Universitetet i Sørøst-Norge

TSD2090V-1 24H Nettverk og sikkerhet

Lab 1(HTTP/SMTP)

Hva HTTP er og hvordan det fungerer.

HTTP eller Hypertext Transfer Protocol er et protokollsystem som brukes på internett. Den er basert på TCP-transportprotokollen over port nummer 80 og består av spørringer og svar mellom klienten og HTTP-serveren. Kommunikasjon er delt inn i 6 trinn:

1. Klienten oppretter en TCP-forbindelse til http-tjeneren (f.eks. www.usn.no på port 80).
2. HTTP-serveren som mottar koblingen, godtar koblingen og sender et svar til klienten som den godtar. Trinn 1 og 2 sammen er det som kalles et HANDSHAKE – fasen der forbindelsen etableres og aksepteres.
3. Klienten sender deretter en forespørsel (request message) som inneholder en URL tilbake til serveren. Dette kan være tekst, bilde, en nettside eller annet.
4. Serveren mottar meldingen og svarer med ønsket innhold.
5. Serveren lukker TCP-tilkoblingen.
6. Klienten mottar det forespurte innholdet.

Hvis en nettside skal lastes ned, og HTML-koden refererer til flere objekter, må disse trinnene gjentas så mange ganger som antallet objekter som skal lastes ned [1].

Hvordan kommunikasjonen ser ut:

Kommunikasjonen som foregår på HTTP-protokollen husker ingenting og er såkalt stateless [2]. Eksempel på en spørring finner du under. Vi bruker netcat (nc) for å etablere kontakt med serven og lytte til svaret fra serveren med kommandoen ”***nc -v -C -4 web.d3-101.usn 80***» og sender følgende forespørsel.

```
GET /test.html HTTP/1.1
Host: web.d3-101.usn
Connection: close
```

I svaret fra HTTP-serveren får vi blant annet vite hvilken type server det er (Apache eller nginx), hvilket operativsystem den kjører på, serverversjon, adresse, når den sist ble oppdatert. Vi kan legge til linjer i spørringen vår for å tvinge visningen av ønsket språk. Dette gjør du ved å legge til «Accept-Language: xx-XX». NB! Dette må skje etter at du har angitt hvilken vertsmaskin du vil nå, og før du lukker TCP-koblingen. I vårt tilfelle ønsket vi norsk språk og linjen vil være som følger**: «Accept-Language: nb-NO»**

Mangler:

De tilfellene vi har sett på til nå har alle vært spørringer der vi ønsker å hente informasjon som skal inn i en HTML-mal eller som filer (tekst eller bilde) [2]. Vi har ikke sett på filformater som ikke støttes av et kommandolinjegrensesnitt (forkortes «CLI» heretter) – som for eksempel bilder. Hvis man etterspør et bilde via CLI og prøver å se på det, får man bare opp uleselig tekst uten mening for et menneske. Den

merkelige teksten er en representasjon av bildet i ASCII-verdi som kan oversettes av programmer som kan vise bilder.

Sikkerhet:

Kommunikasjonen mellom klient og server går over TCP og er dermed ikke kryptert og kan fanges opp av andre som ikke er serveren som igjen kan forfalske (spoofe) kommunikasjonen og sende sine egne pakker til klienten med innhold som klienten mottar uten å vite at det ikke er riktig pakke. [3]

Hva er SMTP.

Simple Mail Transfer Protocol (SMTP) er en protokoll som brukes til å overføre epost over internett. Denne protokollen brukes til å lage ett sett med regler for hvordan leveringen av epost skal foregå mellom avsender og mottaker uavhengig av programvare eller komponenter. Denne brukes i samarbeid med protokoller som POP3 eller IMAP4 som er brukt for å motta epost. For at man skal kunne sende og motta epost over internett så trenger man også en epost klient som Gmail eller Outlook samt en epost server slik som Postfix. SMTP standardiserer måten epost beveger seg fra sender til mottaker, som gjør epost levering på stor skala mulig. [4][2]

Hvordan fungerer det.

SMTP bruker Transmission Control Protocol (TCP) og lager en forbindelse mellom klienten og serveren via porter (f.eks. port 25). Klienten sender informasjon om avsenders epost adresse (MAIL FROM) og mottakers epost adresse (RCPT TO) samt innholdet i eposten til serveren. Adressene blir sjekket av serveren via Mail Transfer Agent (MTA). MTA sjekker domene til mottakeren sin epost adresse, og hvis det avviker fra senderen sin, så blir det gjort en spørring til Domain Name System (DNS) for å finne mottakeren sin IP-adresse. Eposten blir sendt fra klienten til serveren. Eposten blir videresendt til mottakerens epost server. Eposten lagres på mottakerens server frem til den er klar til å hentes av mottaker. Protokoller som Post Office Protocol 3 (POP3) brukes til å hente eposten fra serveren til klienten. [4] [2]

SMTP kommandoer bruk og oppsett.

SMTP bruker ferdig lagde tekst baserte instruksjoner til å fortell en klient eller server hva den skal gjøre med dataene den mottar.

Eksempel på dette er vist nedenfor. [4]

DATA

Date: Mon, 4 April 2022

From: Alice alice@example.com

Subject: Eggs benedict casserole

To: Bob bob@example.com

Hi Bob,

I will bring the eggs benedict casserole recipe on Friday.

-Alice

.

- RSET: This command resets the connection, removing all previously transferred information without closing the SMTP connection. RSET is used if the client sent incorrect information.
- QUIT: This ends the connection.

Konklusjon

SMTP er brukt over hele verden i stort omfang, med sin høy kvalitets implementasjoner har vist seg å være meget sterk. Imidlertid anser internettfelleskapet nå noen tjenester som viktige, som ikke ble forutsett da protokollen først ble designet. [5]

Dette betyr at det er viktig å gjennomføre ting på en slik måte at tidligere iterasjoner av protokollen fortsetter å virke.

Referanser

[1] B. T. M. S. A. A. S. R. David Gourley, HTTP: The Definitive Guide, O'Reilly Media, Inc., 2022.

[2] USN, «TSD2090, Forelesning 3, Uke 35, Nettverk og sikkerhet,» USN, 2024.

[3] L. S. o. E. technology, “The Art of Ethical Hacking: Understanding TCP/IP Hijacking” [Internett]. Hentet fra: https://lset.uk/learning-resources/the-art-of-ethical-hacking-understanding-tcp-ip-hijacking/#h-different-types-of-tcp-ip-hijacking-attacks. (Lastet ned 3 September 2024).

[4] Cloudflare. “What is the Simple Mail Transfer Protocol (SMTP)?” [Internett]. Hentet fra https://www.cloudflare.com/learning/email-security/what-is-smtp/. (Lastet ned 03. september 2024.)

[5] IETF, "RFC 5321: Simple Mail Transfer Protocol (SMTP)," August 2008. [Internett]. Hentet fra: https://www.rfc-editor.org/info/rfc5321. (Lastet ned: 05-Sep-2024.)