BRO NETWORK SECURITY MONITOR

2014 NSF Cybersecurity Summit: Bro Platform Training Workshop

The Bro Team

- Robin Sommer
- Justin Azoff
- Doris Schiöberg
- Jeannette Dopheide

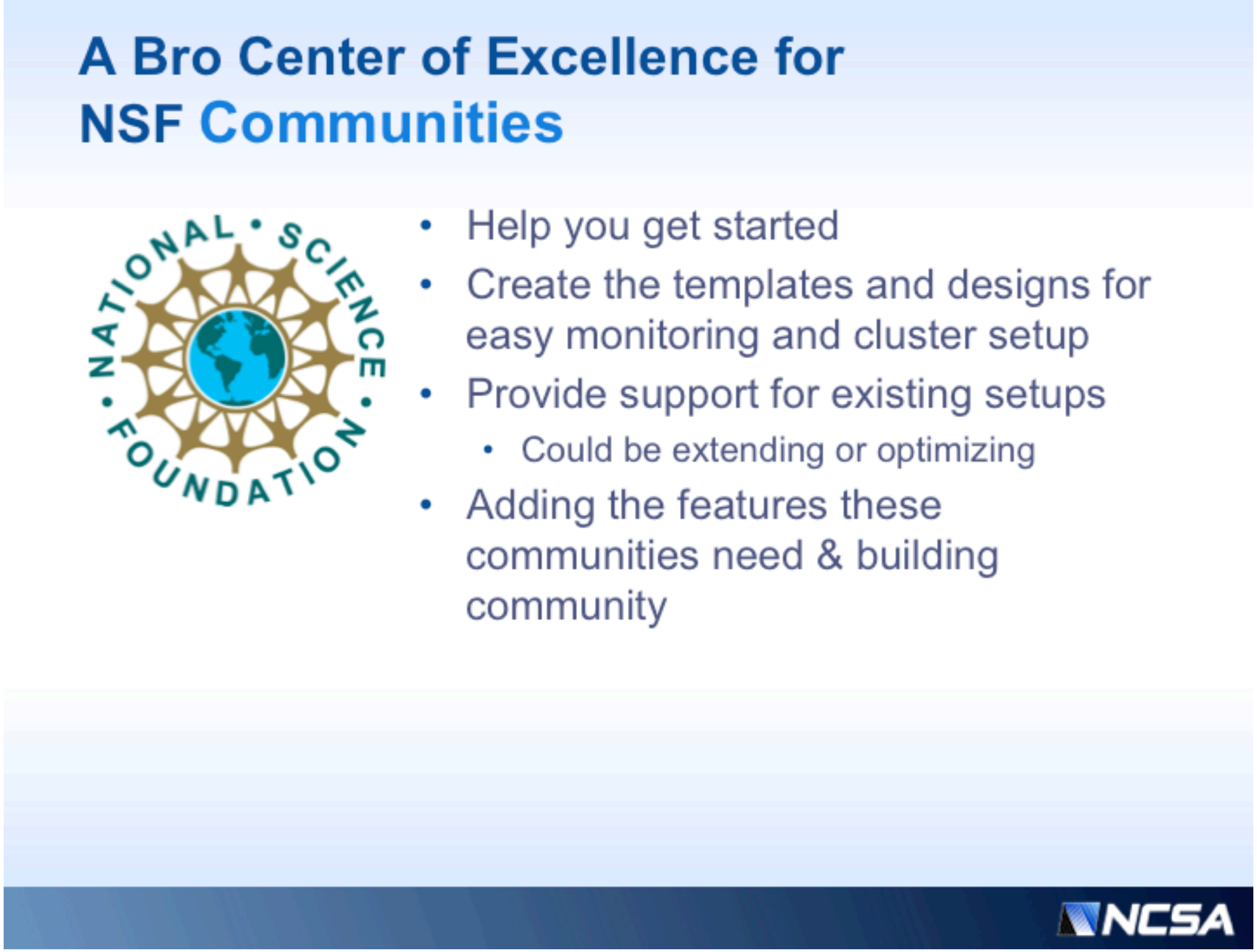
BRO NETWORK SECURITY MONITOR

The NSF Bro Center of Expertise:
The first year

A history of support

- Started at LBL, but quickly spread beyond DOE
- NSF has long funded R&D that fed Bro development in 2003
- NCSA started using Bro in 2003
- In 2009, Office of Cyberinfrastructure funded in a huge way
  - Kicked off Bro 2.0 and a huge adoption in EDUs
  - Marked a transition from R&D to operational value

