VITMAC07

TTMER104: Bevezetés a Wireshark használatába
jelenléti mérés

Mérési jegyzőkönyv 2022

Mérést végezte: <Hallgató neve>, <Hallgató neptun kódja>
(a mérést egyedül kell elvégezni)

Mérés időpontja: <Dátum>

A mérést kidolgozták: Marosits Tamás

 Skopkó Tamás

 BME TMIT, 2020. február – 2022. február

A mérés előkészítéseként rögzítettünk és lementettünk egy csomagfolyamot. A mérés során ezeket a folyamokat kell feldolgozni és ez alapján az alábbi kérdéseket megválaszolni. Kérjük, hogy az eredmények értékeléséről ne feledkezzen el és ahol szükséges, válaszait indokolja meg!

Rögzítse a mérésvezető által megadott weboldal letöltésének csomagfolyamát!

**Figyelem:** A webes forgalom szinte bizonyosan TLS titkosítású. Ahhoz, hogy ezt dekódolva láthassa, a TLS protokoll elemezőnek szüksége van a kommunikációs végponton használt privát kulcsokra. Ezeket a letöltés során ki kell menteni a böngészőből (Firefox vagy Chrome) és a Wireshark beállításaiban, a Protocols > TLS > Pre-Master Secret log filename mezőnél az elmentett file nevét meg kell adnia[[1]](#footnote-1).

*Tipp: Windowsban használja az alábbi parancsot a Firefox indításához:*

*SET SSLKEYLOGFILE=D:\tmp\sslkeylog.txt*

*"%ProgramFiles%\Mozilla Firefox\firefox"*

*De a mérésvezető is segíteni fog.*

A rögzítés után a csomagfolyamot mentse el, az 1. és a 2. feladat megoldása során ezzel fog dolgozni. A csomagfolyam elemzése után válaszolja meg a következő kérdéseket!

# 1. DNS névfeloldás

## 1.1 DNS lekérdezés

Határozza meg az igénybe vett DNS-szerver IP-címét!

Törölje ki ezt a sort, és ide írja a választ! A zöld keret maradjon itt és a későbbiekben is, hogy könnyebb legyen javítani!

TCP vagy UDP protokollt használ a kliens? Melyik portra kapcsolódik?

válasz

## 1.2 DNS válasz

Milyen típusú DNS-rekordo(ka)t tartalmaz a válasz?

válasz

Válasszon ki egy lekérdezést, amely IP-címe(ke)t adott vissza:

válasz

Trace route segítségével határozza meg, hogy hány ugrásnyi távolságra van a webszerver!

*Tipp: Használja a traceroute parancsot -T kapcsolóval! vagy Windows alatt a tracert-t*

***képernyőfotóval is támassza alá az eredményt!***

fotó és magyarázat

# 2. A webes forgalom elemzése

## 2.1 A teljes oldalletöltés vizsgálata

Próbálja meg kideríteni, mely weboldalt vagy szolgáltatást tekintették meg:

válasz

Mennyi ideig tart a teljes oldal letöltése? Az indoklásban írja le, mely időpillanatot tekinthetjük az oldal letöltésének kezdeteként és mikor tekinthető a folyamat befejezettnek.

válasz

Hány TCP szálat használunk ehhez?

válasz

Mennyi a teljes letöltött adatmennyiség? Hogyan határozta meg ezt?

válasz

## 2.2 TCP szintű elemzés

A Wireshark Analysis > Conversation menüpontjának használatával töltse ki az alábbi táblázatot három, az oldal letöltése során legtöbbet forgalmazó TCP szálra vonatkozóan!

*Tipp: Használja a Copy > as CSV funkciót és folytassa Excelben a feldolgozást.*

|  |  |  |  |
| --- | --- | --- | --- |
| Host A | Host B | Transferred bytes | Connection  |
| IP address | Port | IP address | Port  | A->B | B->A | start | duration |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

## 2.3 Egy konkrét TCP-kapcsolat vizsgálata

Válasszon ki egy TCP-kapcsolatot és ábrázolja az átviteli görbéjét!

fotó

Az átviteli görbe alapján becsülje meg, mennyi ideig tartott a slow start fázis!

válasz, indoklás

Állapítsa meg, mekkora volt az adott TCP-kapcsolaton a legnagyobb meghirdetett fogadási ablakméret!

válasz, indoklás vagy fotó

Használta-e a kiválasztott TCP-kapcsolat a Window Scale Factort?

*Tipp: Használjon szűrést az adott portszámra!*

válasz, indoklás vagy fotó

A HTTP-kérések fejlécének vizsgálatával határozza meg a kliens által közölt user agentet (operációs rendszer-böngésző típus)!

válasz

# 3. VoIP hívás elemzése

Töltse be a VoIP hívás rögzítéséből származó csomagfolyamot és ez alapján válaszolja meg az alábbi kérdéseket!

## 3.1 A hívás vizsgálata

Mennyi ideig tart a hívás?

válasz

Ki a hívó, ki a hívott?

hívó IP címe:

hívott IP címe:

Ki kezdeményezi a hívás bontását? Mi alapján tudja megállapítani?

válasz és indoklás

## 3.2 A hívás közben átvitt médiafolyam vizsgálata

Vizsgálja meg, milyen gyakran jönnek RTP-csomagok irányonként!

*Tipp: Használja a Decode as menüpontot!*

válasz és indoklás

Milyen a média kódolása az RTP-n belül?

*Tipp: Keresse a Payload type mezőt az RTP fejlécben!*

válasz és indoklás

# 4. Nagy mennyiségű adatátvitel vizsgálata\*

A SmartComLab által fejlesztett Szélessáv mérőrendszer használatával vizsgálja meg hálózati kapcsolatának átviteli paramétereit.

## 4.1 Hálózati paraméterek

Végezze el a mérés a mérésvezető által megadott webcímre látogatva. Használja a Wireshark-ot a forgalom rögzítésére!

*Tipp: Erőforrás takarékosság céljából próbálja meg úgy beállítani az elkapást, hogy a forgalomnak csak a releváns részét tartsa meg.*

*Megjegyzés: Amennyiben a laborhálózatban többen is mérnek, a mérést torzíthatja a konkurencia, ahogy a munkaállomás erőforrásainak korlátai is.*

Milyen sávszélességet és késleltetést mért? Válaszában ügyeljen a mennyiségekre és mértékegységekre!

válasz

## 4.2 Az átviteli karakterisztika vizsgálata

A Wireshark segítségével vizsgálja meg, hány kapcsolat segítségével történt a le- ill. feltöltési sebességek vizsgálata.

képernyőfotó, jelölje meg vagy szavakkal írja le, mely adatok adják meg a választ

Milyen időbeli intenzitással történt ezek nyitása?

válasz

Mennyi volt a várakozási idő a két mérési fázis között? Miért lehet rá szükség?

válasz

Ábrázolja az I/O Graph segítségével a le- és feltöltési fázisokat eltérő színekkel.

képernyőfotó, ill. az egyes fázisok kirajzolásához szükséges megjelenítési szűrő

1. https://www.steffr.ch/inspect-ssl-tls-traffic-from-chrome-firefox-curl-with-wireshark-no-mitm/ [↑](#footnote-ref-1)