Palvelunestohyökkäykset

Ari Keränen

Helsinki 27. helmikuuta 2003
Tietoturvallisuus nykyaikaisessa liiketoimintaympäristössä – seminaari: Laajennettu tiivistelmä
HELSINGIN YLIOPISTO
Tietojenkäsittelytieteen laitos

Palvelunestohyökkäykset

Ari Keränen

Tietoturvallisuus nykyaikaisessa liiketoimintaympäristössä – seminaari: Laajennettu tiivistelmä
Tietojenkäsittelytieteen laitos
Helsingin yliopisto
27. helmikuuta 2003, 4 sivua

Tässä tutkielmassa tarkastellaan palvelunestohyökkäyksiä, joiden tarkoituksena on kuluttaa jokin tietokonejärjestelmän tai tietoverkon rajallinen resurssi loppuun niin, etteivät palvelun käyttöön oikeutetut käyttäjät pääse käyttämään palvelua, tai sitten palvelun käyttö hidastuu ja hankaloituu huomattavasti. Aluksi hahmotellaan erilaisia yleisiä hyökkäystyyppejä, joilla pyritään vaikuttamaan normaalin tietoliikenteen esteettömään ja turvalliseen kulkuun. Seuraavaksi tarkastellaan tietoturvarikkomuksia koskevaa tutkimustietoa, jonka avulla voidaan hahmottaa palvelunestohyökkäyksien esiintymistä ja osuutta tietoturvarikkomuksista. Vaikka Suomessa havaittujen palveluestohyökkäysten määrä on vähäinen, niin USA:ssa tehdyssä tutkimuksessa niiden osuus kaikista havaituista tietoturvarikkomuksista nousi huomattavan korkeaksi.

Sitten tarkastellaan palvelunestoon pyrkivien hyökkäysten toteuttamistapoja, joita on useita. Palvelunestohyökkäykset jakautuvat kolmeen perustyyppiin, jotka ovat niukkojen, rajallisten tai uusiutumattomien resurssien loppuunkuluttaminen, konfigurointitietojen tuhoaminen tai muuttaminen, ja tietoverkkojen komponenttien fyysinen tuhoaminen tai muuttaminen. Hyökkääjän tavoitteena voi olla pyrkimys estää verkkoliikenne tulvittamalla verkko suurilla datamäärillä. Kahden isäntäkoneen välinen yhteys voidaan yrittää katkaista. Hyökkääjät voivat yrittää estää jonkin tietyn yksittäisen henkilön pääsyn palveluun. He voivat myös yrittää häiritä jonkin tietyn järjestelmän palvelujen käyttöä. Jonkin palvelun laiton käyttö voi myös johtaa palvelun käytön estoon. Palvelunestohyökkäykset voivat olla myös osa jotakin toista laajempaa hyökkäystä.

Palvelunestohyökkäyksien vaikutus ja laajuus vaihtelee. Ne voivat kohdistua yksittäiseen palvelimeen, tai sitten useampaan palvelimeen samanaikaisesti. Ne voivat häiritä ja hidastaa palvelun käyttöä, tai sitten ne voivat kaataa koko järjestelmän ja estää täysin sen käytön. Niitä voidaan käynnistää

pienin resurssein laajoja ja monimutkaisia järjestelmiä vastaan. Ne voivat tehokkaasti lamaannuttaa tietoliikenneyhteyksistä riippuvaisten yritysten tai organisaatioiden toimintaa.

Viimeisessä kappaleessa tarkastellaan tapoja, joilla palvelunestohyökkäyksiltä voidaan suojautua. Yleinen asiaan vaikuttava tekijä on tietoisuus ongelman luonteesta. Turvallisuus Internetissä on yhteinen asia ja se on sidoksissa Internetin yleiseen turvallisuuteen. Yhden osapuolen laiminlyönnit turvallisuuden suhteen vaarantavat myös muiden osapuolten turvallisuuden, vaikka hyökkäys ei vahingoittaisi turvatoimenpiteet laiminlyönyttä tahoa, niin se voi aiheuttaa huomattavia vahinkoja ulkopuolisille. On tärkeää, että turva-asioista vastaavat tahot ovat kaikkialla tietoisia uhkaavista vaaroista.

