

Research Update

James Kearney
SFS Presentation

April 4, 2005



1



4 April 2005

Research Update

- Bait and Switch routing
- Analysis of unknown executables
- Other



Bait and Switch

- Overview
 - Hardware/Software requirements
 - Network topology
 - Our configuration

Bait and Switch

- Iproute2 Issues
- Unknown Protocol Issues
- Outdatedness
- Rule-Building

Bait and Switch

- Iproute2
 - Choice over traditional ip_forward (and masquerading)
 - How to choose appropriate proctols

Bait and Switch

- Unknown Protocols
 - Not traditionally dealt with in Snort
 - Building new modules vs. implementing a catch-all rule

Bait and Switch

- Aged Software
 - Most recent update of codebase in 2003
 - The search for existing implementations



7

Bait and Switch

- Rule Building

Snort Rule

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-IIS view source via translate header"; flow:to_server,established; content: "Translate|3a| F"; nocase; reference:arachnids,305; reference:bugtraq,1578; classtype:web-application-activity; sid:1042; rev:6;)
```

Executable Analysis

- Attempts to automate process of new rule creation for Snort
- Built in feedback to improve the IDS/IPS in real-time (or at least close)
- Minimal progress to date

Unsorted Research

- Honeynet Reverse Challenge
- Integrating Bait and Switch with honeyd



References

- The Bait and Switch Project:
<http://baitnswitch.sourceforge.net>
- Snort: <http://www.snort.org>
- Work done by Scott and myself: /
home/toasty/documents/work/PST
- The HoneyNet Alliance:
<http://www.honeynet.org>