Honey pot

- Salem

WTW ?

- What exactly happens on the end of internet connection ?
- Open Source tools to setup your own honeypot & IDS and how to tie them together ?

- What I've done ?!

Internet Connection

- Imaginary world

Internet Connection

- Real world

Honey , WTW ?

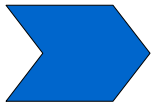
- Used to convince an attacker a computer is a high-value , badly secured device
  - while in reality it is a device used to monitor the attacker actions and tactics.

Types of honeypot ?

- High interaction
  - Physical or Virtual System
  - Provides attacker with a real computer
  - Real computer = real threat = more problems
- Low interaction
  - Nephentes , Kippo , honeyd
  - Provides attacker with a movie set computer
  - Fake computer = less threats = less problems

High interaction

- Real computer
  - Physical or virtual computer with actual vulnerabilities
  - Vmware , Xen , mode Linux , Beater Box
- Real Problems
  - Attacker can and will use your honeypot to attack other systems
  - IDS (Snort inline), Helps ?! you need to keep it on top



Lots of Risks , But Lots of rewards

Low interaction

- Fake Computer
  - Spoofed device
  - Physical or virtual device that spoofs vulnerabilities
- Less of an attack profile
  - Not actually exposing a real computer
- Not as realistic as “ high interaction “ but will save you from many headaches

How high interaction works ?

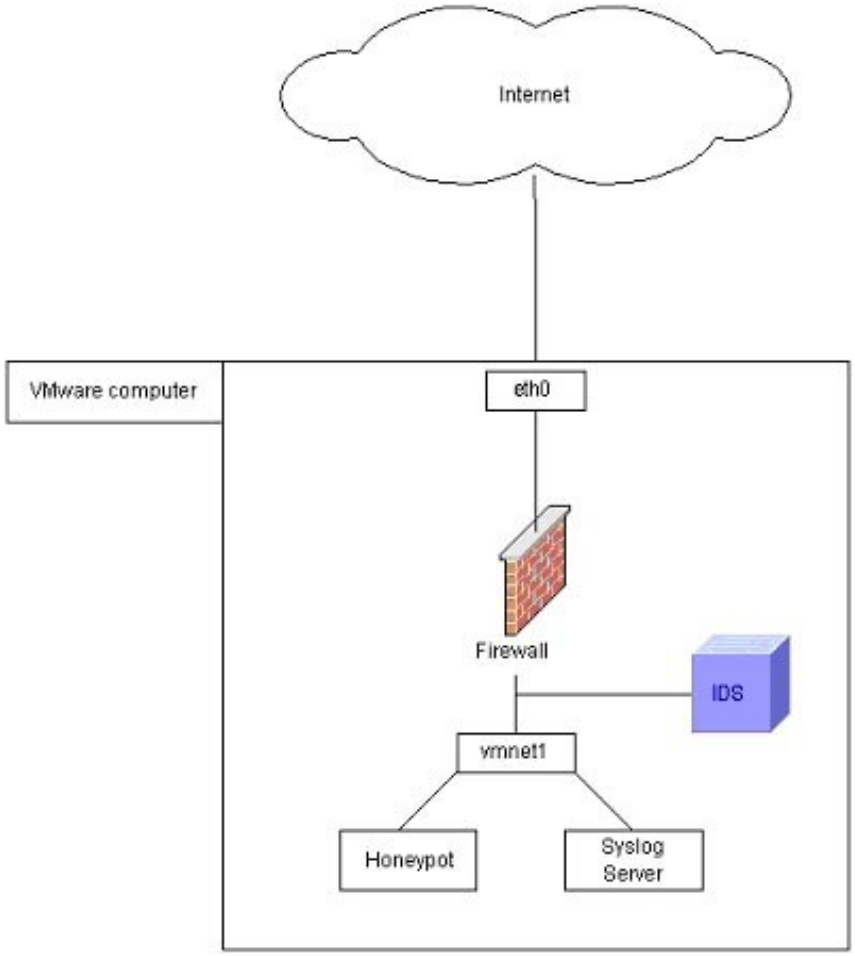
How High interaction works ?

- To stop attack:

