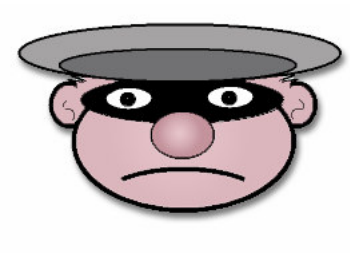
# IDS - hyökkäysten havaitseminen ja torjunta verkossa



Tietoturvaseminaari

Tietoturva ry

23.9.1999
Jari.Pirhonen@atbusiness.com
Projektipäällikkö, CISSP
AtBusiness Communications Oy
http://www.atbusiness.com/

AtBusiness Communications Oy / Jari Pirhonen © 1999

# Intrusion Detection Systems

- Sovelluksessa
- Käyttöjärjestelmässä
- Verkkoliikenteessä

- IDS vs. vulnerability scanners vs. honeypots

- allekirjoitukset - tilastoanalyysi - eheys

# Miksi palomuuri ei riitä?

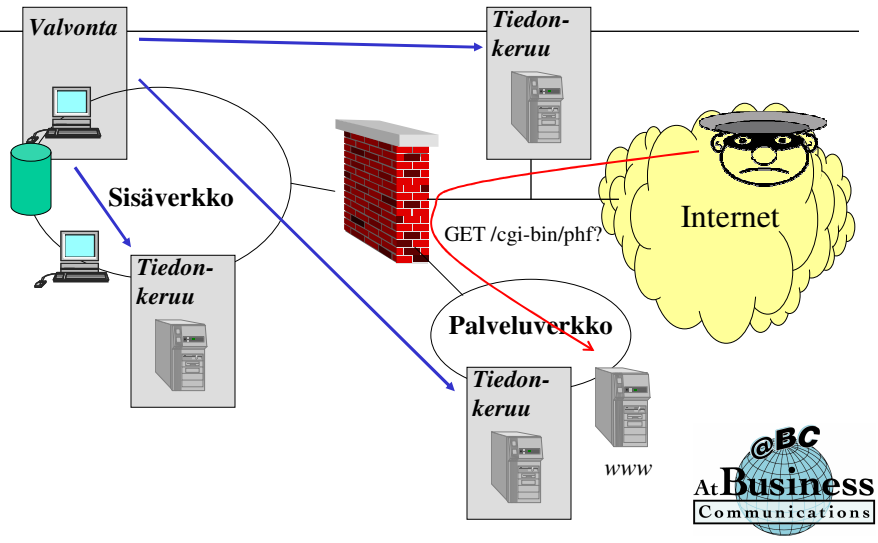
- Palomuuri ei huomaa sallitulla liikenteellä yritettäviä hyökkäyksiä: http, ftp, email, dns,…
- Palomuuri ei talleta historiatietoa liikenteestä
- Palomuuri on portinvartija - tarvitaan myös varashälytin
- Intranet - palomuuri ei valvo kaikkea liikennettä
- Ongelmat protokollissa, sovelluksissa?
- Onhan tietoturvakorjaukset asennettu?
- Mistä tiedät palomuurin toimivan?

AtBusiness Communications Oy / Jari Pirhonen © 1999

# NIDS
## Network Intrusion Detection System

- Tutkii verkkoliikennettä reaaliajassa
- Raportoi / hälyttää poikkeavuudet ja tunnetut hyökkäykset
- Tunnistaa “vialliset” TCP/IP paketit
- Voi suorittaa vastatoimenpiteitä
- Tallettaa historiatietoa -> analysointi, todisteet
- Todentaa turvajärjestelyjen riittävyyden
- Läpinäkyvä käyttäjille ja sovelluksille