Last October…



A Bro Center of Excellence for NSF Communities

- Help you get started
- Create the templates and designs for easy monitoring and cluster setup
- Provide support for existing setups
  - Could be extending or optimizing
- Adding the features these communities need & building community

Major Training Events

- BroCon 2014 (Aug 18-20)
  - 150+ attendees!
- DOE Workshop Spring 2014
- Cyber Security Summit
  - Oct. 2013, Aug 2014

Collaborations

- Helping CTSC with Summit and engagements
- Working with ESNet & Others on SDN integration
  - Join sdn@bro.org list
- Expect to see us at Internet2 Tech Exchange & SC

Engagements

- Who are we working with?
  - Universities: Big & small
  - NSF MFRCs
  - Even K-12 School districts
  - Corporations interested in EOT
- What are we doing
  - Developing materials
  - Helping troubleshoot setups
  - Taking feedback for future features
  - Helping plan for new installations

Bro Skunkworks

- *We’ve been working on a few things…*
- Try.Bro (Justin Azoff)
- Bro-Live (Jon Schipp)
- Bro Teaching Community (Doris Schioberg)
- The More You Bro (Jeannette Dopheide)

try.bro.org

Barriers Between Users and Bro

- Installation requires a fair amount of knowledge of operating system and package management details
  - Prevents quick demos
  - User is limited to a computer with the required dependencies installed
- No simple tool for educators
- No way to embed interactive examples in blog posts, websites, etc.

Solution

- Try.bro
  - Web-based sandbox
  - Allows users to write/paste scripts directly into the dialog box
  - Run scripts against sample pcaps and see output
  - Or upload your own pcaps

Under the Hood

- Try.bro
  - AngularJS, Python, Redis, Docker
  - Front end web application is written in AngularJS and talks to the Python backend
  - Backend receives requests from the browser and submits the code samples to a message queue built on top of Redis
  - Backend workers subscribe to the queue and start up a docker container to run each code snippet in isolation
  - Code output and log files are then stored back in Redis so they can be fetched by the web application

Bro-Live

Motivation

- Too much time spent passing around, downloading, and copying VMs or other materials
  - Networks are slow
  - Virtual harddisks are big
- Technical difficulties can occur, which puts the group behind schedule
- Wanted to reduce the burden on the users

Solution

- Avoid distributing VMs by giving users access to your server
- Make the barrier to participation as thin as possible
  - Require only a simple program (e.g. ssh)
  - Expands access via more products (phones, tablets, etc.)
- Admins manage via automated account management
- Changes may be easily updated
  - Especially useful when working collaboratively
- Ultimately passing the burden back onto the admin
- Bro-Live!

Implementation

- Users log into a non-privileged system account via SSH
  - Strong crypto, ubiquitous, low overhead
- Automated account creation via shell script
- Docker is called and ships each user in their own container
  - Each container instance is an isolated process
- User performs work in the container
  - Runs UNIX commands, traverses file systems, runs Bro
- User may log out and back into container for the duration of the training session
  - SSH into the same non-privileged user account
  - Re-enter credentials
  - Automatically reattached to their Docker container instance

Securing the Container

- Networking is disabled
  - Prevent attacks against other hosts, containers, or self
- System resources are limited per container to prevent resource abuse
- Containers and users are automatically removed after a period of time
  - Admins set the time based on the length of conference/ workshop
- Containers that grow too large are automatically removed to prevent disk space abuse
  - Helps defend against a denial of service attack

