Sigurnosne Prijetnje na Internetu

Laboratorijska vježba  
Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva

MITM (čovjek-u-sredini) napad u kontroliranom okruženju

Ante Čavar

Zagreb, 10. Sječanj 2025

# Uvod (do 1000 znakova)

SSL/TLS protokoli osiguravaju povjerljivost, integritet i autentifikaciju u mrežnim komunikacijama. No, nepravilna konfiguracija ili korištenje zastarjelih verzija ovih protokola otvara vrata napadačima.

MITM napadi mogu biti izuzetno neprimjetni što je razlog više zašto moramo podgnuti svijest o ovom problemu. Naime dolaze u raznim oblicima (fizički – danas rijetki; virtualni – sve prevalentniji i češći)

Cilj ove laboratorijske vježbe je:

* simulirati ranjivosti u SSL/TLS komunikaciji točnije u pogrešnoj konfiguraciji istih
* analiza mrežnog prometa i probijanje jednostavne zaštite
* demonstracija praktičnih tehnika napada, poput presretanja mrežnog prometa uz pomoću ParrotOS-a i njegovih alata.

# Zadatak (do 1000 znakova)

Naš zadatak biti će presretanje mrežnog prometa između klijenta i servera. Konkretno biti će potrebno postaviti virtualke na VirtualBox-u, pokrenuti server na računalu „Žrtva/Server” te testirati povezivost iz prespektive napadača.

Server će te konfigurirati sa predanom http\_server.py datotekom.

Za pregled prometa preporučamo alat Wireshark no nije jedini koji smijete koristiti.

Cilj vježbe je shvaćanje mrežnog prometa kao i važnost dobre enkripcije.

Za one koji žele znati više:

Pogledajte http\_server.py datoteku. U njoj možete mijenjati kako se podatci enkriptiraju. Potičemo vas da se igrate za raznim šifiranjima te vidite kako se to mijenja u zahtjevima kojima šaljete.

# Teorijska podloga (do 4000 znakova)

Sigurnost mrežnih komunikacija ključan je aspekt suvremenog računalnog sustava. U ovoj vježbi istražujemo tehničku podlogu presretanja mrežnog prometa s ciljem razumijevanja ranjivosti koje nastaju nepravilnom konfiguracijom mrežnih aplikacija ili korištenjem nesigurnih protokola. Presretanje prometa (sniffing) i napadi čovjek-u-sredini (MITM) pružaju uvid u metode kojima napadači kompromitiraju privatnost korisnika i integritet podataka.

#### Osnove mrežne komunikacije i protokola

Mrežni protokoli poput HTTP i HTTPS definiraju kako se podaci prenose između klijenta i servera:

* HTTP (HyperText Transfer Protocol): Osigurava prijenos podataka u običnom tekstu. Ovaj protokol je nezaštićen, što znači da svatko tko presretne mrežni promet može vidjeti podatke u čitljivom obliku.
* HTTPS (HTTP Secure): Nadogradnja HTTP-a koja koristi SSL/TLS za šifriranje podataka. Šifriranje osigurava da su podaci nečitljivi za napadače, čak i ako presretnu promet.

Glavna razlika između ova dva protokola je u tome što HTTPS koristi SSL/TLS certifikate kako bi osigurao šifriranje podataka i autentifikaciju servera.

#### Napad čovjek-u-sredini (MITM)

MITM napad omogućuje napadaču da presreće i manipulira prometom između klijenta i servera. Cilj ovog napada može biti krađa osjetljivih podataka poput lozinki ili kompromitacija komunikacije.

##### Koraci u MITM napadu:

1. Presretanje prometa: Napadač koristi ARP spoofing ili slične metode kako bi preusmjerio promet kroz svoj uređaj.
2. Pristup podacima: U slučaju nezaštićenih protokola poput HTTP-a, podaci se lako mogu iščitati.
3. SSL downgrade: Ako se koristi HTTPS, napadač može pokušati preusmjeriti promet na HTTP koristeći alat poput sslstrip.

