Cvicenie11

OBSAH

Aplikačná vrstva

Úloha 0: Výhrady, komentáre, úprava bodov max. do konca 11. týždňa, Course Feedback [editovať]

Prosíme venovať pozornosť týmto oznamom:

- Ak vaše skóre z niektorého minulého testu (testy 1-10), alebo DÚ, nie je ešte doriešené (napríklad mal ste zle formulovanú otázku, alebo chybnú otázku, alebo systém vám nesprávne spočítal body a pod.), nahláste a vyriešte to so svojim vyučujúcim na tomto cvičení, najneskôr však do konca 11. týždňa. Za vyriešenie nepovažujeme napísať post niekam do kanála, ale aktívne a osobne

to riešiť s niektorým učiteľom, ideálne počas cvičenia, alebo si ho odchytíte v inom čase. Neskôr už reklamácie neprijímame, preto ustrážte si to a vyriešte najneskôr do konca 11. týždňa.
    - opravné testy sa budú nahlasovať až na ďalšom cvičení v 12. týždni, a písať v 13. týždni
- Z domu do konca tohto týždňa do 23:59, vyplňte dotazník Course Feedback, nájdete ho tu (učiteľ skontroluje na cvičení v 12. týždni):

  www.Netacad.com

    - > PIKS_aktuálnyRok > [po vojdení do kurzu sa presuňte dole] > Course Feedback (sekcia): Course Feedback (test/Assignment)
        - je to Cisco dotazník (v angličtine), pre zisťovanie vašej spokojnosti s Cisco kurzom, s materiálmi ktoré sú v rámci neho ponúkané, a aj inštruktormi, na základe ktorého sme hodnotení ako inštruktori, ako aj celá Cisco akadémia. Bez jeho vyplnenia vás nevieme v tomto kurze uzavrieť a vyžiadať pre Vás certifikát

Z čoho a ako sa robí domáca úloha (hodnotená, dobrovoľná):

K nasledujúcim úlohám 1-3 máme na hlavnej Moodle stránke v 11. týždni pripravený test "DU_11":

- je to priestor pre zadávanie vašich odpovedí na otázky k nasledujúcim úlohám 1, 2 a 3
    - keď začnete riešenie, máte na to max. 6 hodín, a iba jeden pokus na test
    - každý otázka je ale v adaptívnom režime, t.j. ak zadáte, alebo vyberiete nesprávnu odpoveď, zistíte to tak, že si ju dáte Skontrolovať, systém vám dá penalizáciu, zväčša mínus 0,33 bodu, alebo 0,25 bodu, ale môžete si odpoveď opraviť
    - neoplatí sa preto tipovať, ale zároveň máte možnosť sa opraviť, ak ste sa niekde naozaj pomýlili
- odporúčame tento test spúšťať až **po** cvičení
- cvičenie odporúčame využiť na prejdenie si daných úloh spolu s učiteľom, diskutovať o krokoch v úlohách, a následne by si z domu do nedele pol noci mal študent spraviť dané úlohy sám
    - otvorí si tieto zadania úloh, a v druhom okne test DU_11, kde bude zadávať odpovede

Úloha 1: Preskúmajte HTTP a HTTPS [editovať]

Odsledujte HTTP komunikáciu medzi Vami a webovým serverom http://example.org

Komunikáciu zachyťte a analyzujte v programe Wireshark.

- V programe **Wireshark** kliknite pravým tlačidlom myši na **HTTP** paket, vyberte "**Follow**" a následne "**TCP stream**".
  Zobrazí sa Vám okno, kde sú červeným písmom napísané požiadavky klienta a modrým odpovede servera.
- Niektorá HTTP komunikácia nemusí byť dobre čitateľná, aj keď nie je šifrovaná, pretože je komprimovaná:
  - vtedy nájdete vo Wiresharku vypísané "gzip"
  - pokúste sa preto nájsť aj komunikáciu, ktorá nebude komprimovaná
- Aký transportný protokol sa použil a prečo?
- Aký zdrojový a aký cieľový port sa použil?

Odsledujte HTTPS (šifrovanú) komunikáciu medzi Vami a webovým serverom www.uniza.sk

Odporúčame spraviť najprv filter **ip.addr == IP_servera** (alebo, ak sa komunikuje cez protokol IPv6, tak **ipv6.addr == 2001:...**), kde IP_servera www.uniza.sk, si zistíte pri pingu na túto doménu **ping www.uniza.sk**.
Upozornenie: Pokiaľ ste v laboratóriu (napr. RB003, ..), v ktorom máte dual stack, čiže podporu aj TCP/IPv4 aj TCP/IPv6, tak OS na danom PC, a v ňom implementované dané TCP/IP v4 a v6 sady protokolov (stacks), sa správajú takto:

