# KPOV – vprašanja 1,2,3

**Ali lahko na enem računalniku poganjamo več SNMP agentov? Če da, kako?**

Da, na sistemu lahko teče več procesov in vsak je lahko SNMP agent.

**Kako RFC 2131 ureja obstoj večih DHCP strežnikov?**

Določa, da se odjemalec sam odloči, katero DHCP ponudbo bo upošteval.

**Ali naprava z IP naslovom 192.168.2.10 lahko pošlje omrežni paket napravi z IP naslovom 192.168.3.15?**

Da, če je prisoten usmerjevalnik, ali če je število bitov omrežnega naslova 23 ali manj.

**Prejeli smo naslednji niz zlogov v TLV zapisu (najprej onega povsem na desni, vrednosti so desetiške)  33 73 82 70 04 02 33 73 82 70 04 04**

 "FRI!" 1179797793

**Ali lahko stanje omrežnega (IEEE 802.3) stikala nadziramo brez SNMP?**

Da, ampak je zaradi velikega števila orodij, ki ga podpirajo, SNMP bolj prikladen.

**Kaj naj bi ščitil SecureBoot?**

Sistem pred zagonom nepodpisanega zagonskega nalagalnika.

**Razvili smo lasten aplikacijski protokol ABC. Na transportni plasti smo se odločili za UDP protokol. Kako to vpliva na zanesljivost komunikacije med dvema udeležencema v ABC protokolu (en odgovor)?**

Komunikacija je lahko zanesljiva, če ABC protokol sam poskrbi za zanesljivost.

**Ali IPv4 podpira razpošiljanje (multicast)?**

 Da, obstaja in se uporablja.

**Kako SNMPv3 preprečuje napade s ponovitvijo (replay attack)?**

Z uporabo žetonov (token, nonce) pri šifriranju sporočil.

# KPOV – vprašanja 4,5

**Če se odjemalec želi prijaviti v skupino, potem uporabi naslednji protokol:**

MLD, IGMP

**Aplikacija v stvarnem času prenaša govor oseb. Kako naj obravnava izgubo manjšega števila paketov?**

Aplikaciji ni potrebno ukrepati, saj zaradi manjšega števila izgubljenih paketov poslušalec izgube verjetno sploh ne bo zaznal.

**Kam bo IPv6 paket s ciljnim naslovom FF02::D dostavljen?**

Vsem PIM usmerjevalnikom na lokalnem omrežju.

**Ali stikalo lahko pridobi informacije o skupinah razpošiljanja in se tako izogne razpošiljanju paketov vsem članom podomrežja?**

Da, s pomočjo IGMP vohljanja.

**Kakšna je najmanjša enota časa, ki jo lahko predstavimo v NTP (v obliki NTP Date format)?**

Malo več kot 5\*10-20s

**Katero polje opisuje število virov, ki jih je združil mešalec?**

Polje CC v RTP paketu.

**SRTP je varni RTP protokol. Koliko RTP paketa kriptiramo z njim?**

Samo vsebino kriptiramo. Integretiramo celoto

**Kako lahko ugotovimo, ali je kateri koli računalnik na omrežju prijavljen na neko konkretno razpošiljevalno skupino (multicast group)?**

 Z uporabo IGMPv1, IGMPv2 ali IGMPv3 poizvedbe

**Ali sme na Internetu obstajati več kot ena razpošiljevalna skupina z naslovom 224.0.0.32? Kaj pa 239.2.1.13?**

224.0.0.32 - ne, 239.2.1.13 - ne

**Vir toka podatkov (SSRC) pošilja podatke sprejemniku. Kako lahko sprejemnik ugotovi kaj je pošiljatelj (kamera, mikrofon, ...)?**

Z uporabo NAME polja v RTCP protokolu.

# KPOV – vprašanja 6,8

**Kako protokol CHAP preprečuje napade s ponavljanjem?**

Z uporabo naključnega izziva.

**Peter Zmeda se je odločil zasoliti shranjena in zgoščena gesla, da bi ne bila ranljiva na mavrični napad. Žal je vrednost soli izgubil. Je to pomembno?**

Da, ker brez soli ne more preveriti pravilnosti gesla.

**Peter Zmeda je na računalnikih v službi poskrbel za avtentikacijo z uporabo protokola RADIUS. Njegov paranoični sodelavec sedaj vsako jutro vdira v računalnik, saj je prepričan, da mu zaradi Petrove rešitve nekdo lahko ukrade geslo. Je njegov strah utemeljen?**

Da - gesla pri RADIUS so shranjena v tekstovni datoteki, ki jo lahko prebere kdorkoli.