#### Korisni alati za presretanje prometa

U ovoj vježbi koristit ćemo sljedeće alate za analizu i manipulaciju mrežnog prometa (studenti nisu limitirani na ove alate, koristite što god vam je lakše):

* Wireshark:
  + Popularni alat za analizu mrežnog prometa.
  + Omogućuje pregled i filtriranje paketa u mreži.
  + Ključan za analizu HTTP zahtjeva i otkrivanje potencijalnih ranjivosti.
* Ettercap:
  + Alat za provođenje MITM napada pomoću ARP spoofinga.
  + Preusmjerava promet između klijenta i servera kroz napadačev uređaj.
* SSLstrip:
  + Koristi se za uklanjanje SSL/TLS sloja iz komunikacije.
  + Preusmjerava HTTPS promet na HTTP, omogućujući nešifrirano presretanje podataka.

#### Primjeri ranjivosti

Kroz ovu vježbu istražujemo nekoliko uobičajenih ranjivosti:

1. HTTP bez enkripcije: Osjetljivi podaci, poput lozinki, prenose se u običnom tekstu, što omogućuje njihovo jednostavno presretanje.
2. Neadekvatno hashiranje lozinki: Ako lozinke nisu šifrirane prije prijenosa, čak i promet zaštićen HTTPS-om može biti kompromitiran putem napada na klijentsku stranu.

#### Mrežna okolina

Vježba se odvija u simuliranoj Host-only mreži unutar VirtualBox-a:

* Jedna virtualka djeluje kao server i klijent.
* Druga virtualka je napadač koji koristi Wireshark, Ettercap i SSLstrip za presretanje prometa.

#### Uloga studenata

Studente potičemo na eksperimentiranje s izmjenama u dostavljenom http\_server.py kodu. Time se demonstrira kako različite implementacije šifriranja utječu na razinu sigurnosti. Također, istražuje se kako alati poput Wiresharka i Ettercapa mogu pomoći u identifikaciji i razumijevanju potencijalnih prijetnji.

# Postavke za vježbu (do 5000 znakova)

Opisuje se okolina u kojoj se postavlja zadatak te u kojoj će se rješavati zadatak. Opis treba biti takav da svakome omogućava repliciranje okoline za vježbu. Nije nužno ići u opisu do najsitnijih detalja, može se u nekom trenutku samo napisati **što** je potrebno napraviti, ne i **kako**.

Primjerice:

* za MITM napad, složiti računalo žrtve i poslužitelja s kojim komunicira, te računalo napadača. Sve to je potrebno spojiti. Za računalo napadača može se koristiti distribucija Kali. U opisu, dovoljno je reći da se koristi Kali, eventualno s popisom dodatnih paketa koje treba instalirati, ali se ne mora za svaki paket detaljno raspisivati instalacija.
* u slučaju alata za istraživanje, ako je to sve što je potrebno, dovoljno je napisati da se instalira distribucija Kali te kako se sam alat pokreće. Eventualno, ako je potrebno nešto doinstalirati – uključivo sam alat – treba to također napomenuti.

Vježba se provodi unutar simulirane mrežne okoline sastavljene od dvije virtualke u VirtualBox-u, postavljene u Host-only mrežni način rada. Jedna virtualka djeluje kao klijent i server, dok druga virtualka ima ulogu napadača. Ova konfiguracija omogućuje polaznicima da praktično istraže sigurnosne ranjivosti mrežnih komunikacija i razumiju metode presretanja prometa.

#### Mrežna konfiguracija

1. Mrežni način rada:
   * Obje virtualke koriste Host-only Adapter kako bi komunicirale unutar iste privatne mreže, izolirane od vanjskog interneta.
2. IP adrese:
   * Virtualke automatski dobivaju IP adrese unutar Host-only mreže. Preporučuje se da provjerite dodijeljene IP adrese pomoću naredbe ip addr show.
3. Promiscuous Mode:
   * Na napadačevoj virtualki omogućite Promiscuous Mode na mrežnom adapteru:
     + U VirtualBox-u: Settings → Network → Advanced → Promiscuous Mode → Allow All.
4. Testiranje mrežne povezanosti:
   * Provjerite povezivost između virtualki koristeći ping naredbu:

ping <IP\_SERVER\_KLIJENT>

#### Virtualka 1: Klijent i server

* OS: Preporučuje se korištenje Ubuntu-a ili slične Linux distribucije.
* Funkcionalnost: Virtualka pokreće server i generira promet kao klijent.
* Priprema:
  1. Instalirajte Python 3 i generirajte TLS certifikat pomoću OpenSSL:

openssl req -new -x509 -keyout server.pem -out server.pem -days 365 -nodes

* 1. Pokrenite dostavljeni http\_server.py za HTTPS komunikaciju:

python3 http\_server.py

* 1. Klijent šalje zahtjeve prema serveru koristeći:
     + curl:

curl -k https://<IP\_SERVER>:8443

* + - ili preglednik (unesite URL: https://<IP\_SERVER>:8443).