- klient (vy siediaci za daným PC) napíše do prehliadača www.uniza.sk, pretože si chce zobraziť obsah daného webu
- v pozadí vaše PC posiela DNS request, ktorým potrebuje zistiť na akej IP (v4 alebo v6) adrese je dostupný daný server, ktorý poskytuje aj dané web služby
  - ak dané PC má podporu aj IPv4 aj IPv6, tak si vypýta (požiada) aj o IPv4 aj IPv6 adresu pre danú doménu (www.uniza.k)
  - ak získa len IPv4, tak použije tú
  - ak ako odpoveď získa obe adresy, preferovane využije tú IPv6
    - v tomto prípade preto musíte zistiť, aké je táto IPv6 adresa, aj tu si viete pomôcť pingom v príkazovom riadku na www.uniza.sk, a vo výpise uvodíte, z akej IPv6 adresy získavate odpoveď - a túto IPv6 adresu použijete do filtra vo Wiresharku
      - vôbec nevadí, ak nedostanete odpoveď pri danom pingu, pretože cieľom nie je zistiť dostupnosť daného servera, na ktorom beží daný web www.uniza.sk, ale dopátrať sa k IP adrese daného servera - a to uvidíte hneď v prvom riadku v CMD:
        Pinging .... [2001:4118: .....] -- a túto IPv6 adresu použijete ako prvý filter vo Wiresharku

- to že ping nevracia odpoveď, môže byť z dôvodu, že admini na CeIKT UNIZA blokujú ICMPv6 správy typu echo-request a echo-reply, čo sú typy ICMPv6 správ ktoré sa využívajú v utilite ping

Následne v programe Wireshark kliknite pravým tlačidlom myši na ľubovoľný riadok z tejto komunikácie (napr. TCP) a vyberte "Follow" a následne "TCP stream".

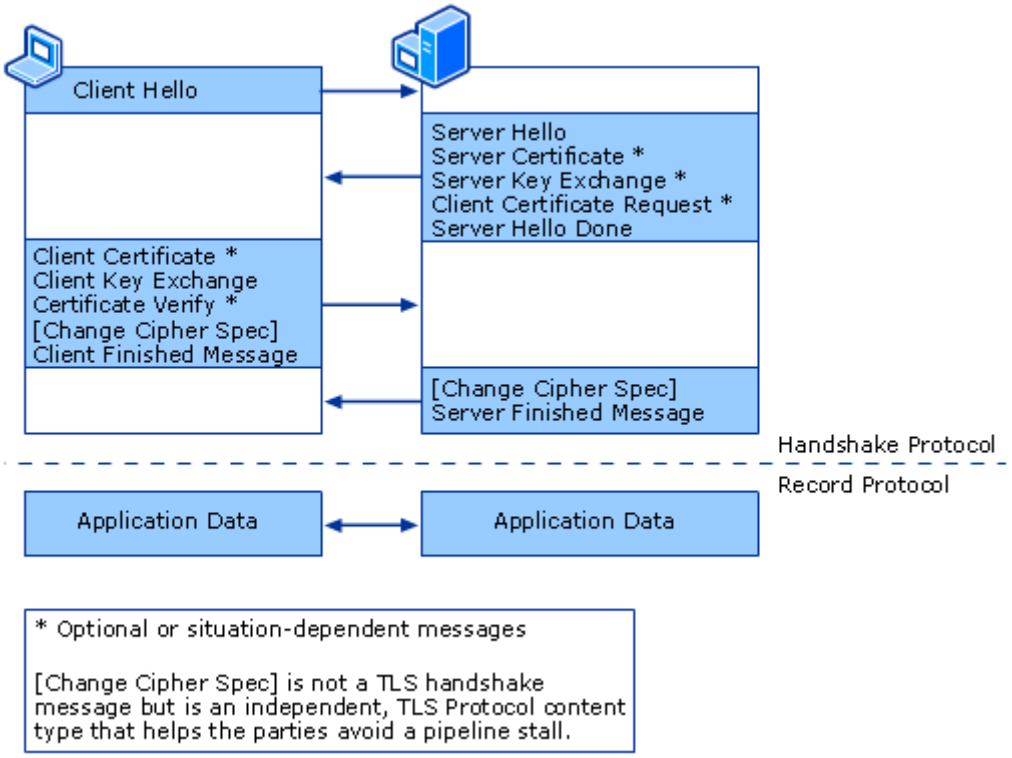
Zobrazí sa Vám okienko, kde sú červeným vypísané požiadavky klienta a modrým odpovede servera. Nie sú čitateľné, keďže sú šifrované, preto budeme analyzovať iba hlavičky TCP a TLS. Okno TCP stream môžete zavrieť, ale pozrite aký filter vám to pridalo do poľa filter (tcp.stream eq ...) a ten si tam ponechajte.

- Pozn.1: Keď chcete nájsť vo Wiresharku protokol HTTPS, hľadajte **TLSv1.3**, na čo môžete použiť filter SSL (TLS ako filter sa použiť nedá, funguje iba SSL).
- Pozn.2: Všimnite si že to, čo Wireshark zobrazuje ako TLSv1.3 môžu byť v skutočnosti rôzne aplikačné dáta (napr. IMAP, HTTP, ...), ktoré použili na šifrovanie protokol TLSv1.3. V našom prípade je to HTTPs.
- Nás ale v tejto úlohe zaujíma iba HTTPS, t.j. dáta HTTP protokolu šifrované pomocou protokolu TLS, zabalené v TCP segmente, ktorý je zabalený v IPv4 alebo v IPv6 pakete, a ten je zabalený v Ethernetovom rámci.
- Čo ale vieme, že HTTPs používa ako cieľový TCP port 443 (z klienta smerom na server),
- Pozn.3: Ak sa vám nepodarilo spraviť filter pomocou TCP stream, môžete použiť najprv tento filter **tcp.port==443 && ip.addr==*IP_servera*** (IP_servera - zistite v CMD príkazom ping www.uniza.sk) a následne na jeden takto vyfiltrovaný HTTPs paket použite Follow > TCP Stream.

