Leksion 3

Frida GJERMENI

Protokolli SMTP

- MTA-te jane 2 llojeshe: MTA Client (MTA per Klientin) dhe MTA Server (MTA per Serverin).
- Protokolli qe perdoret nga MTA Client dhe MTA Server eshte SMTP (Simple Mail Transfer Protocol).
- MTA klient me ane te komandave (Commands) ben kerkesa tek MTA Server, i cili pergjigjet me *Responses*
- Ky protokoll sherben vetem per transferimin e emaileve midis llogarive te perdoruesve.
- Porta standarte e komunikimit eshte 25.
- Eshte protokoll text-based qe do te thote se perdoruesi ndervepron me protokollin nepermjet utilitetit telnet ne nje nderfaqe komandash (shell) duke shkruar rreshta komandash (commands) dhe duke marre pergjigje (responses) zakonisht te identifikuara nga kodet perkatese.

KOMANDA	EMRI I PLOTE	KUPTIMI
HELO	Introduction	Nis komunikimin midis hosteve (sesionin SMTP)
EHLO	Introduction (extended SMTP mode)	Perdoret ne versionin me te detajuar te SMTP-se; Nis komunikimin midis hosteve
RSET	System Reset	Nderpret dhe rivendos automatikisht komunikimin
EXPN	Expand Mailing List	Me ndihmen e SMTP Server, afishohet adresa destinacion per cdo email qe dergohet nje adrese te specifikuar
NOOP	No Operation	Komanda nul. Nuk kryen asnje funksion
VERB	Verbose mode	I pergjigjet nje mesazhi te derguar me opsionin verbose (ne forme te zgjeruar)
MAIL	Specify Mail Sender	Specifikon email derguesin
TURN	Mail Turn	Nxjerr emailet nga rradha ne SMTP Server dhe i ridrejton ne hostin (sipas domainit te specifikuar) qe nisi sesionin SMTP
ETRN	Extended Turn	Nxjerrja dhe ridrejtimi i emaileve drejt hostit behet duke analizuar MX Record e domainit te specifikuar. Kjo komande nuk zbatohet nga te gjitha versionet e SMTP
RCPT	Specify Mail Recipient	Specifikon email marresin
HELP		Afishon ndihmen elektronike
DATA	Specify Message Content	Specifikon permbajtjen e mesazhit
VRFY	Verify Address	Verteton me ndidhmen e SMTP Server vlefshmerine e adreses se specifikuar me qellim evitimin e listave spam
DSN	Delivery Status Notifications	Njofton rreth dergimit me sukses ose jo te mesazhit
QUIT	Quit	Mbyll sesionin SMTP (komunikimin midis hosteve)

Tabela 8 – Disa Kode (Pergjigje) te Protokollit SMTP

KODI	KUPTIMI
Komunikim me Sukses - (Pergjigjet Pozitive)	
211	Jep informacion mbi Statusin e sesionit
214	Jep informacionin rreth kerkesave te bera
220	Sherbimi i emailit eshte gati dhe komunikimi mund te nise
221	Mbyllja e komunikimit
250	Kerkesa e bere ka perfunduar me sukses
251	Perdoruesi nuk eshte lokal ndaj mesazhi duhet pasohet ne hostin destinacion
354	Konfirmim per te nisur dergimi i emailit
Komunikim pa Sukses (Pergjigjet Negative)	
421	Sherbimi i emailit nuk ofrohet
450	Nuk ka komunikim me Mailbox-in
451	Nderprerje komande: gabim ne makinen lokale
452	Nderprerje komande: kujtese e pamjaftueshme
500	Gabim Sintaksor: Komanda nuk njihet
501	Gabim Sintaksor: Parametra ose argumenta te pavlefshme
502	Komande e pa implementuar
503	Sekuence jo e vlefshme komandash
504	Komande perkohesisht e pa implementuar
550	Mos ekzekutim komande; nuk ka komunikim me mailbox-in
551	Perdorues jo lokal
552	Nderprerje e veprimit te kerkuar; tejkalim kujtese te lejuar
553	Nuk ndermerret veprimi i kerkuar; emer i palejuar i mailbox-it
554	Transaksion i deshtuar

Protokolli SMTP dhe Komunikimi MTA Klient - MTA Server

- *Vendosjen e lidhjes,* Dergimi *e mesazhit* dhe *Shkeputjen e lidhjes.*
- *Shembujt-Detyre shtepie/sqarim ne klase*
- dy shembuj te realizuar ne shell (nderfaqe komandash) duke perdorur utilitetin telnet dhe komandat e SMTP-se

Protokolli POP3 *(Post Office Protocol)*

- Protokolli POP3 percaktuar sipas standarteve RFC 1939 - STD 0053, sherben vetem per marrjen dhe leximin e emaileve.
- Porta e kornunikimit eshte 110.
- Eshte protokoll text-based.
- Veprimet qe kryen jane: ruajtja, kopjimi, fshirja e emaileve.
- Mesazhet ruhen ne email server derisa klienti logohet;
- Me pas ato fshihen nga email serveri dhe shkarkohen si nje grupim i vetem ne kompjuterin lokal te email klientit.
- Ne keto raste email serveri njihet ndryshe si POP3 Server.

