PRAKTILINE ÜLESANNE – KOMMUNIKATSIOONIPROTOKOLLID

Eesmärk

Tuvastada ja selgitada, milliseid **kommunikatsiooniprotokolle** kasutatakse erinevates internetiga seotud olukordades.

Oskad pärast ülesande täitmist:

- seostada protokolle nende kasutusotstarbega,
- aru saada, miks konkreetne protokoll on vajalik,
- ning tuua näiteid nende kasutusest päriselus.

Ülesanne 1 – Millist protokolli kasutatakse?

Allpool on toodud olukorrad.
Iga olukorra juures:

- **Kirjuta, millist protokolli kasutatakse.**
- **Põhjenda oma valikut ühe lausega.** (Miks just see protokoll sobib?)

Sul saabub e-kiri, millele soovid vastata ja lisada manuseid.
→ **Protokoll: IMAP**
→ **Põhjendus: See lubab sul sõnumeid lugeda mis on sulle saadetud su meili serverile. Lisaks sa saad sõnumit lugeda erinevates seadmetes.**

Soovid laadida üles suure faili ettevõtte serverisse.
→ **Protokoll: SFTP**
→ **Põhjendus: turvaline andmete jagamine serveriga**

Avad veebilehe aadressi www.google.com.
→ **Protokoll: DNS**
→ **Põhjendus: mugav viis minna domeenile ilma kirjutamas pikka rea, DNS tõlgib sinu eest aadressi kuhu sa soovid minna**

Arvuti küsib serverilt, milline IP-aadress kuulub domeeninimele "example.com".
→ **Protokoll: DNS**
→ **Põhjendus: DNS tõlgib domeeni aadressiks**

Laadid alla e-kirjad oma seadmesse ja soovid, et need kustutataks automaatselt serverist.
→ **Protokoll: POP3**
→ **Põhjendus: See jagav sulle andmed ja kustutab andmed enda serverist kui see on sulle saabunud-.**

Veebibrauser palub veebilehe sisu laadida.
→ **Protokoll: TCP**
→ **Põhjendus: tagab andmed jõuaksid turvaliselt ja õigesti kohale**

Soovid oma e-kirju hallata mitmes seadmes ja hoida neid sünkroonis serveriga.
→ **Protokoll: IMAP**
→ **Põhjendus: võimaldab lugeda andmeid ilma , et server see kustutaks endalt ära ja lubab seda lugeda iga kell, igas seadmes kui ligipääs on olemas**

Kasutad turvalist failiedastusprotokolli, mis krüpteerib kõik andmed.
→ **Protokoll: HTTPS**
→ **Põhjendus: Krüpteerib kõik andmed mis sa saadad serverile**

Server saadab e-kirju teistele serveritele.
→ **Protokoll: SMTP**
→ **Põhjendus: Edastab andmed teise serverile**

Tahad turvata oma veebilehte, et kasutajad tunneksid end andmete jagamisel turvaliselt.
→ **Protokoll: HTTPS**
→ **Põhjendus: krüpteerib andmed**

Soovid üles laadida ja alla laadida faile, kuid ilma turvameetmeteta.
→ **Protokoll: FTP**
→ **Põhjendus: algne versioon SFTPs, ebaturvaline ja mitte soovituslik**

Tahad teada, kuidas arvutid edastavad omavahel andmepakette, sõltumata sellest, millist rakendust kasutatakse.
→ **Protokoll: TCP**
→ **Põhjendus: määrab kuidas andmed liiguvad**

Avad veebilehe, mis ei kasuta turvalist ühendust (lukku ei ole).
→ **Protokoll: HTTP**
→ **Põhjendus: algne versioon HTTPs protokollist, ei krüpteeri andmed, andmed on avalikud**

Arvuti peab IP-aadressi leidmiseks pöörduma vastava serveri poole.
→ **Protokoll: DNS**
→ **Põhjendus: DNS tegeleb serverite suhtlemisega**

Kasutad veebilehitsejat ja soovid kindel olla, et keegi ei näe sinu edastatavaid andmeid (nt pangas).
→ **Protokoll: HTTPS**
→ **Põhjendus: krüpteerib su andmed**

Veebiserveri ja arvuti vaheline ühendus on turvamata.
→ **Protokoll:**
→ **Põhjendus:**

Tahad failid serverisse saata üle võrgu ning kaitsta neid turvariskide eest.
→ **Protokoll: SFTP**
→ **Põhjendus: krüpteerib liikluse**

Kasutad oma seadmes e-posti programmi ja laed alla uued kirjad, kuid tahad, et need jääksid ka serverisse alles.