Porovnajte HTTP a HTTPS komunikáciu

Odpovedzte na nasledujúce otázky

- Sú HTTP a HTTPS textové protokoly?
- Líšia sa HTTP a HTTPS na úrovni transportu (zapúzdrenie na transportnej vrstve)?
- Je v HTTPS oproti HTTP potrebná dodatočná réžia na zostavenie spojenia?
- Pokúste sa identifikovať správy, ktoré si vymieňajú klient so serverom, ešte pred odoslaním samotných aplikačných dát. Pozorne si preštudujte obrázky nižšie. Následne sa pokúste nájsť tieto správy vo Wiresharku, a pokiaľ riešite **DU_11**, odpovedzte potom na otázky na 1. stránke v DU_11 k tejto úlohe 1.



- pozri tiež https://hpbn.co/transport-layer-security-tls/ - obrázok 4.1 (Transport Layer Security (TLS)) a obrázok 4.2 (TLS handshake protocol):

When SSL is used correctly, a third-party observer can only infer the connection endpoints, type of encryption, as well as the frequency and an approximate amount of data sent, but cannot read or modify any of the actual data.

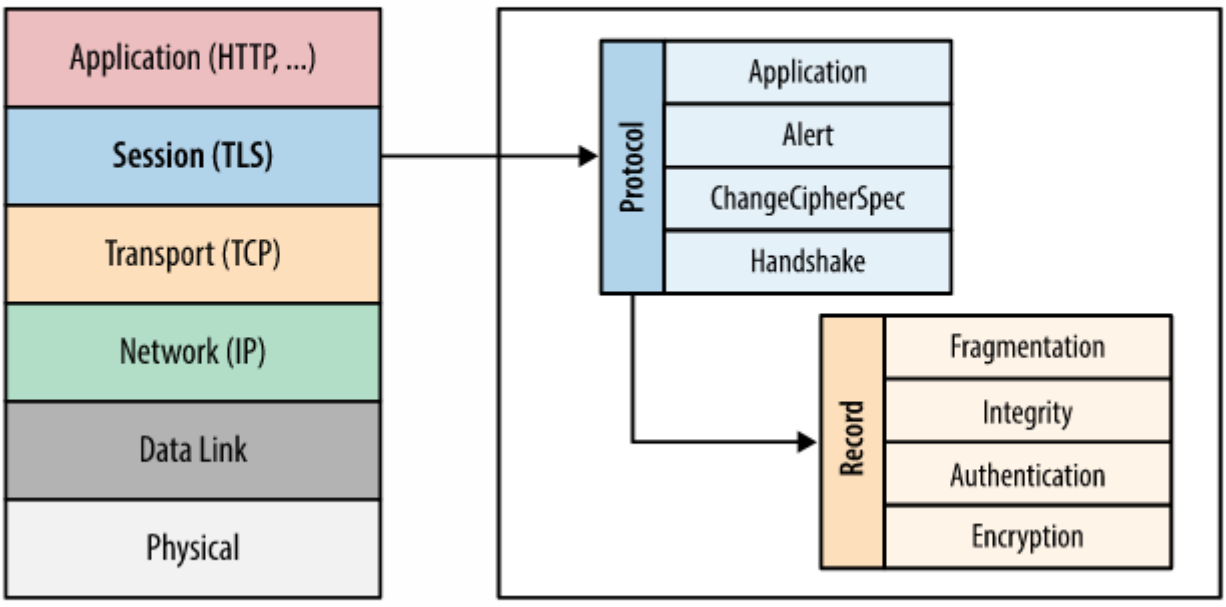


Figure 4-1. Transport Layer Security (TLS)

Note

When the SSL protocol was standardized by the IETF, it was renamed to Transport Layer Security (TLS). Many use the TLS and SSL names interchangeably, but technically, they are different, since each describes a different version of the protocol.

TLS Handshake §

Before the client and the server can begin exchanging application data over TLS, the encrypted tunnel must be negotiated: the client and the server must agree on the version of the TLS protocol, choose the ciphersuite, and verify certificates if necessary. Unfortunately, each of these steps requires new packet roundtrips (Figure 4-2) between the client and the server, which adds startup latency to all TLS connections.

