SURFnet IDS honeypots

Jonel Spellen en Mark Meijerink

Begeleider: Rogier Spoor

Amsterdam 8-2-2006

Agenda

- Introductie
- Project omschrijving
- Aanpak
- Resultaten
- Conclusie
- Toekomstig werk
- Ervaringen
- Vragen

Introductie

- Honeypots
- SURFnet IDS service
- Aanleiding voor project
- Gerelateerd werk

Project omschrijving

- Onderzoeksdoelen
  - Analyseren van Nepenthes in het vangen van malware
  - Zoeken van interessante tools voor de IDS service
  - Protectie methoden onderzoek tegen TCP fingerprinting

Aanpak

- Literatuur onderzoek
- Analyseren van Nepenthes
- Opzoeken en analyseren van alternatieve honeypots
- Informatieve gesprekken
- Verslag schrijven

Resultaten

- Onderzoeksdoelen
  - Tools buiten beschouwing gebleven
  - Geen onderzoek naar TCP fingerprinting
- Onderzoek Nepenthes honeypot
- Honeypot selectie
  - Mwcollect
  - Honeyd
  - Honeynet
  - Argos

Resultaten – Nepenthes / Mwcollect

- Markus Koetter / Georg Wicherski
- Low-interaction honeypot
- Emulate vulnerabilities
- Downloads malware
- Modular

Resultaten - Honeyd

- Niels Pavos, Univeristy of Michigan
- Arpd
- Virtuele hosts en netwerk emulation
- Subsystem emulatie op TCP/IP stack niveau

Resultaten - Honeynet

- The Honeynet Project
- Honeywall CDROM
- Data Control, Data Capture, Data Analysis

Resultaten - Argos

- Herbert Bos, Georgios Portokalidis, Asia Slowinska
- Vrije Universiteit van Amsterdam
- Onderdeel van Noah project
- Emulatie van meerdere platformen
- Detecteren van flow control en code uitvoering
- Detecteren van aanvallen op bekende en nieuwe exploits

Analyse

- Functionaliteit
- Vulnerability emulatie
- Ondersteunende community
- Ontwikkeling activiteit

Conclusie

- Nepenthes blijven gebruiken als honeypot
- Argos is een goede aanvulling voor de IDS service

Toekomstig werk

- Implementatie van Argos
  - subsystem van honeyd
  - twee openVPN verbindingen vanaf sensor

- Onderzoek naar meerdere honeypots als end-point in de IDS infrastructuur

Ervaringen

- Kennis van honeypots
- Gesprekken vs. literatuuronderzoek
- Tijdindeling
- Prioriteitbepaling

Vragen

?