Segédlet a Wireshark tematikájú egész órai számonkérésre való felkészüléshez (is)

DISCLAIMER

Nem hivatalos anyag, lehetnek benne hibák, ha találtok, azt valamilyen úton légyszíves jelezzétek felém.

A dokumentum tartalmazza az órai WS tematikájú CooSpace tesztek kérdéseit, illetve azt, hogy a kérdések helyes megválaszolásához milyen lépéseket kellett volna elvégezni. Az elméleti kérdések megoldásai nincsenek leírva, a rájuk adandó helyes válaszok fellelhetők a kiadott gyakorlati anyagokban. A félreértések elkerülése végett megjegyezném, hogy az ebben a dokumentumban szereplő gyakorlati kérdések is teljes mértékben megválaszolhatók a kiadott anyagok alapján, ez a dokumentum csak az egész órai számonkérésre való felkészülést hivatott megkönnyíteni és nem a kiadott anyag nemlétező hiányosságait pótolni.

Üdvözlettel: Maczák Bálint

HTTP

1) **Milyen megjelenítési szűrővel kaphattuk a megnyitott dump-ot?**
   A "Protocol" oszlopban látható, hogy tcp http üzenetek találhatók a dump fájlban, így erre kell megadnunk megjelenítési szűrőt: „**tcp.port == 80**” (ezzel ekvivalens a „**tcp.port eq 80**” és a „**http**” is). Helyességét ellenőrizhetjük is, ha ezt a szűrőt ki is adjuk, akkor sem fog csökkenni a sorok száma, vagyis minden sor megfelelt neki. Nyilván lehetne más olyan megjelenítési szűrőt megadni, ami ennek a feltételnek eleget tenne, de kellően szűk kifejezést kellett megadni.

2) **Mi volt a monitorozó host lokális IP-címe?**
   Mint ismert, a HTTP GET kérést minden esetben a kliens („monitorozó host”) küldi a szerver felé, így a kérdés megválaszolásához keresni kell egy GET kérést, és megnézni a forrás IP-címét ennek az üzenetnek. Utóbbi leolvasható a "**Source**" oszlopból. GET kérésre az alábbi megjelenítési szűrővel érdemes szűrni: „**http.request.method == "GET"**”.

3) **Mi volt a web-szerver IP-címe, amely felé küldtük az első HTTP kérést?**
   Szintén egy HTTP GET kérést kell keresni, jelen esetben a legelsőt, és megnézni a cél IP-címét ennek az üzenetnek. Utóbbi leolvasható a "**Destination**" oszlopból. GET kérésre még mindig az alábbi megjelenítési szűrővel érdemes szűrni: „**http.request.method == "GET"**”.

4) **Mi volt a web-szerver host neve, amely felé az első HTTP kérést indítottuk?**
   Az előző (3.) feladatban megtalált üzenetet kell tovább elemezni, abból megismertük, hogy mi a web-szerver IP-címe, most nézzük meg, hogy mi a host neve. Ezen üzenet részletes információinál le kell nyitni a "**Hypertext Transfer Protocol**" fület, meg kell keresni a "**Host:**" kezdetű sor, **a kettőspont után található a web-szerver host** neve (a "\" és az azutáni karakterek nélkül), ha van „www” előtag, akkor az is a host név része.

5) **Melyik sorszámmal ellátott HTTP kérés indult az elsõ kéréssorozatban másodjára?**
   Még mindig ugyan azt az üzenetet vizsgáljuk, amit a 3-5. feladatban, vagyis az első http GET kérést. Ezen üzenet részletes információinál le kell nyitni a „**Hypertext Transfer Protocol**” fület, meg kell keresni a „**Next request in frame:**” kezdetű sor, **a kettőspont után látható a keresett sorszám**.

6) **Milyen metódusokkal ellátott HTTP kéréseket találsz? Ott milyen URL-ekre irányult a kérés?**
   Ennek legegyszerűbb módja, ha **a dump fájlt az „Info” oszlop alapján sorba rendezzük**, és megnézzük, hogy ezen oszlopba milyen kérések vannak írva (például „**GET**”, „**POST**”, „**DELETE**”, „**PUT**”), az „**Info**” mező mindig a kérés fajtájával kezdődik, így könnyű megtalálni őket. Ha nem akarjuk végig görgetni a listát, akkor a különböző metódusokra specifikusan írhatunk megjelenítési szűrőket, és megnézhetjük, hogy volt-e olyan üzenet, mely megfelelt ezeknek („**http.request.method == "GET"**”, „**http.request.method == "POST"**”, „**http.request.method == "DELETE"**”, „**http.request.method == "PUT"**”).

