# Oppsett av WLAN og hacking

Gruppe 20

av

Pål, Ola og Kristoffer

i

IKT106

Nettverksadministrasjon

Veiledet av Erlend Fredriksen

Fakultet for teknologi og realfag

Universitetet i Agder

Grimstad, Mars 2020

# Innhold



# Figurer

# Introduksjon

I denne oppgaven skal vi sette opp et trådløst aksesspunkt og gi det et 11 siffer passord. Etterpå skal vi bruke diverse verktøy til å finne info om nettverket som ESSID, BSSID osv. Når alt det var gjort måtte vi sette nettverkskortet vår i monitor mode for så å bruke airodump-ng å fremtvinge en handshake mellom AP og klienten. Når vi får en handshake skal vi prøve og knekke passordet med aircrack-ng.

# 1 Konfigurer trådløse nettverk

Power over Ethernet eller PoE beskriver flere forskjellig standarer og ad hoc systemer der elektrisitet sammen med data på twisted pair Ethernet kabling. Dette tillater at en enkel kabel kan føre både elektrisitet og data til enheter som f.eks. Aksesspunkter som er tilfelle i denne oppgaven[3].

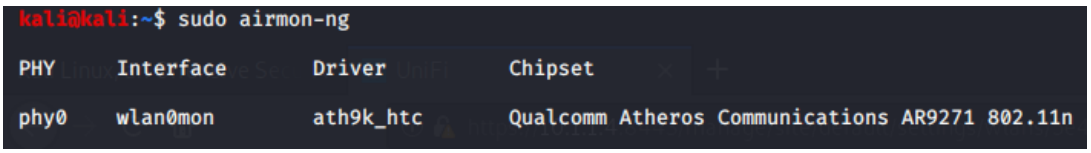
For å sette opp APen, så måtte vi endre PoE porten vår tilbake til LAN fra VLAN som vi satte opp i oppgave 3. Etter det fikk vi en IP til APen og SSHet inn på APen med SSH admin@10.1.1.7"og brukte set-inform commanden som i oppgave 3.

Når alt var adopta gikk vi innpå settings->Wireless network"og la til et nettverk og endret det sånn at 2.4G og 5G fekk individuele navn. Vi satte også opp et WPA2 passord på 11 siffer med 1-4 som tegn. Den opprinnelige oppgaven sa 9 tegn, men fordi vi er dårlige til å telle så vi endte opp på 11.

# 2 Sjekk nettverkskort

Vi hadde en del problemer med denne oppgaven, fordi vi oppdaget at driveren som var installert på nettverkskortet ikke var støttet av Kali-5.4.0. oppdatering av denne driveren var litt for avansert for oss.

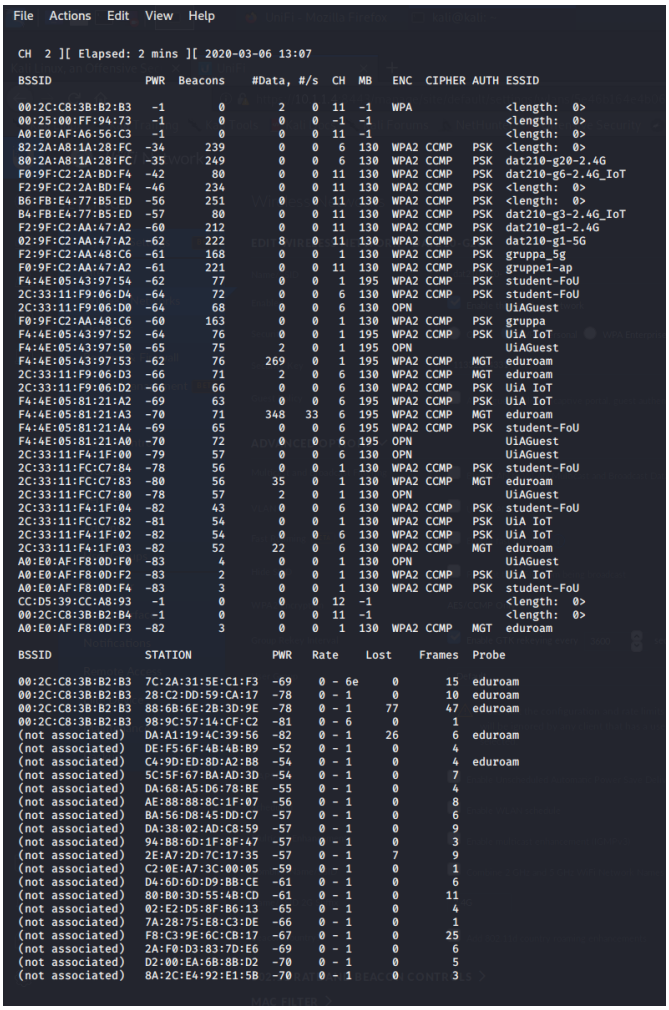
Vi fikk tilslutt et nettverkskort som hadde en nyere driver som Kali-5.4.0 støttet. Da gikk vi inn i terminalen og skrev “airmon-ng”



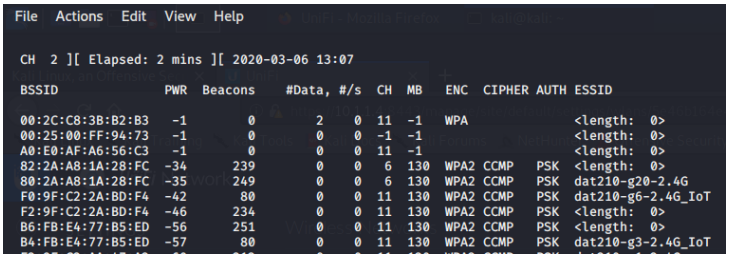

**Figur 1:** Airmon-ng

Når vi fant interface navnet til nettverkskortet vårt brukte vi kommandoen “sudo airmon-ng start wlan0mon”, men dette ble et problem senere i oppgaven siden vi ikke spesifiserte hvilken kanal den skulle på. Monitoring lar en datamaskin med wireless network interface controller monitere all trafikk motatt på en trådløs kanal[2].

