

Komunikacijski protokoli in omrežna varnost 2010/11

Pisni izpit 28. prosinec 2011

Izpit morate pisati posamič. Pri reševanju je literatura dovoljena.

Če boste uspešno vsaj delno odgovorili na vsa vprašanja, bo možno dobiti 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: Peter Zmeda je v podjetju, kjer skrbi za računalniški sistem, zmanjšal stroške sistema tako, da je namesto celotnih delovnih postaj namestil računalnike brez diskov. Za njihov zagon je uporabil bootp protokol. Ko se naloži operacijski sistem, se morajo prijaviti s svojim uporabniškim imenom in geslom.

VPRAŠANJA:

1. Zapišite korake DHCP protokola in čemu je namenjen vsak od korakov.
2. Nekateri zaposleni uporabljajo operacijski sistem *IR* in drugi *kHTW*. Peter mora sistem tako namestiti, da si bo do uporabniki lahko izbrali sistem, ki se jim bo namestil. Opišite, kako se naj Peter loti tega in pri tem uporablja zgolj bootp in tftp protokola.
3. Poredni Miha si uspe dobiti nadzor nad bootp strežnikom. Kaj lahko naredi, da si pridobi gesla uporabnikov. Opišite ključne korake čim bolj natančno.¹
4. Kako lahko Peter zaščiti uporabnike pred Mihatovim strežnikom.

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

VPRAŠANJA:

1. V čem je razlika med MIB in MDB?
2. V MIB imamo definirane:

ID predmeta	ime	tip
1.3.6.1.2.1.7.1	UDPInDatagrams	Counter32
1.3.6.1.2.1.7.2	UDPNoPorts	Counter32
1.3.6.1.2.1.7.3	UDInErrors	Counter32
1.3.6.1.2.1.7.4	UDPOutDatagrams	Counter32
1.3.6.1.2.1.7.5	udpTable	SEQUENCE

Kaj lahko poveste o medsebojnih odnosih med posameznimi identitetami/predmeti glede na njihove *ID*eje.

3. SNMP uporablja običajno UDP prenosni protokol in vrata številka 161 oziroma 162. Kje ali točneje kako (kdo) je definirano, da SNMP uporablja ta vrata?

NAMIG: Odgovor ni v predavanju o upravljanju omrežij.

¹Dejansko je Gašper na vajah ušpičil v resnici nekaj podobnega, da ste lahko v miru delali vaje.

4. Poleg SNMP smo omenjali še druga orodja za nadzor in upravljanje omrežja. Naštejte še vsaj dve in za eno od njih opišite situacijo, ko je primernejše od SNMP.

3. naloga: Stvarni (realni) čas je ena od vrednosti, ki bi jo Peter rad čim natančneje nastavil na svojih računalnikih.

VPRAŠANJA:

1. Da bi stvari poenostavil, se je odločil postaviti v podjetju strežnike omrežnega časa. i) Kateri protokol lahko uporabi v ta namen? ii) Ali je dovolj, da postavi en sam stražnik? Utemeljite odgovor. iii) Ali menite, da bi bilo smiselno, da Peter postavi v podjetju tudi atomsko uro? Zelo dobro utemeljite odgovor – predstavljajte si, da morate za direktorja napisati utemeljitev in je od vaše odločitve odvisen nakup in namestitvev.
2. Žal pa poredni Miha ponovno poskuša zmešati štrene ter mu je uspelo vriniti v sistem svoj strežnik omrežnega časa. Kako naj se Peter brani pred njim?

NAMIG: Pri odgovoru upoštevajte, kako se konfigurira odjemalec. Upoštevajte tudi možnost, da si Miha prisvoji možnost konfiguriranja odjemalca ali še lažje, da izvede zastrupljanje z ARPom.

3. Peter je prišel na idejo, da bi usklajeval ure stvarnega časa v omrežju tako, da bi njegovi strežniki preprosto oddajali uro v rednih časovnih periodah z uporabo razpošiljanja (multicast). Ali bo to delovalo dovolj dobro?

NAMIG: Pri odgovoru razislite in upoštevajte, kako natančno želi Peter nastavljati uro, kako izgleda in kako veliko je njegovo omrežje ter kako pogosto strežniki oddajajo uro. Odgovor bo vrednoten na podlagi vaših argumentov, ki morajo biti oblike: „Ker ima Petrovo, velja, da”

4. naloga: Kot smo dejali Peter upravlja z omrežjem v podjetju. Kljub temu, da se računalnikom naloži ob zagonu operacijski sistem preko omrežja, občasno želi dopolniti ali popraviti določene konfiguracijske parametre. V ta namen je razvil svoje programske agente, ki so nameščeni na vseh računalnikih. Podatke o popravkih se je agentom odločil sporočiti z razpošiljanjem (*multicast*). Njegova ideja je, da agentom občasno sporoči, da morajo naložiti s pomočjo tftp programa nove podatke s strežnika. Ta sporočila so občasna - morda nekaj sporočil na uro.

VPRAŠANJA:

1. Ker uporablja razpošiljanje, bo moral na prenosni (transportni) plasti uporabljati kateri protokol?

2. Petrovi računalniki na omrežni plasti uporabljajo IPv6 protokol. Zapišite predlog razpošiljevalnega naslova (razpošiljevalna skupina). Utemeljite vrednosti v posameznih delih naslova. Točke dobite tudi, če opišete strukturo naslova.
3. Kateri protokol sodeluje pri samem razpošiljanju (dostavi) sporočila: i) IGMP, ii) MLD, iii) PIM ali iv) nobeden od naštetih. Vprašanje preberite zelo natančno.

5. naloga: Imeniška storitev.

VPRAŠANJA:

1. Za delovanje imeniške storitve je pomemben obstoj razločevalnega imena. Kaj je to in čemu služi.
2. Peter je za potrebe podjetja postavil tudi strežnik imeniške storitve. Nekje je slišal, da lahko podatke za svoj imenski prostor hrani na večih strežnikih. Kakšni možnosti hranjenja podatka na večih strežnikih ima in čemu služi vsaka od njih? Katero, menite, naj Peter uporabi?
3. V čem je razlika med ukazoma `search` in `compare`?

6. naloga: AAA in IEEE 802.

VPRAŠANJA:

1. Peter posodablja svoje omrežje. Poleg tega, da operacijski sistem na računalnike naloži ob zagonu, se je odločil, da bo tudi zaščitil storitev dostopa do mrežja. Slednje velja tudi za računalnike, ki naj bi si naložili operacijski sistem. Kateri protokol se prej uporabi pri teh računalnikih: IEEE 802.1x ali bootp? Utemeljite svoj odgovor.
2. Uh, saj res. Peter Uporablja IPv6. Ali to kaj vpliva na rabo RADIUS protokola? Mora zaradi tega preiti na protokol DIAMETER?
3. 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 enolično opisuje odtis prsta. Kaj in kako mora popraviti CHAP protokol, da bo vse skupaj delovalo?

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.