLAN-Netzwerk-Eigentümers durchgeführt.

Beginnen wir:

Letzte Woche war ich mit meiner Freundin im Urlaub (Ferien auf dem Bauernhof). Da ich mich auch mal erholen wollte, entschied ich mich, nur zwei Notebooks, einen mobilen Drucker und mein neustes Spielzeug, den MDA III mitzunehmen.

Bei der Ankunft habe ich aus Spaß mal meinen MDA III auf WLAN-Betrieb gestellt und durch die Gegend geschleppt ... und Das Ergebnis: Zwei WLANs.



Das Bild zeigt den MDA III und mein Toshiba Notebook mit einer WLAN Verbindung. Das Problem war jetzt, das ich nicht so einfach eine WLAN Verbindung hergestellt bekommen habe, weil das Netzwerk dann wohl doch rudimentär geschützt war.

Eigentlich hatte ich mir ja vorgenommen, so einmal täglich das Internetcafe im Nachbarort aufzusuchen, aber da ich sah, das der Sohn unserer Vermieter jetzt WLAN hatte, fragte ich ihn, ob ich das WLAN nutzen kann (wir sind schon seit fast 8 Jahren einmal im Jahr dort zu Besuch). Scherzhaft sagte er, wenn ich wüsste, wie ich eine Verbindung herstellen kann, könnte ich seine Internet-Verbindung nutzen. Daraus machte ich dann eine Aufgabe und verzichtete auf die Bekanntgabe der Verbindungsdaten *gg* und stellte mich der Herausforderung, ein Netzwerk zu knacken (hatte ich bisher nur in Schulungsumgebungen gemacht).

Also den MDA III und das Toshiba Notebook für die Verwendung von WLAN konfiguriert.

WEP wurde nicht verwendet, nur ein MAC-Filter. Die SSIDs wurden auch angezeigt, It. XP Konfig und MDA III Konfig wurde kein WEP verwendet (was man ja auch leicht hätte knacken können, denn alle Tools hatte ich wie immer auf meinem Notebook dabei).

Also was tun? MAC-Adressen spoofen? Als erstes habe ich mal den Netzwerkmonitor angeschmissen und geschaut, was so alles passiert. Welcher Netzwerkmonitor – natürlich der von Windows (besser SMS 2003 – ist ja alles lizensiert):



Prima, da war doch schon mal etwas Verkehr im Netz 🗷

Die Details waren auch sehr aufschlussreich.

