Gyakorlati jegyzet

HTTPS, TLS és tanúsítványok

Célja, hogy lépésről lépésre bemutassa a HTTPS, TLS és tanúsítványok működését valós eszközök segítségével.

A gyakorlat időtartama: 2 × 45 perc

1. rész – HTTPS és tanúsítványok megfigyelése

Feladat 1 – HTTP vs HTTPS összehasonlítás

Nyisd meg a következő oldalakat böngészőben:

• http://httpbin.org
• https://httpbin.org

Figyeld meg:
• a címsorban megjelenő lakatot vagy figyelmeztetést
• az automatikus HTTPS-re irányítást

Feladat 2 – Tanúsítvány vizsgálata böngészőben

Nyisd meg:
• https://www.google.com
• https://expired.badssl.com

Kattints a lakatra → Tanúsítvány megtekintése.

Vizsgáld meg:
• Issuer (ki adta ki)
• Érvényességi idő
• Subject Alternative Name (SAN)
• Tanúsítványlánc

Feladat 3 – Tanúsítványlánc

Vizsgáld meg a tanúsítvány hierarchiát:

Root CA
└─ Intermediate CA
  └─ Server tanúsítvány

Figyeld meg, hogy a böngésző csak megbízható Root CA esetén fogadja el a láncot.

Feladat 4 – Domain mismatch

Nyisd meg:
https://wrong.host.badssl.com

Figyeld meg a böngésző figyelmeztetését.
Ez akkor történik, ha a tanúsítványban szereplő domain nem egyezik meg az URL-lel.

2. rész – TLS és HTTPS handshake elemzése

Feladat 5 – HTTPS handshake Wiresharkkal

Indíts Wireshark capture-t az alábbi szűrővel:

tcp port 443

Nyisd meg böngészőben:
https://example.com

Állítsd le a capture-t és alkalmazd a következő display filtert:

tls.handshake

Feladat 6 – ClientHello elemzése

Nyisd meg a ClientHello csomagot és vizsgáld meg:
• TLS verzió
• Cipher suite lista
• SNI mező

Feladat 7 – HTTPS handshake összefoglalása

Rajzold fel a HTTPS handshake lépéseit:

ClientHello
ServerHello
Certificate
Kulcscsere
ChangeCipherSpec
Finished

Ezután indul a titkosított HTTP kommunikáció.

A gyakorlat végére meg kell értened:
- miért szükséges a HTTPS
- hogyan működik a tanúsítványellenőrzés
- hogyan jön létre a biztonságos TLS csatorna

MELLÉKLET – Bónusz gyakorlat

Tanúsítvány elemzése KeyStore Explorerrel

Ez a bónusz gyakorlat célja, hogy a hallgatók vizuálisan is megismerjék egy X.509 tanúsítvány belső felépítését.

KeyStore Explorer letöltése: https://keystore-explorer.org/

Ajánlott idő: 10–15 perc

1. lépés – Tanúsítvány letöltése böngészőből

Nyisd meg:
https://www.google.com

Kattints a lakatra → Tanúsítvány → Részletek → Exportálás
Mentsd el a tanúsítványt PEM formátumban (pl. google.pem).

2. lépés – Megnyitás KeyStore Explorerben

Indítsd el a **KeyStore Explorer** programot.
Examine Certificate (File) → válaszd ki a letöltött PEM fájlt.
Dupla kattintással nyisd meg a tanúsítványt.

3. lépés – Vizsgálandó mezők

Vizsgáld meg az alábbi mezőket:

- Subject / SAN – mely domainek szerepelnek?
- Issuer – mely CA adta ki?
- Validity – érvényességi idő
- Public Key – algoritmus és kulcsméret
- Signature Algorithm

Figyeld meg, hogy a privát kulcs nem része a tanúsítványnak.

Kapcsolat a HTTPS handshake-kel

A HTTPS handshake során a szerver ezt a tanúsítványt küldi el a kliensnek.
A böngésző a tanúsítvány publikus kulcsát és aláírását használja a hitelesség ellenőrzésére és a biztonságos kulcscsere előkészítésére.