Honey Pot

Be afraid
Be very afraid

Presented By
Shubha Joshi
M.Tech(CS)
Problems with internet

Why?
Problems

• The Internet security is hard
  - New attacks every day
  - Our computers are static targets
• What should we do?
  • The more you know about your enemy, the better you can protect yourself
  • Fake target?
Contents

• What are Honey pots?
• Etymology
• History
• Classification
• How do Honey pot work?
• Advantages
• Disadvantages
• Honeyd
• Honey Nets
• Google Hack Honey pot
• Conclusion
A honeypot is an information system resource whose value lies in unauthorized or illicit use of that resource.

- Has no production value; anything going to/from a honeypot is likely a probe, attack or compromise
- Used for monitoring, detecting and analyzing attacks
- Does not solve a specific problem. Instead, they are a highly flexible tool with different applications to security.
• A trap set to detect and deflect attempts at unauthorized use of information systems.

• It consist of a computer, data or a network site that appears to be part of a network but which is actually isolated & protected.

• Whatever they capture is supposed to be malicious & unauthorized.
Etymology

• The term refer to the English children’s character “Winnie-the-Pooh”

• During the cold war it was a technique which inspired spy fiction.

• It is a reflection of the sarcastic term for outhouses and other methods of collecting human waste in places that lack indoor plumbing.
History of Honeypots

- **1990/1991** The Cuckoo’s Egg (Clifford Stoll) and Evening with Berferd (Bell Cheswick)
- **1997** - Deception Toolkit
  It is one of the original & landmark honey pots. It is generally a collection of PERL scripts designed for UNIX system
- **1998** - CyberCop Sting
  It is a component of the CyberCop intrusion protection software family which runs on NT. It is referred as “decoy” server as it can emulate a big network containing several different types of network devices.
- **1998** - NetFacade (and Snort)
  It has same functionality as Cybercop but in a much larger space.
• 1998 – Back Officer Friendly
  It runs in Windows and was free thus giving more people access to Honey pot Technology.
• 1999 - Formation of the Honey net Project
  A group of people led by “Lance Spitzner”, form this project which is dedicated to researching the black hat community and to share their work to others.
• 2003 – Some Honey pot Tools
  Snort-Inline 12: used not only to detect but also to block & disable attack.
  Sebek: used to capture hacker activities by logging their keystrokes.
  Virtual Honey nets: used to deploy multiple honey nets with just one computer.
Classification

- By level of interaction
  - High
  - Low
- By Implementation
  - Virtual
  - Physical
- By purpose
  - Production
  - Research
Level of Interaction

Interaction defines the level of activity a honey pot allows an attacker

• Low Interaction
  • Simulates some aspects of the system
  • Easy to deploy, minimal risk
  • Limited Information
  • Honeyd

• High Interaction
  • Simulates all aspects of the OS: real systems
  • Can be compromised completely, higher risk
  • More Information
  • Honey-net
Level of Interaction

Low

High

Fake Daemon

Disk

Other local resource

Operating system
Difference b/w Low & High Interaction

**Low-interaction**
Solution emulates operating systems and services.
- Easy to install and deploy. Usually requires simply installing and configuring software on a computer.
- Minimal risk, as the emulated services control what attackers can and cannot do.
- Captures limited amounts of information, mainly transactional data and some limited interaction.

**High-interaction**
No emulation, real operating systems and services are provided.
- Can capture far more information, including new tools, communications, or attacker keystrokes.
- Can be complex to install or deploy (commercial versions tend to be much simpler).
- Increased risk, as attackers are provided real operating systems to interact with.
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
Production Honey Pots: Protect the systems

Production Honey pots are systems that are used in organization to mitigate risk. They help in securing systems & network.

The security has been divided into three categories:

• **Prevention**
  • Keeping the bad guys out
  • Not effective prevention mechanisms.
  • Deception, Deterence, Decoys do NOT work against automated attacks: worms, auto-rooters.
Continue.....

