Ohud võrgus

- Ohtude liigid
- Internet
- Info lekkimine
- Aktiivne sekkumine
- Turvaaugud programmides
- Teenusetõkestus
- Hüppelauad
- Maine kahjustamine

Mis ohud meid võrgus varitsevad?

- Info lekkimine arvutivõrgu kaudu
- Aktiivne volitamata sekkumine
- Teenusetõkestus
- Arvuti kasutamine hüppelauana edasi tungimiseks
- Maine rikkumine

Võrk == Internet

- Miks Internet pole turvaline?
  - Disainitud ilma turvalisuseta
  - Turvalisust on juurde lapitud tükikaupa
  - Kasutajad ei hooli
- Miks Internet muudab tihti ka mitte otseselt võrguga seotud tarkvara ebaturvaliseks?
  - Programmidele tulevad andmefailid mitteusaldatud allikast (teisest turvakontekstist) ning senised lihtsad programmivead saavad turvaaukudeks
  - Näide: Windowsi .HLP-failid

Info lekkimine

- Konfigureerimise ja administreerimise vead
  - Liigsed teenused
  - Failisüsteemi jagamine liiga laiale ringile (SMB, NFS, HTTP)
  - Aktiivsisu liiga automaatne käivitamine
  - . . .
- Vead teenuseid pakkuvates programmides
- Võrguliikluse pealtkuulamine
  - Ethernet
  - *Switch* — kas lahendus?
  - Muud võrgud (modemside, DSL, kaabelvõrgud, raadiovõrgud, . . .)
  - Turvasüsteemi disainimisel tasub eeldada, et pidevalt võidakse kusagil liiklust pealt kuulata

Aktiivne sekkumine

Arvuti identiteedi võltsimine (ründav arvuti imiteerib rünnatava poolt usaldatud arvutit)

- IP aadressi vahetus
- MAC aadressi vahetus
- IP aadressi võltsimine (*IP spoofing*)
- MAC aadressi võltsimine
- ARP võltsimine
- DNS kirjete võltsimine, valed pöördteisendused
- Source ruuting
- Marsruutimisinfo võltsimine
- Ühenduste kaaperdamine (*hijacking*)

Turvaaugud programmides

- Auklikud on nii server- kui kliendiprogrammid (brauserid kui palju võrgust tulevat infot töötlevad programmid!)
- Regulaarne turvaparanduste rakendamine on kohustuslik
- Disaini vead (JavaScript, ActiveX, . . .)
- Implementatsiooni vead, näiteks:
  - Puhvri ületäitumised
  - Failisüsteemi ja juurdepääsu semantika
  - Probleemid erinevate turvatsoonide segamisel
- Konfiguratsioonivead

Ettevaatust

Kõik võrgust tulevad andmed on ebausaldusväärsed!!!

Denial of Service — teenusetõkestus

- Ülekoormus
- Ressursside ammendamine
  - Kettaruum (näiteks aetakse logisid täis)
  - Mälu, protsessitabel
  - Protsessoriaeg (näiteks tehakse "tühja" krüptimist)
  - Võrguriba (ujutatakse pakettidega üle)
- Vead süsteemi ja protokollide disainis ja realisatsioonis
- Hajus teenusetõkestus (*Distributed DoS*)
- Üldiselt on seda tüüpi rünnetega väga raske võidelda

Hüppelauad

Ründaja ei vaja saavutatud juurdepääsu tihti otseselt, vaid mingi järgmise eesmärgi saavutamiseks

- Kasutajatunnuse hõivamine superkasutaja või teiste kasutajate ründamiseks
- Lüüsarvuti hõivamine sisevõrku juurdepääsu saamiseks
- Strateegiliselt olulises punktis asuva arvuti hõivamine liikluse pealtkuulamiseks
- Arvuti hõivamine teistele arvutitele teenusetõkestusrünnete tegemiseks
- Arvuti hõivamine jälitamise raskendamiseks
- Vahendusmasin rämpsposti laiali saatmiseks

Maine kahjustamine

- Veebilehtede näotustamine
- (Piisavalt) avalikud rünnakud kellegi kolmanda vastu vallutatud arvutist
- Rämpsposti saatmine