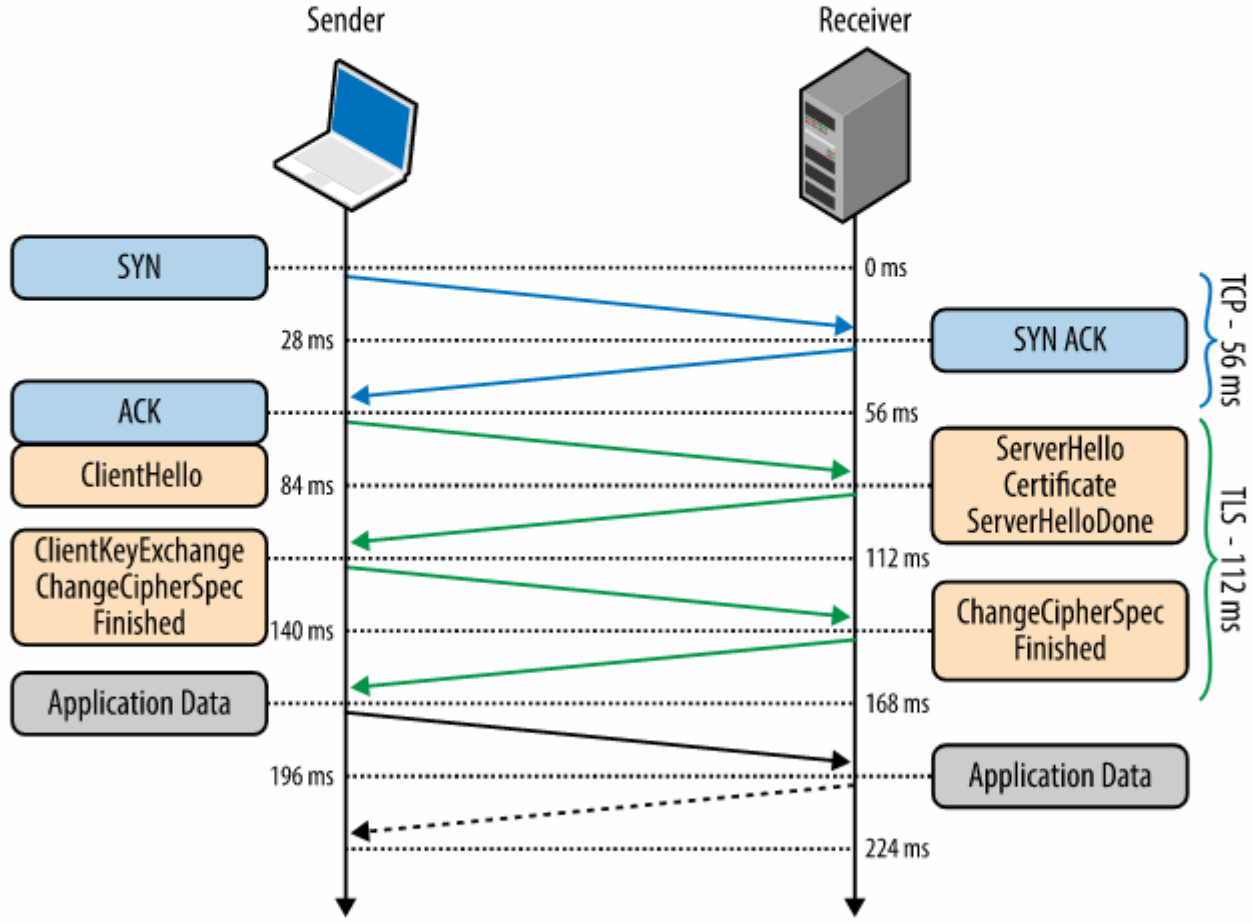


Figure 4-2. TLS handshake protocol

Note

Figure 4-2 assumes the same (optimistic) 28 millisecond one-way "light in fiber" delay between New York and London as used in previous TCP connection establishment examples; see Table 1-1.

Úloha 2: Preskúmajte DNS [editovať]

Pozrite si IP adresy DNS serverov, ktoré pozná váš počítač (ipconfig /all)

Odsledujte vami zvolenú **DNS** komunikáciu v programe Wireshark.

Spustite príkazový riadok v OS Windows. Program (príkaz) **nslookup** štandardne vyhľadáva IPv4 adresu. Ak zadáte **nslookup www.icann.com**, odpoveď bude 192.0.43.22.

Ak chcete vyhľadávať iné typy RR (Resource Record), musíte spustiť program **nslookup** bez parametra. Objaví sa Vám ">" a program očakáva vstup. Tu mu môžete nastaviť požadovaný typ RR,

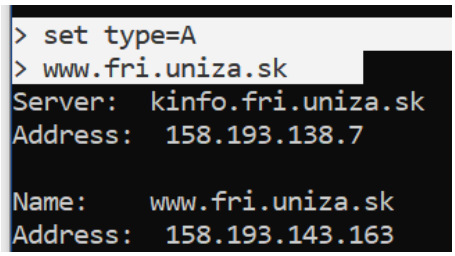
ako napríklad "set type=AAAA" (bez medzier okolo =).

nslookup -q=aaaa www.kis.fri.uniza.sk

Vyplňte tabuľku:
Pokiaľ riešite DU_11, zadávajte vaše odpovede na 2. stránku v DU_11 pre túto úlohu 2. Budete vypĺňať odpovede do buniek na pozíciách 1B, 1C, 2B, ..., spolu 14 odpovedí.

```
C:\Program Files (x86)\Windows Resource Kits\Tools>nslookup
Default Server:  kinfo.fri.uniza.sk
Address:  158.193.138.7

> ?
Commands:   (identifiers are shown in uppercase, [] means optional)
NAME            - print info about the host/domain NAME using default server
NAME1 NAME2     - as above, but use NAME2 as server
help or ?       - print info on common commands
set OPTION      - set an option
    all                 - print options, current server and host
    [no]debug           - print debugging information
    [no]d2              - print exhaustive debugging information
    [no]defname         - append domain name to each query
    [no]recurse         - ask for recursive answer to query
    [no]search          - use domain search list
    [no]vc              - always use a virtual circuit
    domain=NAME         - set default domain name to NAME
    srchlist=N1[/N2/.../N6] - set domain to N1 and search list to N1,N2, etc.
    root=NAME           - set root server to NAME
    retry=X             - set number of retries to X
    timeout=X           - set initial time-out interval to X seconds
    type=X              - set query type (ex. A,AAAA,A+AAAA,ANY,CNAME,MX,NS,PTR,SOA,SRV)
```



Tabuľku si skopírujte do Word-u a tam vložte odpovede.

