Komunikacijski protokoli in omrežna varnost
2010/11
Pisni izpit 14. svečan 2011

Izpit morate pisati posamič. Pri reševanju je literatura dovoljena.

Če boste uspešno vsaj delno odgovorili na vsa vprašanja, boste morda dobili dodatne točke.

Čas pisanja izpita je 90 minut.

Veliko uspeha!

NALOGA	TOČK	OD TOČK	NALOGA	TOČK	OD TOČK
1			4		
2			5		
3			6		

IME IN PRIIMEK: _____

ŠTUDENTSKA ŠTEVILKA: _____

DATUM: _____

PODPIS: _____

1. naloga: Osnove, uvod in nalaganje OS.

VPRAŠANJA:

1. Pri IPv6 smo srečali tri načine naslavljanja z angleškimi imeni: *unicast*, *multicast* in *anycast*. (i) opišite vsakega od načinov; in (ii) za vsakega od načinov opišite primer uporabe.

2. Pogostokrat smo omenjali koncept *integritete sporočila*. (i) kaj pravzaprav to pomeni; (ii) kako lahko zagotavljamo *samo* integriteto vsebine IP paketa; in (iii) recimo, da na spodnjih plasteh ni možno zagotoviti integritete, pa bi jo želeli zagotoviti v sporočilu e-pošte – kako lahko to naredimo?

   NAMIG: Pri slednjem lahko opišete svojo rešitev ali priporočite uporabo standardne rešitve, v katerem primeru pa morate obrazložiti, kako je zagotovljena celovitost (integriteta) sporočila.

3. Peter Zmeda se je tokrat podal v povsem nove vode. Naredil je svoj prvi procesor PZ-1. PZ-1 ima povsem identičen nabor ukazov kot Intel Pentium, le ob zagonu (priklopu napajanja) postavi svoj programski števec na vrednost 0xFACAFACA (zapisana šestnajstiško). Peter bo uporabil novi procesor v računalnikih v svojem podjetju. Le-ti si nalagajo operacijski sistem z omrežja s pomočjo bootp protokola. Kaj mora Peter popraviti na vseh računalnikih in kaj na strežniku?

2. naloga: Pri upravljanju z omrežji smo srečali protokol SNMP.

VPRAŠANJA:

1. Za kratico SNMP smo povedali, da pomeni *Simple Network Management Protocol*. Ali lahko Peter uporabi SNMP za nadzor in upravljanje programske opreme, ki izvaja IDS? Utemeljite odgovor.

2. Med tipi SNMP sporočili je posebno sporočilo *InformRequest*. Zakaj je posebno in za kaj se uporablja? Zapišite scenarij in primer konkretne uporabe.

3. Protokol SNMP.v2 uporablja za prenos preproste UDP pakete in Peter je spet v težavah. Dejansko ima njegovo podjetje dve pisarni – eno v Butalah in drugo Spodnjem griču. Peter je uspešno zagotovil varnost v lokalnem omrežju posamezne pisarne, žal pa promet med obema pisarnama poteka preko internetnih povezav. Kaj naj naredi Peter, da bo zaščitil SNMP sporočila, ki jih pošiljajo agenti z naprav v Spodnjem griču do SNMP upravljalca v Butalah?

3. naloga: Stvarni čas in omrežni promet.

VPRAŠANJA:

1. Pri protokolu RTP smo navedli dve osnovni funkcionalnosti: skrb za pravilno zaporedje paketov in skrb za časovne značke. (i) opišite vsako od funkcionalnosti ter jo dodatno poudarite s *primerom rabe*; (ii) kako konkretno je vsaka od funkcionalnsti *podprta v protokolu*? Pri odgovoru pomaga poznavanje oblike paketa.

2. Pogosto so protokoli razdeljeni na dva dela. En del je namenjen prenosu podatkov in drugi upravljanju in nadzoru delovanja protokola. Naštejte nadzorne protokole za naslednje podatkovne protokole: IP, RTP in PPP.

3. Peter preko RTP protokola prenaša podatke iz nove merilne naprave. Kako naj odjemalcu prenese s pomočjo protokola RTCP sporočilo o tem, da se njegova naprava imenuje *Petrovnik*? Za vse točke zapišite celoten RTCP paket z ustreznimi vrednostmi.

