asleap-imp - recovers weak LEAP password. Pronounced "asleep".
Copyright(c) 2004, Joshua Wright <jwright@hasborg.com>
$Id: README.WIN32,v 1.3 2004/03/28 15:37:02 jwright Exp $
Espero haber medio traducido comprensiblemente el texto original, por ello el no borrarlo, para no desvirtuar mi possible mala traduccion.
Suerte (Juan: www.websecurenet.tk)

USING ASLEAP ON WINDOWS

I have successfully compiled and tested the asleap and genkeys tools under the cygwin environment on Windows XP sp1, using the WinPcap developer's pack (winpcap.polito.it).

Since there are no openly available drivers for RFMON packet capture on Windows systems (or packet injection), Windows users can't take advantage of most of the asleap features that scan for vulnerable LEAP networks. However, I have added functionality to read from AiroPeek NX files. If you are lucky enough to own a copy of AiroPeek NX (I do not), you can use it to capture a LEAP exchange and save it to a file. Pass the .apc file to asleap with the "-r" command line parameter. If you have WinPcap files captured from a different system, you can extract LEAP password from them as well, using the same "-r" parameter.

He compilado y probado con éxito el asleap y las herramientas de los genkeys bajo entorno del cygwin en Windows.xp sp1, usando el paquete de WinPcap developer's (winpcap.polito.it). Puesto que no hay drivers para la captura del paquete de RFMON en los sistemas de Windows (o inyección del paquete), los usuarios de Windows no pueden aprovecharse de la mayoría de las características del asleap que exploran vulnerabilidades en redes con protocolo LEAP. Sin embargo, he agregado funcionalidades para leer en los archivos de AiroPeek NX. Si usted es afortunado y posee una copia de AiroPeek NX (no), puede utilizarla para capturar un intercambio del LEAP y para grabarlo en un archivo. Pase el archivo .apc al asleap con el parámetro "-r" en línea de comando . Si tiene archivos de WinPcap capturados de diferente sistema, puede extraer contraseña del LEAP de ellos también, usando el mismo parámetro "-r".

COMPILING ASLEAP ON CYGWIN

If you want to compile asleap for Windows, follow these steps:

1. Download and install WinPcap. I used version 3.0.
2. Download and install cygwin. Be sure to install the win32api package and development tools.
3. Download and unzip the WinPcap developer's pack.
4. Edit the file makefile.cygwin and change the WPDPACK line to reflect the path where you extracted the WinPcap developer's pack.
5. Run "make -f makefile.cygwin" to build the tools.

If you transfer the asleap.exe and genkeys.exe files to another system that doesn't have cygwin installed, you'll also need to copy the files cygwin1.dll and cygcrypt-0.dll files.

Si usted desea compilar el asleap para Windows, siga estos pasos:

1. Descargue e instale WinPcap. Utilicé la versión 3.0.
2. Descargue e instale el cygwin. Esté seguro de instalar el paquete de win32api y las herramientas de desarrollo.
3. Descargue y descomprima el paquete de WinPcap developer's.
4. Edite el archivo makefile.cygwin y cambie la línea de WPDPACK para reflejar el path donde usted extrajo el paquete de WinPcap developer's.
5. Ejecute "make - f makefile.cygwin" para construir las herramientas. Si usted transfiere los archivos de asleap.exe y de genkeys.exe a otro sistema que no tenga cygwin instalado, también necesitara copiar los archivos cygwin1.dll y cygcrypt-0.dll.

INSTALLATION

Simply running "make" will compile the genkeys and asleap tools. If you want to actively deauthenticate users on wireless networks, you will need the AirJack drivers from http://802.11ninja.net/. Reading from a live interface or from a capture file requires the interface/capture to be in RFMON mode (DLT_IEEE802_11). You can also supply an AiroPeek NX capture file if you have that tool available (just pass the filename to asleap with the "-r" flag).

Simplemente ejecute "make", compilará los genkeys y las herramientas del asleap. Si usted desea activamente [deauthenticate] a los usuarios de la red WiFi ,necesitará los "drivers" de AirJack de http://802.11ninja.net/. lectura de un interfaz vivo o de captura un archivo

requiere el interface/capture estar en el modo de RFMON (DLT_IEEE802_11). Puede también proveer un archivo de la captura de AiroPeek NX si tiene esta herramienta disponible (pasa justo el nombre de fichero al asleap con el parametro "-r").

QUESTIONS, COMMENTS, CONCERNS

Please contact jwright@hasborg.com with any questions, comments on concerns.
My PGP key is located at http://home.jwu.edu/jwright/pgpkey.htm.

900bf728765bc0dd4ec50f77fd601862 *asleap-1.0win32.zip