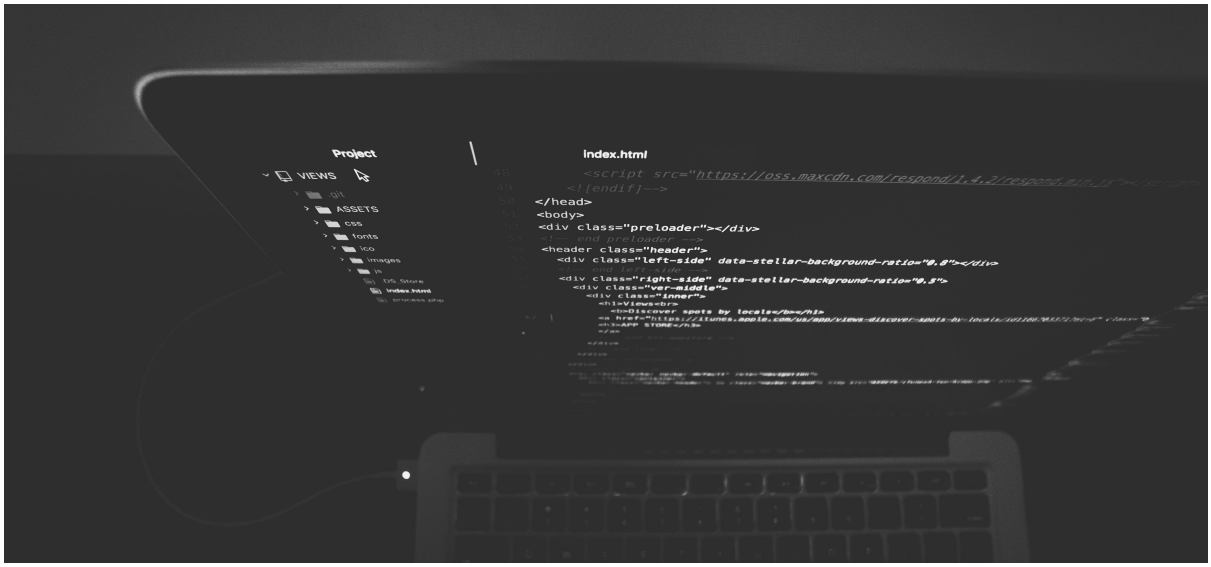


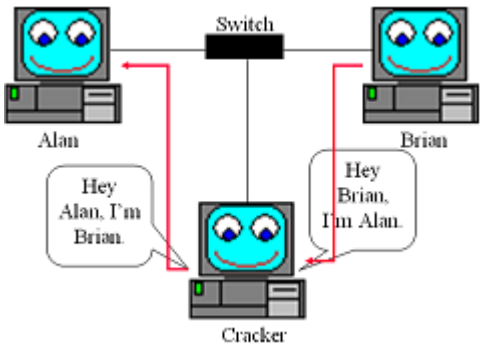
1. laboratorijska vježba: Man-in-the-middle attacks

Studentica: Emilija Sarić

Smjer: 112

Predmet: Sigurnost računala i podataka

Mitm (Man-in-the-middle) napad je aktivni napad gdje napadač upada u komunikaciju između klijenta i servera tako da ih uvjeri da komuniciraju direktno jedno s drugim dok napadač u stvari preuzima cijelu komunikaciju bez znanja ostalih sudionika.



ARP (Adress Resolution Protocol) je komunikacijski protokol kojim se dobiva fizička adresa na lokalnoj mreži iz poznate mrežne adrese.

U ovoj je vježbi analizirana je ranjivost ARP-a koja upravo omogućuje izvođenje Mitm i DoS (denial of service) napada na računala koja dijele zajedničku lokalnu mrežu (LAN).

Kako bi se realizirao mitm napada u virtualiziranoj Docker mreži kreirana su 3 virtualizirana Docker računala: dvije žrtve station-1 i station-2 te napadač evil-station.

IZVOĐENJE VJEŽBE:

1. pokretanje Windows terminal aplikacije i otvaranje Ubuntu terminala
2. stvaranje direktorija i poddirektorija naredbom mkdir
3. pozicioniranje u odgovarajući direktorij naredbom cd
4. stvaranja triju Docker računala : station-1, station-2 i evil-station
5. uspostavljanje bash-a naredbom docker exec - it _(stanica) bash
6. provjeravanje dostupnosti servera naredbom ping
7. uspostavljanje komunikacijskog kanala između station-1 i station-2 naredbom netcat
8. korištenje naredbe arpspoof kod evil-station računala kako bi se "prisluškivala" komunikacija između drugih dvaju računala
9. ispisivanje "priskluškivanog" sadržaja kod evil-station-a pomoću tcdump -i etho

Zaključak: Korištenjem mitm metode napadač lako može presresti komunikaciju između dva računala i preusmjeriti je preko sebe. "Lažnim predstavljanjem", bez znanja ostalih sudionika, postaje sudionik u komunikaciji i ima mogućnost mijenjati sadržaj poruka čime se narušava integritet podataka.