Operativni Sistemi i Računarstvo u Oblaku

II Semestar - 2022/23 - Vježbe

Sedmica 13

Handout za Vježbe

Agenda:

• Protokoli

• Enkripcijske osnove

Kontakt:

Narcisa.hadzajlic@size.ba

Adin.jahic2019@size.ba

vernes.vincevic@unze.ba

SCP

SCP (Secure Copy Protocol) je sigurni protokol za kopiranje datoteka između računara na udaljenim mrežama. Ovaj protokol koristi enkripciju i autentifikaciju kako bi osigurao sigurnu razmjenu podataka.

SCP se najčešće koristi u UNIX i UNIX-sličnim operativnim sustavima, kao što su Linux i macOS. On omogućuje korisnicima da kopiraju datoteke između lokalnog računara i udaljenog računara na mreži. SCP koristi **SSH (Secure Shell) protokol** za enkripciju i autentifikaciju, što osigurava povjerljivost podataka i sprječava neovlašten pristup.

Da biste koristili SCP, morate imati SSH pristup udaljenom računalu. Možete koristiti naredbu ili razne alate i programsku podršku koja podržava SCP protokol. Primjer naredbe za kopiranje datoteke s lokalnog računara na udaljeni računar koristeći SCP izgleda ovako:

scp lokalna_datoteka korisnik@udaljeni_racunar:putanja/na/udaljenom/racunaru

U ovoj naredbi "lokalna_datoteka" je putanja do datoteke na lokalnom računaru koju želite kopirati, "korisnik" je korisničko ime na udaljenom računaru, "udaljeni_racunar" je adresa ili naziv udaljenog računara, a "putanja/na/udaljenom/racunaru" je odredišna putanja na udaljenom računalu gdje želite spremiti datoteku.

SCP protokol je vrlo koristan kada trebate prenijeti datoteke između računara na siguran način, posebno kada radite s udaljenim poslužiteljima ili serverima.

DNS

DNS (Domain Name System) protokol je sustav koji prevodi domenska imena (npr. www.example.com) u IP adrese (npr. 192.0.2.1) i omogućuje povezivanje korisnika s odgovarajućim mrežnim resursima.

DNS se primjenjuje na internetu i lokalnim mrežama kako bi se omogućilo lakše prepoznavanje i pristupanje računalima, poslužiteljima, web stranicama i drugim mrežnim uslugama. Umjesto da korisnici moraju upisivati brojevne IP adrese za pristup određenim mrežnim resursima, DNS im omogućuje da koriste lako pamtljiva domenska imena.

DNS radi po principu hijerarhijske strukture. Na vrhu hijerarhije nalaze se korijenski DNS poslužitelji koji sadrže informacije o autoritativnim poslužiteljima za najviše razine domenskih imena, poput ".com", ".org" ili državnih oznaka kao što su ".ba" za Bosnu ili ".de" za Njemačku.

Kada korisnik upiše domensko ime u web pregledniku ili drugom programu, uređaj koristi DNS protokol kako bi poslao upit DNS poslužitelju koji je odgovoran za određeno domensko ime. DNS poslužitelj zatim pretražuje svoju bazu podataka kako bi pronašao odgovarajuću IP adresu za to domensko ime i vraća tu informaciju korisnikovom uređaju. Nakon toga, uređaj koristi dobivenu IP adresu za uspostavljanje veze s odgovarajućim mrežnim resursom.

DNS je ključna komponenta internetskog sustava jer omogućuje korisnicima da pristupaju web stranicama, šalju e-poštu, pristupaju poslužiteljima i koriste razne mrežne usluge koristeći lako prepoznatljiva domenska imena.

SHH

SSH (Secure Shell) protokol je sigurni protokol za udaljeni pristup i upravljanje računarima preko nesigurnih mreža. Ovaj protokol omogućuje enkriptiranu komunikaciju između klijenta i poslužitelja kako bi se osigurala povjerljivost podataka i spriječio neovlašten pristup.

SSH se primjenjuje na različitim platformama, uključujući UNIX, UNIX-slične operativne sustave (kao što su Linux i macOS) i Windows. On pruža siguran način za daljinsko upravljanje računarima, izvršavanje naredbi, prijenos datoteka i druge administrativne zadatke.

Kada korisnik uspostavi SSH vezu s udaljenim računarom, sva komunikacija između klijenta i poslužitelja je enkriptirana. To znači da podaci koji se prenose, uključujući naredbe, lozinke i druge osjetljive informacije, ne mogu biti lako snimljeni ili pročitani od strane neovlaštenih osoba.