Seuraavaksi tarkastellaan yksityiskohtaisesti niitä teknisiä menettelytapoja, joiden avulla voidaan suojautua palvelunestohyökkäyksiltä, tai vähentää potentiaalisten hyökkäysten vaikutuksia. Reitittimissä on syytä käyttää erityisiä reititinsuodattimia, joiden avulla voidaan valvoa IP-osoitteiden oikeaa käyttöä. Tämä vähentää eräiden verkon ulkopuolisten palvelunestohyökkäysten aiheuttamaa vaaraa ja estää tehokkaasti myös eräitä verkon sisältä käynnistettäviä muihin verkkoihin kohdistuvia palvelunestohyökkäyksiä. On syytä kytkeä pois käytöstä kaikki käyttämättömät tai tarpeettomat verkkopalvelut, sillä tämä voi rajoittaa tunkeutujan kykyä hyödyntää näitä palveluja palvelunestohyökkäysten suorittamiseksi. On syytä ottaa käyttöön käyttöjärjestelmän tarjoamat kiintiöjärjestelmät, jos niitä on käytettävissä, sillä niillä voidaan suojautua tilanteelta, jossa yksi taho voisi kuluttaa järjestelmän resurssit loppuun. On tarkkailtava järjestelmän suorituskykyä ja määriteltävä tasot normaalikäytölle. Tällöin näitä määrittelyjä voidaan käyttää poikkeuksellisen levyn ja keskusmuistin käytön, ja verkkoliikenteen havaitsemiseen.

Rutiininomaiset laitteiston fyysiseen turvallisuuteen kohdistuvat tarkastukset ovat tarpeen, jolloin voidaan havaita vastaavatko ne olemassaolevia tarpeista. On tarpeen käyttää sopivia ohjelmistotyökaluja, että voidaan havaita, jos konfigurointitiedoissa tai muissa tiedostoissa on tapahtunut muutoksia. On tarpeen pitää varalla nopeasti käyttöönotettavissa olevia koneita, jos vastaavanlainen kone tulee toimintakyvyttömäksi. Verkkokonfigurointitietojen on syytä olla vikasietoisia ja niistä on syytä olla kopioita. On tarpeen kehittää ja ylläpitää säännöllisiä varmuuskopiointitoimintoja. Salasanojen suhteen on noudatettava tarkkoja varotoimenpiteitä, etenkin silloin, kun kyseessä ovat pääkäyttäjän oikeudet.

Edellisten toimien lisäksi voidaan käyttää myös joukkoa yleisiä suunnitteluperiaatteita kehitettäessä palvelunestohyökkäyksiltä suojaavia verkkoprotokollia. Resursseja ei tulisi sitoa tietoliikenneyhteyteen, ennen kuin asiakas on autentikoinut itsensä. Koska useimmat palvelunestohyökkäykset perustuvat osoitevääränn ökseen, on muistin allokoimista mielivaltaisen asiakkaan pyynnöstä kuitenkin voitava välttää. Asiakkaan autentikointiin tulee ryhtyä vasta sitten, kun helpommat tavat havaita hyökkäys on loppuunsuoritettu, koska autentikointi on toimenpide, joka kuluttaa paljon laskentatehoa.

Asiakkaan työtaakan tulisi aina olla palvelimen työtaakkaa suurempi. Tällöin voidaan asiakkaalta eliminoida hänen kykynsä käynnistää useita hyökkäyksiä, koska suurempi työtaakka kuluttaa loppuun hänen hyökkäyksen käynnistämiseksi tarvittavat resurssit. Asiakkaan työtaakan tulisi kasvaa lineaarisesti, kun taas palvelimen työtaakan tulisi säilyä niin vakioisena, kuin mahdollista ja tämän työtaakan tulisi olla asiakkaan työtaakasta riippumatonta.

Asiakkaan työtaakan tulisi olla parametrisoitavissa ja palvelimen tulisi kyetä helposti muuttamaan sitä. Tämä mahdollistaisi protokollien modifioimisen erilaisille sovellusskenaarioille ja asiakkaan laitteistoille. Lisäksi mahdollisuus muuttaa asiakkaan työtaakkaa mahdollistaa verkkoliikenteeseen reagoimisen ja puuttumisen. Jos epäillään hyökkäystä, niin protokollan vaikeusastetta voitaisiin vähitellen kasvattaa, jotta voitaisiin taata järjestelmän toimintakyky epäillystä hyökkäyksestä huolimatta, vähentämättä kuitenkaan huomattavissa määrin järjestelmän palvelujen saatavuutta laillisille käyttäjille.

Aiheluokat(Computing Reviews 1998): C 2.0, K 6.5

Avainsanat: Palvelunestohyökkäykset, tietoturva

Lähteet:

CER97 CERT Coordination Center: Denial of Service Attacks. http://www.cert.org/tech_tips/denial_of_service.html

CER00 CERT/CC and FedCIRC: CERT Advisory CA-2000-01 Denial-of-Service Developments. http://www.cert.org/advisories/CA-2000-01.html

CER02 CERT/Coordination Center Statistics 1988-2002, October 2002. http://www.cert.org/stats/cert_stats.html

CSI02 2002 Computer Crime and Security Survey, 2002. http://www.gocsi.com/press/20020407.html

LAN00 Leiwo, Aura, Nikander: "Towards network denial of Service resistant protocols". IFIP TC11 16th Annual Working Conference on Information Security, 2000.

Paa00 Paavilainen, J, Tietoturva 2000: Tietoturvan kyselytutkimus, Tampereen yliopisto, 2000.

Sta99 Stallings,W, Cryptography and network security: Principles and practises, Prentice-Hall, 1999.