Technical seminar
on
HoneyPots
BY
YASHWANTH MOULI
(07821A0232)
Security Problems in Internet

- The Internet security is hard
  - New attacks every day
  - Our computers are static targets
Problems

Why?
Solution

What should we do?

- The more you know about your enemy, the better you can protect yourself.

Other way is

Creating VIRTUAL PORTS or FAKE TARGETS.
Solutions

Real

Fake

A Detected....
Honeypots?

- Fake Target
- Collect Information
- Honeypots are programs that can distract possible attackers from attacking a computer system.
HONEYPOTS

- A HONEYPOT is a resource (computer, program, web page, piece of information) whose value lies in being attacked.
Physical V.S. Virtual Honeypots

- Two types
  - Physical
    - Real machines
    - Own IP Addresses
    - Often high-interactive
  - Virtual
    - Simulated by other machines that:
      - Respond to the traffic sent to the honeypots
      - May simulate a lot of (different) virtual honeypots at the same time
How do HPs work?

Prevent
Detect
Response
Monitor

No connection

Attacker

Gateway

Honeypot A

Attack Data
Location of Honeypots

- In front of the firewall
- Demilitarized Zone
- Behind the firewall (Intranet)
Capturing Information

- **Host based:**
  - Keystrokes
  - Syslog

- **Network based:**
  - Firewall
  - Sniffer
  - IP name resolver
Overview of Complex Honeypots
Terms are related to HONEYPOT

- Honeyd
- HONEYNET
- HONEYFARM
HONEYD

- A virtual **honeypot application**, which allows us to **create** thousands of IP addresses with **virtual machines** and corresponding network **services**.
A honeynet is a network of high interaction honeypots that simulates a production network and configured such that all activity is monitored, recorded and in a degree, discretely regulated.
HONEYFARM

- A honeyfarm is a centralized collection of honeypots and analysis tools.
THANK YOU
ANY QUERIES???