		A	B	C
	Doménové meno	**Požadovaný záznam**	**Typ RR**	**Odpoveď**
1	www.fri.uniza.sk	IPv4 adresa		
2	www.kis.fri.uniza.sk	IPv6 adresa		
3	fri.uniza.sk		MX	
4	fri.uniza.sk		NS	
5	netacad.uniza.sk		AAAA	
6	www.postoj.sk	DNS server		
7	217.67.31.48	Reverzný preklad		

Pre ukončenie práce s programom nslookup, zadajte **exit**.

DNS cache:

- V tejto úlohe sme si umelo vyžiadali odpovede z DNS servera na naše DNS requesty.
- V realite sa podobné dotazovanie deje automaticky, vždy keď nejaká aplikácia potrebuje komunikovať v sieti a používa doménové mená.
- Dotazovanie sa nedeje v prípade, že odpovede sme už získali pred tým a ešte sú k dispozícii v DNS cache tabuľke, kde si určitý čas daný PC uchováva výsledky DNS dotazov.
- Výpis tejto cache tabuľky vieme pozrieť príkazom: cmd:> **ipconfig /displaydns**. Overte si.
- Zmazať ju vieme príkazom: **ipconfig /flushdns**, na čo väčšinou ale nie je dôvod.
- Pokiaľ riešitu DU_11, odpovedajte teraz na otázky na 3. stránke v DU_11 k tejto úlohe 3, týkajúce sa DNS cache.

Úloha 3: Stiahnite si súbor z FTP servera [editovať]

Pri práci doma, na notebook si nainštalujte program WinSCP zo stránky winscp.net**.**

Testovacia dobrovoľná úloha, ak pracujete doma

Ak pracujete doma, môžete cvične vyskúšať stiahnutie súboru z FTP servera z internetu.
Programomom **Wireshark** zaznamenajte stiahnutie (alebo nahratie) krátkeho súboru z ftp servera.
Odštartujete program **WinSCP**, nastavte ho ako ftp klienta a pristúpte na ftp server:
- Prenosový protokol: **FTP**
- Hostiteľ: **ftp.cert.dfn.de**
- Meno používateľa: **anonymous** Heslo: žiadne
- Pokročilé – Pripojenie - Pasívny režim
- **Propojiť**
- vojdite do priečinka /pub/

Ďalšie dostupné servery si môžete pozrieť na Ftp Sites. Zaznamenanú komunikáciu analyzujte. Použite filter **tcp || ftp || ftp-data && ip.addr==X.Y.Z.V** (kde za X.Y.Z.V doplňte IP adresu daného FTP servera) . Nájdite správy, v ktorých sa prenáša meno a heslo ako plain-text, nešifrovane.

Povinná úloha, stiahnite si súbor z katedrového FTP servera

K tejto úlohe sa viažu aj otázky pre DÚ_11, preto túto povinne zrealizujte (na cvičení len cvične, doma aj so zadaním odpovedí na otázky do DU_11).

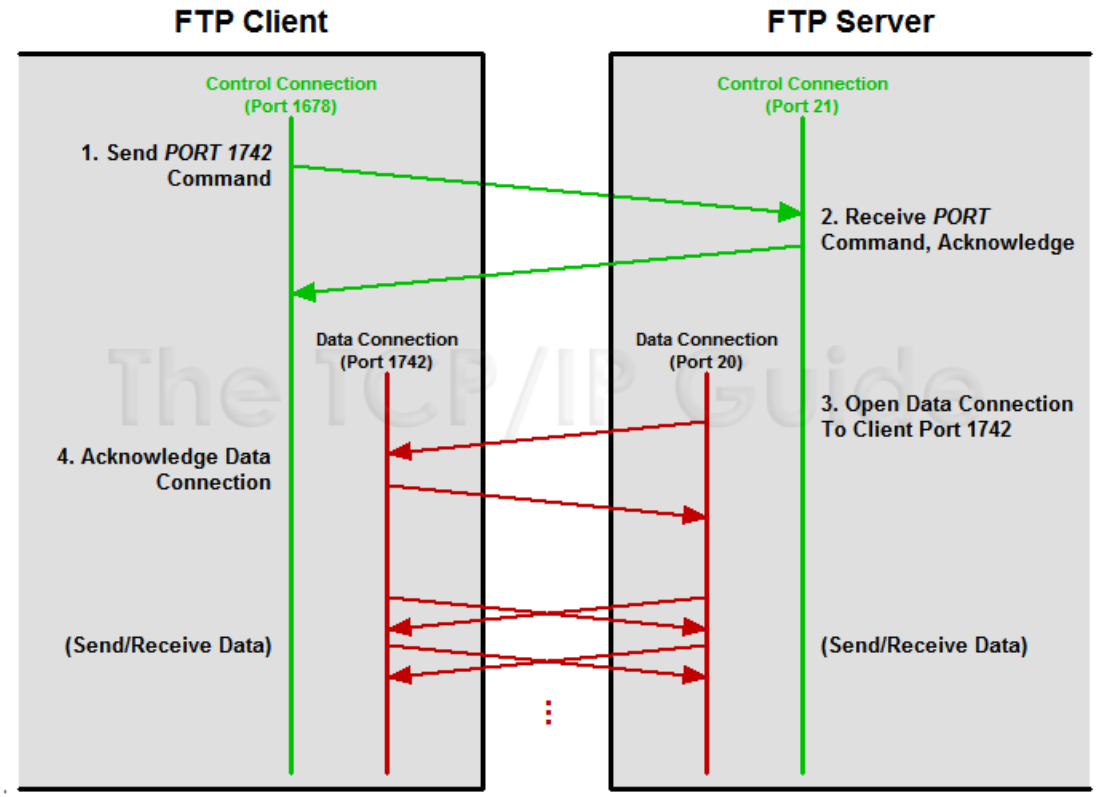
Prístup na dva pripravené FTP servery, je len počas jedného týždňa, kedy beží cvičenie 11, prístup je dovolený **len zo siete UNIZA** (158.193.0.0/16), pripojte sa teda z domu do tejto siete pomocou OpenVPN (https://nic.uniza.sk/zuwiki/doku.php?id=zu:net:bezpecnost:vpn:openvpn).
Ak sa pripájate na ftp server **z internátu**, tak sa pripojte cez **kábel**, nie cez wifi.
Ak sa na ftp server pripájate **v aktívnom móde**, a WinSCP Vás nepripojí a zobrazí správu "Permition denied",
tak na chvíľu si na počítači **vypnite Windows Defender** (alebo do Defendera pridajte pravidlo, ktoré povolí FTP serveru komunikovať).

