Ethical Hacker 10 – Wireless Hacking

* **Crack WPA (2) with airmon-ng and aircrack-ng from Kali Linux**.

I have downloaded a new kali virtual machine using this link: [https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/](https://eur01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.offensive-security.com%2Fkali-linux-vm-vmware-virtualbox-image-download%2F&data=04%7C01%7Cf.pana%40student.fontys.nl%7C617e498c0bf14179a54708d98e354c4c%7Cc66b6765b7944a2b84ed845b341c086a%7C0%7C0%7C637697182641574247%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000&sdata=2wyc%2BX%2F5r9PJhmoTUGr%2FU9DuisA1r8Vm5Go9LWS8Ecs%3D&reserved=0)

I have installed it and entered it. Afterwards, I have used s WiFi USB-stick Netgear WNA1100, which I have borrowed from the ISSD.

Afterwards, I have started the wireless interface using airmon-ng:

Graphical user interface, application

Description automatically generated

Then, I am typing iwconfig to make sure there are no other athX interfaces.

Text

Description automatically generated with medium confidence

Using airmon-ng again, this time in order to start the wireless card on channel 9 in monitor mode:

Text

Description automatically generated

Using airodump-ng to discover the information I need from the wi fi network that I am about to attack: megabeast1:

A picture containing text

Description automatically generated

Copying the authentication handshake and pasting it next to the capture instruction from airodump-ng:

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

The handshake has happened after opening a separate terminal and using the aireplay-ng instruction along with the authentication handshake. The initial terminal is notified and displays the WPA handshake on the botton left of the screenshot:

Graphical user interface, text

Description automatically generated

After obtaining the needed information and creating the handshake, I can now stop wlan0mon and move on to the next step: unzipping the rockyou.txt file:

A screenshot of a computer

Description automatically generated with medium confidence

Using the aircrack-ng instruction to start the password cracking process:

Text

Description automatically generatedText

Description automatically generated

The process has started, the program tries different elements of the rockyou file until it finds the one that matches the actual password. In this case, the correct password is Zanzibar and it has been cracked after 2 minutes and 57 seconds.

A screenshot of a computer

Description automatically generated with medium confidence