Praktický test ze 4IZ110

Pouze pro cvičení vedené Ing. Dočekalem!

Vytvořte si textový dokument, kam umístíte odpovědi na jednotlivé úkoly a kde budete také počínaje úlohou č. **3** dokumentovat postup. Postup dokumentujte pořízením screenshotů (klávesa **PrintScreen** a **Ctrl-V** do dokumentu), přidat můžete i stručný komentář. Screenshoty příliš neořezávejte, klidně v práci nechte celé snímky obrazovky.

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

Oba soubory (vyřešené síťové schéma FLS z úlohy č. **2** a PDF dokument s postupem a odpověďmi) odevzdejte do odevzdárny „**Praktický test č. 4**“. a ujistěte se, že jste odevzdali korektně. V případě problému při odevzdávání do InSIS nouzově odevzdejte mailem cvičícímu na adresu: 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) Máte k dispozici IP adresu **10.10.10.56** s maskou **28** (CIDR notace).
   a) Patří IP adresa **10.10.10.64** do této sítě? (1b) ano / ne
   b) Rozdělíte-li tuto síť na 4 stejně velké podsítě, jakou budou mít: (1b)
      - masku sítě _____ (CIDR notace)
      - čistou kapacitu? _____ (počet IP adres použitelných pro koncové stanice)

1) Určete adresu sítě a masku tak, aby IP adresy **10.10.10.63** a **10.10.10.47** ležely v této síti, ale současně aby tato síť byla nejmenší možná. (1b)

   adresa sítě: _____ maska: _____ (CIDR notace)

2) V síťovém simulátoru **Filius** (model **prakticky_test_4.fls**) proveďte následující (8b):
   a) Do sítě **147.65.12.224/27** přidejte **2** počítače pro *Arnolda* a *Sylvestra*. (0.5b)
   b) Do sítě **147.65.12.224/27** přidejte **DHCP server** a zařiďte, aby všechny počítače v dané síti (i Petra a Gertrudy) přebíraly IP adresu a ostatní síťová nastavení z vámi **korektně a plně** nastaveného DHCP serveru. Jako DNS server pro tuto síť použijte počítač **ns.kvetinka.cz**. (2b)
   c) Na počítač **ns.kvetinka.cz** nainstalujte **DNS server**. Vytvořte na něm záznamy typu **A** pro doménová jména **web.kvetinka.cz** a **kvetinka.cz**, která nasměrujte na IP adresu počítače **web.kvetinka.cz**. Nastavte též **MX** záznam (doména: **kvetinka.cz**, poštovní server: **kvetinka.cz**). Pozn: ve Filiusu nelze u **MX** záznamů nastavovat prioritu, tak ji ani nehledejte. Není tam. (2b)
   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 počítači **web.kvetinka.cz** tak, aby propouštěl pouze provoz na nešifrované porty služeb **SMTP** a **HTTP**, nikam jinam. ICMP povolte. (0.5b)
   f) Gertruda poslala Petrovi mail s názvem rostliny, kterou chce Petr objednat pro svoje zákazníky. Na počítači Petra je nakonfigurovaný poštovní klient (uživatel **petr**, heslo: **petr**). Mail stáhněte a zjistěte, o jakou rostlinu se jednalo: (1b)

      _____

      _____

Pokračování na další straně →

3) Prověřte míru implementace protokolu IPv6 **Vysoké školy chemicko-technologické v Praze** zjištěním, zda-li existuje **AAAA** DNS záznam pro hlavní web této školy a také pro autoritativní **NS** servery domény druhého řádu, kterou škola používá. (2b)
- hlavní web školy: _____
- autoritativní NS servery: _____

4) Zjistěte, kolik směrovačů je mezi vámi a serverem **krkavec.net**. Vyberte si jeden ze směrovačů a spočítejte průměrnou dobu jeho odezvy. (2b)
počet směrovačů: _____
zvolený směrovač:_____
průměrná doba doba odezvy zvoleného směrovače: _____ ms

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

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

- Vysvětlete, o co se útočník snažil a zda-li se mu to povedlo. (2b)
  _____
  _____
- Proběhlo **ukončení TCP spojení** korektně (čtyřcestným handshakem)? Pokud ne, k čemu došlo? Vysvětlete. (1b)
  _____
  _____
  _____
- Zjistěte, jaké **firmě** patří **IP adresa**, která na server **krkavec.net** útočila: (1b)
  _____

Bonus: V souboru **wireshark-prakticky-test-4-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