7) **Használ-e sütiket a web-szerver, amelynek küldtük az elsõ HTTP kérést? Ha igen, van-e olyan komponens, amelyet még nem látogattunk?**
   A 3-as feladatból ismerjük a web-szerver IP-címét, ezáltal könnyen írhatunk egy olyan megjelenítési szűrőt, ami már csak olyan üzeneteket fog kilistázni, amiben sütik vannak, és a web-szerver felé tartanak. Az alábbi megjelenítési szűrővel érdemes szűrni: „**http.cookie && ip.dst == web-szerver-ip**”. **Ha találtunk ilyen üzeneteket, akkor a web-szerver használ sütiket**, már csak azt kell ellenőrizni, hogy **volt-e újonnan látogatott komponens**, erre is érdemes egy megjelenítési szűrőt írni: „**http.set_cookie && ip.dst == web-szerver-ip**”. Ennek segítségével a leszűrt listában láthatjuk, hogy volt olyan üzenet, ami olyan komponenst tartalmaz, amit még nem látogattunk. **Ha találtunk ilyen üzenetet, akkor volt újonnan látogatott komponens.**

8) **Milyen státusz kóddal és megnevezéssel (status code & phrase) volt ellátva az elsõ hagyományos HTTP válasz üzenet?**
   Írjunk egy megjelenítési szűrőt, ami csak azokat az üzeneteket listázza ki, amiknek a cél IP-címe a monitorozó host lokális IP-címe (ezt tudjuk a 2-es feladatból, „**http.response && ip.dst == monitorozo-host-ip**”), és keressük meg az első olyan http üzenetet az „**Info**” oszlop alapján, aminek van **státuszkódja, és szöveges megfelelője** (pl.: „**200 OK**”).

DNS

1) **Melyik parancs segítségével érhetjük el terminálban, hogy a www.origo.hu web-szerver IP-címeit a huni6.cc.u-szeged.hu autoritatív szerveren keresztül kérdezzük le? A teljes felparaméterezett parancsot add meg válaszként!**
   Az nslookup segítségével indíthatunk manuális DNS kérést. Általános formája: „**nslookup -type=XXXX keresett-host dns-szerver**”, ahol a type és a dns-szerver paraméterek megadása nem kötelező. Jelen esetben meg kellett adni a dns-szervert, hiszen a feladat kiköti, hogy mely autoritatív szerveren keresztül kérdezzük le az információt: „**nslookup www.origo.hu huni6.cc.u-szeged.hu**”.

2) **Melyik parancs segítségével kaphatjuk meg a www.origo.hu kanonikus (canonical) nevét? A teljes felparaméterezett parancsot add meg válaszként!**
   Az 1. feladathoz hasonlóan itt is nslookup-ot kell használni a megoldáshoz, azonban itt már nincs definiálva a dns-szerver, így azt nem kell megadni, viszont a keresett host kanonikus nevét (**CNAME**) kell lekérdeznünk, így a type paraméternek ezt kell megadni: „**nslookup -type=CNAME www.origo.hu**”.

3) **Az 1. DNS kérés kibocsátója melyik portját használta?**
   Először is egy olyan megjelenítési szűrővel kell szűrnünk, mely csak a DNS kéréseket (query) fogja visszaadni, ez a „**dns.flags.response == 0**” (hiszen ami nem válasz, az kérés). Az **első üzenetet kell vizsgálni**, ezen üzenet részletes információinál le kell nyitni a „**User Datagram Protocol**” fület, meg kell keresni a „**Source Port:**” kezdetű sort, **a kettőspont utáni szám a keresett portszám.**

4) **Az 1. DNS kérés fogadója melyik portját használta?**
   Még mindig a 3. feladatban vizsgált üzenetet nézzük, ezen üzenet részletes információinál le kell nyitni a „**User Datagram Protocol**” fület, meg kell keresni a „**Destination Port:**” kezdetű sort, **a kettőspont utáni szám a keresett portszám.**

5) **Milyen IP-címre lettek kiküldve a DNS kérések (ha nem összes, akkor melyikre a legtöbb)?**
   Ha még **mindig le van szűrve a dump a 3. feladatban megadott megjelenítési szűrővel**, akkor csak DNS kéréseket látunk. Meg kell számolni, hogy a DNS kérések többsége milyen IP-címmel rendelkezik a „**Destination**” oszlopban.

