LINUX RENDSZERFEJLESZTÉS ÉS ÜZEMELTETÉS

6. forduló

ONE IDENTITY by Quest

A kategória támogatója: One Identity

RENDELKEZÉSRE ÁLLÓ IDŐ:

30:00

Ismertető a feladathoz

Felhasznált idő: 01:40/30:00 **Elért pontszám:** 0/25

1. feladat 0/10 pont

Adott egy kliens és egy szerver. A kliens a szerveren található HTTPS felett futó szolgáltatást próbálja meg elérni. Miután a kliens nem tudja elérni a weboldalt, a mérnök a kliens mellett a szerver oldalt is megvizsgálja. Azt látja, hogy az IPv4 TCP forgalom elindul a klienstől, de nem érkezik meg a szerverhez.

A hálózat a következőképpen néz ki:

A kliens egy hálózatban van az R1 routerrel, a kliensnek a default gateway az R1 router.

A szerver egy hálózatban van az R2 routerrel, neki a default gateway az R2 router.

Az R1 és az R2 router között egy ismeretlen hálózat van, de a két router között VPN kapcsolat épült ki AES256 titkosítással.

A kliens és a szerver között VPN kapcsolat van RC4 titkosítással.

A szerver használ stateful tűzfalat, ahol csak az UDP 53 és a TCP 443 van beengedve. A kliens használ stateful tűzfalat, ahol minden ki van engedve és semmi nincs beengedve.

Mi lehet az oka annak, hogy a kliens nem tudja elérni a szerver oldalon a weboldalt?

Válasz

- ◯ Át kell engedni a kliens és szerver tűzfalakon az icmp forgalmat a két végpont közötti csomag fragmentációja miatt
- ◯ Az RC4-et nem lehet AES256-ba tunelezni. Ezért úgy fest mintha a VPN kapcsolat élne, de valójában nincs benne forgalom.

- ( ) Ki kell nyitni a 80-as portot is, hogy a webszerver teljesen tudjon funkcionálni
- ( ) A 443-as port HTTPS portokollt jelent, A HTTPS forgalom nem tud a két egymásba ágyazott titkosított csatornán átmenni.

Magyarázat

Át kell engedni a kliens és szerver tűzfalakon az icmp forgalmat a két végpont közötti csomag fragmentációja miatt.

2. feladat 0/15 pont

A munkahelyeden a saját személyes szerveredre szeretnél bejutni, és ehhez SSH kapcsolatot használsz, ahol az authentikáció jelszóval történik. Az SSH kapcsolat létrejön, elkéri a jelszót, és ezzel sikeresen authentikálsz.

Közben a konyhában azt a hírmorzsát hallod, hogy a céges security csapat MITM monitorozó eszközt telepített a hálózatba.

Hogy biztos legyél benne, hogy nem történt-e valami turpisság a te SSH kapcsolatodban, megpróbálsz nyomokat keresni.

Mit teszel, hogy felderítsd ezt a MITM szituációt?

Válaszok

- [ ] SSH kapcsolódsz lokálisan, és összehasonlítod a két SSH kapcsolat felépülésének sebességét.
  Ha nagy a különbség, akkor az gyanús.
- [ ] A kapcsolat felépítésekor ezt a parancsot használod:

  ```
  ssh –o VisualHostKey=yes
  ```

  és megvizsgálod a fingerprintet, hogy passzol-e a nemzetközi adatbázisokban található gyanús fingerprintekhez
- [x] Ha az SSH kapcsolat felépülésekor nem láttál üzenetet arra vonatkozóan, hogy a fingerprint nem egyezik, akkor az MITM támadás nem történhetett meg.
- [x] A távoli szerveren kiadod ezt a parancsot:

  ```
  ssh -vvv localhost
  ```

  és összehasonlítod a választott algoritmusokat .

Magyarázat

ssh -vvv localhost esetén a -v kapcsolók miatt látszani fog a teljes felépülése a kapcsolatnak, azaz láthatóak lesznek a két fél által felajánlott kriptográfiai algoritmusok. Felettébb gyanús, ha a felajánlott algoritmusok nem egyeznek, az elvártak szerint.

KÉSZÍTETTE

Megjelenés

Világos