Wifi-Analyse – WPA2

# 

Contents

[Problemstilling 3](#_Toc494198509)

[Fremgangsmetode 3](#_Toc494198510)

[Hvorfor gør vi dette / Hvad får vi ud af det? 3](#_Toc494198511)

[Password sikkerhed. 4](#_Toc494198512)

[Kryptering. 4](#_Toc494198513)

[Password politikker 4](#_Toc494198514)

[Connection handshake (the weakest link) 4](#_Toc494198515)

# Problemstilling

Svagheder omkring WPA2 Personal, I dette indgår der f.eks. password sikkerhed, politikker, kryptering og generel opbygning af connections.

Hvordan bliver disse udnyttet af hackere til at få fat i personlige oplysninger omkring den enkelte client, og hvordan kan man sikre sig imod det.

# Fremgangsmetode

Vi vil, ved brugen af en Wifi-Pineapple (nano), se hvor let det er at komme igennem WPA2 sikkerheden og tjekke på hvilke angrebs vektorer den kommer igennem, for at kunne sikre sig imod disse former for angreb (Man in the middle).

# Hvorfor gør vi dette / Hvad får vi ud af det?

Ved at gøre dette bliver vi mere opmærksom på sikkerhed ved netværk. Ved at forsøge og bryde WPA2’ netværksprotokolen ned og angribe den fra så mange vektorer som muligt vil vi kunne bruge denne erfaring.

Vi vil kunne bruge den erfaring til at skrive bedre kode. Der eventuelt bliver bedre struktureret, så den kan håndtere angreb, men stadig være robust.

Ved brugen af access modifieres vil vi kunne sikre vores fremtidige kode imod ”cheat engine” og andre programmer der går ind og ændre i variabler som den ikke skulle have adgang til.

Dette gør det også nemmere for andre programmører der skal rette i vores kode, da de ikke bliver forvirret af en masse variabler der ikke har noget med deres opgave at gøre.

# Password sikkerhed.

Password sikkerhed er en ubeskrivelig vigtig del af vores teknologiske verden

## Kryptering.

Sha

Rsa

Md5

## Password politikker

# Connection handshake (the weakest link)