## Tiedätkö, mitä tietoverkossasi tapahtuu?






# Tutkimuksia 1999

- InformationWeek (2700)
  "37% of survey respondents reported using intrusion-detection product, up from 29% last year"
- Information Security Magazine (745)
  "41% of respondents are using IDS-products"
  "23% experienced unauthorized access by outsiders"
- Internet Auditing Project 98-99
  - tutkittiin n. 35 miljoonaa konetta
  - 18 tunnettua ongelmaa: tooltalk, bind,wu_imapd, qpopper, wwwcount, rpc_mountd,...
  - 450.000 haavoittuvaa laitetta

# Hakkerin toiminta

1 Verkkotopologian selvittäminen
- IP-osoitteet, nimet, käyttöjärjestelmät, palvelut,...
- skannerit (nmap), antisnifferit, DNS zone transfer,...

2 Haavoittuvan kohdan hakeminen
- tunnetut ongelmat, väärin konfiguroidut järjestelmät, troijalaiset, hyväksikäytettävät palvelut,…
- IMAP, FTP, Web CGI, BackOrifice, Hack'a'Tack,…
- CyberNotes http://www.fbi.gov/nipc/nipcpublic.htm

AtBusiness Communications Oy / Jari Pirhonen © 1999

# Hakkerin toiminta

3 Tunkeutuminen järjestelmään
- Haavoittuvan kohdan hyväksikäyttö, turvajärjestelyjen kierto, palvelujen väärinkäyttö,…
- bugit, tunnelit, salasanakrakkerit,...

4 Järjestelmän haltuunotto
- tunkeutumisen "varajärjestelmät"
- rootkit, systeemiohjelmien korvaaminen,...

# Hakkerin toiminta

5 Levittäytyminen, jälkien peittäminen
- hyökkäys verkon muihin koneisiin, lokien ”siivous”
- snifferit

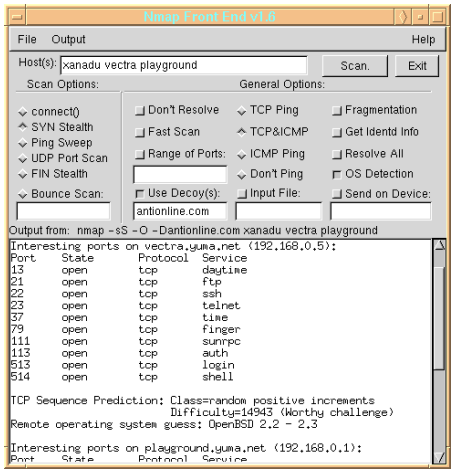
6 Luetaan, kopioidaan, muutetaan, tuhotaan,…
- toteutetaan hyökkäyksen päämäärä

7 Järjestelmän käyttäminen jatkohyökkäyksiin
- hyökätään muualle käyttäen jo vallattua järjestelmää alustana => jälkien peittäminen



# nmap

http://www.insecure.org/nmap/index.html




- Vanilla TCP connect() scanning
- TCP SYN (half open) scanning,
- TCP FIN, Xmas, or NULL (stealth) scanning
- TCP ftp proxy (bounce attack) scanning
- SYN/FIN scanning using IP fragments
- UDP raw ICMP port unreachable scanning
- ICMP scanning (ping-sweep)
- TCP Ping scanning
- Remote OS Identification
- Reverse-ident scanning

# Sscan: remote attack tool

README:
"you can have sscan launch off programs, initiate tcp connections and have dialogs with hosts that fit certain criterian, negotiate telnet connections and have sscan log into a host and execute shell commands (useful in coding internet worms), etc, all via a simple built in scripting language"

```
os[irix]
starttelnetdialog[23]
wait[2] # wait for login:
read[ogin:]
send[lp]
wait[2] # delay a bit..
read[$] # are we logged into a shell?
enddialog
print[successfully logged into unpassworded lp account!]
```

```
os[windows]
port[80]
cgi[/cgi-bin/_vti_inf.html]
registervuln[frontpage extensions are being used here.]
cgi[/cgi-bin/_vti_pvt/authors.pwd]
registervuln[authors.pwd is world readable]
```

