Welcome!

Our presentation will begin shortly…

Audio for today’s presentation will be streamed through your computer speakers.

All participants are in listen-only mode.
Two $5,000 scholarships to be awarded
Open to any student studying or using Snort in a university setting
Application deadline is 15, April 2009
Apply online at: http://www.snort.org/community/scholarship.html
How To Create Useful False Positive Reports
Yes, We Want Bug Reports

- Many people think that sending in a problem report irritates the VRT.
- Reality is that we *want* to get problem reports of any kind.
- …as long as they contain useful, actionable information.
False negatives are very high-priority
If you have a preprocessor alert problem, send it our way
We’ll take issues with SO rules as well
  • Especially if a rule you know works on platform X doesn’t on platform Y
Make sure to send the GID if it’s not a plaintext rule
Anyone testing 2.8.4 RC-1 – we want to hear from you about dcerpc2 preproc

Requests for new coverage
  • If you want us to write rules for something, be prepared to share PCAPs with us!
  • The more people who request a certain type of coverage, the more likely we provide it

Crashes in Snort are especially interesting – please send backtraces
Actual FP report I got in from the field once:

From: <obfuscated@xxx.com>
To: <research@sourcefire.com>
Subject: FP on SID 2183

I have lots of F +s with this rule. Can u help me plz?
URGENT!!!
Problems With Skimpy Reports

-we don’t write rules with known FPs
  -If one emerges, we’ll document it
  -That means we don’t know about what’s causing your FP, so we can’t fix it

-Misconfiguration can cause FPs
  -If you upgrade Snort and don’t upgrade your config, it can be a huge problem

-If we can’t reproduce the problem, we can’t fix the rule
Where Do I Start?

Before you report a FP, you need to be sure it really is a false positive

Review the rule documentation

- Is the attack directed at a valid target?
- Are there known FPs that match your alerts?
- Does the rule require any special configuration?

If relevant, run Snort in debug mode

- export SNORT_DEBUG="16384"
- See src/debug.h for other modes
If you see shellcode, it’s probably a true positive, and should be investigated.

Sometimes sample exploit code is in a legit web page / e-mail.

One potential FP on a really old vulnerability isn’t enough to worry about.
It’s time for a PCAP

- ASCII alert dumps are **NOT** useful!!!
- FP reports without PCAPs go to the bottom of our queue, since we can’t verify them

All PCAPs are treated as private unless you specify otherwise

- If you’re really concerned about privacy, use Snort’s “-O” option or otherwise clean the PCAP
- Just be sure to tell us you did so!
How To Make Useful PCAPs

📍 Standard tcpdump command line:
  - sudo tcpdump –n –i <interface> –s0 –w <filename.pcap> <bpf filter>

📍 Relevant for lots of reasons:
  - Resolving DNS in your PCAP is unnecessary and can generate garbage traffic
  - Default tcpdump snapshot length is 64 bytes – not useful for most exploits!
  - Good BPF filter takes 200-packet PCAP and focuses in on the 2-3 relevant packets
Bad checksums are often caused by recording from the machine sending the exploit; easily fixed:

- Written by Brian Caswell, head of the VRT infrastructure group, resident Perl god

Please record full sessions!

- Sometimes required to determine if it’s a FP
- The more relevant data we have, the better!
PCAPs are preferred, but on rare occasions they can’t be collected.

We’ll take unified log files in those cases:
- We’ve got a Wireshark plug-in to view unified files as PCAPs.
- Unified logging is fastest method anyway.
- See your snort.conf to enable it.
We Need Your Config

Version information – Snort and the SID
  • Your bug may have been fixed with a newer version of Snort or the rule itself

Full snort.conf
  • You might not know which config options are relevant – sometimes even we don’t
  • Allows us to easily reproduce your results
We Need Your Config (con’t)

- Command line options passed to Snort
  - Don’t assume that your config options are standard!

- Operating system version
  - Please include if Snort was built from source or came from a binary package
  - If you’ve used a non-standard PCAP library, that’s critical information!
Most important piece of all: why do you think this is a false positive?

- 99.99% of the time, the packet will match the rule
- We need to know why you think the alert should not exist in order to test your theory
- The more data you can supply about the environment, the more likely we can determine what’s going on
- Any recent upgrades/major config changes are crucial to highlight, as they can help pin down the problem
Where To Send Reports

- Snort-Sigs mailing list
- fp@sourcefire.com
- #snort on Freenode
- If you put in a FP report somewhere else, and you don’t get any reply at all, chances are the VRT hasn’t seen it
We’re Only Human

- We try to respond to all FP reports in a timely manner, but sometimes we get swamped
- Some FPs simply can’t be fixed
  - Sorry, we won’t compromise legitimate detection to get rid of your FP
  - Sometimes there’s just not enough information to fix the rule
New - Snort Training Classes

3-Day Rule Writing Best Practices Workshop
- Instructor led class with hands on labs
- Courseware and labs developed with the VRT
- Open to both Sourcefire and Snort users

Exploit Development for Snort Rule Writers
- Taught by the VRT
- Requires security expertise & low level programming experience
- Will provide an understanding of exploit development to help the user write better Snort Rules

For more information & course schedules visit: http://www.sourcefire.com/services/education
Questions?

Please submit questions via the Q&A interface in the lower-right corner of your screen.