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

9.1.2013

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 tietoverkkoja koskettava esimerkki.

   Security mechanisms can be based primarily on prevention, detection or recovery. Present an example for each case with short reasoning. The example needs to be about communication networks (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. Miksi nykyisessä Internetissä on vaikea suojautua palvelunestohyökkäyksiltä? Onko jotain, mitä asialle voitaisiin tehdä. (6 p)

   Why denial of service is hard to protect from in current Internet? Is there something that can be done for that (6 p)

4. Miten salausta käytetään tietoliikenteessä?
   Millaisia vaatimuksia tietoliikennejärjestelmissä käytetyille salausjärjestelmille on? (6 p)

   How encryption is used in data communication? What kind of requirements there are for encryption systems used for communications(6 p)

5. 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