Hyökkäysten havainnointi - teoriasta käytäntöön

AtBusiness

Jari.Pirhonen@atbusiness.com
Senior Security Consultant, CISSP, CISA
AtBusiness Communications Oyj

www.atbusiness.com

Scanners are out there…

- Joulukuussa 2001 avattiin testimielessä C-luokan testiverkko (netmask 255.255.255.0)
  - ei nimipalvelua
  - ei verkkoliikennettä ulos
  - ei mitään ”mainostusta” ko. verkon olemassaolosta
  - kaikkien IP-osoitteiden kaikkia portteja monitoroitiin
- Tulokset ensimmäisten 24-tunnin aikana
  - 1702 eri osoitteesta yritettiin vähintään yhtä TCP-yhteyttä
  - 1026 näistä osoitteista yritti useampaa yhteyttä
  - 335 koetti useampaa kuin 20 yhteyttä
  - 71 osoitteesta skannattiin koko aliverkko

SANS June 2002 Webcast, Tom Liston

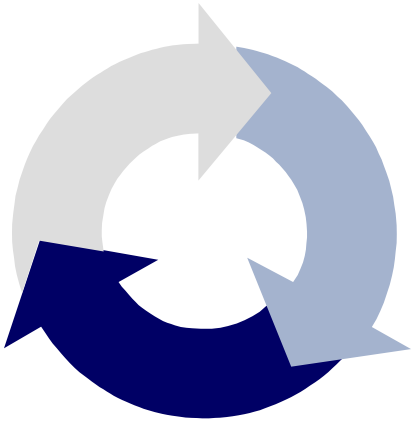
Hallittu hyökkäys

1. Verkkotopologian selvittäminen
2. Haavoittuvan kohdan hakeminen
3. Tunkeutuminen järjestelmään
4. Järjestelmän haltuunotto
5. Levittäytyminen, jälkien peittäminen
6. Toteutetaan hyökkäyksen päämäärä
7. Järjestelmän käyttäminen jatkohyökkäyksiin
8. Julkistus keskusteluryhmissä, iltapäivälehdissä,…

Missä vaiheessa hyökkäys huomataan?

Tietoturva-askeleet

1. *Halu* tehdä turvallinen järjestelmä
2. Järjestelmän *suunnittelu* turvalliseksi
3. Turvaratkaisujen *käyttöönotto*
4. Turvallisuuden *tarkastaminen*
5. Järjestelmän **monitorointi**
6. Rikkomuksiin ja ongelmiin *reagointi*



Miten monitoroida?

- Haavoittuvuustestaus **[nmap, Nessus, Whisker, SARA, ISS, Qualys]**
- Lokien tarkkailu **[Swatch, LogSentry, NTLast]**
- Eheystarkistukset **[Tripwire, Intact, Aide]**
- Tietoturvatiedon hallintajärjestelmät (SIM) **[e-Sentinel, netForensics, e-Audit]**
- Hyökkäysten havainnointijärjestelmät (IDS)
  - Työasemassa **[ZoneAlarm, Tiny Personal Firewall]**
  - Palvelimessa – järjestelmä (HIDS) **[NFR, RealSecure, SELM]**
  - Palvelimessa – verkkoliikenne (NNIDS) **[NFR, RealSecure]**
  - Verkossa (NIDS) **[Snort, Shadow, Secure IDS, RealSecure]**
  - Sovelluksessa
- Ansat (honeypots, honeytokens) **[honeyd, Specter,ManTrap]**
- Hyökkäyksen estojärjestelmä (IPS) **[TopLayer, Hogwash, AppShield, Kavado]**
- Ulkoistettu valvontapalvelu (MSS) **[Symantec]**
- Ulkoistettu monitorointi (MSM) **[Counterpane, Defcom]**

Hälytykset perustuvat

- Kiellettyihin tapahtumiin
- Sormenjälkiin
- Toistuviin virhetilanteisiin
- Poikkeaviin/epänormaaleihin tapahtumiin
  - käyttöprofiilit
  - tilastot
  - protokollat

IPS vs. IDS

- IPS pyrkii estämään hyökkäyksen, IDS hälyttää
- IPS yleensä tarkemmin kohdistettu: laite, protokolla, sovellus
- IPS-tarkkuuden täytyy lähennellä 100% - laillista liikennettä ei saa estää
- IPS voi mahdollistaa DoS-hyökkäyksen
- IPS ja IDS eivät ole toisiaan poissulkevia

IDS-projekti

1. Tee selväksi tavoiteltavat hyödyt
2. Tee vaatimusmäärittely
3. Suunnittele
   - seurantapisteet ja käytettävät tekniikat
   - arkkitehtuuri
   - tarvittavat verkkomuutokset, liitynnät verkonvalvontaan
   - hallinta ja valvonta, vastuuhenkilöt
   - raportointi, hälytykset
   - hälytyksiin reagointi, sisäinen CERT/CIRT toiminta
4. Tuotevalinta
5. Koulutus
6. Käyttöönotto
7. Tiedotus
8. Hälytysten viritys 3-6 kk