→ **Protokoll: IMAP3**
→ **Põhjendus: võimalik lugeda kirja kindla sissepääsuga mitmes seadmes**

Server saadab kirju kliendile ja ei vaja nende salvestamist serveris.
→ **Protokoll: POP3**
→ **Põhjendus: kustutab kirja serverist kui kiri on saabunud**

Tahad turvaliselt suhelda serveriga, et edastada oma isikuandmeid (nt sisselogimisel).
→ **Protokoll: HTTPS**
→ **Põhjendus: krüpteerib andmed**

Ülesanne 2 – Üldisemad tehnilised küsimused

Vasta allolevatele küsimustele oma sõnadega. Vajadusel kasuta internetti või oma tunnimaterjale.

Püüa vastata selgitavalt, mitte ainult ühe sõnaga.

- Mis vahe on **HTTP** ja **HTTPS** vahel ning miks enamik veebilehti on tänapäeval HTTPS-ile üle läinud?

  HTTP edastab andmed omavhale serveriga ja arvutiga, see ei taga sellega ,et keegi saab lugeda seda, mis on ebaturvaline, õige oskusega, iga inimene pahatahtlikud saab lugeda su andmeid aga HTTP(S-Secure) edastab andmeid omavahel aga krüpteerib selle enne saatmist ja tõlgib selle uuesti arusaadavase andmeisse kui jõuab turvalise kohta.

- Selgita oma sõnadega, mis on **DNS** ja miks seda peetakse interneti “telefoniraamatuks”.

  DNS suhtleb serveritega ja nõuab õiget andmed õige domeeni järgi, kui sa avad Google.com DNS tõlgib selle arvutikeelte mis on palju numbreid ja õige numbriga sa saad õige andmed kui sa kirjutad Hoogle.com siis see annab sulle kas valed andmed või error serverit pole olemas. Seda nimetakse telefoniraamatuks sest see on nagu otsid telefoniraamatus kellegi nime(Domeeni nimi) ja siis sa leiad selle nime juures telefoninumbri(IP) millega sa saad kontakti võtta.

- Mis juhtub, kui DNS-server ei tööta? Milline on kasutaja kogemus?

  Kui dns ei tööta, siis sa pead kas ise parandama selle, kutsuma abi või otsima veebilehte nende IP järgi mitte domeeni järgi aga see on päris keeruline.

- Mis vahe on **IMAP-il** ja **POP3-l**? Too näide, millal kumb sobib paremini.

  IMAP edastab kirja õigele kontole ja salvestab selle serverise selle puhul, kui kasutaja logib oma kontole teise seadmesse siis ta saab lugeda sama kirja.
  POP3 edastab kirja ja kui kasutaja on kirja avanud siis see kiri laetakse ta seadmesse ja serveris kustutakse.

- Mille poolest erinevad **FTP** ja **SFTP**? Miks tuleks eelistada SFTP-d?
  FTP on failide edastamine arvutise ilma turvalise viisiga, SFTP on uuem versioon FTP-ist mis on palju turvalisem sellepoolest, et see krüpteerib andmed.

- Kuidas **TCP** ja **IP** omavahel koostööd teevad? Mis oleks, kui TCP-d ei oleks?

  IP määrab kuhu andmed saadetakse ja TCP teeb kindlaks andmed jõuavad ohutult kindlasse kohta , ilma TCP võib juhtuda, et andmed liiguvad vahest valesse kohta ja võib juhtuda see läheb kurjategija kätte.

- Too üks **päriseluline olukord**, kus andmete turvamata edastus (nt HTTP, FTP, POP3) võib olla ohtlik.

  Sisestad andmed HTTP keskkonnal, teiselpool häkker jälgib sind , sisesta eesnime, perekonnanime, koduaadressi, telefoninumber, emaili, pangainfo ja häkker näeb kõike ilma probleemidega. Ta saab kindlasti sissepääsu su emaili , kuritarvitada su telefoninumbrit, kasutada su kaarti infot, et osta endale pudel viina.

- Miks on vaja, et kõik need protokollid oleksid standardiseeritud ja kokkulepitud?

