Tentti S-38.3153 Tietoliikenteen tietoturva
Exam S-38.3153 Security of Communication Protocols

16.5.2012

Put your name, student number, course code and date to each exercise paper. This helps you to receive your credits in fast and reliable manner. Answers are accepted in Finnish, Swedish or in English. Answers are judged based on their quality and clarity. A short and down to the fact answer will get better points than an excursive one. You may explain things further but beware that errors may lower your points (even if they are in extra matter).

1. Turvamekanismit voivat perustua ensisijaisesti estämiseen, havaitsemiseen tai toipumiseen. Esitä kustakin tapauksesta lyhyesti havainnollinen ja perusteltu esimerkki.

   Security mechanisms can be based primarily on prevention, detection or recovery. Present an example for each case with short reasoning. (6 p.)

2. Kurssilla on esitelty useita Ethernet-hyökkäyksiä, esimerkiksi ARP-myrkytys, DHCP-myrkytys, tai STP-juurihyökkäys. Valitse yksi näistä hyökkäyksistä ja kuvaa:
   - mitä resursseja tai järjestelmään pääsyjä hyökkääjä tarvitsee
   - kuinka hyökkäys toteutetaan protokollatasolla (protokollaviestit ja siihen osalliset)
   - mitä tapahtuu kohdesolmuille. Mikä on näiden tila ennen ja jälkeen hyökkäyksen
   - miten hyökkääjä hyötyy hyökkäyksestä
   - kuinka suojata järjestelmää tältä hyökkäykseltä

   Several Ethernet based attacks have been shown in class, such as ARP poisoning, DHPC poisoning or STP root attack.Select ONE of these attacks. Describe:
   - what resources or access the attacker needs
   - how the attack is performed on protocol level (what are the protocol messages and participants)
   - what happens in the target nodes (what is their state before and after the attack)
   - what the attacker gains from this attack
   - how to protect the system against this attack (6p.)

3. Kurssilla on esitelty useita turvallisuusprotokollia TCP/IP-pinon eri kerroksissa. Selitä lyhyesti turvallisuustarpeet IP-, kuljetus- ja sovellustasoilla ja anna esimerkki turvallisuusprotokollasta kullakin tasolla. Kuvaa lyhyesti mitä turvallisuusongelmia valitsemasi protokollat ratkaisevat, eivät ratkaise ja mitä mekanismeja ne käyttävät.

   During the course, several security protocols have been presented - at different layers of the TCP/IP stack. Explain shortly the security needs at IP layer, transport layer, and application layer and give an example security protocol at each layer. Explain shortly what security problems the chosen protocols solve, what they don't solve, and the mechanisms they use. (6p.)

4. Vastaa seuraaviin kysymyksiin lyhyesti

   a) Kuvaile välimieshyökkäys

      Describe Man-in-the-Middle attack (1p.)

   b) Mitä tietoturvassa pyritään suojaamaan?

      What are the things information security aims to protect? (2p.)

KÄÄNNÄ! TURN PAGE!

c) Perustele lyhyesti mitkä seuraavista väitteistä pitävät paikkansa ja mitkä eivät (pisteet tulevat perusteluista).

Justify briefly the following statements as either correct or false. Grading is based on the justification you give.

i. Ethernetistä ei ole mahdollista tehdä turvallista, joten sitä ei pitäisi käyttää mihinkään.

It is impossible to make Ethernet secure, so it should not be used for anything at all. (1p.)

ii. Järjestelmän turvallisuutta voidaan aina parantaa sillä, että parannetaan minkä tahansa järjestelmäkomponentin turvallisuutta.

You can always improve the security of a system by improving the security of any component of the system. (1p.)

iii. Palomuuri suojaa verkkoa palvelunestohyökkäyksiltä.
Firewall protects the network from denial of service attacks. (1p.)

5. Al Qaeda on tämän tehtävänannon puitteissa hierarkisesti toimiva terroristijärjestö, joka koostuu soluista. Organisaation tulee kestää se, että osa sen jäsenistä jää kiinni ja kertoo kaiken, mitä tietää. Lisäksi ylin johto ei saa tuntea alaisiaan, eivätkä alaiset liikaa ylimmästä johdosta tai naapurisoluista.

Suunnittele turvallinen pääsynvalvontajärjestelmä Al Qaedalle. Arvioi missä ovat suunnittelemasi järjestelmän heikkoudet turvallisuuden näkökulmasta.

For the purpose of thie question, Al Qaeda is a hierarchically operating terrorist organization composed of terrorist cells. The organization needs to be resilient to some of its members getting caught and telling everything they know to the captors. The leaders should not know the people below them and the terrorists should not know too much about the upper management or neighboring cells.

Design a secure access control system for Al Qaeda. Evaluate your design and discuss the security weaknesses in your design. (6p.)

6. Mitä kirjaa/joja ja materiaalia käytit opiskeluun (rehellinen vastaus ½ p)
What book(s) and materials you used for studying (truthful answer ½ p)

Mikko Särelä