Komunikacijski protokoli in omrežna varnost
2014/15
Pisni izpit 2. kimovca 2015

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			3		
2			4		

IME IN PRIIMEK: _____

ŠTUDENTSKA ŠTEVILKA: _____

DATUM: _____

PODPIS: _____

1. naloga: Osnovni protokol, ki se uporablja za nalaganje operacijskega z oddaljenega strežnika je `bootp`.

VPRAŠANJA:

A) (i) Ali protokol `bootp` omogoča sámo nalaganje operacijskega sistema? Utemeljite odgovor. (ii) Peter Zmeda ima postavljen svoj bootp strežnik, s katerega nalaga operacijski sistem na vse računalnike v podjetju. Ta strežnik je res dobro zaščiten in tudi Cefizlju ni uspelo prodreti vanj. Opišite kako lahko Cefizelj vseeno Cefizelj napade, da bi Petrovi računalniki nalagali operacijski sistem, ki ga je sam pripravil.

B) Peter je za zaganjanje prek mreže poskrbel tako, da je z žive zgoščenke skopiral vse datoteke in spremenil datoteko `pxelinux.cfg/default`, da vsebuje naslednje vrstice:

```
label zagon
        menu label ZAGON SISTEMA
        kernel /casper/vmlinuz
        append initrd=/casper/initrd.lz \\
        file=/cdrom/preseed/moj.seed boot=casper \\
        netboot=nfs nfsroot=10.5.1.1/netboot/
```

Prenašanje `initrd.lz` ob zagonu sedaj traja skoraj minuto. Ta čas bi rad skrajšal. (i) Kaj lahko naredi z `initrd.lz`, da ga zmanjša? (ii) Ali je zagon povsem brez `initrd.lz` sploh mogoč? Utemeljite odgovor!

C) Kako odjemalec pri protokolu TFTP vé, da ni dobil zadnjega paketa s podatki?

2. naloga: Upravljanje omrežij.

VPRAŠANJA:

A) Nekaj s prosojnic in nato razmislek. (i) Katera so štiri področja upravljanja? (ii) Za vsako od področij opišite primer upravljanja in sistemsko programsko opremo, ki omogoča to upravljanje.

B) Peter v službi išče razloge za omrežne težave – računalnik 192.168.1.10 se včasih ne uspe povezati s privzetim prehodom. Na svojem računalniku je pognal ukaz arp in dobil naslednji izpis:

```
Address           HWtype  HWaddress           Flags Mask Iface
192.168.1.10      ether   00:1d:72:07:3f:25   C          eth0
streznik.zmeda.si ether   00:1d:72:07:3f:25   C          eth0
192.168.1.11      ether   00:1d:72:07:3f:25   C          eth0
192.168.1.1       ether   00:22:75:24:65:64   C          eth0
```

(i) Ali mu je dani izpis povedal kaj o razlogu za napako? Utemeljite odgovor.
(ii) Kako bi lahko prišlo do takšnega stanja v tabeli ARP?

C) Kakšen mehanizem uporablja protokol SNMPv3 za preprečitev napadov s ponavljanjem *replay attack*? Opišite delovanje mehanizma.

3. naloga: Stvarni čas in okoli njega. Peter je dolga leta namesto budilke uporabljal naslednje zaporedje ukazov:

```
sleep 7h; mplayer -loop 0 vivaldi.mp3
```

Argument `-loop 0` pomeni, da se datoteka `vivaldi.mp3` ponavlja v neskončnost. Pred kratkim je slišal, da je za človeka bolje, če se zbuja postopoma. Sedaj bi rad vstajal tako, da mu bo po 7h glasba začela igrati povsem potihem, ob 7:05, 7:10, 7:15, 7:20 bo glasba vedno bolj glasna, od 7:25 pa bo glasnost na najvišji stopnji. Za nastavljanje glasnosti Peter lahko uporabi ukaz `amixer` – na primer:

```
amixer cset name='Master Playback Volume' 0
```

glasbo povsem utiša, med tem ko jo

```
amixer cset name='Master Playback Volume' 65536
```

naredi kar se da glasno.

VPRAŠANJA:

A) Da Petru ne bo treba vsakič pisati „Master Playback Volume“ mu pomagajte. (i) Napišite ukaz, ki v okoljsko spremenljivko `M` spravi vrednost „Master Playback Volume“ z narekovaji vred. (ii) Kako potem spremenljivko `M` uporabi, da glasnost nastavi na 30000? (iii) Napišite ukaz ali zaporedje ukazov, ki Petra zbudi, kakor si je zamislil. Glasba naj igra celo noč, le zvok naj bo povsem utišan. Pri zviševanju glasnosti ni nujno, da jo ukaz zvišuje povsem enakomerno. Privzamete lahko, da je spremenljivka `M` že nastavljena.

B) Glej ga zlomka, Peter je po dveh tednih spet zamudil na predavanja, saj ga je budilka zbudila prepozno. (i) Katero storitev ozirom protokol naj uporabi, da bo ura na njegovem računalniku vedno točna. (ii) Kako naj Cefizelj napade protokol/storitev, da bo ura na Petrovem računalniku vedno zaostajala točno za eno uro? (iii) Se Peter lahko brani pred takšnim napadom?

C) Če se želi odjemalec prijaviti v skupino, potem naj uporabi kateri protokol? Utemeljite odgovor.

4. naloga: Varnost in navihanost.

VPRAŠANJA:

1. Protokol IEEE 802 je umeščen v protokolni sklad na drugo, povezavno plast. Sestoji se iz dveh podplasti. (i) Katerih? (ii) Ena od funkcionalnosti, ki jih omogoča IEEE 802 so tudi navidezna lokalna omrežja – VLAN. Katera od podplasti skrbi za njihovo delovanje in opišite, kako delujejo.

2. Peter si je namestil program za zaznavanje vdorov `netdetect`. Postavil ga je nekam na datotečni sistem ter popravil svoj `~/.bashrc` tako, da se mu ob zagonu okoljska spremenljivka `NETDETECT` nastavi na imenik, v katerem je program. (i) Kako lahko Peter izve, v kateri imenik je spravil program? (ii) Kako ga lahko s čim manj tipkanja požene? Ime samega programa je `netdetect`.

3. Petru Zmedi je vseeno, če drugi prisluškujejo prenešenim sporočilom v njegovem VPN, za katerega uporablja protokol IPSec, le to bi rad zagotovil, da bo prejemnik prepričan, da je sporočilo res poslal pošiljatelj. Kakšno glavo naj uporabi? Utemeljite odgovor.