Praktický test ze 4IZ110

Pouze pro cvičení vedené Ing. Dočekalem!

Model sítě pro úlohu č. 1 naleznete v souboru **prakticky_test_3.fls** v materiálech spolu se zadáním testu. Model si načtěte v programu Filius a průběžně si jej ukládejte. Zároveň si vytvořte textový dokument, kam umístíte odpovědi na jednotlivé úkoly a kde budete také dokumentovat postup, a to od úlohy č. 2 dále. Postup dokumentujte pořízením screenshotů (klávesa PrintScreen a Ctrl-V do dokumentu), přidat můžete i stručný komentář.

Správné odpovědi bez zdokumentování postupu nebudou uznány a zdokumentovaný postup bez správné odpovědi také ne!

Oba soubory (vyřešené síťové schéma FLS a PDF dokument s postupem a odpověďmi) odevzdejte do odevzdárny „**Praktický test č. 3**“ a několikrát se ujistěte, že jste odevzdali korektně. V případě, že se vám nebude dařit odevzdat přes InSIS, alternativně můžete odevzdat na mail cvičícímu (docm01@vse.cz).

Test vypracovávejte samostatně, nekomunikujte s nikým kromě cvičícího. Případné problémy, nejasnosti a nesrovnalosti řešte s cvičícím. Čtěte zadání vždy velmi pozorně.

Úkoly

0) Rozdělte síť **74.16.0.0/15** na tři podsítě pro níže uvedený počet uzlů. (3b)
Síť A (min. 17000 PC): Adresa sítě: _____ Maska: _____ Kapacita: _____
Síť B (min. 60000 PC): Adresa sítě: _____ Maska: _____ Kapacita: _____
Síť C (min. 30000 PC): Adresa sítě: _____ Maska: _____ Kapacita: _____
Masku udávejte v CIDR formě a kapacitu v hrubém stavu (s adresou sítě i broadcastem).

1) V síťovém simulátoru **Filius** (model **prakticky_test_3.fls**) proveďte následující (8b):

   a) Do sítě **147.65.12.224/27** přidejte **2** počítače pro *Šárku* a *Zuzanu*. (1b)

   b) Do sítě **147.65.12.224/27** přidejte **DHCP server** a zařiďte, aby všechny počítače v dané síti (i Petra a Agáty) přebíraly IP adresu a ostatní síťová nastavení z vámi **korektně a plně nastaveného DHCP serveru**. (2b)

   c) Na počítači **ns.kvetinka.cz** je nainstalovaný DNS server. Vytvořte na něm dva záznamy typu **A** pro doménová jména **web.kvetinka.cz** a **kvetinka.cz**, přičemž obě domény musí směřovat na IP adresu počítače **web.kvetinka.cz**. (1b)

   d) Nastavte směrovací pravidla tak, aby se počítače v sítích **147.65.12.224/27** a **146.102.173.144/28** dostaly na **ns.kvetinka.cz**. (2b)

   e) Nastavte firewall na vhodném místě tak, aby se nikdo (včetně Záškodníka) nemohl spojit s žádným **TCP** portem počítače **web.kvetinka.cz** s výjimkou portů pro nešifrované služby **HTTP** a **SMTP**. Žádná jiná komunikace nesmí být omezena (včetně **ICMP** a všech **UDP** portů na **web.kvetinka.cz**, které musí zůstat otevřené). (2b)

- Výsledkem vaší práce by mělo být schéma, kde je možné z počítačů *Petra, Šárky, Agáty a Zuzany* prohlédnout webovou stránku **web.kvetinka.cz** ve webovém prohlížeči a kde si Petr a Agáta mohou posílat e-maily (webový a poštovní server na **web.kvetinka.cz** jsou plně nastaveny, stejně tak poštovní klienti **Petra** a **Agáty**)

Pokračování na další straně →

2) Zjistěte obě jména **administrativních kontaktů** pro hlavní doménu **Univerzity Tomáše Bati ve Zlíně**?_____,_____ (2b)

3) Kolik **směrovačů** na trase mezi **vámi** a serverem **4iz110.vse.cz** se nachází v ČR? Odhad můžete založit na DNS názvech směrovačů: _____ (1b)

4) Kolik poštovních serverů určených **IP adresou** má k dispozici **Česká zemědělská univerzita v Praze**? Uveďte i konkrétní IP. _____ (2b)

5) Pomocí programu Wireshark analyzujte útok na server **krkavec.net** v souboru **wireshark-prakticky-test-3.pcap**. Odpovězte na všechny podotázky. (4b)

- Povedl se útočníkovi útok? Vysvětlete. (2b) _____
  _____
  _____
- Jaká je **maximální** velikost **e-mailu**, který lze na server **krkavec.net** doručit? (1b)
  _____
- Zjistěte, z jaké **země** pocházel **vlastník IP adresy**, která na server **krkavec.net** útočila: (1b) _____

Bonus: V souboru **wireshark-prakticky-test-3-bonus.pcap** naleznete **HTTPS** komunikaci, která je samozřejmě šifrovaná (pomocí protokolu **TLS**).

V **HTTP** komunikaci je v dnešní době zvykem v požadavcích *klienta* uvádět **DNS jméno** serveru, jehož prezentaci chcete zobrazit (server může totiž hostovat více prezentací, a na základě klientem zadaného **doménového jména** pak server určí, co vám má zobrazit).

- Prověřte, zda-li je možné **DNS název** klientem požadované webové prezentace z této šifrované komunikace zjistit, aniž by bylo třeba prolomit šifrování samotné – podaří-li se vám to, uveďte daný DNS název (1b):

  _____

  _____

Pokud to možné je, podstatně to usnadňuje např. sledování aktivit uživatelů státem v méně svobodných zemích, a také to usnadňuje realizaci cenzury internetu, protože i navzdory šifrování lze určit doménové jméno webové prezentace, ke které chcete přistupovat.

Konec testu