Vo FTP klientovi (WinSCP alebo Total Commander - oba sú nainštalované na PC v laboratóriách UNIZA, doma si nainštalujte WinSCP) nastavíme **pripojenie k nižšie uvedeným FTP serverom**, z ktorých si následne **stiahneme jeden ponúkaný súbor** v hlavnom priečinku. Na server **nie je povolené nič nahrávať**, iba súbory stiahnuť. **Celú komunikáciu zaznamenajte a odsledujte v programe Wireshark**
Pre pripojenie použite tieto údaje:

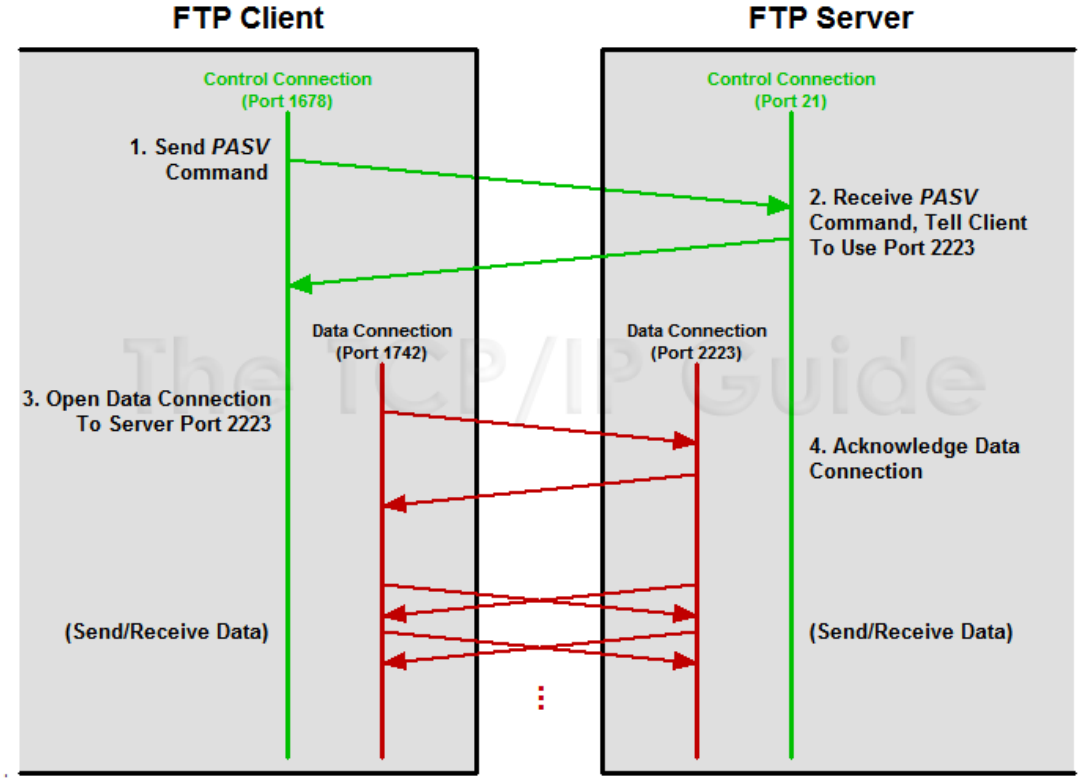
- IPv4 adresa servera pre **pasívny** mód **158.193.153.121,** pre **aktívny** mód **158.193.153.119** (pozn. pre učiteľa: už aktualizované pre školský rok 2022/2023, v každom roku máme iné IP adresy oboch serverov, spúšťa ich Marek Moravčík)