🖗 Micros	oft Netzw	erkmonitor - [Sammlur	ng: 2 (Zusammenfass	ung)]						_8×
🛺 Datei	Bearbeiter	n Anzeige Extras Opti	ionen Fenster ?							_6×
6	8 00	<u>eee</u> 6 2	Q 🔸 🕆 🌱 🗑	👌 🐴 (A) (A)	·]					
Rahnen	Zeit	MAC-Quelladresse	MAC-Zieladresse	Protokoll	Beschreibung		Andere Quelladresse	Andere Zieladresse	Andere Adr	esstypen 🔺
1	69	LOCAL	*BROADCAST	ARP_RARP	ARP: Request, Target IP: 172.16.0.19					
2	70	LOCAL	XER0X 000002	Bone	Security Check (0x03)					
3	70	LOCAL	*BROADCAST	ARP_RARP	ARP: Request, Target IP: 172.16.0.19					
4	71	LOCAL	*BROADCAST	ARP_RARP	ARP: Request, Target IP: 172.16.0.19					
5	72	LOCAL	*BROADCAST	NBT	NS: Registration req. for	<00≻	172.16.0.19	172.16.255.255	IP	
6	73	LOCAL	*BROADCAST	NBT	NS: Registration req. for the second	<00≻	172.16.0.19	172.16.255.255	IP	
7	74	LOCAL	*BROADCAST	NBT	NS: Registration req. for the second	<00>	172.16.0.19	172.16.255.255	IP	
8	74	LOCAL	*BROADCAST	NBT	NS: Registration req. for	<00>	172.16.0.19	172.16.255.255	IP	
9	75	LOCAL	*BROADCAST	NBT	NS: Registration req. for the second	<00>	172.16.0.19	172.16.255.255	IP	
10	76	LOCAL	*BROADCAST	NBT	NS: Registration req. for the second	<00>	172.16.0.19	172.16.255.255	IP	
11	??	LOCAL	*BROADCAST	MBT	NS: Registration req. for	<00≻	172.16.0.19	172.16.255.255	IP	
12	77	LOCAL	*BROADCAST	MBT	NS: Registration req. for addition	<00>	172.16.0.19	172.16.255.255	19	
13	79	LOCAL	*BROADCAST	NUT	NS: Registration req. for		172.16.0.19	172.16.255.255	IP	
14	79	LOCAL	*BROADCAST	NBT	NS: Registration req. for the second		172.16.0.19	172.16.255.255	19	
10	80	LOCAL	XE00X 000002	Bone	Security Check (0x03)		172 16 0 10	100 14 000 000	**	
10	80	LOCAL	*BROADCAST	NBI	NS: Registration req. for the con-		172.16.0.19	172.16.255.255	17	
17	01	LOCAL	-BROADCASI	ND I	NS: Regiscracion red. for the second		172.16.0.19	1/2.10.200.200	11	
10	100	LOCAL	XEROX 000002	Done	Security Check (0x03)					
19	100	00092D1103EF	*PROADCAST	bone papp	Security Check (0x03)					
20	106	0009201104FE	*DROADCASI	NRY_RAFY	Mar: Request, larget ir: 1	1005	1 and the second state of the second state of the	and the second secon	**	
5.A 2.2	106	000920110488	*BROADCAST	ADD DADD	ADD: Demiest Termet TD:	-00-		100 March 100 Ma	**	
23	106	000920110488	*BDOADCAST	NDT	MS: Degistration reg for the	<00>	We want to be a set of the set of	100.00	TD	
24	107	0009201104FF	*BROADCAST	NET	MS: Registration reg. for	000	1	NAME OF COMPANY	TD	
25	107	000920110AFE	*BROADCAST	NET	NS: Registration reg. for	<00>	and the second second second		TP	
26	107	000920110AFE	*BROADCAST	APP PAPP	APP: Remiest, Target IP: 40 445 12		Serie Party Series			
27	110	LOCAL	XER0X 000002	Bone	Security Check (0x03)					
28	113	00092D110AFE	*BROADCAST	DHCP	Discover (xid=DAE3DCOF)		0.0.0.0	255.255.255.255	IP	
29	120	LOCAL	XER0X 000002	Bone	Security Check (0x03)					
30	130	LOCAL	XER0X 000002	Bone	Security Check (0x03)					
31	140	LOCAL	XER0X 000002	Bone	Security Check (0x03)					
32	150	LOCAL	XER0X 000002	Bone	Security Check (0x03)					
33	160	LOCAL	XER0X 000002	Bone	Security Check (0x03)					
34	170	LOCAL	XEROX 000002	Bone	Security Check (0x03)					
35	180	LOCAL	XER0X 000002	Bone	Security Check (0x03)					
36	190	LOCAL	XEROX 000002	Bone	Security Check (0x03)					
37	200	LOCAL	XEROX 000002	Bone	Security Check (0x03)					
38	210	LOCAL	XEROX 000002	Bone	Security Check (0x03)					
39	220	LOCAL	XER0X 000002	Bone	Security Check (0x03)					
40	230	LOCAL	XER0X 000002	Bone	Security Check (0x03)					
41	231	LOCAL	*BROADCAST	ARP_RARP	ARP: Request, Target IP: 10.19.0.19					
42	232	LOCAL	*BROADCAST	ARP_RARP	ARP: Request, Target IP: 10.19.0.19					
43	233	LOCAL	*BROADCAST	ARP_RARP	ARP: Request, Target IP: 10.19.0.19					
44	234	LOCAL	*BROADCAST	ARP_PARP	ARP: Request, Target IP: 10.19.0.19					-
						5		la a china a		5 at at

Nach ein paar Versuchen mit den beiden WLANs habe ich eine SSID als nicht interessant befunden (keine Internet Verbindung möglich) und widmete mich der anderen SSID, wo MAC-Adressen Filterung aktiv war.

Ich musste jetzt nur noch ne MAC-Adresse ermitteln. Da meine WLAN-Karte vom Toshi Notebook zum Glück den ORiNOCO-Chipsatz hatte, konnte ich den NetStumpler anwenden. Einfach das Tool starten, nen paar Sekunden warten und dann werden Dir die SSIDs und MAC-Adressen angezeigt.



