Hacking Wi-Fi

CATALIN BOJA

CATALIN.BOJA2IE.ASE.RO, WWW.ISM.ASE.RO

Hacking a Wireless Network

- Needed tools
  - A Wi-Fi board that can do packet injection (https://null-byte.wonderhowto.com/how-to/buy-best-wireless-network-adapter-for-wi-fi-hacking-2019-0178550/)
  - Aircrack-ng (https://www.aircrack-ng.org/doku.php?id=Main)
- Hacking WEP
- Hacking WPA2
- Hacking WPS
- DoS on the Wi-Fi router in order to force the user to reset it

Hacking a Wireless Network

Set the Wi-Fi board in monitor mode

#set bord in monitor mode

- ifconfig wlan1 down
- iwconfig wlan1 mode monitor
- ifconfig wlan1 up

#check for possible problems

- airmon-ng check wlan1

Hacking a Wireless Network - WEP

- Wired Equivalent Privacy (WEP) - a security algorithm for IEEE 802.11 wireless networks introduced in 1997
- replaced in 2003 by Wi-Fi Protected Access (WPA)
- had a security vulnerability in the way the algorithm was used
  - Standard 64-bit WEP uses a 40 bit key (also known as WEP-40), which was concatenated with a 24-bit initialization vector (IV) to form the RC4 key
  - The key was composed from ASCII symbols
  - The router can be forced to reset IV

Hacking a Wireless Network - WEP

Involves 4 steps

1. Capture the handshake
2. Inject packets – deauthentication requests
3. Capture Authentication Requests replies
4. Brute force WEP key based on captured packets

Hacking a Wireless Network - WPA

- Wi-Fi Protected Access (WPA), Wi-Fi Protected Access II (WPA2) introduced in 2003
- hacking WPA/WPA2 is a very tedious job in most cases.
- A dictionary attack may take days, and still might not succeed.
  - good dictionaries are huge
  - a brute force including all the alphabets (uppercase lowercase) and numbers, may take years, depending on password length
  - Rainbow tables can speed things up but they have huge sizes (hundreds of GBs).
- https://www.kalitutorials.net/2015/10/wpawpa-2-cracking-using-dictionary.html

Hacking a Wireless Network - WPA

Involves 2 steps

- Capture the handshake
- Crack the handshake to get the password
  - using a dictionary attack
  - aicrack-ng

Hacking a Wireless Network - WPA

- WPA2 has been attacked using an implementation flaw in devices – KRACK - **K**ey **R**einstallation **A**tta**ck**s (https://www.krackattacks.com/)
- More efficient approaches are based on hacking the WPS Pin
- Social engineering attacks may prove more efficient – Fluxion, https://github.com/FluxionNetwork/fluxion
  - https://www.kalitutorials.net/2016/08/hacking-wpawpa-2-without.html

Hacking a Wireless Network - WPS

- WPS (Wi-Fi Protected Setup)
- Introduced in 2006 by the Wi-Fi Alliance, https://en.wikipedia.org/wiki/Wi-Fi_Protected_Setup
- major security flaw was revealed in December 2011 (https://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf)
  - No external intervention is needed by the users
  - The service is enabled by default
  - The authentication requires a 8 digit pin value but the maximum possible authentication attempts is reduce from 10^8 (=100.000.000) to 10^4 + 10^4 (=20.000) – the algorithm checks only half of the provided pin

Hacking a Wireless Network - WPS

1. Set the Wi-Fi card to monitor mode
2. Check for Wi-FI AP (Access Points) using
   - airodump-ng
   - wash
3. Brute force the WPS pin using
   - reaver
   - bully (https://null-byte.wonderhowto.com/how-to/hack-wi-fi-breaking-wps-pin-get-password-with-bully-0158819/)

- Wait for it

Hacking a Wireless Network - WPS

- WPS default pins are generated by an algorithm that starts with an initial value (in most cases determined by the router MAC address
- The algorithm can be reversed
  - https://wpsfinder.com/wps-pin-generator
  - http://wpspinleri.blogspot.com/p/wps-default-pin-generator.html
  - https://3wifi.stascorp.com/wpspin

Hacking a Wireless Network - WPS

Other resources:

- https://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf
- https://null-byte.wonderhowto.com/how-to/hack-wi-fi-breaking-wps-pin-get-password-with-bully-0158819/

Hacking a Wireless Network - DoS

- Very difficult to protect against
- De-authenticate some or all clients of a Wi-Fi router making the service unavailable
- Tools needed
  - airodump-ng
  - aireplay-ng
- Will force the user to reset the router