# 3 Vurder trådløs nettverk




**(a)** Airodump alle




**(b)** Airodump gruppe20

**Figur 2:** Airodump

Det første bildet er en skjermdump av airodump.ng kommandoen. Her er alle nettverkene som nettverkskortet 'ser' listet opp. Som en ser så bruker alle nettverkene kanal 1,6 og 11. Dette er for å minimere støy mellom nettverkene. Man ser også at alle nettverkene utenom UIAGuest bruker WPA2 og UIAGuest bruker OPN.

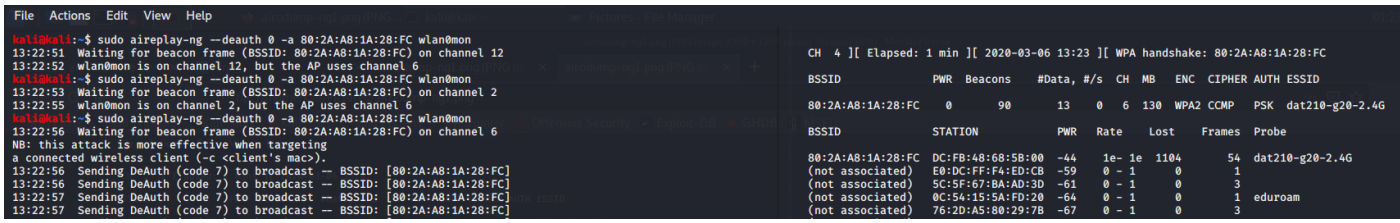
Alle nettverk som bruker WPA2 anser vi som trygge, men selv om det kjører WPA2 så er de ofte bakoverkompatible WPA1 som har en del sikkerhetsfeil. Et nettverk som bruker MGT auth key er enklere og forsvare siden alle har eget brukernavn og passord for å komme seg inn. Dersom en bruker blir kompromittert på noen måte, holder det å stenge brukeren istedenfor å bytte passord for alle. Sikkerhetsprotokollene som man ser er brukt i airodump-bildet er regnet som sikre, men det kan allikevel være WPA1 er brukt i bakgrunnen, som da gjør nettverket usikkert.

# 4 Finn informasjon om målet

Vi satt opp nettverket vårt til å ha ESSID til dat210-g20-2.4G og fant den tilhørende BSSID'en via airodump bildet BSSIDen vår høre til Ubiquiti Networks Inc. dette fant vi ut med å bruke nettsiden aruljohn.com[1].

# 5 Sniff kryptert passord

Før vi startet denne oppgaven måtte vi sette nettverkskortet vårt i monitor mode med kommanden iwconfig wlan0mon mode Monitor. Etter dette var gjort brukte vi "Airodump-ng –essid dat210-g20-2.4G" for å kun holde øye med vårt nettverk. Problemet med dette er at det kan ta tid før vi får en handshake, så vi tvinger det fram med "aireplay-ng -deauth 0 -a 80:2A:A8:1A:28:FC wlan0mon".

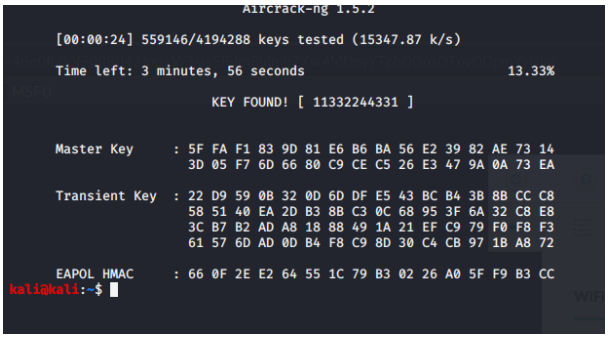



**Figur 3:** Handshake

# 6 Knekk det krypterte passordet

siden vi fikk til oppgave 5 så går vi videre til å prøve å knekke passordet, men før vi begynner må vi lage en ordlist av passord med kommanden "crunch 11 11 1234 -o ordliste.txt" for å lage alle mulige kombinasjoner av 1234 11 ganger og lagre det i ordliste.txt.

så testet vi ordliste.txt oppmot informasjonen vi fikk av handshaken.




**Figur 4:** Fant passordet

Når vi ser på hvor fort en datamaskin går gjennom et 11 siffer passord med 4 karakterer, så ser en kor viktig det er å bruke lange passord med flere karakterer.

# 7 Konklusjon

Etter å ha utført oppgaven har vi innsett hvor viktig det er med gode passord med god variasjon av tegn, og hvor lett det er å knekke et dårlig passord. Iløpet av denne oppgaven lærte vi også hvordan man kjører et operativsystem (Kali i denne sammenheng) fra en minnepenn.

# Referanser

[1] Arul's utilities. *MAC Address and OUI Lookup*. URL: https://aruljohn.com/mac/802AA81A28FC.
[2] Wikipedia. *Monitor mode*. URL: https://en.wikipedia.org/wiki/Monitor_mode.
[3] Wikipedia. *Power over Ethernet*. URL: https://en.wikipedia.org/wiki/Power_over_Ethernet.