#### Virtualka 2: Napadač

* OS: Preporučuje se korištenje ParrotOS-a (Security Edition) ili Kali Linux-a.
* Funkcionalnost: Ova virtualka pokušava presresti promet između klijenta i servera.
* Priprema:
  1. Instalirajte potrebne alate:
     + Wireshark: Za snimanje i analizu mrežnog prometa.
     + Ettercap: Za provođenje MITM napada koristeći ARP spoofing.
     + SSLstrip: Za preusmjeravanje HTTPS prometa na HTTP.
     + Instalacija svih paketa može se izvršiti pomoću:

sudo apt update && sudo apt install wireshark ettercap-graphical sslstrip

* 1. Pokrenite ARP spoofing koristeći Ettercap:

sudo ettercap -T -M arp:remote /<IP\_KLIJENT>/ /<IP\_SERVER>/

* 1. Preusmjerite promet na HTTP pomoću SSLstrip:

sudo sslstrip -l 8080

* 1. Snimajte mrežni promet pomoću Wiresharka:
     + Odaberite mrežni adapter Host-only mreže.
     + Postavite filter za portove:
       - HTTPS:

tcp.port == 8443

* + - * HTTP:

tcp.port == 8080

#### Struktura zadatka

1. Pokretanje servera i klijenta:
   * Na virtualki klijent/server pokrenite HTTPS server koristeći dostavljeni http\_server.py.
   * Generirajte promet između klijenta i servera pomoću curl ili preglednika.
2. Provođenje napada:
   * Na napadačevoj virtualki:
     + Pokrenite ARP spoofing koristeći Ettercap.
     + Preusmjerite promet na HTTP pomoću SSLstrip.
     + Snimajte promet i analizirajte podatke pomoću Wiresharka.
3. Analiza podataka:
   * Na napadačevoj virtualki identificirajte osjetljive podatke u nezaštićenom HTTP prometu (korisničko ime, lozinka).
   * Usporedite promet između HTTP-a i HTTPS-a.
4. Eksperimentiranje:
   * Polaznici mogu modificirati http\_server.py kako bi eksperimentirali s različitim implementacijama šifriranja i autentifikacije.

#### Rezultati vježbe

* Polaznici trebaju prepoznati osjetljive podatke u presretnutom prometu i dokumentirati svoje zaključke.
* Dodatni cilj je usporedba sigurnosti HTTP i HTTPS komunikacije te demonstracija kako jednostavne sigurnosne mjere, poput pravilnog korištenja TLS-a, mogu značajno smanjiti rizik od presretanja prometa.

# Rješenje vježbe (do 5000 znakova)

U ovom poglavlju detaljno opisujemo postupak izvođenja MITM napada u kontekstu zadanog laboratorijskog okruženja. Rješenje je strukturirano kroz nekoliko ključnih faza koje omogućuju potpunu replikaciju postupka.

**Inicijalna provjera okruženja**

Prije početka napada, potrebno je provjeriti:

1. **Povezanost između virtualki:**

ip addr show # Provjera vlastite IP adrese

ping <IP\_druge\_virtualke> # Test povezivosti

2. **Omogućen Promiscuous Mode na napadačevoj virtualki:**

- Kroz VirtualBox sučelje provjeriti je li postavljen na "Allow All"

- Provjeriti status kroz terminal: `ip link show`

### **Implementacija MITM napada**

#### **1. Priprema napadačke virtualke**

Prvo osiguravamo da su svi potrebni alati instalirani i pravilno konfigurirani:

sudo apt update

sudo apt install -y wireshark ettercap-graphical sslstrip

#### **2. Pokretanje presretanja prometa**

Proces se izvodi sljedećim redoslijedom:

1. **Pokretanje Wiresharka za snimanje prometa:**

- Odabrati odgovarajuće mrežno sučelje (obično eth0)

- Postaviti filter: `tcp.port == 8443 || tcp.port == 8080`

- Započeti snimanje

2. **Aktivacija ARP spoofinga:**

sudo ettercap -T -M arp:remote /<IP\_klijenta>/ /<IP\_servera>/

3. **Preusmjeravanje HTTPS prometa:**

sudo iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 8080

sudo sslstrip -l 8080

#### **3. Analiza presretnutog prometa**

Nakon uspješnog postavljanja MITM napada, fokusiramo se na:

