BEZIT – 8. cvičení

Radek Janoštík

Univerzita Palackého v Olomouci

3. 4. 2024

Wi-Fi Protected Access(WPA)

- Z roku 2002 – Dočasná nástupce WEP (podpora tehdejšího HW)
- Rozšířena podpora autentizace (EAP, WPA Enterprise – 802.1x – přemostění na RADIUS server)
- Šifrování stejně slabé jako u WEP, vylepšeno přidán proměnlivý klíč

Wi-Fi Protected Access(WPA)

- Z roku 2002 – Dočasná nástupce WEP (podpora tehdejšího HW)
- Rozšířena podpora autentizace (EAP, WPA Enterprise – 802.1x – přemostění na RADIUS server)
- Šifrování stejně slabé jako u WEP, vylepšeno přidán proměnlivý klíč
- Integrita dat chráněna proti „inteligentnímu útočníkovi“
  - 64b kód za daty
  - Klient i AP mají svůj klíč – obdoba digitálního podpisu
  - Při narušení dojde k deasociaci

Wi-Fi Protected Access(WPA)

- Z roku 2002 – Dočasná nástupce WEP (podpora tehdejšího HW)
- Rozšířena podpora autentizace (EAP, WPA Enterprise – 802.1x – přemostění na RADIUS server)
- Šifrování stejně slabé jako u WEP, vylepšeno přidán proměnlivý klíč
- Integrita dat chráněna proti „inteligentnímu útočníkovi“
  - 64b kód za daty
  - Klient i AP mají svůj klíč – obdoba digitálního podpisu
  - Při narušení dojde k deasociaci
- WPA-PSK (Pre-Shared Key) – šifrovací klíče generovány(4096 hashů) z předsdíleného klíče a SSID
  - Při znalosti hesla a odchycení úvodního „handshake“ lze snadno dopočítat

Wi-Fi Protected Access(WPA)

- Z roku 2002 – Dočasná nástupce WEP (podpora tehdejšího HW)
- Rozšířena podpora autentizace (EAP, WPA Enterprise – 802.1x – přemostění na RADIUS server)
- Šifrování stejně slabé jako u WEP, vylepšeno přidán proměnlivý klíč
- Integrita dat chráněna proti „inteligentnímu útočníkovi“
  - 64b kód za daty
  - Klient i AP mají svůj klíč – obdoba digitálního podpisu
  - Při narušení dojde k deasociaci
- WPA-PSK (Pre-Shared Key) – šifrovací klíče generovány(4096 hashů) z předsdíleného klíče a SSID
  - Při znalosti hesla a odchycení úvodního „handshake“ lze snadno dopočítat
- Šifrování pomocí Temporal Key Integrity Protocol(TKIP)
  - RC4 šifra – klíč 128b – dvojí hash tajného klíče (104b), pořadového čísla rámce (32b) a MAC
  - Dále hash s iniciálním vektorem

Prolomení WPA

- Pro prolomení WPA PSK potřebujeme zachytit *Four-way handshake*
- Můžeme čekat až se někdo připojí a odposlechnout
- Nebo začít poslouchat a provést deautentizační útok

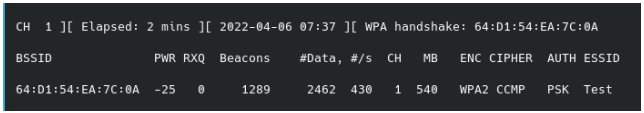
```
airodump-ng --channel 1 --bssid C4:AD:34:25:79:B1 --write soubor
                        --output-format pcap wlan1mon
```

Prolomení WPA

- Pro prolomení WPA PSK potřebujeme zachytit *Four-way handshake*
- Můžeme čekat až se někdo připojí a odposlechnout
- Nebo začít poslouchat a provést deautentizační útok

```
airodump-ng --channel 1 --bssid C4:AD:34:25:79:B1 --write soubor
                        --output-format pcap wlan1mon
```

- O zachycení handshake se dozvíme v pravém horním rohu



- Nyní můžeme přejít k offline prolomení klíče
- Situace je náročnější, musíme použít slovník či bruteforce

Prolomení WPA

- `aircrack-ng` má parametr `-w`, kterým specifikujeme slovník
  `aircrack-ng -w rockyou.txt wpa.cap`
- Známý slovník rockyou `https://github.com/brannondorsey/naive-hashcat/releases/download/data/rockyou.txt`
- $\approx$ 14 milionů hesel, $\approx$ 134MB
- Dokáže využít všechna vlákna CPU
  - Např. na Threadripper 1950X 16-Core dosahuji $\approx$ 27000 klíčů/s
- Existují nástroje umožňující zapojit grafické karty (násobně vyšší rychlost)
- Možné využít *Rainbow tables*

Prolomení WPA

- `aircrack-ng` má parametr `-w`, kterým specifikujeme slovník
  `aircrack-ng -w rockyou.txt wpa.cap`
- Známý slovník rockyou `https://github.com/brannondorsey/naive-hashcat/releases/download/data/rockyou.txt`
- $\approx$ 14 milionů hesel, $\approx$ 134MB
- Dokáže využít všechna vlákna CPU
  - Např. na Threadripper 1950X 16-Core dosahuji $\approx$ 27000 klíčů/s
- Existují nástroje umožňující zapojit grafické karty (násobně vyšší rychlost)
- Možné využít *Rainbow tables*
- Po neúspěšném slovníkovém útoku můžeme využít hrubou sílu:
- Nástroj `crunch` pro generování kombinací

```
crunch 8 8 abcdefghijklmnopqrstuvwxyz0123456789 |
    aircrack-ng -w - wpa-01.cap
```

Úkol 1 – Deautentizace

- V maximálně tříčlenných týmech si zprovozněte `monitor mode`
- Nemáte-li v týmu promiskuitní WiFi kartu, půjčím vám
  - Zprovozněte drivery podporující `monitor mode`
  - Pro Archer T2UPlus
    `https://github.com/morrownr/8821au-20210708?tab=readme-ov-file`
  - Skript pro monitor mode `https://github.com/morrownr/Monitor_Mode`
- Na routeru nakonfigurujte WiFi s WPA
- Proveďte deautentizační útok na klienta
- Nápověda: `airplay-ng -0 n` (viz man)

Úkol 2 – Prolomení WPA

- Zjistěte sdílený klíč sítě `HackMe`
- Byla použita pouze písmena (malá)
- Délka 8 znaků

Úkol 3

- Doporučte obranu případně HW, který ji implementuje