Haasteita IDS-projektille

- ”Piilokustannukset”: koulutus, prosessit, valvonta,…
- Tuotteiden kirjo, erilaiset tekniikat, monimutkaisuus, hype
- Tuotteet ovat toisaalta kehittyneitä (IDES ~1983, NFR ~1996, Snort ~1998), mutta toisaalta kypsymättömiä
- Syvällisen verkko-osaamisen tarve
- Hyökkäysten erottaminen kohinasta
- Tiedonlouhinta, raportointi, analysointi
- Nopeat/kuormitetut verkot
- Kytkimet
- Salattu verkkoliikenne
- Muutosten hallinta
- Tietosuojasta huolehtiminen
- Hälytyksestä työ vasta alkaa…

Edut yritykselle 1/2

- Tietoturvarikkomusten aikainen huomaaminen ja vaikutusten minimointi
- Todellisten vahinkojen kartoittaminen
- Historiatietojen ja todistusaineiston kerääminen
- Suojaavien tietoturvaratkaisujen tehokkuuden parantaminen
- Muiden tietoturvaratkaisujen toimivuuden todentaminen
- Tietoturvaohjeistuksen ja –käytäntöjen noudattamisen seuranta
- Yritykseen kohdistuvien uhkien monitorointi, mittaaminen ja trendiseuranta

Edut yritykselle 2/2

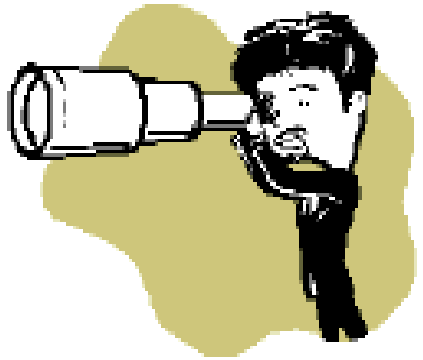
- Asiakkaiden ja kumppaneiden vakuuttaminen yrityksen vakavasta suhtautumisesta tietoturvaan
- Asiakas- ja kumppanisovellusten riskitason pienentäminen
- Yrityksestä ulospäin suuntautuvien rikkomusten huomaaminen
- Lakien noudattamisen varmistaminen
- Lisäpuolustuslinja

Oma vai ulkoistettu IDS?

	Oma	Ulkoistettu
Työmäärä	-	+
Osaamistarve	-	+
Kustannukset	-	+
Joustavuus	+	-
Valvonta, tuki	-	+
Käyttöönoton nopeus	-	+
Kontrolli	+	-
Luottamus	+	-
Integrointi	+	-

Kuumia aiheita

- IPS
- Palvelu-/protokollakohtainen IDS/IPS
- Honeypots
- Poikkeamien tunnistaminen (anomaly detection)
- Tiedonlouhinta
- Gigabit-tuki
- IDS kytkimessä
- Snort tietoturva-aukot



AtBusiness IDS – tekniikka

- PC-laitteet
  - tehokas CPU ja verkkokortti
  - paljon levyä
  - riittävästi muistia
- Open Source
  - IDS-ohjelmisto – *Snort*
  - Tietokanta - *MySQL*
  - Kovennettu Linux – *Bastille-Linux, Tripwire*
  - Sääntöhallinta – *IDS Policy Manager, OpenSSH*
  - Seuranta/analysointi – *ACID*, *PureSecure* ($)
  - Web-palvelin – *Apache*

AtBusiness IDS – miksi Snort

- Open Source
  - paljon apuohjelmia, innovaatiot
- Laaja kehittäjäjoukko
  - freshmeat.net: 51 Snort-projektia
- Laajasti käytössä
- Standardi PC-ympäristö
  - helppo päivittää ja lisätä toiminnallisuutta
- Pärjää täysin kaupallisille tuotteille
  - AtBusiness oma evaluointi (Snort vs. NFR vs. RealSecure)
  - NSS Network Testing Laboratories IDS Group test
  - Gartner
- Myös muiden valinta
  - SiliconDefense, PureSecure, PacketAlarm, NitroGuard

Snort vs. ”kaupallinen IDS”

	Snort	”kaupallinen IDS”
Hinta	++	--
Tuki	+	+
Suorituskyky	+	++
Päivitykset	++	+
Ominaisuudet	+	++
Monipuolisuus	+	++
Innovatiivisuus	++	+
Ylläpito	+/-	+
Jatkuvuus	-	+
Käyttöliittymä	+	+
Raportit	-	+
Joustavuus/muokattavuus	++	+

Hyvän tuotteen 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 sormenjälkitietokanta
- Integroitavissa verkonvalvontaan
- Tukeutuu standardeihin
- Yhteensopivuus muiden tuotteiden kanssa