Njepat Wireless Hacking Tools
User Guide

© njepat crew
codename: NKRI

by: Xsan-Lahci
Introduction

Njepat Wireless Hacking Tools – V1
User Guide

Document Version : 1.0 – Tested On Backtrack 5R3 - Gnome
Coded By : Xsan-Lahci | idea name : 4J4l 13

Report Bugs : xsanlahci[at]gmail.com
Website : xsanlahci.org / xsanlahci.tv / xsanlahci.wordpress.com
Table of Contents

Cover
Introduction
Table of Contents
Requirements Tools
How to used
Thanks To

..........................................................
..........................................................
..........................................................
..........................................................
..........................................................
..........................................................
Requirements Tools

The required packages to run NWHT:

[+] Script Inside [+] 

- **Auto WPACrack-ng**
  - Airmon-ng
  - Airodump-ng
  - Aireplay-ng
  - Aircrack-ng
  - Kismet

- **Auto WPA2Crack-ng**
  - Airmon-ng
  - Airodump-ng
  - Aireplay-ng
  - Aircrack-ng
  - Kismet

- **WGUI (Wireless Hacking GUI)**
  - FernWifi Cracker
  - Grimwepa
  - Gerix Wifi Cracker
  - Airoscript-ng GTK
  - Evil Twin Tool

- **Auto Reaver (reaverX)**
  - reaver

- **Wifihoney.sh**

- **ANTM (Auto Network Traffic Monitoring)**
  - netdiscover
  - kismet
  - TCP-dump
  - etherape
  - airodump-ng
  - ssidsniff
  - airmon-ng

- **ANST (Auto Network Stress Testing)**
  - Airmon-ng
  - mdk3
  - flood_router6
○ aireplay-ng
○ smurf6
○ RocketLauncher.sh
  ~ t50
  ~ hping3
  ~ udp.pl
  ~ inviteflood
  ~ siege
  ~ inundator
  ~ mac0f
  ~ arp-flood.py
  ~ airmon-ng
  ~ etterD0sX.sh
• ANFT (Auto Network Forensics Toolkit)
  ○ wireshark
  ○ netcutkiller
  ○ driftnet
  ○ p0f
• Another Tools
  ○ WiPhire
  ○ wifite.py
  ○ macchanger
  ○ Wifi-jammer.sh
  ○ Find Hidden Wireless
    ▪ airmon-ng
    ▪ airodump-ng
    ▪ mdk3
  ○ AirFakeAP-ng
    ▪ airmon-ng
    ▪ Configuration dhcpd
    ▪ airbase-ng
  ○ Wish
  ○ airmon-ng

Tutorial

1. AutoWPAcrack-ng
root # ./NWHT-V1
and clink OK
1) Cracking wifi WPA
Choose number one

Next Image Please choose your Target Access Point Like This
ok Please check this out

WPA > 2

Warning After you running this step,dont forget to stop it (ctrl+c)

BSSID Target : 84:A8:E4:AF:66:5F
Channel Target : 6
Next Step Please check this image

Airodump-ng will running with specific target and will capture package for get WPA-Handshake like this
The next step .. please Write BSSID and Station on gedit/nano

Running Aireplay-ng
and boom :D

oke after you run aireplay-ng and running deauth attack you will get WPA-Handshake like this image
Lets cracking this file .cap :D with aircrack-ng

more info http://xsanlahci.org/2013/05/08/backtrack-5r3-wireless-hacking-wpa/
2) Cracking Wifi WPA2 with WPA2CRACK-NG

1. choose number 2

2. Choose Active mon0.
3. Choose number 2 for Running Airodump-ng for choose target

4. Choose Number 3 For Specific Target and capture package
Look the blue line :D you need WPA-Handshake , please running Aireplay-ng

5. Aireplay-ng For Deauth attack

:D I got WPA-Handshake bro.. lets prepare aircrack-ng
6. Aircrack-ng .ivs cracking

Keyfound : x$an-l@hci
3) Wireless Hacking GUI
Inteface About WGUI

1. Fern Wifi Cracker
2. GrimWepa


3. Gerix Wifi Cracker

4. Airoscript-ng GTK

5. EvilTwin Tool
4) WPS Hacking Tool

- ReaverX-Auto Reaver easy Usage
5) Wifi Honey

Five ESSID Has been Created
6) Auto Network Traffic Monitoring - ANTM
Menu:

- **Netdiscover**

- **Kismet**

- **TCP-dump**
• EtherApe
- **SSIDNSIFF**
7) Network Stress Testing

Note: Before you running this script please Active mon0 interfaces

3) Flood Wireless with Fake AP

Insert your interface: (wlan0/eth0)>> wlan0

wlan0     Scan completed:
Cell 01 - Address: 84:A8:E4:AF:66:5F
Channel:1
Frequency:2.412 GHz (Channel 1)
Quality=70/70  Signal level=-27 dBm
Encryption key:on
ESSID: "Mr.g00gle"

Insert Mac Address / BSSID target: >> 84:A8:E4:AF:66:5F

Wait :D and Boom

8) Auto Network Forensics Toolkit (ANFT)
Another Tools For Wireless Hacking

Welcome To Another Tools For Wireless Hacking
Coded By xsan-lahci

^_^ ^\+^ */++*

> codename : Spizaetus bartelsi

Select From Menu :
1) WiPhire
2) wifi.py
3) macchanger
4) Wifi-Jammer
5) Create Fake Access Point
6) Find Hidden Wireless
7) Wifi Protected Setup Scan Tool
8) Activate mon0
9) Stop mon0 Interface
0) Back to Menu

9 ) Another Tools For Wireless Hacking

Thanks To :
Thanks for your nice ideas and help to make this tool more useful, My God
My Teacher Zee Eichel, Ikonspirasi, Mywisdom
Nice Idea For Name AJ4l_13
All My Friends [at] facebook thanks for your suport
My Forum > IBTeam (indonesianbacktrack.or.id) | indonesian blackhat (idblackhat.org) | BNT (forum.blacknewbieteam.org) | MadLeets (madleets.com) | forummikrotik.com

[My Forum = My Family]