HÁLÓZATI ISMERETEK

1. forduló

A kategória támogatója: Deutsche Telekom IT Solutions

RENDELKEZÉSRE ÁLLÓ IDŐ:

15:00

Ismertető a feladathoz

Fontos információk:

A kérdésekre **mindig van helyes válasz**! Ha csak egy helyes válasz van az adott kérdésre, rádiógombos választási lehetőségeket fogsz látni.

Kérjük, hogy a feladatok szövegeit **ne másold**, és a böngésződ fejlesztőeszközét/konzolját se nyisd meg feladatmegoldás közben! Mindkettő kizárást vonhat maga után.

Minden forduló után a **megoldások csütörtök reggel 8 órakor** lesznek elérhetőek.

A megoldásokkal kapcsolatos esetleges **észrevételeket a megoldások megjelenését követő kedd éjfélig** várjuk.

A több válaszlehetőségű feleletválasztós kérdéseknél járnak **részpontszámok, ha egyik rossz választ sem jelölöd be**.

Ha kifutsz az adott feladatlap kitöltésére rendelkezésre álló időből, a felület **automatikusan megpróbálja beküldeni** az addig megadott válaszokat.

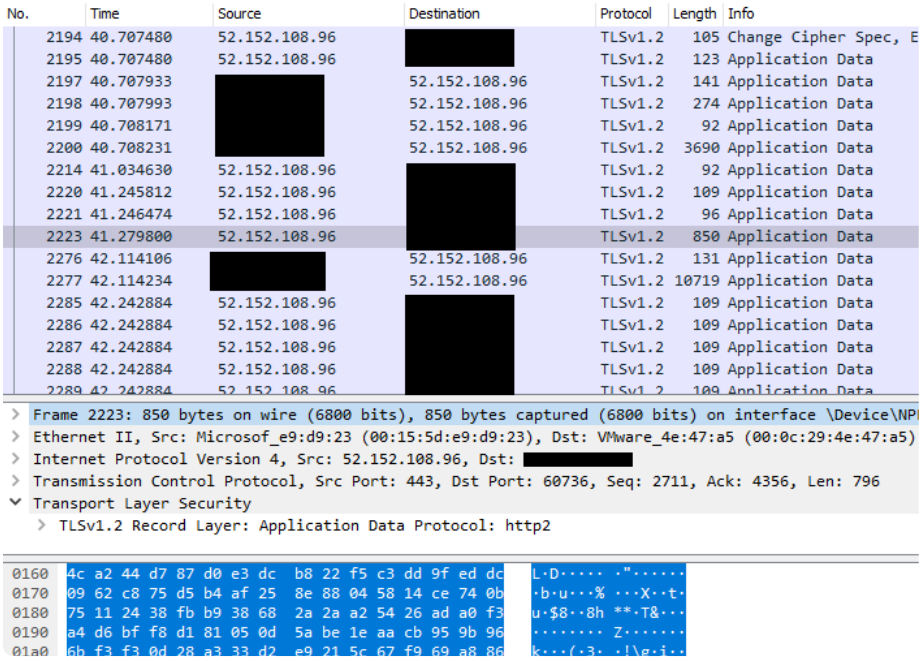
Minden feladatsornak van egy **becsült minimum megoldási ideje** (legalább a feladat elolvasási ideje). Aki ennél rövidebb idő alatt oldja meg, kizárható a versenyből.

Az első kategória után, amelynek a feladatlapját megoldod a fordulóban, kapni fogsz egy 2-3 perc alatt kitölthető **kérdőívet**. Az ezekből összeállított piackutatás legfontosabb eredményeit a díjátadót követően Veled is megosztjuk majd. Formáljuk közösen a piacot!

Felhasznált idő: 02:07/15:00 **Elért pontszám:** 0/20

1. feladat 0/2 pont

Egy hálózati hiba után nyomozva kaptál egy Wiresharkkal rögzített felvételt. A felvételt megnyitva a következőt látod:



(Néhány IP-cím adatvédelmi okokból törölve lett.)

Milyen hálózati rétegbeli protokoll látható a képen?