Tabela 9 – Disa Komanda te Protokollit POP3

KOMANDA	SINTAKSA	KUPTIMI
USER	user *Username*	Merr si argument Username: Emrin e perdoruesit te llogarise se emailit (emri i mailbox) qe duhet identifikuar ne POP3 Server. Kjo komande paraprin gjithnje komanden PASS.
PASS	pass *Password*	Merr si argument Password: Fjalekalimin qe i duhet perdoruesit per t'u identifikuar ne POP3 Server. Perdoret gjithnje pas komandes USER.
STAT	stat	Afishon numrin e mesazheve dhe madhesise totale te mailbox-it.
LIST	list list *MessageNumber*	Nese nuk merr argument, afishon per cdo mesazh: numrin e tij identifikues dhe madhesine ne disk. Nese merr argumentin MessageNumber, pra numrin identifikues te nje mesazhi, afishon madhesine e tij ne disk.
LAST	last	Afishon numrin identifikues te mesazhit te fundit ne listen e mailbox n.q.s nuk eshte shenjuar si i lexuar ose i fshire.

RETR	retr *MessageNumber*	Merr si argument numrin identifikues te nje mesazhi, afishon permbajtjen e plote te tij dhe e shenjon ate si te lexuar.
TOP	top *MessageNumber lines*	Merr si argumenta numrin identifikues te nje mesazhi (MessageNumber), numrin e rreshtave te tij (lines) dhe i afishon ato rreshta.
DELE	dele *MessageNumber*	Merr si argument numrin identifikues te nje mesazhi dhe e selekton per ta fshire nga mailbox-i.
RSET	rset	Kthen te gjitha mesazhet e shenjuara si te lexuara ose te fshira ne mesazhe te palexuara.
NOOP	ñoop	Kthen nje pergjigje konfirmuese (acknowledgement) por pa ndonje funksion. .
APOP	apop *Usemame EncryptedKey*	Merr si argument emrin e perdoruesit (Username) qe duhet identifikuar, dhe e dergon fjalekalimin e koduar me frazen e dhene si argument (EncryptedKey) ne POP3 Server. Fjalekalimi dergohet si tekst MD5 i gjeneruar nga kodimi i: fjalekalimit, numrit identifikues te procesit, dates dhe ores ne kompjuter.
QUIT	quit	Mbyll sesionin POP3.

Protokolli IMAP4

Protokolli IMAP versioni 4 percaktuar sipas standarteve RFC 2060, RFC 2061, sherben vetem per marrjen dhe leximin e emaileve. Porta e komunikimit eshte 143. Eshte protokoll **text-based.** Veprimet qe kryen jane: ruajtja, kopjimi, fshirja e emaileve. Mesazhet ruhen ne email server derisa klienti logohet; me pas nje kopje e mesazheve dhe direktorive te mailbox ruhen ne kompjuterin lokal te email klientit. IMAP4 perdor mekanizmin e sinkronizimit te veprimeve te kryera (kur perdoruesi ose klienti ka qene ne statusin offline), sapo email klienti identifikohet ne email server. Ne keto raste email serveri njihet ndryshe si IMAP4 Server.

Komanda te prottokollit IMAP4

KOMANDA	SINTAKSA	KUPTIMI
LOGIN	login *Username Password*	Merr si argumenta Username: Emrin e perdoruesit te llogarise se emailit (emri i mailbox) dhe Password: Fjalekalimin qe duhen identifikuar ne IMAP4 Server. Fjalekalimi mund te te dergohet i pakoduar ne IMAP4 Server.
CAPABILITY	capability	Afishon funksionalitetet qe ofron email serveri ne menyre te detajuar.
STATUS	stat	Komande analoge e komandes STAT qe perdorej nga protokolli POP3.
SELECT	select Directory	Merr si argument nje direktori: psh, Inbox, dhe e selekton ate per te kryer veprime ne vazhdim.
LOGOUT	last	Perdoruesi perfundon sesionin IMAP4.

Shembuj

Skedaret Binare *(Email Altachmen/t)* :dhe Protokollet MIME, SMIME, PEM

- Fillimisht, SMTP u dizenjua per te derguar vetem mesazhe tekst.
- Me rritjen e kerkesave te perdoruesve per te derguar vecmas mesazheve tekst edhe skedare binare, u ndryshuan standartet e protokollit SMTP per te mundesuar edhe dergimin e ketyre skedareve.
- Skedaret binare ose skedaret e bashkangjitur jane te tipit: grafike, microsoft office documents, audio, video.