- Na tieto FTP servery sa môžete **prihlásiť** ako anonymný používateľ (vo WinSCP stlačí vybrať zaškrtávacie políčko Anonymné prihlásenie).
- Aktívny a pasívny mód si vyberá klient
- V klientovi - programe **WinSCP** sa mód nastaví nasledovne:
    - Na úvodnej obrazovke je potrebné vybrať protokol **FTP** a v rozšírených možnostiach **Pokročilé** vo voľbe **Pripojenie** je označený **Pasívny mód**.
- Najprv povolíte **Pasívny mód** a odchyťte komunikáciu programom WireShark. Pripojíte sa, prihlásite ako anonymous, a stiahnete si súbor z hlavného priečinka a WinSCP zavriete, aby sme videli aj ukončenie FTP spojenia iniciované klientom. Následne ak vypracovávate DU_11, odpoviete na otázky na 3. stránke, ktoré sa viažu k tejto úlohe 3, a pasívnemu módu. Dočítajte ale tento postup až do konca, aby ste vedeli, čo máte robiť.
- Doma (alebo v škole ale na vlastnom notebooku), vypnite na chvíľu firewall a použite **Aktívny mód** (zakážete Pasívny mód, aby nebol zaškrtnutý check box v nastaveniach, viď vyššie vyššie) a znovu odchyťte komunikáciu programom WireShark, pripojíte sa, prihlásite ako anonymous, stiahnite si súbor .txt a odpojte sa, alebo zavrite WinSCP. (Ak sa nepripojíte a zobrazí sa správa "**Permition denied**", tak na chvíľu si na svojom počítači vypnite Windows Defender.)
  Následne ak vypracovávate DU_11, odpoviete na otázky na 3. stránke, ktoré sa viažu k tejto úlohe 3, a pasívnemu módu. Dočítajte ale tento postup až do konca, aby ste vedeli, čo máte robiť.
    - Tu zafunguje Windows Firewall, ktorý chce blokovať aktívny mód, a pre povolenie by bolo potrebné heslo admina na danom PC.
        - Ak pracujete v RB303, tu bude cieľom sa dopracovať aspoň k tej hláške z Windows Firewallu
        - Ak pracujete na vlastnom PC, vypnite na chvíľu Windows Firewall, a/alebo povoľte aktívne FTP spojenia (môže vyskočiť hláška). Pokiaľ vás server odmietne, je to celkom určite preto, že ste nevypli Firewall.
- **Celú komunikáciu zaznamenajte a odsledujte v programe Wireshark:**
    - efektívny filter: **tcp || ftp || ftp-data && ip.addr==IP_FTP_servera** (IP si zmeňte podľa toho, či riešite aktívny, alebo pasívny mód, .127 pre passive, .110 pre active)
    - Preštudujte si obrázky uvedené nižšie, ktoré popisujú FTP komunikáciu, a následne sa vráťte a anlyzujte čo vidíte vo Wiresharku
        - Je viditeľné meno, prípadne aj heslo?
            - Kedy by sme ho tu nevideli ako plain-text? Čo by bolo potrebné spraviť? (spomeň si na TLS...)
    - Ďalej ak vypracovávate DÚ_11, sa zamerajte na otázky, ktoré máte na 3. stránke v pripravenom Moodle test (DU_11) k tejto úlohe 3, kde budete zadávať svoje odpovede. Využiť musíte to, čo ste odchytili vo Wiresharku.

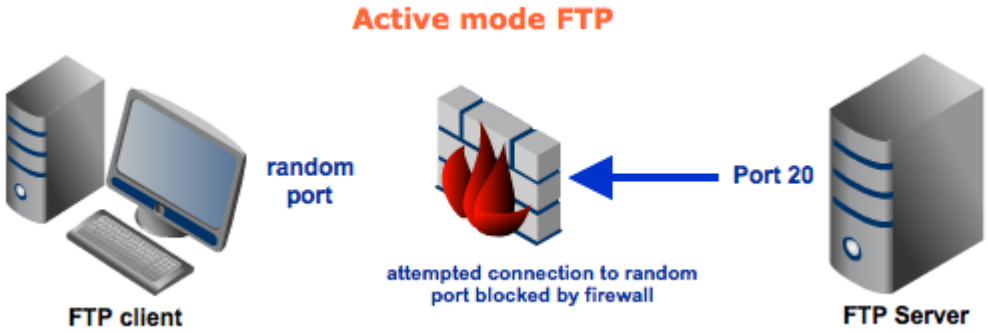
Aktívny mód - klient oznámi serveru číslo portu - ktoré bude používať na prenos údajov:



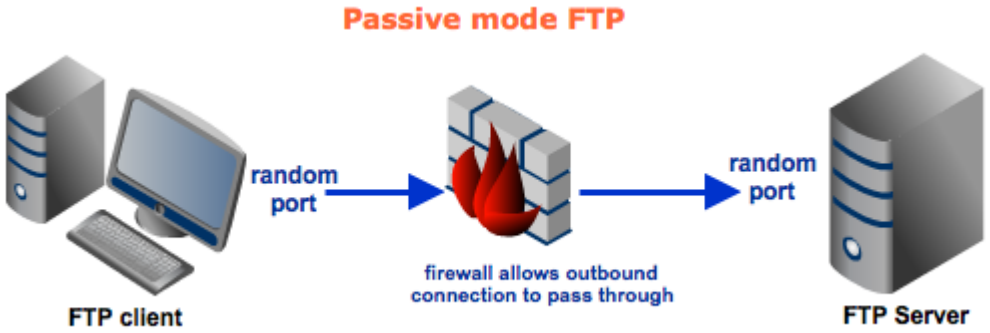
Pasívny mód - server oznámi klientovi číslo portu - ktoré bude používať pre prenos údajov:



- Problém s aktívnym módom nastáva pri použití Firewallu na klietskej stanici (čo je dnes takmer vždy), kedy Firewall zväčša blokuje všetky spojenia, ktoré sú iniciované zvonku (teda mimo danej LAN v ktorej je daný klient):



  -
- Firewall zväčša povoľuje iba také spojenia zvonku siete do vnútra danej siete, ktoré boli iniciované zvnútra -- tu nastupuje FTP v pasívnom móde, ktoré nemá problém s Firewallom, pretože dátové spojenie (data connection) pre FTP iniciuje klient:



Úloha 4: Vyplňte Výstupný test a Didaktický test (nutné pre projekt IT Akadémia, od roku 2020 nerobíme)

[editovať]

Nájdete na hlavnej stránke predmetu, v 11. týždni.