Válasz

- ○ Ethernet
- ◯ IP
- ○ TCP
- ○ UDP
- ○ HTTP
- ○ TLS
- ○ NetBIOS
- ○ IPv6

Magyarázat

A felsoroltak közül csak az IP(v4) és az IPv6 tartozik a hálózati réteghez, akár az OSI, akár a TCP/IP modellben gondolkozunk. A kettő közül pedig csak az előbbi jelenik meg a képen. (A rétegekről: Wikipedia - OSI model)

2. feladat 0/2 pont

Az alábbi portszámok közül melyek kapcsolódnak internetes levelezési szolgáltatásokhoz?

Válaszok

- ☑ TCP 25

- [ ] TCP 1433
- [x] TCP 465
- [x] TCP 110
- [ ] UDP 123
- [x] TCP 587
- [ ] TCP 3389
- [x] TCP 993
- [ ] TCP 1337

Magyarázat

Helyes válaszok:

- TCP 25 (SMTP, MTA -> MTA kommunikációhoz)
- TCP 587 (SMTP, MUA -> MSA kommunikációhoz)
- TCP 465 (SMTPS, mint TCP 587, de explicit TLS-sel)
- TCP 110 (POP3)
- TCP 993 (IMAPS, IMAP explicit TLS-sel)

Helytelen válaszok:

- TCP 3389 (RDP)
- TCP 1433 (MSSQL)
- UDP 123 (NTP)
- TCP 1337 (több célból is találkozni vele, de egyik sem köthető levelezéshez)

(Érdeklődőknek: Wikipedia - List of TCP and UDP port numbers).

3. feladat 0/2 pont

Egy probléma felderítése közben egy switchen kiadod a *show mac address-table* parancsot, majd a kimeneten azt látod, hogy az egyik, egy szerverhez menő porthoz 6 különböző MAC-cím is tartozik. Először arra gyanakszol, hogy valaki egy idegen switchet kapcsolt a hálózatra, de a kábeleket végigkövetve kiderül, hogy a portra valóban a szerver van csatlakoztatva.

Mi lehet a jelenség magyarázata?

Válasz

- ( ) A szervernek 6 IP-címe van.
- ( ) A szerver 6 hálózati kártyával rendelkezik.

- ◯ A szerver virtuális gépeket futtat.
- ◯ A szerver nemrég lett újraindítva.
- ◯ A szerver nagyon le van terhelve.
- ◯ Meghibásodott a szervert és a switchet összekötő valamelyik kábel.

Magyarázat

A mai virtualizációs megoldásokban van lehetőségünk a virtuális gépek virtuális hálózati kártyáit összekapcsolni a fizikai hálózattal, így a VM-ek közvetlenül kommunikálhatnak az ott lévő eszközökkel, a hálózat teljes értékű tagjai lehetnek. Az ilyen módon hálózatba kötött VM-ek MAC-címei jelentek meg a parancs kiadásakor. A gazdagépen ilyenkor létrejön egy virtuális switch, amelybe saját maga, a VM-ek és az uplink csatlakoznak, így az sem volt egy rossz tipp, hogy valaki egy idegen switchet kapcsolt a hálózatra; technikailag ez történt.

Helytelen válaszok:

A szervernek 6 IP-címe van. Még ha igaz is, ettől nem lesz 6 különböző MAC-címe is egy switchporton.

A szerver 6 hálózati kártyával rendelkezik. Ha igaz is, a switchhez egy kábellel egyszerre csak az egyik lesz összeköttetésben, annak az egynek fog látszódni a MAC-címe.

A szerver nemrég lett újraindítva. Ennek nincs köze a MAC-címek számához.

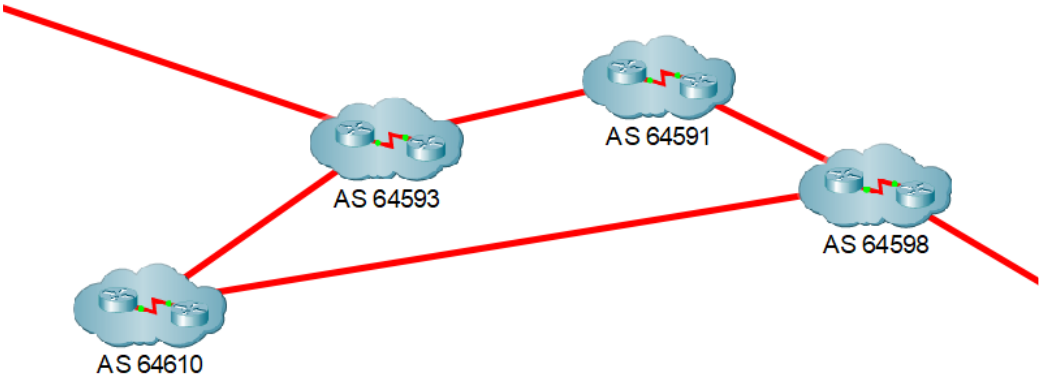
A szerver nagyon le van terhelve. Ennek sincs.