Dergimi i skedareve binare me email

- Ne te shkuaren: - Konvertuesi binar-ascii dhe ascii binar.
- Ne sistemet UNIX, nje utilitet i quajtur *uuencode* perdorej per te koduar (konvertuar) skedaret binare ne formatin ascii.
- Skedaret ascii dergoheshin me email tek marresi i cili perdorte utilitetin *uudecode* per te dekoduar (konvertuar) skedaret ascii ne formalin binar te kuptueshem nga perdoruesi
- Ne te tashmen: MIME eliminon perdorimin e utiliteteve uuencode/uudecode.
- Me ane te MIME, procesi I dergimit te skedareve binare me ane te emailit eshte transparent dhe perdoruesit mund te ndjekin cdo hap te procesit pasi te percaktojne dhe perzgjedhin skedarin/skedaret nepermjet email klientit ose webmail. Keta te fundit kane pergjegjesi per procesin.
-

Protokolli MIME *(Multipurpose Internet Mail Extensions)*

- Standartet specifikohen nga RFC 1521 dhe RFC 1522
- MIME eliminon perdorimin e uuencode/uudecode
- Mesazhi elektronik (Email) ndahet automatikisht ne pjese ku secila identifikohet nga tipi i permbajtjes (content type) specifik pra tipi I te dhenave qe permban.
- Shembuj: Content type: image/gif, Content-type: text/html
- Keto content types perdoren nga HTTP serverat per te pershkruar permbatjen e faqeve web qe do te shfaqen ne web browser

- Kur MIME perdoret nga email klientet, keta te fundit I konvertojne skedaret binare ne nje format teksti duke perdorur kodimin me baze 64, i cili ndryshon nga uuencode
- MIME u lejon email klienteve te perdorin bashkesi karakteresh te shumellojshme duke plotesuar kerkesat e perdoruesve per te derguar te dhena te tipeve dhe formative te ndryshme
- Disa email kliente qe perdorin MIME: Pine, Outlook Express, Netscape, Microsoft Outlook, Eudora

Protokolli PEM dhe S/MIME

- PEM *(Privacy Enhanced Mail)* eshte nje protokoll qe perdoret per shifrimin, autentifikimin dhe integritetin e mesazheve eleldronike te tipit tekst.
- S/MIME (Secure/ Multipurpose Internet Mail Extensions): Versioni hibrid i protokollit MIME. Ai mbart edhe karakteristika te prolokollit PEM.
-

Protokolli PEM dhe Struktura e nje Mesazhi PEM

- Cdo mesazh PEM filloi me stringun BEGIN PRIVACY ENHANCED MESSAGE,te dhenat dhe perfundon me stringun END PRIVACY ENHANCED MESSAGE.
- -----BEGIN PRIVACY ENHANCED MESSAGE----
- ...<data>...
- -----END PRIVACY ENHANCED MESSAGE-----

- Tipet e te dhenave qe permban nje mesazh PEM kategorizohen si me poshte:
- Te dhena te zakonshme, te pakoduara (Ordinary, unsecured data)
- 2. Te dhena te pandryshuara me integritet ose MIC-CLEAR (Integrity protected unmodified data)
- 3. Te dhenale koduara me integritet ose MIC-ONLY (Integrity-proteced encoded data)
- 4. Te dhena te koduara dhe shifruara me integritet ose ENCRYPTED (Encoded encrypted intgrity-protected data)

- Kater tipet e te dhenave te mesiperme mund te kombinohen ne nje mesazh PEM si dhe te nderfuten tek njera tjetra

Kodimi PEM

- PEM mud te perdoret per infrastrukturat me celes sekret dhe ato me celes publik por vlen te thuhet se nuk shfaqet interes -ne perdorimin e PEM me celes sekret.
- Eshle nje kodim me Baze 64 (base-64 encoding) ku cdo 6-bite kodohen si 6-bite karakter ne bashkesine e karaktereve {A-Z,a-z,0-9,+,I}
- Cdo rresht qe fillon me karakterin "-", zevendesohet nga PEM me "- ": pra shtohet nje hapesire boshe pas vizes. Kjo ilustrohet si me poshte:
- -----END PRIVACY ENHANCED MESSAGE----
- Do te transformohej ne:
- - ----END PRIVACY ENHANCED MESSAGE-----
    - Rregulla te·Pasimit (Forwarding) dhe te Paketimitle Mesazheve (Enclosure)

Dallimi midis PEM dhe S/MIME

- S/MIME ofron keto elemente sigurie per mesazhet e sistemeve te postes elektronike:

- autentlfikimin, integritetin e mesazhit dhe identifikimin e sakte te burimit te mesazhit (duke perdorur nenshkrimet dixhitale) dhe sigurine e te dhenave me ane te skemave te shifrimit.
- SIMIME specifikon tipin e te dhenave smime-type "enveloped-data" per shifrimin e te dhenave: i gjithe mesazhi mime, i shifruar paketohet dhe mbartet nga nje objekt qe do transferohet si nje entitet application/pkcs7-mime MIME.
- S/MIME eshte i ngjashem me PEM. Dallimet shihen ne disa fjale kyce te flllimit dhe fundit te mesazhi