TALLINNA TEHNIKA ÜLIKOOL

Eksam aines Kommunikatsiooni võrgud

Pilet 31

2 . HTML-lehekülg : www.online.ee/~solman

3. Pakettid filtreerimise põhimõtted. Filtreerimisreeglite koostamise alused : reeglites kasutatavad parameetrid, reeglite tabel. Analüüsida loegus esitatud või mõnda muud näidet.

Pakettide filtreerimine on ennekõike vajalik võrgu turvalisuse tõstmiseks. Pakette filtreeritakse kasutades tulemüüri, mida reeglina rakendatakse eraldi arvutis ja mis on vaatab üle kõik võrku saabuvad paketid.

Filtreerimisel kasutatavad parameetrid on : Saatja IP aadress, vastuvõtja IP aadress, IP teenust kasutav protokoll Näiteks TCP või UDP, saatja port, vastuvõtja port, TCP flag ACK=1 või ACK=0, paketi liikumise suund, serveri asukoht.
Juhul kui meil on HTTP Serverile väljuv pakett, siis Saatja IP aadress = Kohalik IP aadress, vastuvõtja IP aadress = vastuvõtja serveri aadress, protokoll = TCP, saatja port = suvaline mittereserveritud port, vastuvõtja port = 80.
Juhul kui meil on HTTP Serverilt sissetulev pakett, siis Saatja IP aadress = suvaline IP aadress, vastuvõtja IP aadress = Kohalik aadress, protokoll = TCP, saatja port = 80, vastuvõtja port = mingi suvaline mittereserveeritud port.
Reeglite tabelis otsitakse sobivat reeglit alati ülalt-alla, kui leitakse sobiv reegel, siis seda rakendatakse. Kui meil on näiteks vaja, et lubatakse ainult proxy serveri HTTP protokolli, siis oleks reeglite tabel järgmine:

	Suund	Saatja aadr	Vastuvõtja aadr	Proto	Saatja port	Vastuvõtja port	ACK	Otsus
A	Välja	Kohal	Proxy aadress	HTTP	>1023	23	0 / 1	OK
B	Sisse	Proxy aadress	Kohal	HTTP	80	>1023	1	OK
C	suva	Suva	Suva	Suva	suva	suva	0 / 1	keelatud

Suund on ülalt – alla, järjestus A->B->C

Loengus käsitlesime näidet, kus vaatlesime tulemüüri toimimist. Sellest näitest tuleb välja,et tulemüüri kasutadest tuleb tabeli etteotsa panna piirangud, mis vastavaid pakette filtreerivad ja lõppu need mis kehtivad muude pakettide puhul, seega on reeglite tabeli ja tulemüüri tabeli koostamisel kõige tähtsam järjestus.

4. Protokoll IP. Internet Datagram'I päise struktuur. Protokoll IPSEC iseloomustus.

IP protokoll on selleks, et meil oleks võimalik kasutada Internetti, põhiparameeter IP protkollil on IP aadress, mis on kõigil jaamadel unikaalne ja 32 bitine. IP protokolli eelis on ka see,et meil on võimalik ühendada kokku erinevaid võrke. IP-aadress on jagatud kaheks või kolmeks osaks. Esimene osa on võrguaadress, teine (kui on olemas) on alamvõrgu aadress ning kolmas on hosti aadress. IP adresseerimine toetab viit erinevat võrguklassi, tähistusega klass A kuni klass E. Klassis A võrguaadressiks 7 bitti, klassis B 14 bitti, klassis C 22 bitti, klass D on mõeldud rühmedastuseks (multicasting) ning klass E on reserveeritud tulevikuks.

IP protokoll kasutab andmete edastamiseks IP pakette ehk Datagramme. IP protokoll annab endast parima, et need protokollid kohale jõuaksid, kuid tal ei ole sisseehitatud kontrollimis mehhanismi, seega võivad paketid saabuda sihtjaama erineva järjestusega, või võivad üldsegi mitte saabuda – selle kontrolli eest vastutab TCP protokoll.
IP Datagrami päis koosneb järgmistest väljadest:
Ver – see on IP protokolli versioon, hetkel kasutatakse Ipv4;
Hlen – see on päise pikkus sõnades;
Sc(Service class) - tavaline/väike viide, tavaline/kõrge tootlikus, tavaline/kõrge töökindlus, proriteet – tavaline/prioriteetne/kiire/välk/supervälk
IDLen – ID pikkus baitides;
Ident – määratakse IP kasutaja poolt;
Flags - sõnumi viimane fragment, sõnumi mitte viimane fragment, sõnumi esimene ja ka viimane fragment
Offset – fragmendi suhteline aadress sõnumis
Lc (Life Cycle) – ID eluiga sekundites, iga ruuter vähendab 1 võrra seega hopside arv (Time to live);
Prot – IP teenuse kasutaja identifikaator
Checksum – päise kontrollsumma
Other – tavaliselt ID ruutimisinfo
Destination – ID saatja ja vastuvõtja.

Protokoll IPSEC on lisa IP protokollile, mis pakub krüpteerimise võimalust. Ipsec pakub sarnast teenust SSL-iga, kuid IPSEC toimib võrgu kihis, st. et tegelikkuses ei ole programmidel mingit otsest kokkupuudet IPSEC-iga ja ta on selle osas võimsam kui SSL.
Loogilises mõttes pakub IPSEC järgmiseid ühenduse võimalusi :
Jaam – Jaam
Jaam – Võrk
Võrk – Võrk
Võrgu all võib siin mõista Ruuterit, sest see on ruuter, mis kontrollib mingit kindlat võrku.

5. Mis on anonüümne FTP? Miks on FTP protokollis käsud ascii ja bin?
Anonüümne FTP on FTP server, mis võimaldab anonüümset sisselogimist. Reeglina on anonüümne sisselogimine keelatud, kuid ametlikud informatsiooni ja tarkavara serverid tavaliselt anonüümset sisselogimist võimaldavad näiteks ftp.borland.com .

Käsk *ascii* on vajalik, et faile saaks FTP-s saata ascii koodina.
Käsk bin on vajalik, et faile saaks saata binaar koodina.