SSH protokol se najčešće koristi za sljedeće svrhe:

1. **Udaljeno upravljanje:** Omogućuje administratorima da se sigurno prijave na udaljene poslužitelje i upravljaju njima, izvršavajući naredbe kao da su fizički prisutni na tom računaru.
2. **Sigurni prijenos datoteka:** Omogućuje korisnicima da sigurno prenose datoteke između lokalnog računara i udaljenog računara putem SSH protokola. Ovdje se često koristi SSH protokol s SCP ili SFTP protokolima.
3. **Tuneliranje mrežnog prometa:** SSH omogućuje stvaranje sigurnih tunela za šifriranje mrežnog prometa između lokalnog računara i udaljenog poslužitelja. To se koristi za zaštitu osjetljivih podataka koji se prenose preko javnih ili nesigurnih mreža.

SSH protokol je vrlo važan alat u sigurnosnom kontekstu jer omogućuje sigurno upravljanje udaljenim računarima i osigurava povjerljivost podataka tijekom komunikacije.

FTP

FTP (File Transfer Protocol) protokol je standardni protokol za prenos datoteka između računara na mreži. Omogućuje korisnicima da kopiraju, prenesu i upravljaju datotekama na udaljenim poslužiteljima.

FTP se primjenjuje na internetu i lokalnim mrežama kao sredstvo za prijenos datoteka. Korisnici mogu koristiti FTP klijente, specijalizirane aplikacije ili ugrađene naredbe operativnog sustava kako bi uspostavili vezu s udaljenim FTP poslužiteljem i obavljali operacije prijenosa datoteka.

FTP omogućuje dvosmjernu komunikaciju između klijenta i poslužitelja. Klijent se povezuje s FTP poslužiteljem putem TCP/IP mreže koristeći standardne TCP/IP portove (TCP port 21 za kontrolnu vezu i opcionalno TCP port 20 za prijenos podataka). Nakon uspostavljanja veze, klijent može pretraživati direktorije, prenositi datoteke, preimenovati, brisati ili mijenjati permisije datoteka na poslužitelju.

FTP podržava različite načine autentifikacije, uključujući anonimni pristup (bez potrebe za korisničkim imenom i lozinkom) i autentifikaciju temeljenu na korisničkim imenima i lozinkama. Također podržava pasivni i aktivni način rada prijenosa podataka.

Primjene FTP protokola uključuju:

Web hosting: FTP se često koristi za prijenos web sadržaja na web poslužitelje. Webmasteri i administratori mogu koristiti FTP kako bi prenijeli HTML datoteke, slike, skripte i druge sadržaje na poslužitelje koji hostaju web stranice.

Ažuriranje softvera: Razvojni timovi ili softverske tvrtke mogu koristiti FTP za distribuciju ažuriranja softvera i preuzimanje novih verzija softvera putem interneta.

Sigurnosna kopiranja: FTP se može koristiti za sigurnosno kopiranje (backup) datoteka i podataka s jednog računala na drugo, osiguravajući očuvanje podataka u slučaju kvara ili gubitka.

Važno je napomenuti da FTP nije siguran protokol jer ne koristi enkripciju podataka tijekom prijenosa. Stoga se preporučuje korištenje sigurnijih alternativa poput SFTP (SSH File Transfer Protocol) ili FTPS (FTP over SSL/TLS) protokola koji pružaju enkripciju i dodatnu sigurnost prijenosa podataka.

Enkripcija u Linux okruženju

U Linux okruženju, enkripcija podataka može se postići korištenjem različitih protokola i alata. Ovdje su nekoliko osnovnih enkripcijskih osnova koje se mogu koristiti:

SSH (Secure Shell): SSH protokol pruža enkripciju za sigurnu komunikaciju između klijenta i poslužitelja. To uključuje enkripciju prilikom prijenosa naredbi, lozinki i drugih osjetljivih podataka. SSH također podržava enkriptirane tuneliranje, što omogućuje šifriranje mrežnog prometa između dvije točke.

GPG (GNU Privacy Guard): GPG je besplatna i otvorena implementacija OpenPGP standarda. Omogućuje kriptografsko potpisivanje i enkripciju podataka. GPG koristi asimetričnu kriptografiju s parovima ključeva (javnim i privatnim ključem) kako bi se osigurala povjerljivost, autentičnost i integritet podataka.

OpenSSL: OpenSSL je popularna kriptografska biblioteka koja pruža različite algoritme za enkripciju, kao što su AES (Advanced Encryption Standard), DES (Data Encryption Standard), RSA (Rivest-Shamir-Adleman) i druge. OpenSSL se često koristi za implementaciju SSL/TLS protokola za sigurno šifriranje komunikacije između klijenta i poslužitelja.