Meghibásodott a szervert és a switchet összekötő valamelyik kábel. Ennek sincs. Esetleg CRC hibákat vagy link flapet okozhat.

(Érdeklődőknek: NAKIVO blog - What Is VMware vSwitch?)

4. feladat 0/2 pont

Adott négy egymástól teljesen független szervezet, melyek az alábbi ábra szerint csatlakoznak egymáshoz és további szervezetekhez.



Legnagyobb valószínűséggel milyen routing protokollt használnak egymás között az útvonalinformációk cseréjére?

Válasz

- ◯ OSPF

- ○ RIP
- ◉ BGP
- ○ ICMP
- ○ EIGRP
- ○ IS-IS

Magyarázat

Az ábrán autonóm rendszerek (AS-ek) láthatók (a szöveg is erre utal). AS-ek között Exterior Gateway Protocol (EGP) jellegű routing protokollokat használunk. Ebből a listában egy található, ez pedig a BGP (Border Gateway Protocol; a gyakorlatban is ez használatos).

A többi válaszlehetőség közül a RIP, EIGRP, OSPF és IS-IS mind AS-en belüli útválasztásra használatos protokoll (úgynevezett IGP). Az ICMP pedig nem routing protokoll.

(Érdeklődőknek: Cloudflare - What is BGP?)

5. feladat 0/2 pont

A felsoroltak közül melyek *loopback* címek?

Válaszok

- ☑ 127.0.0.1
- ☑ 127.13.3.7
- ☐ 0.0.0.0
- ☐ 255.255.255.255
- ☐ 192.168.0.1
- ☐ 198.51.100.254
- ☑ ::1
- ☐ fe80::1
- ☐ ::
- ☐ 00:15:5D:42:55:01

Magyarázat

Az RFC 5735 szerint az egész 127.0.0.0/8-as tartomány loopback célra van kijelölve. Ebbe a felsoroltak közül a leggyakrabban használt 127.0.0.1 és a 127.13.3.7 tartozik bele. IPv6 esetén a loopback cím a ::1 (RFC 4291).

Helytelen válaszok: a 0.0.0.0 és a :: az úgynevezett *unspecified* címek IPv4 és IPv6 esetén (ebben a sorrendben). A 255.255.255.255 a limited broadcast cím. A 192.168.0.1 egy privát cím. A 198.51.100.254 egy demonstrációs célokra használatos tartomány (TEST-NET-2) utolsó használható címe. Az fe80::1 egy IPv6-os link-local cím. Végül, a 00:15:5D:42:55:01 egy MAC-cím.

6. feladat 0/2 pont

A felsoroltak közül melyek létező DNS-rekordtípusok?

Válaszok

- [x] A
- [ ] A6
- [ ] IP
- [x] SRV
- [x] NSEC3
- [x] MX
- [x] TXT
- [ ] CIDR

Magyarázat

Az A (address) rekord egy címet rendel egy szimbolikus névhez (név -> IP). Az SRV (service locator) rekord szolgáltatások megtalálását segíti (pl. LDAP szerverek a tartományban). Az NSEC3 (next secure record, v3) a DNSSEC-hez tartozó egyik rekordtípus. Az MX (mail exchanger) a tartomány egy levelezőszerverét adja meg. A TXT (text) rekordokban tetszőleges szöveg tárolható, a gyakorlatban számos célra használjuk (SPF, DKIM, tulajdonos ellenőrzése, ...).

Helytelen válaszok: A6, CIDR, IP. A CIDR és IP rövidítések létező rövidítések, de nem DNS-rekordtípusok. A6 rekordtípus nincs, AAAA van, amely egy névhez egy IPv6-os címet rendel.