4. naloga: Peter je svoj sistem v podjetju precej nadgradil. Tako je nalagalnik predelal, da ob zagonu s strežnika ne dobi samo operacijskega sistema, ampak celoten sistemski datotečni sistem – nekako 200MB podatkov. Vse skupaj je poslano v obliki `tgz` ali `zip` datoteke. Prejete podatke nalaglanik namesti lokalno na odjemalcu. Ideja se je izkazala za dobro, le zjutraj, ko pridejo zaposleni v službo, vsi najprej prižgejo svoje računalnike, ki takoj pričnо z nalaganjem operacijskega sistema. V tem času je Petrovo omrežje takorekoč neuporabno, saj je odzivni čas izredno dolg. Peter je prišel na idejo, da bi za sam prenos operacijskega sistema uporabil razpošiljevalni (multicast) naslov ter se tako izognil večkratnemu pošiljanju operacijskega sistema preko omrežja. Žal ideje ni razdelal do konca.

VPRAŠANJA:

1. Kako bi Petrovo idejo udejanili? Čim natančnejši bo vaš odgovor, več točk boste dobili. Natančnejši pomeni to, da bo vaš opis lahko dobil sistemski administrator in/ali programer ter bo lahko v sistemu pravilno nastavil protokole ter njihove parametre in/ali sprogramiral, kar bi bilo morda potrebno sprogramirati.

   Pri odgovoru upoštevajte, da se definiriani protokoli ne dajo spreminjati, lahko se nadgradijo ali se uporabijo v lastnih rešitvah.

   NAMIG: Pri rešitvi upoštevajte, da mora vsak odjemalec dobiti celoten operacijski sistem in to brez napak. V rešitvi uporabite čim več že definiranih in narejenih protokolov. Upoštevajte, da je Peter že spreminjal nalagalnik ter ga zato dobro pozna.

5. naloga: Imeniška storitev in varovanje.

VPRAŠANJA:

1. Peter bi za potrebe podjetja postavil tudi strežnika imeniške storitve – enega v Butalah in drugega na Spodnjem griču. Katero od dveh možnih postavitev večih strežnikov za svoj imenski prostor naj uporabi? Utemeljite odgovor.

2. Peter bi rad okrepil zaščito v svojem omrežju. Slišal je, da obstajata sistema IDS in IPS. (i) Ali je kakšna razlika med njima? (ii) Peter že ima požarno pregrado (*fire-wall*). Ocenite in utemeljite ali potrebuje še IDS in/ali IPS?

3. Spet paranoični Peter Zmeda (ali pa ne tako zelo). Pri branju zadnjega izpita je izvedel, da se je Miha naučil namestiti bootp strežnik v njegovem omrežju, pri čemer strežnik preglasi njegove uradne strežnike. Po drugi strani ne želi menjati bootp protokola, ker se je izkazal za tako zelo uporabnega. Kako naj Peter na odjemalcu zagotovi, da je naloženi operacijski sistem resnično tisti, ki je prišel z njegovega strežnika. Pri tem mu je vseeno, če Miha vidi celotno vsebino poslanega operacijskega sistema.

   NAMIG: Peter lahko na vsak računalnik shrani do 256 zlogov informacije. Lahko tudi nekoliko nadgradi nalagalnik, ki uporablja bootp protokol, ne more pa spremeniti samega protokola.

6. naloga: AAA in IEEE 802.

VPRAŠANJA:

1. Tako, zgodilo se je. No, skoraj. Pred slabim mesec so oddali takorekoč zadnjo skupino IPv4 naslovov v uporabo in naučiti se bomo morali živeti v IPv6 svetu. Ali in kako bo to vplivalo na protokol IEEE 802.1x? Utemeljite odgovor. Upoštevajte vse korake protokola vključno s povezavo do AAA strežnika.

2. Pri IEEE 802.1x je eden od korakov avtentikacija naprave ali uporabnika. Peter bi želel avtenticirati uporabnika in se je odločil za biometrično avtentikacijo. Na vsak računalnik je namestil bralec prstnih odtisov, ki vrne niz zlogov (bajtov), ki enoličo opisuje odtis prsta. Kaj in kako mora popraviti CHAP protokol, da bo vse skupaj delovalo?[1]

   NAMIG: Pomagajte si s skico celotnega sistema od bralca odtisov do AAA strežnika. Sliko opremite s pomembnimi podatki za avtentikacijo. Pomaga tudi, če izhajate iz CHAP protokola.

[1] Isto vprašanje je bilo postavljeno na izpitu 28.1.2011. Osnovni odgovor je dolg nekako pet vrstic. Za popolnejšo analizo lahko dobite dodatne točke.