Essential Wireless Hacking Tools

digg_url = 'http://digg.com/security/Essential_Free_Wireless_Hacking_Tools';

| del.icio.us

Discuss in Forums {mos_smf_discuss:Hoffman}

By Daniel V. Hoffman, CISSP, CWNA, CEH

Anyone interested in gaining a deeper knowledge of wireless security and exploiting vulnerabilities will need a good set of base tools with which to work. Fortunately, there are an abundance of free tools available on the Internet. This list is not meant to be comprehensive in nature but rather to provide some general guidance on recommended tools to build your toolkit.

See Dan Hoffman Hack a Blackberry LIVE

at ChicagoCon 2007
Finding Wireless Networks

Locating a wireless network is the first step in trying to exploit it. There are two tools that are commonly used in this regard:

Network Stumbler a.k.a NetStumbler – This Windows based tool easily finds wireless signals being broadcast within range – A must have. It also has ability to determine Signal/Noise info that can be used for site surveys. I actually know of one highly known public wireless hotspot provider that uses this utility for their site surveys.

(NetStumbler Screenshot)

Kismet – One of the key functional elements missing from NetStumbler is the ability to display Wireless Networks that are not broadcasting their SSID. As a potential wireless security expert, you should realize that Access Points are routinely broadcasting this info; it just isn’t being read/deciphered. Kismet will detect and display SSIDs that are not being broadcast which is very critical in finding wireless networks.

(Kismet Screenshot)

Attaching to the Found Wireless Network

Once you’ve found a wireless network, the next step is to try to connect to it. If the network isn’t using any type of authentication or encryption security, you can simply connect to the SSID. If the SSID isn’t being broadcast, you can create a profile with the name of the SSID that is not being broadcast. Of course you found the non-broadcast SSID with Kismet, right? If the wireless network is using authentication and/or encryption, you may need one of the following tools.

Airsnort – This is a very easy to use tool that can be used to sniff and crack WEP keys. While many people bash the use of WEP, it is certainly better than using nothing at all. Something you’ll find in using this tool is that it takes a lot of sniffed packets to crack the WEP key. There are additional tools and strategies that can be used to force the generation of traffic on the wireless network to shorten the amount of time needed to crack the key, but this feature is not included in Airsnort.

(Screenshot of Airsnort in Action)

CowPatty – This tool is used as a brute force tool for cracking WPA-PSK, considered the “New WEP” for home Wireless Security. This program simply tries a bunch of different options from a dictionary file to see if one ends up matching what is defined as the Pre-Shared Key.

(Cowpatty Options Screenshot)

ASLeap – If a network is using LEAP, this tool can be used to gather the authentication data that is being passed across the network, and these sniffed credentials can be cracked. LEAP doesn’t protect the authentication like other “real” EAP types, which is the main reason why LEAP can be broken.

(Asleap Options Screenshot)

Sniffing Wireless Data

Whether you are directly connected to a wireless network or not, if there is wireless network in range, there is data flying through the air at any given moment. You will need a tool to be able to see this data.

Wireshark (formerly Ethereal) – While there has been much debate on the proper way to pronounce this utility, there is no question that it is an extremely valuable tool. Ethereal can scan wireless and Ethernet data and comes with some robust filtering capabilities. It can also be used to sniff-out 802.11 management beacons and probes and

subsequently could be used as a tool to sniff-out non-broadcast SSIDs.

(Screenshot of Ethereal in Action)

(Yahoo IM Session being sniffed in Ethereal)

The aforementioned utilities, or similar ones, will be necessities in your own wireless security toolkit. The easiest way to become familiar with these tools is to simply use them in a controlled lab environment. And cost is no excuse as all of these tools are available freely on the Internet.

Protecting Against These Tools

Just as it’s important to know how to utilize the aforementioned tools, it is important to know best practices on how to secure your Wireless Network Against these tools.

NetStumbler – Do not broadcast your SSID. Ensure your WLAN is protected by using advanced Authentication and Encryption.

Kismet – There’s really nothing you can do to stop Kismet from finding your WLAN, so ensure your WLAN is protected by using advanced Authentication and Encryption

Airsnort – Use a 128-bit, not a 40-bit WEP encryption key. This would take longer to crack. If your equipment supports it, use WPA or WPA2 instead of WEP (may require firmware or software update).

Cowpatty – Use a long and complex WPA Pre-Shared Key. This type of key would have less of a chance of residing in a dictionary file that would be used to try and guess your key and/or would take longer. If in a corporate scenario, don’t use WPA with Pre-Shared Key, use a good EAP type to protect the authentication and limit the amount of incorrect guesses that would take place before the account is locked-out. If using certificate-like functionality, it could also validate the remote system trying to gain access to the WLAN and not allow a rogue system access.

ASLeap – Use long and complex credentials, or better yet, switch to EAP-FAST or a different EAP type.

Ethereal – Use encryption, so that anything sniffed would be difficult or nearly impossible to break. WPA2, which uses AES, is essentially unrealistic to break by a normal hacker. Even WEP will encrypt the data. When in a Public Wireless Hotspot (which generally do not offer encryption), use application layer encryption, like Simplite to encrypt your

IM sessions, or use SSL. For corporate users, use IPSec VPN with split-tunneling disabled. This will force all traffic leaving the machine through an encrypted tunnel that would be encrypted with DES, 3DES or AES.

Questions or comments can be sent to Daniel V. Hoffman, CISSP, CWNA

danielvhoffman@yahoo.com