6) **Mi a host neve a cél web-szervernek az elsõ kérésben?**
   Ha még **mindig le van szűrve a dump a 3. feladatban megadott megjelenítési szűrővel**, akkor csak DNS kéréseket látunk, keressük meg azt az **első** DNS kérést, ezt kell vizsgálni. A keresett információ, az „**Info**” oszlopban ezen **DNS kérés típusát jelző mezőjé után olvasható**. A keresett információ leolvasható akkor is, ha lenyitjuk a hozzá tartozó „**Domain Name System (query)**” fület, és azon belül a „**Queries**” fület, a „:” előtti rész a keresett hoszt név.

7) **Az 1. DNS kérésre hanyadik elfogott csomag tartalmazta a választ?**
   A 6. feladathoz hasonlóan kell eljárni, ezen üzenet részletes információinál le kell nyitni a „**Domain Name System (query)**” fület, meg kell keresni a „**[Response In:**” kezdetű sort, **a kettőspont utáni szám a keresett érték.**

8) **Milyen típusú (Type) DNS kéréseket találunk a dump-ban? (A, AAAA, CNAME, NS, stb...)**
   A 6. feladatban már láthattunk, hogy az „**Info**” oszlopban jelölve van a DNS kérések típusai, ezeket kell leolvasni, megnézni, hogy milyen fajta kéréseket látunk. Ha nem akarjuk végig görgetni a listát, akkor a különböző kéréstípusokra specifikusan írhatunk megjelenítési szűrőket, és megnézhetjük, hogy volt-e olyan üzenet, mely megfelelt ezeknek (A: „**dns.flags.response == 0 && dns.qry.type == 1**”, AAAA: „**dns.flags.response == 0 && dns.qry.type == 28**”, CNAME: „**dns.flags.response == 0 && dns.qry.type == 5**”, PTR: „**dns.flags.response == 0 && dns.qry.type == 12**”, NS: „**dns.flags.response == 0 && dns.qry.type == 2**”, MX: „**dns.flags.response == 0 && dns.qry.type == 15**”, stb...).

TCP, UDP

1) **Milyen maximális szegmens méretet határozott meg a szerver a TCP kapcsolat kialakításakor?**
   A szerver által küldött **SYN-ACK üzenet** tartalmazza a maximális szegmensméretre vonatkozó információt. Meg kell keresni ezt az üzenetet, az „**Info**” oszlopban „**[SYN, ACK]**” szöveggel van ellátva, vagy szűrünk az alábbi megjelenítési szűrővel: „**tcp.flags.syn == 1 && tcp.flags.ack == 1**”. Ezen üzenet részletes információinál le kell nyitni a „**Transmission Control Protocol**” fület, azon belül pedig az „**Options**” fület, meg kell keresni a „**Maximum segment size:**” kezdetű sort, **a kettőspont utáni szám a keresett érték**.

2) **Mi volt a szerver IP címe? A TCP-s dump alapján.**
   Mint tudjuk a **SYN-ACK üzeneteket a szerver küldi**, így ezen üzenet (amit az első feladatban is vizsgáltunk) „**Source**” oszlopából kiolvasható IP-cím lesz a szerver IP-címe.

3) **Mi volt a szerver portszáma? A TCP-s dump alapján.**
   Még mindig az első feladatban megkeresett **SYN-ACK üzenetet** vizsgáljuk. Ezen üzenet részletes információinál le kell nyitni a „**Transmission Control Protocol**” fület, meg kell keresni a „**Source Port:**” kezdetű sort, **a kettőspont utáni szám a keresett portszám**.

4) **Mi volt a kliens portszáma a TCP kapcsolatnál?**
   Még mindig az első feladatban megkeresett **SYN-ACK üzenetet** vizsgáljuk. Ezen üzenet részletes információinál le kell nyitni a „**Transmission Control Protocol**” fület, meg kell keresni a „**Destination Port:**” kezdetű sort, **a kettőspont utáni szám a keresett portszám**.