1. Identifikaciju HTTP zahtjeva u Wiresharku:

- Pratiti TCP stream za relevantne pakete

- Posebno obratiti pažnju na POST zahtjeve koji mogu sadržavati kredencijale

2. Analizu SSL/TLS handshake procesa:

- Identificirati pokušaje uspostave sigurne veze

- Uočiti eventualne downgrade pokušaje na HTTP

#### **Potencijalna ograničenja i izazovi**

Tijekom izvođenja vježbe mogu se pojaviti sljedeći izazovi:

1. **Detekcija ARP spoofinga**:

- Moderna mrežna oprema može detektirati i blokirati ARP spoofing

- Rješenje: Potrebno prilagoditi timing parametare u ettercap-u

2. **SSL/TLS certifikati:**

- Moderni browseri upozoravaju na nevažeće certifikate

- Neki servisi mogu implementirati HSTS

- Rješenje: Fokusirati se na starije verzije protokola ili konfigurirati vlastiti CA

3. **Mrežna latencija**:

- MITM može uzrokovati primjetno kašnjenje

- Rješenje: Optimizirati konfiguraciju mrežnih adaptera u VirtualBox-u

#### **Verifikacija uspješnosti napada**

Za potvrdu uspješnosti MITM napada, provjeravamo:

1. Prisutnost presretnutog prometa u Wiresharku

2. Uspješnost ARP spoofinga kroz ettercap log

3. Aktivnost sslstrip-a i preusmjerene zahtjeve

#### **Čišćenje nakon napada**

Nakon završetka vježbe, važno je:

1. Zaustaviti sve pokrenute alate pravilnim redoslijedom:

sudo killall sslstrip

sudo ettercap -Q

2. Vratiti mrežnu konfiguraciju u početno stanje:

sudo iptables -t nat -F

sudo iptables -t nat -X

Ovaj postupak omogućuje potpuno razumijevanje MITM napada u kontroliranom okruženju, demonstrirajući važnost pravilne implementacije sigurnosnih protokola i enkripcije u mrežnoj komunikaciji.

# Zaključak (do 1000 znakova)

Tijekom ove vježbe studenti su naučili koliko je jednostavno presresti mrežni promet u nepravilno konfiguriranoj mreži ili aplikaciji. Demonstracija MITM napada pokazala je ranjivosti nezaštićenih protokola poput HTTP-a i važnost korištenja šifriranih komunikacijskih kanala (HTTPS). Polaznici su također stekli praktično iskustvo s alatima poput Wiresharka i Ettercapa, što im je omogućilo razumijevanje kako napadači analiziraju i manipuliraju prometom.

Osim tehničkih aspekata, vježba je istaknula ključnu ulogu sigurnosnih mjera, poput pravilnog šifriranja podataka i implementacije sigurnih protokola, u zaštiti osjetljivih podataka. Time je naglašena potreba za svjesnošću i edukacijom u području mrežne sigurnosti kako bi se smanjio rizik od uspješnih napada.

# Literatura

RFC 2616 - Hypertext Transfer Protocol -- HTTP/1.1  
Dostupno na: <https://www.rfc-editor.org/rfc/rfc2616>

RFC 8446 - The Transport Layer Security (TLS) Protocol Version 1.3  
Dostupno na: <https://www.rfc-editor.org/rfc/rfc8446>

OWASP Foundation, OWASP Top 10: A10 - Insufficient Logging & Monitoring  
Dostupno na: <https://owasp.org/www-project-top-ten/>

Wireshark Documentation - User's Guide  
Dostupno na: <https://www.wireshark.org/docs/>

Ettercap Project Documentation  
Dostupno na: <https://www.ettercap-project.org/>

Al-Shaer, Ehab, and Sherif Abdelwahed. "Network security: A beginner's guide." McGraw Hill Professional, 2013.

OpenSSL Documentation  
Dostupno na: <https://www.openssl.org/docs/>

Hussain, Mustafa, et al. "Man-in-the-Middle Attacks: Detection and Protection Strategies." IEEE Access, 2018.

ParrotOS Documentation  
Dostupno na: <https://www.parrotsec.org/docs/>

Python 3 HTTP server documentation  
Dostupno na: <https://docs.python.org/3/library/http.server.html>