OpenNSM, ContainNSM, and Docker

Jon Schipp

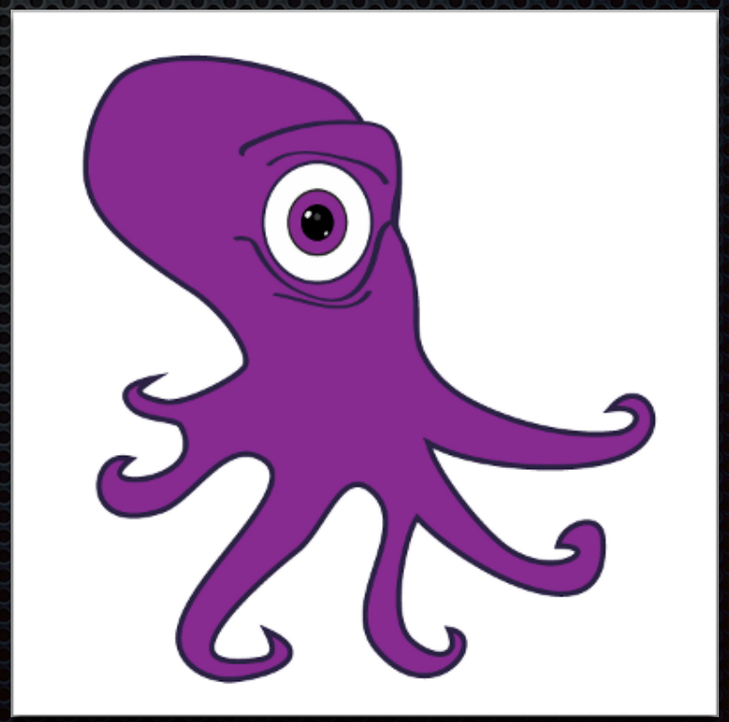
jonschipp@gmail.com

Project Contributions

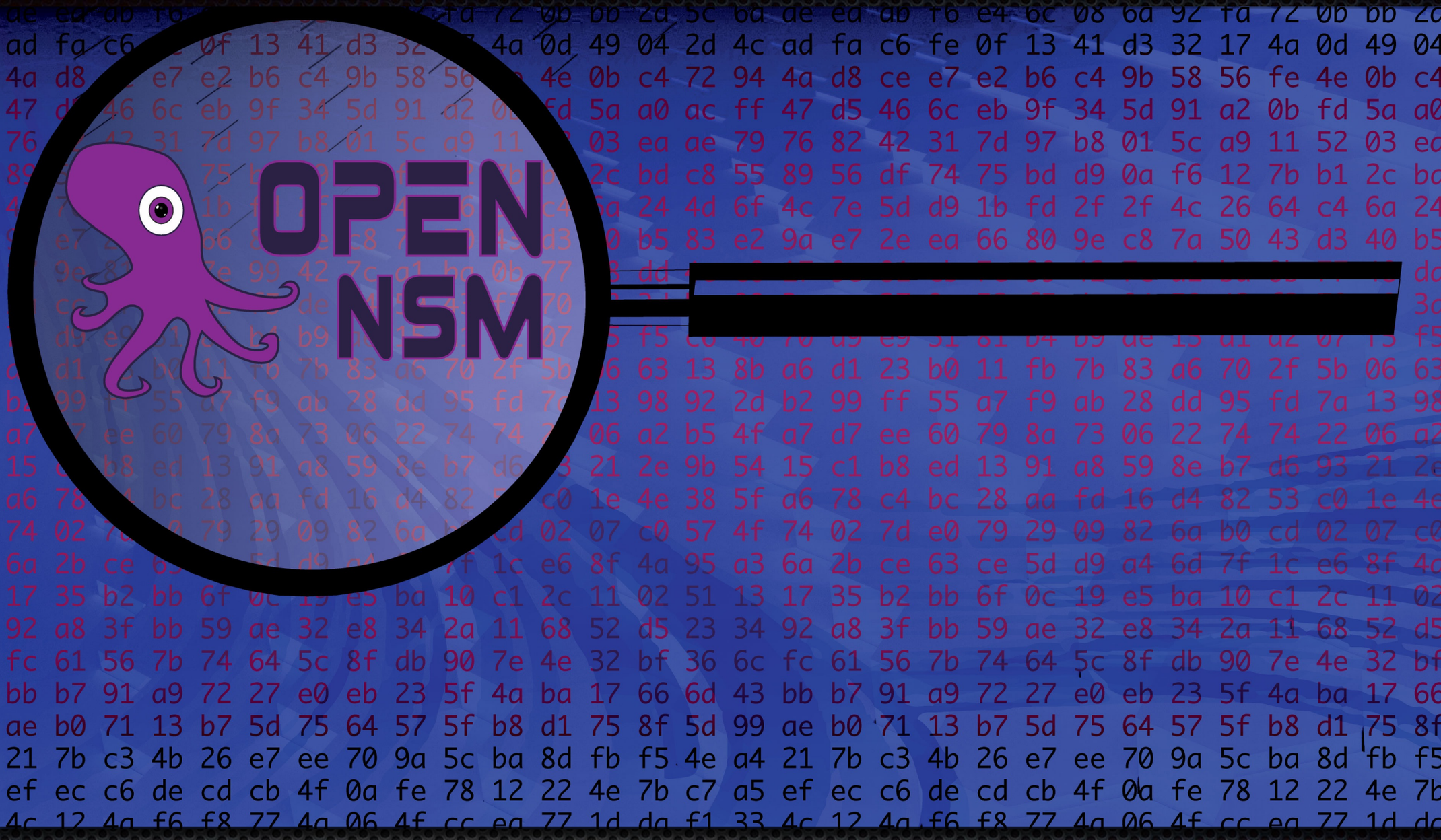
- Bro Team

- The Netsniff-NG Toolkit

- OpenNSM



- SecurityOnion



OpenNSM

A weekly NSM/DFIR group with international participation (www.open-nsm.net, @OpenNSM)

Why

1. I've always loved NSM

2. It didn't exist..anywhere

3. Richard Bejtlich's suggestion

4. NCSA/University of Illinois community

Group Focus

1. Sharing knowledge
2. Software development
3. Research
4. Training

Current Projects:

1. ContainNSM

2. FuzzNSM

3. Dockoo

4. NSM Illustrated (Video course)

Linux Containers

The technology

Isolation

via kernel namespaces and cgroups

The user can’t tell the difference.

Scalability

Horizontally and vertically with faster hardware meaning more users or work can be performed

Lightweight

~100ms startup time, near bare metal performance, JeOS

Density

Higher density than virtual machines

Security

Less secure than virtual machines, containers isolate the user land (e.g filesystem, processes) not the kernel

Portability

Less portable across operating systems. Tends to be portable within an operating system.

Concurrency

Some implementations are designed to run a single application or process

Kernel Versions

Containers must use the same kernel as the host

Containers

- **Important:** **"Linux Based Containers"**
  There is no internal container specification.
  As of recent, there is a container runtime specification called appsec
- **There are different container (and like) technologies**
  Linux: LXC, OpenVZ, Google containers, etc.
  Non-Linux: BSD Jails, Solaris Zones, AIX WPAR, etc.
- **The technology isn't new, but it's gaining great momentum now.**
- **What do containers do?**
  Light-weight process virtualization, A.K.A. operating system virtualization
- **What do virtual machines do?**
  Hardware virtualization

