Praktický test ze 4IZ110

Pouze pro cvičení vedené Ing. Dočekalem!

Model sítě použité v testu naleznete v souboru **prakticky_test_2.filius** 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), které můžete doplnit stručným komentářem.

Správné odpovědi bez zdokumentování postupu nebudou uznány a správný postup bez správných odpovědí také ne!

Vyřešené síťové schéma spolu s dokumentem s postupem a odpověďmi odevzdejte do odevzdárny „**Praktický test č. 2**“ a minimálně dvakrát se ujistěte, že jste test odevzdali korektně včetně všech souborů. V případě nouze můžete test alternativně odevzdat mailem na adresu cvičícího: docm01@vse.cz

Test vypracovávejte samostatně, nekomunikujte s nikým kromě cvičícího. Případné problémy, nejasnosti a nesrovnalosti řešte s cvičícím. Čtěte zadání vždy velmi pozorně, zejména u úlohy č. 4.

Úkoly

0) Rozdělte síť **146.103.0.0/16** na tři podsítě pro níže uvedený počet uzlů. (3b)
Síť 1 pro 8500 uzlů – Adresa sítě: _____ Maska: _____
Síť 2 pro 30000 uzlů – Adresa sítě: _____ Maska: _____
Síť 3 pro 15000 uzlů – Adresa sítě: _____ Maska: _____

1) V síťovém simulátoru **Filius** proveďte následující (8b):

   a) Do sítě **146.102.173.144/28** přidejte **3** počítače pro *Šárku*, *Lenku* a *Zuzanu*. (1b)

   b) Do sítě **146.102.173.144/28** přidejte **DHCP server** a zařiďte, aby všechny počítače v dané síti (i Petr) přebíraly IP adresu a ostatní síťová nastavení z vámi **korektně** a **plně** nastaveného DHCP serveru. Jako DNS server použijte IP adresu počítače **ns.kvetinka.cz**. (2b)

   c) Na počítač **ns.kvetinka.cz** nainstalujte DNS server a vytvořte v něm dva záznamy typu A pro doménová jména **www.kvetinka.cz** a **kvetinka.cz**, obě domény musí směřovat na IP adresu počítače **www.kvetinka.cz**. (2b)

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

   e) Nastavte firewall na vhodném místě tak, aby se nikdo nemohl spojit s žádným TCP portem počítače **www.kvetinka.cz** kromě portu pro službu HTTP (webový server). UDP a ICMP protokoly nesmí být omezeny. Žádná jiná komunikace nesmí být omezena. (1b)

- Výsledkem vaší práce by mělo být schéma, kde je možné z počítačů *Petra*, *Šárky*, *Lenky* a *Zuzany* prohlédnout webovou stránku **www.kvetinka.cz** ve webovém prohlížeči Filiusu zapsáním URL http://www.kvetinka.cz nebo http://kvetinka.cz
- Webový server na **www.kvetinka.cz** je již plně nastaven

Test pokračuje na další straně →

2) Kdo je **administrativním kontaktem** (zjistěte **jméno** daného člověka) pro doménu druhého řádu **Západočeské univerzity v Plzni**? _____ (2b)

3) Jaké **doménové jméno** náleží IP adrese **147.230.16.27?** _____ (1b)

4) Za předpokladu, že je **sekundární** poštovní server **Univerzity Tomáše Bati ve Zlíně** mimo provoz, kterému **poštovnímu serveru** bude doručována pošta pro tuto univerzitu?
_____ (2b)

5) Pomocí programu Wireshark analyzujte podezřelou **HTTP** komunikaci zachycenou na webovém serveru **krkavec.net** do souboru **prakticky_test_2.pcap**. Vyřešte všechny podúlohy této úlohy. (4b)

- Předpokládejte, že odchozí pakety **HTTP klienta** měly výchozí **TTL** 64 a pokuste se odhadnout, přes kolik směrovačů šla komunikace mezi ním a webovým serverem. (2b)_____

- Jaký **port** si zarezervoval **HTTP klient** na svém počítači pro komunikaci s HTTP serverem? (1b)_____

- Z jakého **města** a **státu** pochází **majitel** IP adresy **HTTP klienta**? Buďte co nejpřesnější, tzn. pokud majitel pochází z nějakého státního uskupení typu Spojené státy či Evropská unie, pak jako **stát** označte jak dané uskupení, tak konkrétní stát z daného uskupení, ze kterého majitel pochází. (1b)
  Stát: _____ (např. Česko, EU)
  Město: _____ (např. Praha)

Bonus: Proveďte analýzu aplikačního protokolu HTTP v souboru **prakticky_test_2.pcap** a stručně popište, k čemu v této komunikaci došlo. Odhadněte, zda-li byl klient útočníkem. Pokud se domníváte že ano, pak zkuste zjistit/odhadnout o co se útočník snažil a zda-li mu to vyšlo. (1b)

_____

_____

_____

_____

_____

_____

_____

Konec testu