## Kuidas sissetungijaid avastada?

- Süsteemi kahtlane käitumine
- Logimine ja logide jälgimine
- Muutused süsteemis (failid, konfiguratsioon)
- Kahtlane võrguliiklus
- . . .
- IDS (*Intrusion Detection Systems*) – sissetungi avastamise süsteemid
  - Masinasisesed
  - Tervet võrku valvavad
  - Loomult ebatäpsed
  - Vajavad toimimiseks reageerijat





## Logimine

- Logid ärgu olgu maailmale kirjutatavad
- Logid ärgu olgu maailmale loetavad
- Et logist kasu oleks, peab seda ka lugema
- Milleks lugeda logisid, kui keegi parajasti ei ründa?
- Automaatsed logide analüsaatorid
- Logi "lõhki ajamine" on ka rünnak
- Mõistlik säilitamisaeg on varieeruv, enamasti 1-10 nädalat
- Kohalikud logid on sissetungijale potentsiaalselt kirjutatavad (võltsitavad)
- Lugeda tuleb enne võltsimist, pärast on raske





## Turvalised logid

- Mille vastu me logisid kaitsta tahame?
  - Modifitseerimise
  - Hävitamise
- Üksteist dubleerivad logid, mittetraditsioonilised logid
- Paberkoopia
- Teise arvutisse logimine (konfidentsiaalsus?)
- Logikirjete omavaheline sidumine krüptograafiliste meetoditega (räsiahelad) → ajatemplid
- Üle võrgu logimine koos auditeeritava krüptograafilise sidumisega





## Kuidas sissetungijat avastada – näiteid

- Lisandunud on tundmatuid võrguteenuseid
- Lisandunud on tundmatuid protsesse (ka maskeeruvaid!)
- Lisandunud on tundmatuid kasutajaid
- Failid on muutunud
- Juurde on tulnud peidetud või setuid/setgid faile
- Logis on kahtlasi kirjeid või "auke"
- Mõni kasutaja teeb midagi ebatüüpilist
- Sisselogimiste ajad või kohad on kahtlased
- Võrguliides on *promiscuous* režiimis
- Pilt süsteemist pole kooskõlaline (pooleldi eksisteerivad protsessid, . . . )

## IDS masina tasemel

- Failide õiguste, kontrollsummade, muutmise aegade kontroll
  - Probleem andmebaasi uuendamisega ja hoidmisega
- Logide jälgimine
  - Mustrite sobitamine
  - Toimingud (teavitamine, blokeeringud, . . . )
  - Tehisintellekt ja heuristikad
- Antiviirus
- Levinumate *rootkittide* avastamine
- Peidetud protsesside avastamine
- Käivitatavate programmide signeerimine ja signatuuride kontroll
- Näiteid: Tripwire, LIDS, AIDE





## IDS võrgu tasemel

- Võrgus on seade, mis kuulab teistega toimuvat
- Arhiveerib, analüüsib, saadab mujale edasi
- Edasi saatmisel on konfidentsiaalsus oluline
- Uute aktiivsete seadmete avastamine
- Etherneti pealtkuulamine
  - hub
  - riistvaraline harund (*tap*)
  - spetsiaalne switchi port (port mirror)





## IDS võrgu tasemel

- IDS süsteemid tunnevad paljusid konkreetseid rünnakuid ja rünnakute tüüpe
- Näide: snort
- Meepott (*honeypot*) – spetsiaalne masin ründaja eemale meelitamiseks ja tema meetodite uurimiseks
- Meevõrk (*honeynet*) – terve (virtuaalne) võrk ründaja püüdmiseks
- IDS sarnased on ka turvaskännerid – (oma) võrgust automaatselt aukude otsijad





## Snifferite avastamine

- Teoreetiliselt pole 100% ulatuses võimalik
- Vale MAC aadressiga IP tasemel pingimine
- Muud vastuse välja meelitamised vale MAC aadressiga (ICMP vead jms)
- Sama asi IP broadcastiga (255.255.255.255 või suunatud broadcast 192.168.0.255)
- ARP päringute saatmine mitte-broadcast MAC aadressile
- DNS pöördteisenduste jälgimine

## Snifferite avastamine

- *Source routing*'u kasutamine (saata pakett mitteruutiva masina kaudu)
- Nimelt valede paroolide avatekstina saatmine ja reaktsiooni ootamine
- Masina võrguliidese *promiscuous* režiimis olek
- Suur võrgukoormus (edasisaatva snifferi puhul)
- SNMP abil võrguseadmete info jälgimine (siseneva info maht, *promiscuous* režiim)





## Mida teha augu leidmisel

- *Don't panic!* – alati ei tarvitsegi auku olla
- Eralda süsteem võrgust
- Võimalusel tee uurimiseks madalal tasemel koopia
- Enne igasugust muutmist mõtle asjad hästi läbi
- Vajadusel teavita politseid või muid organeid (CERT, . . . )
- Tee pädevaid märkmeid, mis kõlbaksid kasvõi kohtus
- Turvaprobleemide PR:
  - Ära salga, ära vassi
  - Tunnista, et auk oli ja et parandati
  - Jaga tunnustust oma tootest augu leidjale
  - Kui renomee on väga kallis ja raha piisavalt palju, maksa kinni kõik asjast teadlikud tegelased :)