  Eriprotokollid ja eri kokkulepetega tekkib segadus ja ebaturvalisus.

- Miks kasutatakse sageli korraga mitut protokolli (nt TCP koos HTTP-ga või DNS koos HTTPS-iga)? Too näide.

  Eriprotokoll tagab erineva käskluse, TCP edastab andmed ebaturvaliselt ja HTTP ühendab serveri arvutiga. HTTPS tagab turvalise ühenduse ja DNS tõlgib kasutaja domeeni IP aadressiks ja edastab selle HTTPS mis ühenda sind õigesse serverise ja annab õiged pakid.

Ülesanne 3 – Arutlus

Vasta lühidalt (2–4 lauset):

- Miks võiks öelda, et kommunikatsiooniprotokollid on “interneti keel”?

  Sest neid kasutab peamiselt arvutit ja tavainimesed ei puudu sellega kokku, ainult kes neid kodeerib puudub, aga neid protokolle kasutab ikka arvutid millega nad saavad internetiga ühendust võtta.

- Kuidas mõjutaks nende puudumine meie igapäevast suhtlust ja tööd?

Sa ei saaks ühendata internetti, leida õige domeeni serveri, ei saa turvaliselt või ebaturvaliselt edasta andmed, ei saada emaili kus server kustutab kirja oma serveris või salvestab selle ,et saaksid lugeda teises seadmes

- Kas inimene saab tänapäeval üldse kasutada internetti ilma, et ta teadvustaks endale, millised protokollid tema seadmes töötavad?

  Saab küll aga kui mingi probleem tekkib protokolliga, siis on paanika jaanika, kasutaja ei ole teadlik mis on viga ja eeldab see on ta seadme viga ja kas ostab uue seadme või viib paranduse aga probleem ei ole olnud seadmes vaid protokolli tõrge.

Ülesanne 4 – Konspekti koostamine

Ülesanne:
Koosta oma sõnadega konspekt, kus iga peatükk kirjeldab ühte protokolli.
Konspekt peab olema enda sõnastuses, mitte kopeeritud.

Nõuded:

- Selgita lühidalt, mida iga protokoll teeb ja kus seda kasutatakse.
- Too vähemalt üks päriseluline näide (nt “IMAP – kasutan seda, kui sünkroonin e-kirju telefoni ja arvuti vahel”).
- Kirjelda järgnevaid protokolle: **HTTP, HTTPS, FTP, SFTP, DNS, SMTP, IMAP, POP3, TCP, IP**.
- Leia ja kirjelda veel kolm uut protokolli, mida siin töölehel ei olnud (nt SSH, SNMP, NTP, DHCP, ARP vms).

Iga uue protokolli puhul lisa:

- Kus seda kasutatakse?
- Mis probleemi see lahendab?
- Kuidas see aitab andmeid turvaliselt või efektiivselt edastada?

Ülesanne 5 – Analüüs ja võrdlus

1. Tabeliülesanne:

Koosta tabel, kus on vähemalt viis protokolli ja nende võrdlus järgmiste omaduste alusel:

Protokoll	**Kasutab krüpteerimist?**	**Mis tüüpi andmeid edastab?**	**Päriseluline näide**
HTTPS	**jah**	**pakke**	**Edastab krüpteeritud andmed teise serverile**
Protokoll	**Kasutab krüpteerimist?**	**Mis tüüpi andmeid edastab?**	**Päriseluline näide**
FTP	**ei**	**faile**	**Edastab failid teise arvutise või laeb teise arvuti saadetud failid ebaturvaliselt**
Protokoll	**Kasutab krüpteerimist?**	**Mis tüüpi andmeid edastab?**	**Päriseluline näide**
DNS	**Ei**	**IP aadress**	**Tõlgib domeeni aadressi IP aadressiks.**
Protokoll	**Kasutab krüpteerimist?**	**Mis tüüpi andmeid edastab?**	**Päriseluline näide**
IMAP	**Oleneb kas veebisait on HTTP või HTTPS**	**andmeid**	**Edastab kirju ilma kustumata oma serveris.**
Protokoll	**Kasutab krüpteerimist?**	**Mis tüüpi andmeid edastab?**	**Päriseluline näide**
POP3	**Oleneb kas veebisait on HTTP või HTTPS**	**andmeid**	**Edastab kirju ja kui saadud kätte kustutab serverist ära ja laeb selle avatud seadmesse.**