(Érdeklődőknek: Wikipedia - List of DNS record types)

7. feladat 0/2 pont

Egy böngésző letölt egy weboldalt és még pár képet egy webszerverről, majd a TCP kapcsolatot nyitva hagyja, hátha szükség lesz még rá. A szerver közben összeomlik, de sikeresen újraindul, munkára kész. A felhasználó ezután rákattint egy linkre, melynek hatására a böngésző az előző kapcsolaton keresztül le akar tölteni egy új weboldalt. **Melyik TCP-vezérlőbit értéke**

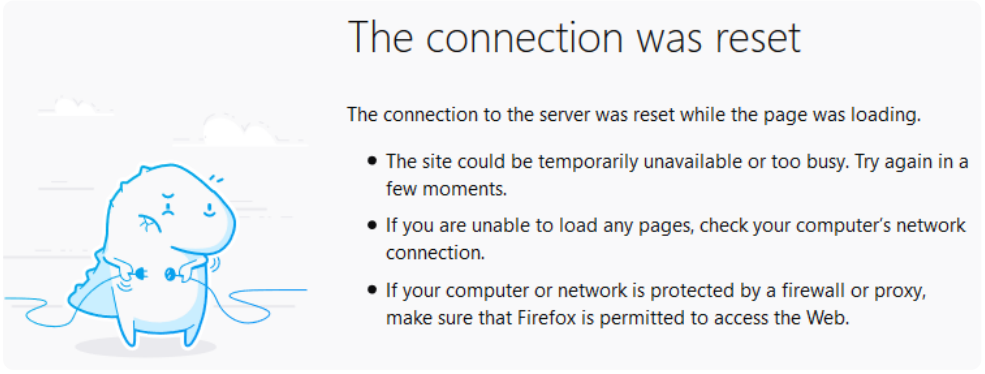
lesz garantáltan 1 a szerver válaszként küldött első üzenetében? Feltételezzük, hogy a kliens és a szerver közvetlenül kommunikál, nincs köztük proxy, sem tűzfal.

Válasz

- URG
- PSH
- RST
- SYN
- ACK
- FIN
- CRC

Magyarázat

Amikor a szerver újraindult, minden létező kapcsolat állapota számára elveszett. Így amikor a böngésző a szerinte még élő kapcsolatot szeretné használni és elküldi a kérést, a szerver számára ez egy ismeretlen kapcsolathoz tartozó, érvénytelen üzenet lesz. Erre az RFC szerint (RFC 793, 34. oldal) RST (reset) jelzéssel kell válaszolni, így ennek a vezérlőbitnek az értéke lesz 1 a válaszban. (CRC vezérlőbit nincs, a többit pedig más célokból használjuk.)



8. feladat 0/2 pont

Egy telephelyen belül az alábbi címtartományokat használjuk:

172.30.12.0/23

172.30.15.64/26

172.30.15.128/25

172.30.6.0/24

172.30.8.0/22

172.30.7.0/24

172.30.14.0/24

172.30.15.0/26

Milyen címtartományt vagy címtartományokat hirdessünk a cég többi telephelye felé, ha azt szeretnénk, hogy a lehető legkevesebb bejegyzés kerüljön be a routing táblákba, ugyanakkor azt nem szeretnénk, hogy olyan hálózatrész forgalma is hozzánk irányítódjon, amelyet nem használunk?

Válasz

- ◯ 172.30.6.0/23 és 172.30.8.0/21
- ◯ 172.30.0.0/20
- ◯ 172.30.6.0/23, 172.30.8.0/21 és 172.30.15.0/24
- ◯ 172.30.6.0/24 és 172.30.8.0/21
- ◯ 172.30.6.0/24, 172.30.8.0/23 és 172.30.12.0/22
- ◯ 172.30.6.0/20

Magyarázat

A feladat lényegében az, hogy minél több alhálózatot vonjunk össze (*supernetting*).

Induljunk ki a legkisebbekből, azaz a leghosszabb maszkúakból.

A 172.30.15.0/26 és a 172.30.15.64/26 összevonható 172.30.15.0/25-té.

Ez összevonható a 172.30.15.128/25-tel 172.30.15.0/24-gyé.

A 172.30.14.0/24 és a 172.30.15.0/24 összevonható 172.30.14.0/23-má.

Ez a 172.30.12.0/23-mal összevonható 172.30.12.0/22-vé.

Végül, ez a 172.30.8.0/22-vel összevonható **172.30.8.0/21**-gyé.

A 172.30.6.0/24 és a 172.30.7.0/24 összevonható **172.30.6.0/23**-má.