**Peter Zmeda je malce zmeden. Namesto v nastavitvene datoteke strežnika DNS in DHCP je namreč podatke o računalnikih - IP naslove, MAC naslove in imena v svojem omrežju vnesel v imenik, dostopen prek LDAP. Sedaj bi rad podatke uporabil za strežnike DHCP in DNS, Pri tem bi rad čim manj podatkov pretipkaval. Kako lahko postavi svoj sistem?**

DHCP in DNS strežnika lahko svoje nastavitve prebereta iz baze LDAP. DHCP and DNS servers can store their data in LDAP.

**Katere so glavne razlike med LDAP v2 in LDAP v3 (prim. RFC 2251)?**

LDAPv3 uporablja močno avtentikacijo in varovanje podatkov z uporabo SASL

LDAPv3 dovoljuje vrednosti prilastkov zakodirane z UTF-8

LDAPv3 podpira porazdeljeno hranjenje podatkov domene tako, da strežnik lahko prenaslovi odjemalca k drugemu strežniku

**Recimo, da prejmemo PPP paket, ki prenaša podatke za avtentikacijo. Kakšna je vrednost prvih dveh zlogov?**

c2h 23h, c0h 23h

**Protokol syslog je zabeležil spodnji zapis. Kateri program je zahteval zabeležko? *Jan  1 21:38:22 svarun dhcpd: uid lease 192.168.127.137 for client 10:9a:dd:a6:dd:38 is duplicate on 192.168.127.0/24***

dhcpd

**Včasih želimo najti objekte na osnovi bolj zapletenih poizvedb. Lahko bi na primer iskali vse ljudi iz Maribora, ki jim je ime Janez ali Borut. Vprašanje je, ali poizvedbeni jezik, s katerim dobivamo podatke iz baze LDAP, kaj takega sploh podpira?**

Takšne poizvedbe so mogoče; za veriženje pogojev uporabljamo prefiksno notacijo. This is supported. The conditions are chained using a prefix notation.

**Ali lahko ime RADIUS kraljestva (realm) vsebuje znak "@"? Kaj pa uporabniško ime?**

'@' lahko nastopa tako v uporabniškem, kot tudi v imenu kraljestva. The '@' can be used in both usernames and realm names.

**Če kot strežnik DNS uporabite dnsmasq, lahko le-ta skrbi, da klienti, ki pridobijo naslov prek DHCP, dobijo tudi vnose v DNS. Ali je to mogoče tudi, če sta DHCP in DNS strežnik ločena programa?**

Avtomatizirano popravljanje vnosov v DNS je opisano v več RFC-jih. Automatic updates of DNS entries are described in multiple RFCs.

# KPOV – vprašanja 7,9

**Protokol IPsec je implementiran na kateri plasti?**

mrežni / network layer

**Kateri izmed naslednjih izrazov v Javi je najbolj primeren za izračun naključne VLAN ID vrednosti (Namig: upoštevajte, vendar ne uporabite, rezervirane vrednosti za VLAN ID (802.1Q))?**

(rand.nextInt() % 4094) + 1

**Katere standardne protokole oz. dele le-teh podpira/implementira OpenVPN?**

OpenVPN ne uporablja standardnih protokolov, uporablja pa knjižnico OpenSSL.

**Kako ESP preprečuje napade s ponavljanjem?**

S pomočjo zaporedne številke v ESP glavi.

**Obstajata dva standarda za brezžična omrežja: IEEE 802.11 in IEEE 802.16. Recimo, da imamo prenosnik, ki ga imamo priključenega na vtičnico po standardu IEEE 802.3 in ga odklopimo ter se pričnemo premikati po prostoru. Sedaj moramo dobiti povezavo z omrežjem preko enega od prej omenjenih standardov. Katera IEEE 802 delovna skupina se ukvarja s tem problemom?**

IEEE 802.21

**Kaj pomeni "tunneling" pri VPN omrežjih?**

Način kriptiranja paketa, tako da kriptira podatke in glavo

**Peter Zmeda je slišal, da postaja internet stvari (IoT - Internet of Things) stvarnost. Zato se je odločil, da bo definiral svojo obliko okvirjev v protokolu IEEE802. Kaj vse mora definirati, da bodo njegovi okviri še vedno nemoteno potovali in da jih nihče drug pomotoma ne bo obdeloval?**

ethertype

**Med katerima dvema stranema poteka pogajanje po EAP protokolu?**

Med odjemalcem (angl. supplicant) in avtentikatorjem.

**Peter in Špela bi rada vzpostavila med sabo SA. Vse ostale elemente za vzpostavitev SA si lahko varno izmenjata po elektronski pošti, samo enega ne. Katerega?**

HMAC key / ključ: ključa za integriteto sporočil, ker bi ga lahko Cefizelj ukradel / key to check the integrity as Cefizelj could steal it

**Za kaj uporabljamo PAM?**

PAM je mehanizem za integriranje več nižje nivojskih avtentikacijskih shem v višje nivojsko