Úloha 5: Prieskum iných aplikačných protokolov v pripravených Wireshark súboroch *.pcap [editovať]

Na cvičení je vhodné stihnúť : pozrieť TELNET - nájsť heslo posielané ako plain-text, a uvedomiť si, že každý jeden znak sa posiela v jednotlivom TCP segmente - heslo hľadajte v 5 po sebe idúcich segmentoch : cisco

Využite možnosť analyzovať aj iné aplikačné protokoly, ktoré sme pre vás odchytili programom Wireshark pri komunikácii klienta s danými aplikačnými servermi. Využite túto možnosť buď počas cvičenia alebo ako prípravu na skúšku, pričom sa prioritne zamerajte na protokoly, ktoré boli preberané na prednáške.
V tomto súbore: PIKS_LAB_11.5_Wireshark_sniff_appplication protocols.zip
nájdete tieto odchytené aplikačné protokoly:

- FTP
- FTP s prenosom dát
- HTTP
- HTTPs
- DNS pri pingovaní danej IP adresy
- TELNET
- SSH
- TFTP_server
- TFTP_klient
- IRC_login
- IRC_komunikacia

Ďalšie úlohy k téme, pre rýchlejšie skupiny študentov, alebo dobrovoľne na doma (nehodnotené):

Úloha 6: Konfigurácia siete malej firmy (opakovanie) [editovať]

Poznámka: Úlohu možno využiť ako opakovanie, alebo prípravu na skúšku. Pokiaľ je čas, možno začať na cvičení, v opačnom prípade dobrovoľná nehodnotená úloha na doma.

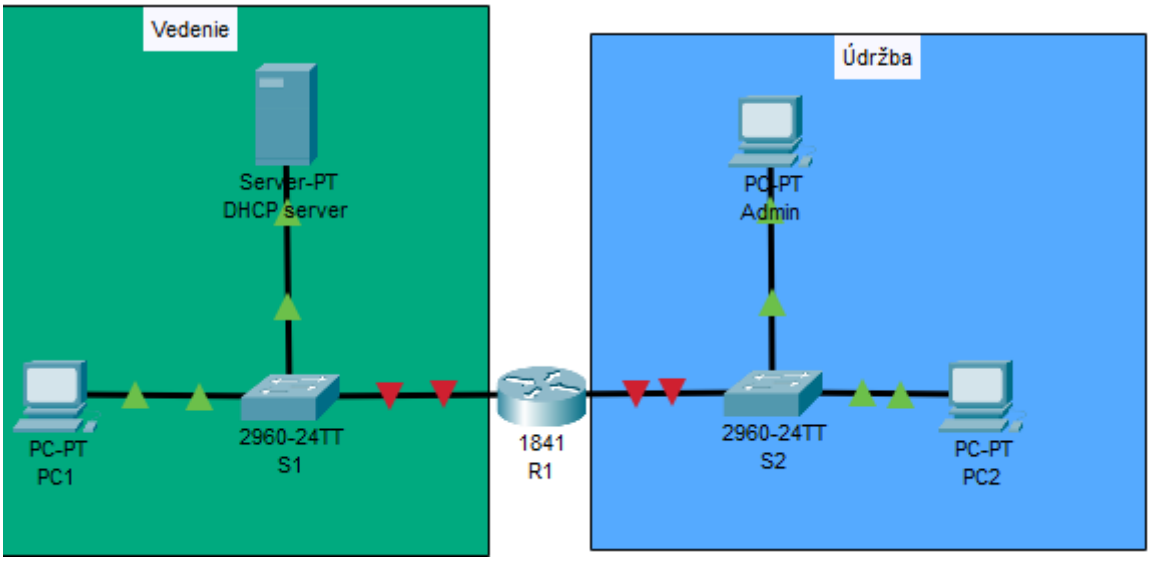
Zadanie: Malá firma má pridelený adresový priestor 192.168.0.0/24. Vašou úlohou je vytvoriť adresový plán pre dve siete: Vedenie a Údržba.

Pri vytváraní plánu použite variabilnú masku, ak viete:

- Sieť Vedenie potrebuje 20 použiteľných adries
- Sieť Údržba potrebuje 7 použiteľných adries
- Smerovač má vždy najnižšiu použiteľnú adresu zo siete
- Prepínače majú druhú najnižšiu použiteľnú adresu zo siete (rozhranie vlan1)
- Počítač Admin má tretiu najnižšiu použiteľnú adresu
- Ostatné počítače majú poslednú použiteľnú adresu.

Na smerovači a prepínačoch nastavte:

- používateľa admin s heslom admin
- heslo na konzolu class
- heslo do privilegovaného režimu cisco
- zakážte prehľadávanie DNS pri preklepoch
- zašifrujte všetky heslá v systéme
- IPv4 adresy



Topológia: PIKS_LAB_11.6_Small_network_configuration_repetition_topology.pkt