AtBusiness Communications Oy / Jari Pirhonen © 1999

# Työkaluja: verkkoliikenteen valvonta

- Shadow, SANS Insitute
- Network Flight Recorder, NFR
- Dragon, Network Security Wizards
- RealSecure, ISS
- Netranger, Cisco
- NetProwler, Axent
- eTrust Intrusion Protection, CA
- BlackIce sentry, Network ICE

# Työkaluja: heikkouksien etsiminen

- Nessus
- Satan
- nmap
- CyperCop Scanner, NAI
- Internet Scanner, ISS
- NetSonar, Cisco
- Hackershield, BindView
- NetRecon, Axent
- Security Analyzer, WebTrends

AtBusiness Communications Oy / Jari Pirhonen © 1999

# Työkaluja: laitteen valvonta

- Tripwire, Tripwire Security Systems
- CyperCop Monitor, NAI
- eNTrax, Centrax
- Intruder Alert, Axent
- Kane Security Monitor, Security Dynamics

# Hyvän IDS-työkalun ominaisuuksia

- Huomaamattomuus, vähäinen resurssitarve
- Vikasietoisuus, luotettavuus
- Helposti muokattavissa yrityksen tarpeisiin
- Mukautuu muutoksiin, skaalautuvuus
- Vaikeasti hämättävissä
- Huomaa poikkeavuudet normaalista
- Helppokäyttöinen, keskitetty hallinta
- Monipuolinen raportointi, analysointi
- Kattava ongelmatietokanta

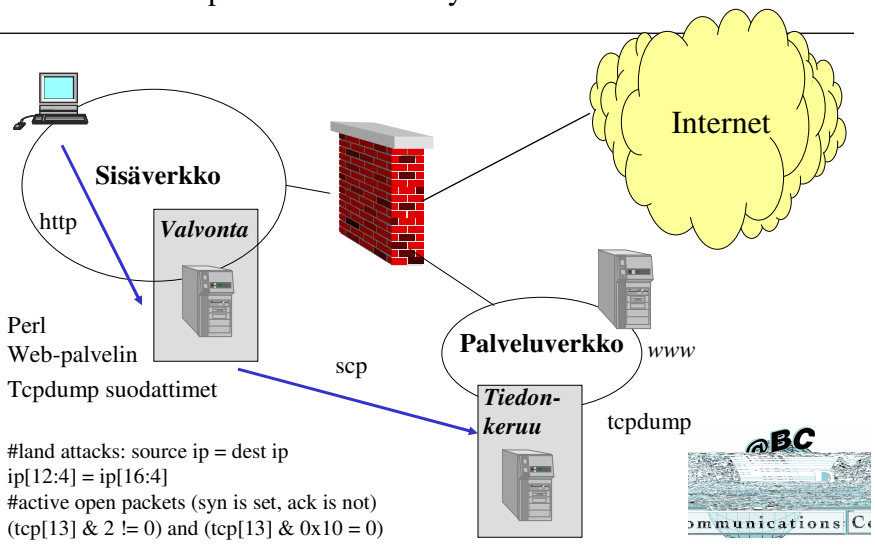
AtBusiness Communications Oy / Jari Pirhonen © 1999

# Hyötyjä

- Ongelmakohdat havaitaan etukäteen
- Parempi löytää ongelmakohdat itse...
- Hyökkäykset havaitaan aikaisessa vaiheessa
- Hyökkäykseen liittyvät tapahtumat ovat tallessa
  => todisteet tapahtuneesta
- Helpottaa tietoturvabudjettikeskusteluissa :-)