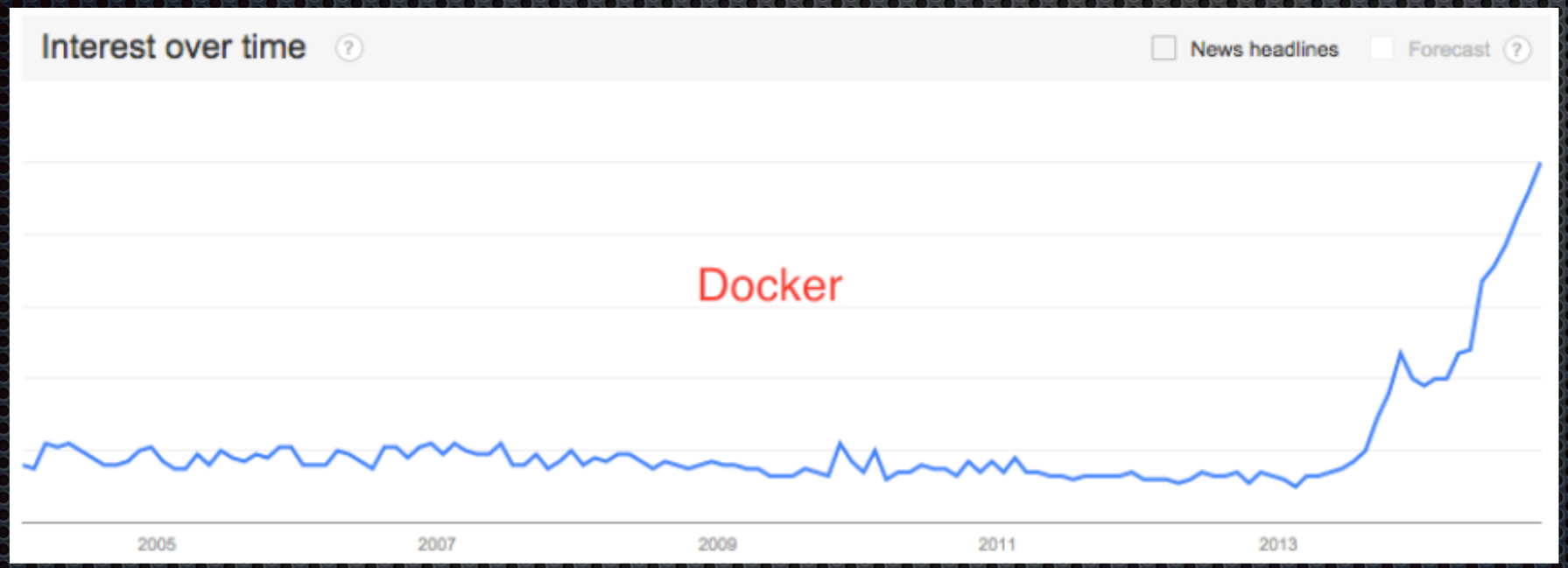
Linux Kernel Stuff

- Support: 3.8 introduce the final building block for containers
  Namespaces: Process isolation
  Currently available: *pid, net, ipc, uts, mnt, and user*
  Control Groups: Resource management
  e.g. *cpu, cpuset, blkio, memory, etc.*

- It's not magic, you can create namespaces and cgroups directly from your shell by modifying procfs and sysfs. That's how they were deployed before userland tools like LXC and Docker existed

Linux Containers?

Docker **popularized** the technology.
It's actually been around for 7 years.



- Automates the deployment of Linux based container
- Provides layers of abstraction
- Various methods of container creation
- Docker hub and registries for sharing and deployment

Research Moment

"In general, Docker equals or exceeds KVM performance in every case we tested."

– IBM Research Report: An Updated Performance Comparison of Virtual Machines and Linux Containers
< http://domino.research.ibm.com/library/cyberdig.nsf/papers/0929052195DD819C85257D2300681E7B/$File/rc25482.pdf>

```
for i in $(docker images -f 'label=program=bro' -q); do docker run -it $i bro --version; done
bro version 2.4
bro version 2.3
bro version 2.2
bro version 2.3.2
bro version 2.3.1
bro version 2.1
bro version 1.5
bro version 2.0
```

ContainNSM

Project to create Docker images of all available Free and Open Source network security monitoring tools for study, evaluation, and training.

Goals

Development: Run and deploy images with debugging information

Research: Comparison and performance evaluation between versions of the tools

Training: Easily run packaged tools with custom configurations on different datasets

Status & Roadmap

1. 100+ images for popular NSM software

2. Develop **./containnsm** for easy use

3. Collect datasets (e.g. PCAPs)

4. User contributed configurations for tools

Get ContainNSM

```
$ git clone https://github.com/open-nsm/containnsm
```

Demo

Directory structure, Docker Hub

Demo

Obtain, building, and run an image

Demo

ContainNSM Offline and Online mode

More information

$ https://www.youtube.com/watch?v=H9QjGxC7LaA

Contact

- **E-mail: jonschipp@gmail.com**
- Website: http://jonschipp.com
- Twitter: @JonSchipp
- keisterstash on freenode

References:

- IBM Research Report: An Updated Performance Comparison of Virtual Machines and Linux Containers < http://domino.research.ibm.com/library/cyberdig.nsf/papers/0929052195DD819C85257D2300681E7B/$File/rc25482.pdf >
- Realizing Linux Containers (LXC): Building Blocks, Underpinnings, and Motivations < http://www.slideshare.net/BodenRussell/realizing-linux-containerslxc >
- Resource management: Linux kernel Namespaces and cgroups. < http://www.haifux.org/lectures/299/netLec7.pdf >
- Linux Containers and the Future Cloud. < http://www.haifux.org/lectures/320/netLec8_final.pdf >
- Lightweight Virtualization with Linux Containers (LXC) < http://www.ciecloud.org/2013/subject/07-track06-Jerome%20Petazzoni.pdf>
- Docker Inc. <www.docker.com>
- ContainNSM Github <https://github.com/open-nsm/ContainNSM>
- ContainNSM Docker Hub <https://hub.docker.com/u/opennsm/>
- OpenNSM <http://open-nsm.net>