Demo

```
$ ssh demo@live.bro.org
demo@live.bro.org's password: BroCon14
…
Welcome to Bro Live!
====================
…
A place to try out Bro.
Are you a new or existing user? [new/existing]: new
…
Enjoy yourself!
Training materials are located in /exercises.
e.g. $ bro -r /exercises/beginner/http.pcap
demo@bro:~$
```

BRO NETWORK SECURITY MONITOR

Bro Teaching Community

Teaching Bro

- Like most programming languages, traditional teaching methods do not fit well with Bro
- Teaching Bro means not only teaching how to use Bro, but also networking and network security
  - Hands-on training is essential
- Requires a lot of tutorials and training materials to bring Bro to a classroom

Bro Teaching Community

Exchange

- knowledge
- experience
- methods
- materials (slides, exercises, etc)

Building the Community

Connect and share with the community through

- teaching mailing list
- weekly online meeting
- teaching git repository

The More You Bro

The Challenge

- Bro and Education Outreach
- Task: produce videos for a new series called The More You Bro
  - 5-10 minutes in length
  - focus on a single task/topic
  - approachable to new users
  - include screencasts of Bro
  - scripted, with good AV quality

First Video

- We reached out for help drafting a short list of topics for videos
- Jon Schipp expressed interest in working on the project
- Brainstorming meeting to identify task list for the first video
  - Settled on "Log Parsing Tips and Tricks" as the first video

The Process

- Pick a topic
- Use blog posts and Bro documentation to draft a script
- Send script to the team for technical feedback
- Shoot the video (set aside enough time)
- Edit the video, request feedback
- Post to YouTube, Twitter, and Google+

Lessons Learned

- Keep the script light
  - Focus on a few main points, relaxed tone
- Learned a lot about video editing
  - Record the screencast first, audio second
  - Software: Camtasia, Snagit, iMovie, QuickTime
  - Recording room and equipment
- Prepare title and transition slides to fill in gaps

The Future of TMYB

- TMYB series is our most popular Bro videos to date
- Goal: hit one thousands views
- Future topics:
  - What is Bro?
  - Installing Bro
  - Loading Scripts
  - Suggestions welcome: info@bro.org

Conclusion: What's coming?

- More focus on SDN & the Science DMZ concept
- More workshops & meetings
- More videos
- Embeddable try.bro.org
- Bro in the classroom
- A new website

Feedback & Contact Info

- Bro-Live and Try.bro have room to grow
  - We welcome your feedback on usability and security
  - Send us feature requests
- Bro-Live, Try.bro, Bro Teaching Community, The More You Bro: contact Bro mailing list at info@bro.org
- Subscribe to YouTube Channel:
  - www.youtube.com/user/BroPlatform

Today's Agenda

- 8:00 am Welcome
- 8:30 am Broverview
- 9:00 am Bro for Beginners
- 9:45 am *Break*
- 10:00 am Bro for Beginners, cntd.
- 10:30 am OpSec Pro's Use of Bro
- 11:00 am Examining Logs
- Noon *Lunch*
- 1:00 pm Bro Script Study
- 2:00 pm Setting up a Bro Cluster
- 3:00 pm *Break*
- 3:30 pm New Analyzers in Bro
- 4:30 pm Pick a Security Pro's Brain
- 5:00 pm Training Session Ends

Want your own Bro-Live?

- Vagrant: http://github.com/jonschipp/vagrant
- Docker: http://hub.docker.com/u/jonschipp/latest-bro-sandbox/
- System configuration is entirely automated
- Written for and tested on Ubuntu, Trusty, and Saucy
- Installation and configuration on Ubuntu
  - $ wget https://raw.githubusercontent.com/jonschipp/vagrant/master/bro-sandbox/provision.sh - | bash
- Testing with Vagrant
  - $ git clone http://github.com/jonschipp/vagrant && cd vagrant/bro-sandbox && vagrant up; ssh -p 2222 demo@127.0.0.1