# Shadow

http://www.nswc.navy.mil/ISSEC/CID/

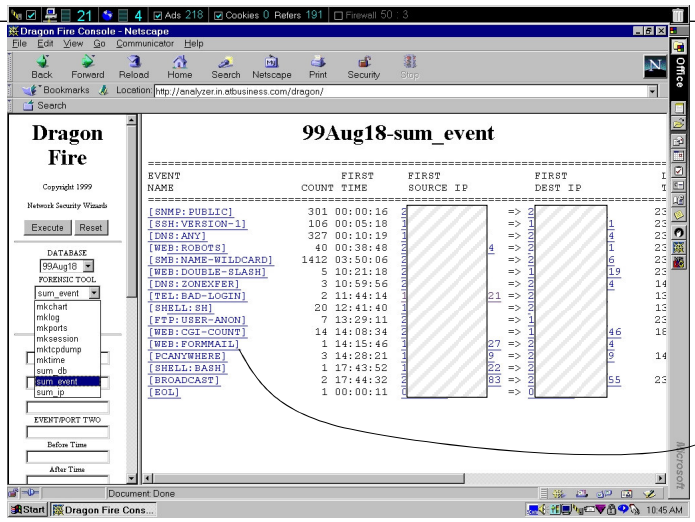



#land attacks: source ip = dest ip
ip[12:4] = ip[16:4]
#active open packets (syn is set, ack is not)
(tcp[13] & 2 != 0) and (tcp[13] & 0x10 = 0)



# Shadow

# Dragon



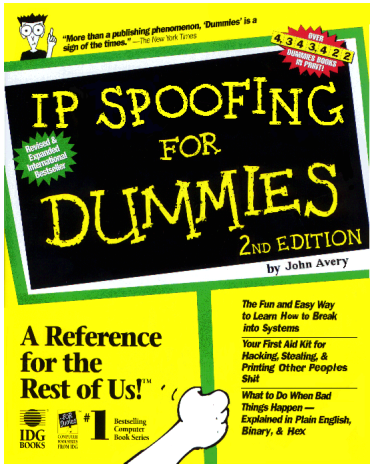

[WEB:FORMMAIL]

This server script allows remote users to execute commands remotely on a web server.



# Viimeisimpiä yrityksiä

- IMAP
- Netbus
- Hack'A'Tack
- FTP
- SunRPC
- Smurf
- nmap



# NIDS ongelmia

- Hyökkäysten tutkiminen vaatii asiantuntijatyötä
- Kuormitetut verkot, nopeus
- Switched networks
- TCP/IP heikkoudet: väärennetty lähdeosoite
- Verkkopakettitason hyökkäykset: fragmentoitu TCP/IP, ”su ro^H^Hroot”
- Salattu verkkoliikenne

AtBusiness Communications Oy / Jari Pirhonen © 1999

# NIDS-työkalun käyttöönotto

- Onko yrityksessä vahva TCP/IP-osaaminen?
- Public Domain työkalu vai kaupallinen?
- Kuinka usein ja miten työkalua päivitetään?
- Minne NIDS-sensorit asetetaan?
- Hälytykset vai loki?
- Yrityksen tietoturvapolitiikan vaikutus?
- Miten reagoidaan hyökkäyksiin? Kuka?
- Kommunikointi yrityksen henkilökunnalle? Seuraamukset rikkomuksista?

# Onhan perusta kunnossa?

5. Auditointi, seuranta, tutkinta
4. Teknologiat ja tuotteet
3. Tietoturvatietoisuus ja koulutus
2. Tietoturva-arkkitehtuuri ja prosessit
1. Tietoturvapolitiikka, standardit

AtBusiness Communications Oy / Jari Pirhonen © 1999

# Kuinka reagoida?

- Olethan valmistautunut, toimintasuunnitelma?
- Tarkista, onko murtoyritys onnistunut
- Siivoa järjestelmä(t), tuki reikä
- Ilmoitus hyökkääjän verkkovastaavalle, yhteistyö

  "We identified the dialup account that was used for this port scan. The account belongs to an local hospital, but apparently is often 'stolen' (or perhaps used unauthorised from employees outside of the hospital).
  We will take this with their management - the account has been temporarily suspended.
  Thanks for letting us know."
- Tarpeen vaatiessa yhteys poliisiin