Ez viszont az előző nagy tartományhoz nem vonható hozzá anélkül, hogy bekerülnének olyan címek, amelyek nem a mieink. (De ez abból is látható, hogy nem egyformák a tartományok.)

(Érdeklődőknek: Wikipedia - Supernetwork)

9. feladat 0/2 pont

Az alábbi állítások közül melyek igazak az NTP-re?

Válaszok

- ☐ Az NTP a Network Trunking Protocol rövidítése.
- ☑ Segítségével az eszközeink órái szinkronizálhatók.
- ☑ Biztonsági szempontból is jelentőséggel bír.
- ☑ Egy eszköz egyszerre NTP kliensként és szerverként is viselkedhet.
- ☐ A protokoll beépítetten lehetőséget nyújt a forgalma titkosítására.

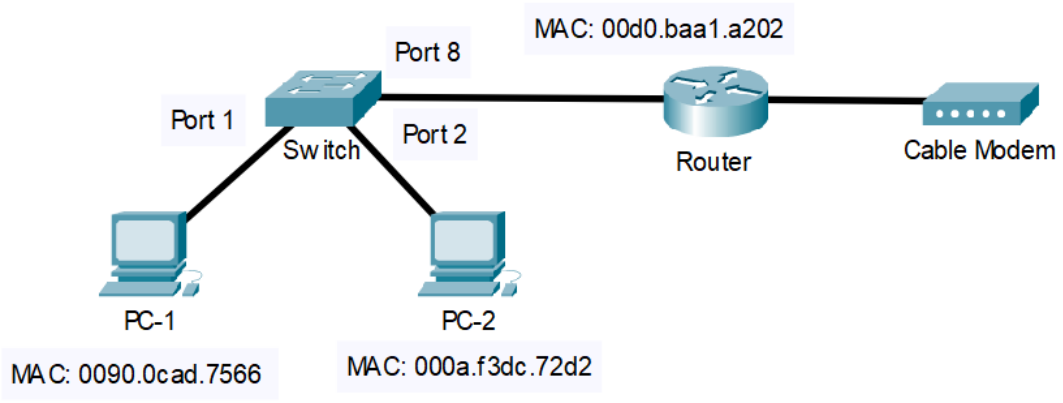
Magyarázat

Az NTP a Network Time Protocol rövidítése. A protokoll segítségével az eszközeink órái szinkronizálhatók. Biztonsági szempontból is jelentőséggel bír, mert több okból is fontos, hogy az eszközeink órája szinkronban és pontos legyen, például tanúsítványok dátumainak ellenőrzése, események naplózása, jelszavak és felhasználói fiókok lejárata. Egy eszköz egyszerre NTP kliensként és szerverként is viselkedhet; gyakran egy-két eszközt szinkronizálunk egy megbízható időforráshoz (ekkor kliensként viselkednek), majd a többi eszközt úgy állítjuk be, hogy ezekről szinkronizáljanak (ekkor szerverként viselkednek). A forgalomra beállíthatunk hitelesítést (nem titkosítást!), hogy támadók ne tudják befolyásolni a rendszerek óráit az NTP-üzenetek módosításával.

(Érdeklődőknek: RFC 5905 - Network Time Protocol Version 4: Protocol and Algorithms Specification)

10. feladat 0/2 pont

Tekintsük az alábbi egyszerű elrendezést.



A switch MAC-címtáblája a következő:

#	MAC	Port	Type	Age
1	00d0.baa1.a202	8	dynamic	15
2	0090.0cad.7566	1	dynamic	0

PC-1 üzenni szeretne PC-2-nek. A MAC-címét ismeri, így küld is neki egy keretet. **Mit fog csinálni a switch a kerettel?**

Válasz

- ○ Eldobja.
- ○ Kiküldi a 2-es porton.
- ○ Kiküldi a 8-as porton.
- ○ Kiküldi az összes porton.
- ○ Kiküldi az összes porton, kivéve az 1-est.
- ○ Kiküldi az összes porton, kivéve a 8-ast.

Magyarázat

A táblázat alapján a switch (még) nem tudja, hogy melyik portján keresztül érhető el PC-2. Ilyenkor a keretet kiküldi minden portjára, kivéve oda, ahonnan jött. Ez pedig az egyes port.

(Érdeklődőknek: Wikipedia - Unicast flood)