Jedan jednostavan primjer enkripcije podataka može biti korištenje alata poput GPG za enkripciju tekstualne datoteke:

Generirajte par ključeva (javnog i privatnog) koristeći GPG:

gpg --gen-key

Enkriptirajte datoteku koristeći javni ključ primatelja:

gpg -e -r primatelj javni_kljuc.asc datoteka.txt

Enkriptirana datoteka sada je spremljena kao datoteka.txt.gpg i može se sigurno podijeliti s primateljem.

Primatelj može dekriptirati datoteku koristeći svoj privatni ključ:

gpg -d -o dekriptirana_datoteka.txt datoteka.txt.gpg

Navedeni primjer koristi GPG za enkripciju i dekripciju tekstualne datoteke, ali enkripcija se može primijeniti i na druge vrste datoteka ili mrežnu komunikaciju, ovisno o potrebama i alatima koji se koriste.

ZADACI

Zadatak 1: Generirajte par SSH ključeva

Napišite program koji generiše par SSH ključeva (javni i privatni ključ) koristeći kriptografsku biblioteku ili alat po vašem izboru. Program bi trebao izbaciti generirane ključeve u datoteke na lokalnom sistemu. Obavezno uključite komentare koji objašnjavaju svaki korak procesa.

Zadatak 2: Šifrirajte datoteku koristeći SCP

Napišite program koji šifrira datoteku koristeći SCP protokol. Program bi trebao uzeti putanju do datoteke, odredišni host i SSH javni ključ kao ulazne parametre. Program bi trebao koristiti SSH javni ključ za šifriranje datoteke, a zatim prenijeti šifriranu datoteku na specificirani odredišni host koristeći SCP. Možete koristiti postojeće biblioteke ili alate koji pružaju SCP funkcionalnost.

Zadatak 3: Dešifrirajte datoteku primljenu putem SCP-a

Napišite program koji prima šifriranu datoteku putem SCP-a i dešifrira je koristeći odgovarajući privatni ključ. Program treba da uzme putanju do primljene datoteke i putanju do privatnog ključa kao ulazne parametre. Program bi trebao koristiti privatni ključ za dešifriranje datoteke i izlaz dešifrovanog sadržaja na konzolu ili spremanje u datoteku.

Zadatak 4: Izvršite DNS pretragu

Napišite program koji uzima ime domene kao ulaz i vrši DNS pretragu kako bi dohvatio odgovarajuću IP adresu. Program bi trebao ispisati IP adresu na konzolu. Možete koristiti postojeće biblioteke ili alate koji pružaju DNS funkcionalnost.

Zadatak 5: Razriješi ime hosta u IP adresu

Napišite program koji uzima IP adresu kao ulaz i rješava odgovarajuće ime hosta koristeći DNS. Program bi trebao izbaciti ime hosta na konzolu. Opet, možete koristiti postojeće biblioteke ili alate koji pružaju DNS funkcionalnost.

Zadatak 6: Izvršite obrnuto DNS traženje

Napišite program koji uzima IP adresu kao ulaz i vrši obrnuto DNS traženje kako bi dohvatio odgovarajuće ime hosta. Program bi trebao izbaciti ime hosta na konzolu. Još jednom, možete koristiti postojeće biblioteke ili alate koji nude mogućnosti obrnutog DNS pretraživanja.

Zadatak 7: Povežite se na FTP server

Napišite program koji uspostavlja vezu sa FTP serverom. Program treba da uzme adresu FTP servera, korisničko ime i lozinku kao ulazne parametre. Nakon uspješnog povezivanja, možete odštampati poruku koja ukazuje na uspješnu vezu.

Zadatak 8: Lista datoteka na FTP serveru

Napišite program koji se povezuje na FTP server i preuzima listu datoteka i direktorija dostupnih na serveru. Program bi trebao prikazati listu datoteka i direktorija na konzoli.

Zadatak 9: Prenesite datoteku na FTP server

Napišite program koji se povezuje sa FTP serverom i prenosi fajl sa lokalnog sistema na server. Program bi trebao uzeti lokalnu putanju datoteke i putanju datoteke udaljenog servera kao ulazne parametre. Nakon uspješnog otpremanja, možete odštampati poruku koja označava uspješan prijenos.

Za sve eventualne primjedbe, komentare, sugestije obratiti se na mail: narcisa.hadzajlic@dl.unze.ba