Ghetto IDS and Honeypots for the home user

I've got a bunch of virtual windows machines networked together, hooked up to an incoming pipe from the net. They execute email attachments, share files, and have no security patches. Between them, they have practically every virus.

There are mail trojans, Warhol worms, and all sorts of exotic polymorphics. A monitoring system adds and wipes machines at random. The display shows the viruses as they move through the network, growing and struggling.

You know, normal people just have aquariums.

Pretty, isn't it?

What is it?

Good morning, Blaster. Are you and W32.Welchia getting along?

Who's a good virus? You are! Yes, you are!

Comic courtesy http://www.xkcd.com

Black Ratchet - The Last HOPE - July 19th, 2008
What are we going to talk about?

- What exactly happens on the end of your Internet connection
- Open Source tools to set up your own Honeypot and IDS setup and how to tie them together
- What you will likely see, what it means, and how to respond.
Who am I?

- Just another Phone Phreak from Boston
- Talked at HOPE #6, DEFCON, and other conferences
- Been using these tools in one form or another since 2002 or so...
- GCIA, so obviously these letters make me smarter than you
- Really nice guy who will talk your ear off about these things if alcoholic beverages are donated
Why are you using PowerPoint?

- Because OpenOffice sucks
- I don’t feel like making you guys flying blind (again)
Your Internet Connection (Imagined)
Your Internet Connection (Reality)
Honeypots
What exactly is a honeypot?

- 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 attackers actions and tactics.
- “An evening with Berferd” Cheswick et. al.
Interaction: High vs. Low

- **High Interaction**
  - Physical or Virtualized System
  - Provides the attacker with a real computer
  - Real computer = Real threats = More problems

- **Low Interaction**
  - Nepenthes or honeyd
  - Provides an attacker with a “movie set” computer
  - “Fake” computer = Less threats = Less problems
High Interaction Honeypots

- Real Computer
  - Physical or Virtual Computer with actual vulnerabilities
  - VMware, Xen, User Mode Linux, Beater Box

- Real Problems
  - Attackers *can* and *will* use your honeypot to attack other systems
  - Snort Inline will protect you somewhat, but you need to keep on top of it

- Lots of risk, but lots of reward
Low Interaction Honeypots

- “Fake” Computer
  - Spoofed device
  - Physical or virtual device that spoofs vulnerabilities
- Less of an attack profile
  - Not actually exposing a real computer, therefore less of a threat of being compromised
- Not as realistic as “high interaction” but will save you many a headaches.
High Interaction Honeypots
How High Interaction Honeypots Work…
Setup

- Operating System
  - Linux
  - Windows

- Hardware
  - Nowadays, most attackers don’t know nor do they care
  - Bandwidth, an exception, sometimes
A word about virtualization

- Are you 100% sure that they won’t break out?
- Are you 100% sure they won’t notice?
- Are you willing to bet a server that contains information you consider “important”?
Stopping Attacks

- You need to be monitoring a high-interaction honeypot 24x7
    - Immediately!
      - No, really. NOW!

- Snort Inline
  - Snort based utility that uses iptable/ipfw to drop malicious packets.
  - Not 100% effective.
Low Interaction Honeypots
Low Interaction Honeypots

- **Nepenthes**
  - Emulates fake vulnerabilities on a physical computer and collects exploits.

- **honeyd**
  - Emulates fake computers on your network in which you can script canned responses.

- **Honeytrap**
  - Dynamically creates a server on every port a client requests to connect to and captures data.
Nepenthes

- Sets up server on a physical computer
- Emulates vulnerabilities
  - Both Windows and Linux
- Automatically collects malware
  - Capable of automatically submitting them to a central collection point
How Nepenthes Works

Act One

“Exploit”

“Oh Noes! You Got Me!”

“Hahaha Take my evil trojan!”

“Psyche! HA HA! Fooled You!”

Attacker

Nepenthes Server
How Nepenthes Works

Act Two

Attacker

Curses! I have been foiled!

Victory!

Nepenthes Server

Monitoring Console
Nepenthes

○ Pros
  • Can be used on any existing server
  • Can catch a number of windows exploits

○ Cons
  • Somewhat 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 get compromised
Honeytrap

- Utility to automatically collect exploits
- Opens a “server” on any port a connection is made to
  - Both Windows and Linux!
- Can be installed on an existing machine
  - Homeless Man’s Honeypot
How Honeytrap Works

![Diagram showing how Honeytrap works]

- Attacker
- "Exploit"
- "OM NOM NOM NOM NOM"
- Honeytrap Server
Honeytrap

- **Pros**
  - Dead Simple

- **Cons**
  - Limited Interactivity
Honeyd

- Developed by Niels Provos
- Emulates hosts on a network that run programs or scripts specified in the config file.
- Takes up spare IPs
- Amazing amount of IP trickery.
- Emulate an entire network!
How honeyd works
honeyd “services”

- Can forward ports back to services hosted somewhere else.
  - Dangerous, these services can get owned

- Scripts
  - Script Kiddie Annoyance Toolkit
  - Scripts also available on the honeyd website

- Tarpits
Honeyd

- **Pros**
  - Quite lightweight
  - 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
Snort – ‘Nuff Said

- Developed by Marty Roesch in 1998 as a “lightweight” IDS
- Gold Standard in OSS IDS systems
- Signature based
Monitoring Snort

- SGUIL
  - http://sguil.sourceforge.net/
- BASE (Basic Analysis and Security Engine)
  - http://base.secureideas.net/
- SnortSnarf
  - http://snort.org/dl/contrib/data_analysis/snortsnarf/
tcpdump

- The swiss army chainsaw of packet sniffing
- You can use it to monitor *everything*
  - Make sure your snaplen is right!
- Handy to piece together new attacks, or see stuff that snort missed
- pcap format allows you to use a lot of tools
  - ngrep, Wireshark, snort
WARNING!