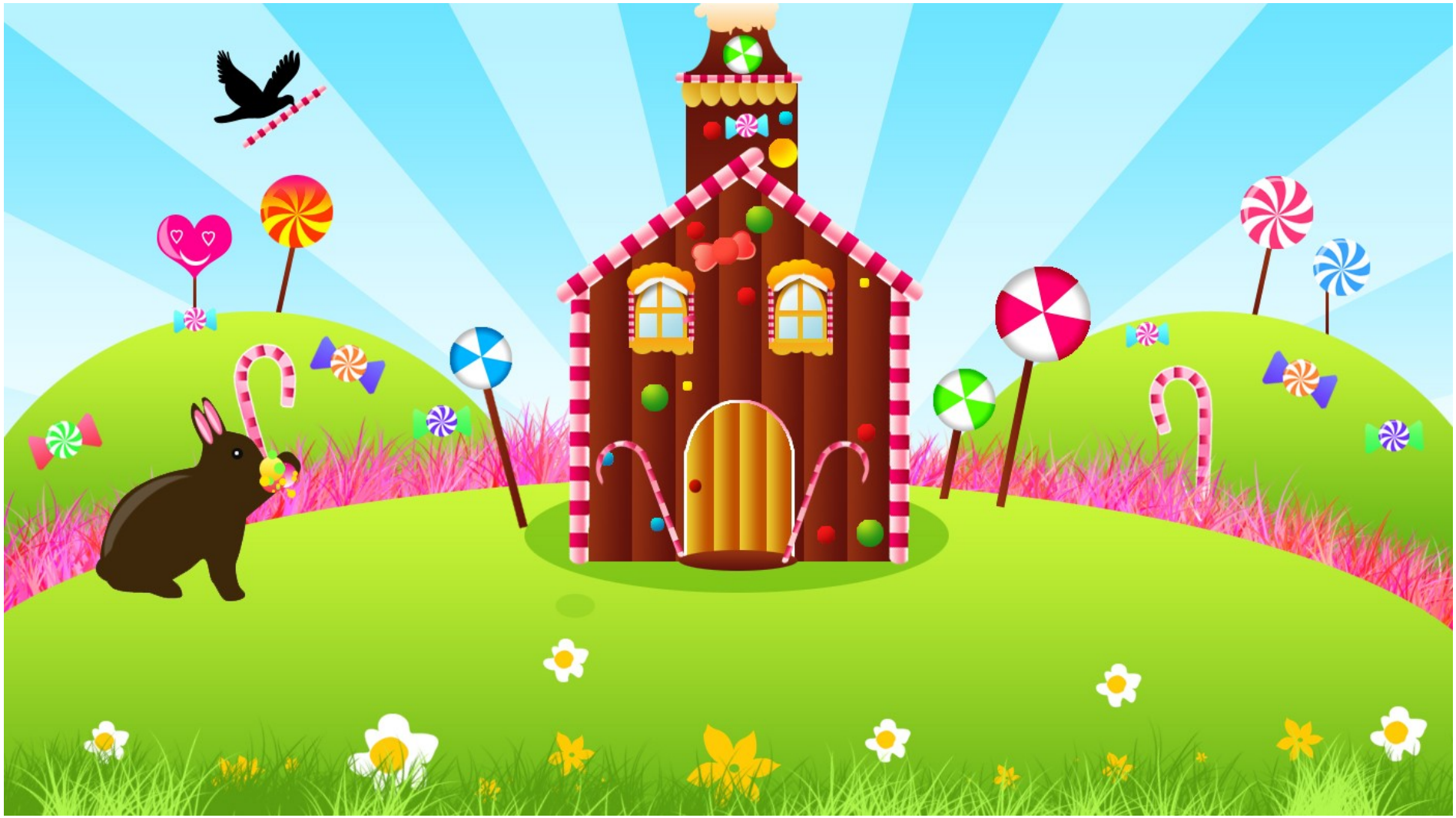
  -Monitoring a high interact honeypot 24/7

  -IDS (Snort) to drop malicious packets

  ~ (Not 100% effective)



Low interaction



Low interaction taking Exp()

- Nephentes
  - Emulate fake vulnerabilities on a physical computer and collects exploits

- Honeyd
  - Emulates fake computers on your network in which script canned responses

- HoneyTrap
  - Dynamically creates a server on every port a client requests to connect to and captures data

Nephentes

Nephentes

- Sets up server on a physical computer
- Emulates vulnerabilities
- Automatically collects malware

WTW ?!

- **Pros :**

  -Can be used on any existing server

  -Can catch a number of windows exploits

- **Cons :**

  -Difficult to setup

  -It's knowledge of exploits is limited

  -Logging is a bear

  -Since it's a program listening on a port , it can be compromised

Honey Trap

- Nephentes Diet !
- Utility to automatically collect exploits
- Open server on any port a connection is made to
- Can be installed on an existing machine
  - (Homeless man's honeypot)

WTW ?

- **Pros :**

  -Dead simple

- **Cons :**

  -Limited interactivity

Honeyd

- Emulates hosts on a network that runs programs or scripts specified in the config file
- Takes up spare Ips
- Amazing amount of IP trickery
- Emulate an entire network

WTW ?

- **Pros :**

  -Can emulate numerous computers , links and devices

  -These ghosts can run almost anything

  -Somewhat harder to compromise

- **Cons :**

  -Requires a separate unused IP for each host

  -Good for monitoring , but difficult to use against advanced attacks

Monitoring

Tools

- Snort
- Tcpdump
- Surf Cert

- WTV ?!

Response

Response

- You got Attacked
  - Do nothing
  - Attack back
  - Take down the server

Do nothing !

Really ?

- **Pros :**

  -Easiest thing to do

  -Saves time, effort and inevitable frustration

- **Cons**

  -Doesn't accomplish anything

Attack Back

- **Pros :**

  -There are none ! You are part of problem

- **Cons**

  -illegal ?

  -Attacking the attacker?

  -Is he the real attacker ?

Take down

- Effective ?!
- Withdrawal ?!