Mérési utasítás **DNS, SSH protokollok**

Mérés célja:

A Domain Name System rendszer működésének megismerése, használata. Az SSH biztonságos távoli elérés működése.

DNS

A DNS egy hierarchikusan felépített rendszer mely a számítógépek, és bármely aktív hálózati eszköz elnevezhető egy szimbolikus névvel, ez által nem kell az eszközhöz tartozó IP címet megjegyezni.

1. feladat

Kérdezze le a root (.) névkiszolgálókat!

```
host -t NS .
```

Ezzel a Linux kilistázza az elérhető root névkiszolgálókat. Ezek a névkiszolgálók felelősek a gTLD, és ccTLD domain-ekért. Ezek a szerverek mondják meg, hogy mondjuk a '.hu' domainért ki felel.

2. feladat

Kérdezze le a '.hu' domain névkiszolgálóit!

```
host -t NS hu.
```

A most kilistázott névkiszolgálók felelnek a '.hu ' domainért. Egy domain-ért több névkiszolgáló felelhet.

A host parancs nem csak az aktuális domain-hez tartozó névkiszolgálót tudja lekérdezni. Hanem a domain-hez tartozó más rekordokat is. Ilyenek lehetnek: A, MX, SOA, CNAME, HINFO.

A – a tulajdonos IP címe

MX – Mail Exchange, a domainhez tartozó levélkiszolgáló

SOA – State of authority, hitelességi specifikációk

CNAME – egy létező A rekordhoz kanonikus név hozzárendelése

HINFO – CPU és Operációs Rendszer meghatározása

3. feladat

Kérdezze le a tilb.sze.hu domain levélkiszolgálóit!

```
host –t MX tilb.sze.hu.
```

Egy adott domainben több levélkiszolgáló is lehet. Ezeket prioritásba kell állítani. Ezért az MX rekordhoz mindig tartozik egy számérték is, minél kisebb ez a szám annál nagyobb a prioritása a levélkiszolgálónak. A legkisebb számmal rendelkező gép a „root” levélkiszolgáló.

4. feladat.

dnsdoctor segítségével ellenőrizze a tilb.sze.hu. domain RFC szerinti hitelességét!

```
dnsdoctor tilb.sze.hu.
```

SSH

Az SSH távoli hozzáférést nyújt azon kiszolgálókhoz, melyeken működik SSH kiszolgáló. A szokásos CLI-n (Command Line Interface) felül Linux és más UNIX-like rendszerekben lehetőség nyílik SSH tunnelezésre, mellyel egy biztonságos adatcsatornát hozhatunk létre.

5. feladat

Lépjen be a szemben lévő fekete gépre root felhasználóként, úgy hogy közben elindít egy Wireshark csomagelkapást az eth4-en!

```
ssh root@fekete<gépszám>  vagy ssh -l root fekete<gépszám>
```

Ha mindent jól csinált, ez lesz az „első” belépés a számítógépre. Ekkor kérdez rá, hogy elfogadjuk-e a szemben lévő gép RSA ujjlenyomatát. Vagyis ekkor történik a kulcscsere. A kérdésre **„yes”** a válasz.
Ez után az SSH véglegesen hozzáadta a szemben lévő gép adatait a */root/.ssh/known_hosts* fájlhoz.
A root jelszót megadva lépjünk be a gépre.
(Amennyiben nem lép be, úgy a szemben lévő gép bontotta a kapcsolatot amíg a feladatot olvasta, kérem lépjen be újra. Ekkor már nem fog semmit kérdezni, hisz az előbb már engedélyeztük a kapcsolódást.)

Ezek után root jogokkal felvértezve adhatunk ki parancsot más gépen.

6. feladat

Adjuk ki az ifconfig parancsot.

```
ifconfig
```

7. feladat.

A mérés végeztével töröljük ki a host információkat a /root/.ssh/known_hosts fájlból, hogy a következő mérésen is az „első” belépést tudjuk szimulálni.

```
echo  >  /root/.ssh/known_hosts
```