• Detection
  • Detecting the attacker when he breaks in.
  • Great work

• Response
  • Can easily be pulled offline
  • Little to no data pollution
Research HPs: gathering information

They capture extensive information and are used primarily by research, military, government organization. They can be used as:

• To capture automated threats, such as worms or auto-rooters
• To Discover new Tools and Tactics
• As an early warning mechanism, predicting when future attacks will happen
• To better understand attackers' motives and organization
• Develop Analysis and Forensic Skills
• To capture unknown tools or techniques
How do HPs work?

Prevent
Detect
Response
Monitor

No connection
Advantages

- Small data sets of high value
- New tools and tactics
- Minimal resources
- Information
- Simplicity
Disadvantages

- **Limited view:** They can only track and capture activity that directly interacts with them.
- **Risk:** They have the risk of being taken over by the bad guy and being used to harm other systems.
Honeyd

- A virtual honey pot application, which allows us to create thousands of IP addresses with virtual machines and corresponding network services.
- It is open source software released under GNU General Public License.
- It is able to simulate big network on a single host.
- It provide simple functionality.
Working of Honeyd

Honeyd monitors unused IP space 1. When an attacker 2 probes an unused IP, Honeyd detects the probe, takes over that IP via ARP spoofing, then creates a virtual honeypot 3 for the attacker to interact with (Honeyd can create multiple virtual honeypots to fool attackers on all unused addresses). The attacker is fooled into thinking he is interacting with a successful hacked system 4. In addition, Honeyd automatically updates its list of unused IPs as systems are added or removed from the network.
Observing hackers

Honey
net
What is a Honeynet

A Honey net are prime example of High-Interaction honey pots. It is basically an architecture, an entire network of computers designed to be attacked.

- It is an architecture, not a product or software.
- Once compromised, data is collected to learn the tools, tactics, and motives of the blackhat community.
- Populate with real systems.
- High-interaction honey pot designed to:
  - capture in-depth information
  - learn who would like to use your system without your permission
How it works

• A highly controlled network where every packet entering or leaving is monitored, captured, and analyzed.

• Any traffic entering or leaving the Honeynet is suspect by nature.
Honey-net Architecture

- The key to the honey net architecture is “Honey wall”. This is a gateway device that separates your honey pots from the rest of the world.
- Any traffic going to or from the honey pots must go through the honey wall.
- This gateway is traditionally a layer 2 bridging device, meaning the device should be invisible to anyone interacting with the honey pots.
There are several key requirements that a honey wall must implement:

- **Data Control**: defines how activity is contained with the honey net without an attacker knowing it. Its purpose is to minimize risk.
- **Data Capture**: It is capturing all of the attacker's activity without the attacker knowing it.
- **Data Analysis**: It is the ability to analyze this data.
- **Data Collection**: It is the ability to collect data from multiple honey nets to a single source.

Of all these requirements, Data Control is the more important. Data Control always takes priority as its role is to mitigate risk.
Honey net Advantages

- High Data Value
  - Small Data
- Low Resource Cost
  - Weak or Retired system
- Simple Concept, Flexible Implementation
- Return on Investment
  - Proof of Effectiveness
- Catch new attacks
Risk & Issues

• In reference to risk, there are four general areas we will cover;
  ❖ *Harm*: When a honey net is used to attack or harm other, non-honey net systems.
  ❖ *Detection*: Once the true identity of a honey net has been identified, its value is dramatically reduced.
  ❖ *Disabling*: Attackers may want to not only detect a honey net's identity, but disable its Data Control or Data Capture capabilities.
  ❖ *Violation*: Attackers may attempt criminal activity from your compromised honey net without actually attacking anyone outside your honey net.
What’s The Difference b/w honeypot & Honeynet

- Honeypots use known vulnerabilities to attract attackers.
  - Configure a single system with special software or system emulations
  - Want to find out actively who is attacking the system

- Honeynets are networks open to attack
  - Often use default installations of system software
  - Capture extensive amount of information
  - Basically a collection of Honey pots
Google Hack Honeypot

- Google Hack Honey pot emulates a vulnerable web application by allowing itself to be indexed by search engines.
- It's hidden from casual page viewers, but is found through the use of a crawler or search engine.
- The transparent link will reduce false positives.
Conclusion

- Honeypots are not a solution, they are a flexible tool with different applications to security.
- Primary value in detection and information gathering.
- Just the beginning for honeypots.
Thanks
Queries??