Komunikacijski protokoli in omrežna varnost
2010/11
Pisni izpit 30. velikega srpana 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 60 minut.

Veliko uspeha!

NALOGA	TOČK	OD TOČK	NALOGA	TOČK	OD TOČK
1			3		
2			4		

IME IN PRIIMEK: _____

ŠTUDENTSKA ŠTEVILKA: _____

DATUM: _____

PODPIS: _____

1. naloga: Nalaganje OS.

VPRAŠANJA:

1. Kot imajo IP paketi svoj ponorni in izvorni naslov, imajo tudi okvirji v Ethernet protokolu svoj izvorni in ponorni naslov. Ali velja kaj posebenega pri ponornem naslovu okvirja, ki ga uporablja bootp protokol?

2. Peter Zmeda je ugotovil, da je bootp protokol zelo nevaren, saj ga je zelo preprosto izkoristiti za namestitev trojanskega konja. Kako lahko to naredimo?

3. Peter ima že pripravljeno rešitev, saj bo v bootp datagram dodal kot razširitev MD5 podpis datoteke, ki naj bi jo naložil odjemalec kot operacijski sistem. V katero polje lahko Peter shrani MD5 podpis?

4. Ali je dobra rešitev? Komentirajete svoj odgovor. Se jo da izboljšati? Če da, kako?

2. naloga: Stvarni čas.

VPRAŠANJA:

1. Omenjali smo vrsto protokolov, ki se uporabljajo za prenos podatkov v stvarnem (realnem) času. Dva med njimi imata zelo podobno kratico: RTCP in RTSP. Kakšna je razlika med njima?

2. Peter Zmeda ima novo inovacijo pred seboj. Dandanes, ko postajajo procesorji vse manjši, se je odločil pričeti izdelovati zapestne ure, v katerih bo uporabil majhen procesor. Prva naloga, ki jo ima zapestna ura, je seveda kazanje pravilnega časa. Sedaj je Peter pred dilemo, ali mora uporabiti protokol RTP ali protokol NTP? Pomagajte mu pri odločitvi in utemeljite svoj odgovor.

3. Kako je z varnostjo izbranega protokola? Ali lahko nekdo Petrovi uri na kakšen način vsili napačen čas?

4. Čemu je namenjen SRTP in kako deluje?

   NAMIG: Razmislite o vseh fazah delovanja od vzpostavitve do zaključka. Najprej razložite delovanje brez napak in nato, kako SRTP obvladuje morebitne napake (izgube) ob prenosu.

3. naloga: Upravljanje. Peter Zmeda je velik ljubitelj kave. Je tudi član društva oboževalcev kave. V društvu ga še posebej cenijo po inženirskih spretnostih in neizmerni iznajdljivosti. Njegova zadnja ideja je kavni avtomat, ki ga priključiš na omrežje. Avtomat omogoča, da preko omrežja sprožiš pripravo kave in, ko prideš do avtomata, te tam čaka sveže pripravljena kava – mnjam! Peter se je ročno lotil izdelave avtomata in vseh potrebnih protokolov za komunikacijo z njim.

VPRAŠANJA:

1. Za upravljanje se je odločil, da bo uporabil protokol SNMP. Avtomatu mora priložiti datoteko MIB. Čemu služi datoteka MIB? Podajte preprost primer datoteke, ki bi bila priložena avtomatu.

   Ali je pri definiranju datoteke povsem neodvisen ali pa mora upoštevati tudi kakšne zunanje organizacije? Utemeljite odgovor.

2. V društvu je tudi nekaj direktorjev podjetij, ki so se zelo zanimali, da bi avtomat namestili pri sebi v zadovoljstvo zaposlenih. Le kava je predraga, da bi bila brezplačno na voljo vsem zaposlenim. Peter je nadgradil avtomat, da zna uporabljati protokol RADIUS. Kako lahko protokol RADIUS pomaga pri tem, da kava ne bo brezplačna?

3. Za protokol RADIUS v osnovi vemo, da nima vgrajenih varnostnih mehanizmov. Kaj narediti, da zaposleni zagotovo ne bodo mogli priti do brezplačne kave? Utemeljite svoj odgovor.

   NAMIG: Razmislite o rešitvi v okviru protokola RADIUS ali morda nižjih plasti.

4. naloga: Podatki o omrežju in protokol IEEE 802.1x.

VPRAŠANJA:

1. Pri brezžičnih omrežjih smo med drugim srečali protokol IEEE 802.1x, ki ga uporablja EDUROAM. Ali je smiselno protokol uporabiti tudi pri ožičenih omrežjih? Utemeljite odgovor.

2. Dva od protokolov, ki smo ju srečali, sta LDAP in zgoraj omenjeni RADIUS. Kako lahko RADIUS uporablja za svoje delovanje protokol LDAP?

3. Ena najbolj pomembnih prednosti verzije v3 pred verzijo v2 protokola LDAP je, varnost prenosa podatkov. Kako je implementirana?

4. Dva od ukazov, ki jih uporablja LDAP protokol sta `bind` in `unbind`. i) Kakšna je vloga ukaza `bind`? ii) Ali mora biti pred vsakim `unbind` ukaz `bind`? Utemeljite odgovor.