A black background with red text

Description automatically generated

***IT381 Zaštita i bezbednost informacija***

***Domaći zadatak br. 10***

***Ime i prezime: Jovan Pavkovic***

***Broj indeksa: 4442***

**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.

Preporučuje se da se ne koristi WEP protokol za bežičnu sigurnost jer je zastareo i nesiguran. WEP (Wired Equivalent Privacy) je bio standard za bežičnu sigurnost, ali je već duže vreme poznato da je lako probijen i da pruža slabu zaštitu. Umesto toga, bolje je korišćenje novijih i sigurnijih protokola poput WPA2 ili WPA3.

Ako ipak neko želi postaviti WEP na svom ruteru, evo osnovnih koraka:

* Povezivanje sa ruterom: putem Ethernet kabla ili bežično koristeći prethodno postavljenu bežičnu mrežu.
* Prijavljivanje na ruter: U web pregledač se unosi IP adresa rutera u traku za pretragu. Obično je to nešto poput 192.168.0.1 ili 192.168.1.1. Sledi prijava, koristeći korisničko ime i lozinku. Podaci za prijavu obično su navedeni na dnu ili na stražnjoj strani rutera.
* Bežične postavke: Traži se opcija "Wireless" ili "Wireless Security" u izborniku postavki rutera.
* WEP: Bira se WEP kao metod enkripcije.
* Postavljanje lozinke: Korisnik unosi željenu lozinku. (WEP koristi ključeve koji su obično u heksadecimalnom formatu npr. 64-bitni WEP ključ je obično 10 heksadecimalnih cifara)
* Čuvanje postavke: Kada se završi sa postavljanjem, sačuvaju se promene i ponovo pokreće ruter kako bi se primenile nove postavke.

Logovanje na mrežu s drugog računara može se razlikovati u zavisnosti od vrste mreže i operativnog sistema koji se koristi. S obzirom na to da ljudi većinom koriste Windows OS evo i koraka za konkretno taj sistem.

Windows OS:

* Otvorite File Explorer: Idite na "This PC" ili "Computer".
* Unesite putanju: U adresnom baru unesite putanju mrežnog resursa. Na primer, \\ime\_računara ili [\\IP\_adresa](file:///\\IP_adresa).
* Prijavite se: Ako se pojavi prozor za prijavu, unesite odgovarajuće korisničko ime i lozinku za računar na koji pokušavate pristupiti.
* Pregledajte resurse: Nakon uspešne prijave, trebali biste videti dostupne resurse na drugom računaru.