Dann habe ich mir eine MAC-Adresse aus dem Scan rausgesucht und dann musste ich nur noch ein Tool haben, mit welchem ich die MAC-Adresse meiner WLAN-Karte

"spoofen" kann. Dazu habe ich SMAC verwendet (ihr kennt die Werbung: Das smackt mir *z*).

🌾 SMAC 1.1 [WBEM On]							
<u>File</u> <u>A</u> bout							
ID	Active	Spoofed	Network Adapter	IP Address	Active MAC		
0001	Yes	No	Realtek RTL8139-Familie-PCI	0.0.0.0			
0002	Yes	No	Toshiba Wireless LAN Mini P		a terration of the second		
0013	Yes	No	Microsoft Loopbackadapter				
0021	Yes	No	Microsoft Loopbackadapter				
Show Only Active Network Adapters							
New Sp	oofed MA	AC Address		Update MAC	Refresh		
	-	-		Remove MAC	Exit		
Spoofed MAC Address							
			A				
KLC CONSULTING, INC							
Active MAL Address www.klcconsulting.net/smac							
Disclaimer: Use this program at your own risk. We are not responsible for any damage that might occur to your system. This							
program shorto be used to any negator directical purpose. Do not use this program in you do not agree with this discialmen.							

Einfach die ermittelte MAC-eintragen, updaten und dann geht es ab. Es gibt zwar noch andere Möglichkeiten, MACs zu fälschen, aber das ist doch für einen Windows User wie mich, ganz praktisch.

Auf meinem Windows XP Notebook werden alle Netzwerke angezeigt. HotelAir ist übrigens nicht das Netz, was ich erreichen wollte, sondern ein Hotspot aus einem Hotel wo ich vor ein paar Wochen war (Windows XP behält ja die Hotspots in seiner Liste *gg*).

🚣 Eigenschaften von Drahtlose Netzwerkverbindung	? ×						
Allgemein Drahtlosnetzwerke Erweitert							
☑ <u>W</u> indows zum Konfigurieren der Einstellungen verwenden							
Verfügbare Netzwerke: Klicken Sie auf die Schaltfläche unten, um eine Verbindung mit einem Drahtlosnetzwerk herzustellen oder zu trennen bzw. weitere Informationen über Drahtlosnetzwerke zu erhalten.							
Drahtlosnetzwerke anzeiger							
Bevorzugte Netzwerke: Verbindung automatisch mit den verfügbaren Netzwerken in der nachfolgend aufgeführten Reihenfolge herstellen: (Automatisch) (Automatisch) (Automatisch) (Automatisch) (Automatisch) (Automatisch)							
Hinzufügen Entfernen Eigenschaften							
Weitere Informationen über die <u>Einrichtung</u> <u>Er</u> weitert							
OK Abbre	chen						

Die Verbindung der WLAN Karten hatte ich mal auf DHCP gestellt und schon hatte ich eine IP – Danke lieber WLAN-Router. Ja, und das war es dann schon. Die Verbindung konnte hergestellt werden und ich konnte surfen (leider nicht immer, da das Netz nicht immer verfügbar war).

((j))Status von Drahtlose Netzwerkverbindung						
Allgemein Netzwerkunterstützung	1					
Verbindung Status: Netzwerk: Dauer: Übertragungsrate:	Verbindung hergestellt r 00:05:25 2,0 MBit/s					
Signalstärke:	UUUGa					
Gesendet —	Empfangen					
Pakete: 50	505					
Eigenschaften Deaktivieren	Drahtjosnetzwerke anzeigen					
	<u>S</u> chließen					

Der Sohn der Vermieter war sichtlich beeindruckt (und ich war auch ganz stolz auf mich, wie einfach so was ist). Ich musste ihm Schritt für Schritt erklären, was ich gemacht habe und daraus ist dieses "Tagebuch" entstanden.

Worauf ich verzichtet habe ist jetzt natürlich die Hauswand unseres Vermieters mit den notwendigen Zugangsdaten zu versehen, damit Wardriver schnell an die Zugangsdaten kommen.

Disclaimer:

Sollten Sie das ganze hier nachvollziehen wollen, stellen Sie sicher, dass Sie NICHT gegen geltende Gesetze verstossen und die Genehmigung des Netzwerkbetreibers haben. Sie machen sich sonst strafbar.