5) **Mi volt az "Acknowledgement number " értéke az utolsó olyan csomagnak, ami a szerver felől érkezett és az ACK mezője 1 volt?**
   A 2. feladatban már megkaptuk a szerver IP-címét, így nincs nehéz dolgunk: „**tcp.flags.ack == 1 && ip.src_host == szerver-ip**”. A szűrt listából az **utolsó üzenetet** kell elemeznünk. Ezen üzenet részletes információinál le kell nyitni a „**Transmission Control Protocol**” fület, és megkeresni az „**Acknowledgment number:**” kezdetű sort, **a kettőspont utáni szám a keresett érték**.

6) **Volt-e retransmission a TCP kapcsolat során?**
   A „**tcp.analysis.retransmission || tcp.analysis.fast_retransmission**” megjelenítési szűrővel le kell szűrni a dump-ot, **ha van akár egy üzenet is ami megfelel a szűrőnek, akkor volt retransmission**, egyébként nem.

7) **Mi az első UDP csomag küldőjének a portszáma?**
   Az előző 6 kérdés a TCP dump fájllal volt kapcsolatos, az utolsó kettőben már az **UDP dump** fájlt kell használni. Kiválasztjuk a listából az **első UDP üzenetet**, és elemezzük. Ezen üzenet részletes információinál le kell nyitni a „**User Datagram Protocol**” fület, meg kell keresni a „**Source Port:**” kezdetű sort, **a kettőspont utáni szám a keresett portszám**.

8) **Mekkora az első UDP csomag hossza?**
   Még mindig ugyan azt az üzenetet vizsgáljuk, amint a 7. feladatban. Ezen üzenet részletes információinál le kell nyitni a „**User Datagram Protocol**” fület, meg kell keresni a „**Length:**” kezdetű sort, **a kettőspont utáni szám a keresett érték**.

ICMP, DHCP

1) **Ha a tracert paranccsal egy külső komponens felé indítunk ICMP csomagokat, melyik interfész fogadja az első ICMP csomagot?**
   Elméleti kérdés, keresd meg a választ a kiadott anyagok alapján.

2) **Hogyan tudunk olyan ping-elést végrehajtani, melynek nincs megállási feltétele?**
   Elméleti kérdés, keresd meg a választ a kiadott anyagok alapján.

3) **Melyik az a megjelenítési szűrő (Display filter), mellyel a DHCP protokollt tartalmazó csomagokra tudunk szűrni Wireshark-ban?**
   Elméleti kérdés, keresd meg a választ a kiadott anyagok alapján.

4) **Mi(k) az oka(i) annak, hogy a pingeléssel indított ICMP csomagokban nem szerepelnek port számok?**
   Elméleti kérdés, keresd meg a választ a kiadott anyagok alapján.

5) **Milyen IP-címmel rendelkezik egy interfész, ha a DHCP szerinti 4 lépés MÉG NEM valósult meg (tehát nincs automatikusan kiosztott címe a host-nak)?**
   Elméleti kérdés, keresd meg a választ a kiadott anyagok alapján.

6) **Mi volt a parancsban kiadott cél host IP-címe?**
   Az „**Info**” oszlop alapján leolvasható, hogy a kiadott parancs „**Echo (ping) request**” üzenetet generált, a kérdés az, hogy a kiadott ping vagy tracert parancsnak milyen célállomást adtunk meg annak érdekében, hogy a kapott üzenetet generálja. A kérdésre a válasz, azaz a keresett IP-cím az „**Echo (ping) request**” üzenetet „**Destination**” oszlopából olvasható le.

7) **Milyen TTL értékkel lett elküldve az a második ICMP üzenet, amelyet a kliensünkkel indítottunk?**
   Az előző kérdésben vizsgált üzenet „Source” oszlopából kiolvashatjuk a monitorozó host („kliensünk”) IP-címét, erre a „**ip.src == kliens-ip**” megjelenítési szűrővel szűrhetünk. A listából megkeressük a második „**Info**” oszlopban valamilyen „**request**” mezőt tartalmazó üzenetet, és ugyan ebből az oszlopból kiolvassuk a „**ttl=**” utáni számot.

8) **Milyen Type és Code értékekkel rendelkezik az első fogadott ICMP üzenet?**
   Az előző feladathoz hasonlóan konstruálunk egy olyan megjelenítési filtert, mely hatására csak azok az üzenetek maradnak a listában, melyek célja mi vagyunk, ez az „**ip.dst == kliens-ip**” megjelenítési szűrő, majd a szűrt lista első üzenetét vizsgáljuk. Nyissuk le az „**Internet Control Message Protocol**” fület, és olvassuk le a „**Type:**” és „**Code:**” után írt számokat.