Jesenji semestar, 2022/23

PREDMET: IT381 - Zaštita i bezbednost informacija

Domaći Zadatak br. 10

Student: **Aleksa Cekić 4173**

Profesor: **dr Milena Bogdanović**

Asistent: **mr Goran Stamenović**

Datum izrade: **19.03.2023**

Tekst Zadataka

1. Instalacija Kali linux OS-a (moguće je podići i sa USB-a) Uraditi, ako je moguće, sledeće operacije (ako to nije moguće, proći kroz vežbu 10 i objasniti razlike izmeću WEP, WPA i WPA protokola).
2. Setovanje kućnog rutera na WEP protokol i postavljanje šifre na neku jednostavnu vrednost (npr 1111111).
3. Logovanje na mrežu sa drugog računara.
4. Početak napada.
5. Prikaz uspešnosti napada tako što će se snimiti slike sa ekrana (engl. snapshot).

Rešenje zadataka

Uloga WEP protokola je da onemogući „prisluškivanje“ sesije između klijenta i pristupne stanice na samoj bežičnoj mreži, ali ovde se javlja jedan od mnogih problema WEP protokola jer on zaprvo ne sprečava prisluškivanje između korisnika koji imaju pristup bežičnoj mreži.
Pored deljenog ključa koji služi da onemogući neautorizovani pristup bežičnoj mreži, WEP omogućava i sigurnosnu enkripciju podataka i kontrolu integriteta podataka. Sigurnosna enkripcija podataka se vrši pomoću RC4 (Rivest Cipher 4) algoritma koji služi za šifrovanje podataka.
Razlika između WEP i WPA protokola se može videti na poljima autentikacije, enkripcije i provere integriteta podataka. Provera autentikacije je potpuno različita, dok se za enkripciju i proveru integriteta podataka koriste isti principi, samo sa dosta boljim algoritmima. A utentikacija kod WPA-PSK bežičnih mreža se vrši pomoću deljenog ključa (engl. PreShared key), odakle i potiče naziv WPA-PSK, koji čini šifru postavljenu na pristupnoj stanici. WPA2 sigurnosni protokol je nastao kao poboljšanje WPA protokola, s tim da je dizajniran tako da dodatno ojača enkripciju.
Umesto TKIP algoritma koji je korišćen u WPA protokolu, uveden je novi, CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) protokol sa algoritmima koji su znatno bolji od TKIP-a. Ključ enkripcije se sastoji od 256 bitova koji enkriptuje podatke koji se šalju bežičnom mrežom. Autentikacija i integritet podataka WPA2 protokola su identični WPA protokolu i koriste iste principe.