



# Network Intrusion Prevention Systems

“Do They have a Place on Your Network”

By Aaron Grothe, CISSP  
NEbraskaCERT



# Introduction

- Disclaimer
- What is a NIPS?
- What can a NIPS do for Me?
- Potential Issues with a NIPS
- How I got interested in NIPS
- NIPS vs NIDS
- Example NIPS
- How to get Started
- Contact Info

# Disclaimer

- The opinions represented here are mine and mine alone
- Implementing a NIPS poorly can do horrific damage to your network and/or career,

# What is a NIPS?

- A NIPS is a Network Intrusion Prevention System
- It is designed to allow/deny/modify traffic going through your system depending on the transformations you request
- Some people refer to it as an active IDS or an intelligent firewall
- Others call it an IDS with attitude :-)

# What can a NIPS do for me

- Buy you time!!! Allowing you to patch on your schedule
- Help you when you can't patch a service!!!
- E.g. Microsoft now releases their monthly patches on Tuesday, what do I do until Friday when I can reboot machines?
- Filter traffic based on criteria such as port, IP address (dest or source) and packet contents

# Potential Issues with a NIPS

- SPF – Single Point of Failure – NIPS are deployed inline
- If it slows down all traffic going through the NIPS is slowed down
- If compromised are a very effective way to monitor a network as a lot of traffic goes through them
- Can drop valid packets
- Most/all can't decode SSL traffic

# How I got Interested in NIPS

- Patching gone wild
- Compromised Production server was disabled when required patch was applied

# IPS vs IDS

- While an IDS can modify firewall rules or send TCP resets, the damage may already be done
- An IDS modifying a rule can give an attacker information about your system
- If an IDS can be tricked into modifying your firewall ruleset, it can be used to perform a wicked DOS attack

# Example NIPS

- HTTP\_Filter
- Hogwash
- Snort-inline
- Tipping Point

# HTTP\_Filter

- Homepage [http://glob.com.au/http\\_filter](http://glob.com.au/http_filter)
- “A while back, I had to set up iis's web access for e-mal (owa). Now, I think IIS has more holes than swiss cheese, so I wrote a simple http tunnel script in perl which allows you to filter requests.” - Byron James

# HTTP\_Filter

- How it Works
- Filter resides on Firewall or bridge machine
- Sees connection attempt
- Validates connection based on ruleset
- Opens connection from firewall to destination
- Monitors traffic going through for violations allowing valid traffic

# HTTP\_Filter

```
# Demo Ruleset
# deny a couple of basics
# .idq and .com requests are denied
all {
    deny regex m|\..idq$|
    deny regex m|\.com$|
}
```

•

# HTTP\_Filter

```
# Demo Ruleset (cont)
#only allow demo.mycompany.com access to /demo
and subdirs
demo.mycompany.com {
    host 192.168.0.252:80
    allow dir "demo"
    #deny everything else
    deny any
}
```

# HTTP\_Filter

## PROS:

- Written in PERL – Cross Platform
- Simple ruleset
- Free – artistic license

# HTTP\_Filter

## CONS:

- Written in PERL
- Only works with Web traffic
- Modified client access IP can complicate logs

# Hogwash

- Homepage <http://hogwash.sf.net>
- Originally based on its own packet capture engine, modified to use snort (0.1-0.4) and then went back to own engine again in 0.5
- Hogwash can do packet inspection and make decisions based upon content
- 0.4 version added a few new commands to Snort drop and mangle

# Hogwash

- Simple 0.4 Example Rule to attempt to get /etc/passwd on a system
- drop tcp \$EXTERNAL\_NET any-> \$HOME\_NET 80 (content: "/etc/passwd"; msg:"WEB: attempt to request /etc/passwd":)

# Hogwash

- Apache Chunk Vulnerability Rule  
alert tcp \$EXTERNAL\_NET any ->  
\$HTTP\_SERVERS 80 \  
(msg:"Apache Chunked Encoding Memory  
Corruption exploit attempt"; \  
flags:A+; content:"|C0 50 52 89 E1 50 51 52 50 B8  
3B 00 00 00 CD 80|"; \  
reference:bugtraq,5033; classtype:web-application-  
activity; rev:1;)  
• Change alert to drop and you have a fix!!!

# Hogwash

- Example 0.5 Rule

```
<rule>
```

```
ip dst(AllServers)
```

```
tcp nocase(/etc/passwd)
```

```
message=attempt to retrieve /etc/passwd
```

```
action=default
```

```
</rule>
```

# Hogwash

## PROS

- Can use almost all SNORT rules (0.4 version)
- Used by quite a few universities in honeynet projects
- Multi-platform (to Linux/BSD/Solaris Boxes)
- Snort rule compatability means you have a way of dealing with Zero day exploits

# Hogwash

## CONS

- New version 0.5 is not mature
- Old versions use potentially vulnerable version of Snort (Snort 1.7 for Hogwash version 0.4)
- Needs new maintainer
- Snort-inline is on the rise, Hogwash may/will die out over time

# Snort-Inline

- Homepage <http://snort-inline.sf.net>
- Similar to Hogwash
- Uses Linux's netfilter/iptables instead of pcap

# Snort-Inline

## PROS

- Is Snort 2.0 Compatible
- Can handle Zero day exploits if Snort rule is available
- Actively developed

# Snort-Inline

## CONS

- Only works with Linux
- Have to configure both iptables/netfilter and Snort
- Building can be a bit difficult
- Distributed as patches to Snort

# Tipping Point

- Homepage <http://www.tippingpoint.com>
- Commercial IPS vendor
- Has some cool features such as the ability to “fail open”
- Has gone through Common Criteria testing

# How to Get Started

Several Live Linux CDs exist that have hogwash on them

- KNOPPIX-STD <http://www.knoppix-std.org> contains Hogwash
- INSERT <http://www.insert.cd> has/had http\_filter on it

# How to Get Started

- Hogwash can be run in promiscuous mode so it doesn't need to be inline. Allows for testing rulesets
- Hogwash/Snort-inline can use alert to log packets instead of dropping them
- Incremental changes are key

## Other Fun things to do With NIPS

- Egress Filtering – Many honeynets use it in this mode to prevent people from using their machines to launch attacks
- Bait & Switch – If you see an IIS vulnerability redirect them to an Apache box or Vice Versa

# Future of NIPS

- Some Firewalls like Checkpoint's are offering more “Deep Packet Inspection” which can provide some of the features of a NIPS
- General Purpose DSPs or custom ASICs may speed up NIPS tremendously
- Snort-inline has a bright future ahead of it and will be available with tools that make it easier to use and configure



# Summary

- The Question asked is “Do Network Intrusion Prevention Systems” have a place on your network?  
I think the answer is a qualified yes



# Contact Me

- E-mail: [aaron.grothe@nebraskacert.org](mailto:aaron.grothe@nebraskacert.org) or [grothe@earthlink.net](mailto:grothe@earthlink.net)