Unix Security Technologies: Firewalls and Honeypots

Peter Markowsky

<peterm@ccs.neu.edu>

Agenda

- Firewalls
  - Tools:
    - fwbuilder
  - OpenBSD’s PF
  - Bridging Firewalls
- Honeypots
  - definition
  - Honeypot Movie
  - Honeynets
  - Tools
    - netcat
    - Honeyd

What is a Firewall?

- ✓ Hard to define
  - ✓ Many appliances are called a firewall
  - ✓ Many are application proxys
- ✓ A Firewall is a device which makes a filtering decision based on network traffic that it

Types of Firewalls

- ✓ Application Firewalls
  - ✓ Understand application protocols
  - ✓ Closer to application proxys
  - ✓ Zorp
- ✓ Packet Filtering
  - ✓ Traditional firewall
  - ✓ Layer 3 and 4
  - ✓ Port and IP based
  - ✓ OpenBSD’s PF

OpenBSDs PF

- ✓ In kernel packet filter
- ✓ Layer 3/4

Taming Babel

- ✓ FWBuilder is a GUI tool to build firewall rules
- ✓ http://www.fwbuilder.org/
- ✓ It stores it's rules in to xml
  - ✓ That xml gets compiled down the specific rules for each firewall
- ✓ DEMO

Bridging Firewalls

- ✓ Smart bridges
- ✓ Filtering occurs at layers 2,3,4
- ✓ Invisible / hard to detect

Honeypots

- ✓ A security resource who's value lies in being attacked or exploited
- ✓ The Cu ckoo's Egg by Cliff Stoll
  - ✓ Tracking hackers hired by the KGB
- ✓ Evening with Berferd
  - ✓ Whitepaper on tracking a hacker through AT&T

Advantages

- ✓ Only produce data of high value
  - ✓ No one should be “talking” with them
- ✓ Not dependent upon signatures
  - ✓ Can be used to discover previously unknown attacks

High Value (data)

- ✓ Collect smaller amounts of data
  - ✓ A few MB a day
- ✓ Dramatically Reduce
  - ✓ False Positives
  - ✓ False Negatives

Low & High Interaction

- ✓ Low Interaction: simulated hosts and services
- ✓ High Interaction: real services and hosts

Roll Your Own

- ✓ Make a port listener
  - ✓ Use netcat
    - ✓ Network swiss army knife
    - ✓ Prompt$ nc -l -p [port number] > output
    - ✓ I’ve called this fishing in the past

Honeyd

- ✓ A daemon to create virtual hosts on a netwrok
- ✓ Allows a single host to be multiple hosts
- ✓ http://www.honeyd.org/

Building Emulated Services

- ✓ Many services are already built
  - ✓ http://www.honeyd.org/contrib.php

Example Honeyd

- Demo
  - Prompt$ honeyd -p /etc/honeypot/nmap.prints -f /etc/honeypot/honeyd.conf

Honeynets

- ✓ A network high interaction h oneypots
  - ✓ Real computers
  - ✓ Honeynet Project
    - ✓ SoTM challenges

Risks Associated With

- ✓Legal Repercussion
- ✓Using as a stepping stone

Elements of a Honeynet

- ✓ Data Control
  - ✓ Contain intruders activities
- ✓ Data Capture
  - ✓ Record attacker's activities
- ✓ Data Collection/Aggregation
  - ✓ Only applies to distrubuted honeynets

Gen I

- ✓ Layer 3 access control
  - ✓ Limit connections outbound
- ✓ Data Capture
  - ✓ Syslog
  - ✓ network

Gen II

- ✓ Easier to deploy
- ✓ Data control
  - ✓ Honeywall Gateway
    - ✓ Intrusion Prevention Systems
    - ✓ Layer 2
    - ✓ Disables attack
- ✓ Data Capture
    - ✓ Capture at kernel level (sebek)

Virtual Honeypots

- ✓ Use virtualization software to simulate machines
- ✓ Can be combined with

Resources