By monitoring your network, you may record traffic that you don’t want recorded. Be sure that tcpdump/snort/whatever else you are using ONLY picks up the traffic you want!
Monitoring Honeyd/Nepenthes

- No good tools
- honeyd files are very arcane
- Nepenthes files are just flat out bad
Monitoring Both – Prelude

IDS

- NOT an IDS
  - More of a utility to correlate events and warnings
- Pretty web-based console
  - Prewikka, not required
- Good program, bad documentation
  - Really bad, I’m not kidding
- Open source, but not really
How Prelude Works

- **Prelude Manager**
  - **prelude-lml**
  - **honeyd logfile**
  - **nepentes logfile**
  - **snort**

Database

- **honeyd logfile**
- **nepentes logfile**

**Diagram:**
- Prelude Manager
- prelude-lml
- honeyd logfile
- nepentes logfile
- snort

**Images:**
- Prelude Manager interface
- Flowchart showing connections between components.
Response
Response

- You got attacked! Now what?
  - Do Nothing
  - Attack Back
  - Take down the server
Do Nothing

- **Pros:**
  - Easiest thing to do
  - Saves you time, effort, and inevitable frustration

- **Cons:**
  - Doesn’t actually accomplish anything
Attacking back

How About No......
Attacking back

- **Cons:**
  - Can we say “illegal” boys and girls?
  - Are you really attacking the attacker?
  - What are you actually accomplishing?

- **Pros:**
  - THERE ARE NONE! YOU’RE PART OF THE PROBLEM!
Takedowns

○ Pros:
  • Legal
  • Effective
  • Removes the immediate problem

○ Cons:
  • Whack A Mole
  • A lot of effort, often with little tangible results
Case Study: Web Takedown
Gentlemen, BEHOLD!

Gentlemen, BEHOLD!

“While I nodded, nearly napping, suddenly there came a tapping,
As of some one gently rapping, rapping at my chamber door.” – Edgar Allen Poe
Looking a bit closer…

<table>
<thead>
<tr>
<th>Create time</th>
<th>Detect time</th>
<th>Analyzer time</th>
</tr>
</thead>
<tbody>
<tr>
<td>2008-07-12 03:06:18.835677 -04:00</td>
<td><strong>2008-07-12 03:06:18.835015 -04:00</strong></td>
<td>2008-07-12 03:06:18.835852 -04:00</td>
</tr>
</tbody>
</table>

**MessageID**
19835372769662

**Text**
WEB-MISC Phorecast remote code execution attempt

<table>
<thead>
<tr>
<th>Ident</th>
<th>Severity</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1:1391</td>
<td>high</td>
<td>other</td>
<td>Web Application Attack</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Origin</th>
<th>Name</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>vendor-specific</td>
<td>1:1391</td>
<td>Snort Signature ID</td>
</tr>
<tr>
<td>cve</td>
<td>2001-1049</td>
<td></td>
</tr>
<tr>
<td>bugtraqid</td>
<td>3388</td>
<td></td>
</tr>
</tbody>
</table>

**Analyzer #1**

<table>
<thead>
<tr>
<th>Model</th>
<th>Name</th>
<th>Analyzerid</th>
<th>Version</th>
<th>Class</th>
<th>Manufacturer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Snort</td>
<td>snort</td>
<td>815997742186628</td>
<td>2.8.0</td>
<td>NIDS</td>
<td><a href="http://www.snort.org">http://www.snort.org</a></td>
</tr>
</tbody>
</table>
Looking a bit closer... (cont)
Another Word of Warning...

DANGER

KEEP AWAY
DO NOT TOUCH
ANYTHING
You can be badly hurt
or killed

TORONTO HYDRO 416-542-8000
Let’s grab it...
You've been living in a dream world, Neo...
What goodies do we have?
What’s behind door #1?
To whom it may concern:

Mayhemic Labs, an independent security research group, has found tools being used to attack systems stored on a website you host. You are receiving this message because you are listed in the contact section of your netblock's WHOIS information.

The URLs are as follows:

These tools are PHP files, despite the .gif extension. The website you host seems to have been compromised by a third party and is using it to probe systems.

If you are responsible for the security of the IP currently hosting the URL above, please take action to close it down as soon as possible, as this will break the attack.

YOUR PROMPT ATTENTION IS VITAL IN ORDER TO LIMIT NUMBER OF POSSIBLE VICTIMS.
A bit later…

“Quoth the Server, ‘404’” – Edgar Allen Poe… Sort Of..
Where to go from here

- Embedded system for friend/relative’s unused broadband systems?
- Centralized IDMEF correlation site in order to precipitate takedowns?
- Real time intelligence gathering system to know what is probing what?
Links

- honeyd
  - http://www.honeyd.org/
- Nepenthes
  - http://nepenthes.mwcollect.org/
- Honeytrap
  - http://honeytrap.mwcollect.org/
- Prelude
  - http://www.prelude-ids.com/
- SKAT
  - http://www.mayhemiclabs.com/
Shouts

- StankDawg, ntheory, and the rest of the DDP
- binrev.com forums
- Boston 2600
- Quine, Beaker, and everyone else from BeanSec
Questions?
Contact Information

- e-Mail – blackratchet@blackratchet.org
- WWW - http://www.blackratchet.org
- Twitter - @innismir