The NSF Bro Center of Expertise

Robin Sommer

International Computer Science Institute, &
Lawrence Berkeley National Laboratory

robin@icsi.berkeley.edu
http://www.icir.org/robin

The Bro Network Monitor

Open Source
BSD License

Analyses

Intrusion Detection | Vulnerabilit. Mgmt | File Analysis | Traffic Measure-ment | Traffic Control | Compliance Monitoring

Platform

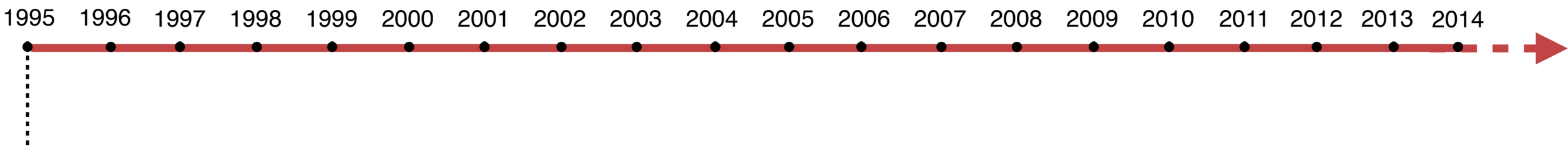
Programming Language | Standard Library

Packet Processing

Tap

Network

Bro History


1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
Vern writes 1st line of code

Bro History

1995 1996 1997 1998 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014

Vern writes 1st line of code

v0.2
1st CHANGES entry

v0.6
RegExps
Login analysis

v0.7a90
Profiling
State Mgmt

v0.8aX/0.9aX
SSL/SMB
STABLE releases
BroLite

v1.1/v1.2
when Stmt
Resource tuning
Broccoli
DPD

v1.5
BroControl

v2.0
User Experience

v2.2
File Analysis
Summary Stats

v2.3
Performance
SNMP,
Radius, SSL++

LBNL starts using Bro operationally

v0.4
HTTP analysis
Scan detector
IP fragments
Linux support

v0.7a175/0.8aX
Signatures
SMTP
IPv6 support
User manual

v1.0
BinPAC
IRC/RPC analyzers
64-bit support
Sane version numbers

v1.4
DHCP/BitTorrent
HTTP entities
NetFlow
Bro Lite Deprecated

Bro SDCI

v2.1
IPv6
Input Framew.

Bro Center

v0.7a48
Consistent CHANGES

0.8a37
Communication
Persistence
Namespaces
Log Rotation

v1.3
Ctor expressions
GeoIP
Conn Compressor

Bro History

Academic Publications

1995 1996 1997 1998 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014

- 1998: USENIX Paper
- 2000: Stepping Stone Detector
- 2003: Anonymizer, Active Mapping, Context Signat.
- 2004: TRW, State Mgmt., Independ. State
- 2005: Host Context, Time Machine, Enterprise Traffic
- 2006: BinPAC, DPD, 2nd Path
- 2007: Bro Cluster, Shunt
- 2008: Autotuning
- 2009: Parallel Prototype
- 2012: Input Framework
- 2013: SSL Trust Relationships
- 2014: Summary Stats, HILTI, DPI Concurrency, PLC Modeling

- Vern writes 1st line of code
- LBNL starts using Bro operationally
- v0.2 1st CHANGES entry
- v0.4 HTTP analysis, Scan detector, IP fragments, Linux support
- v0.6 RegExps, Login analysis
- v0.7a48 Consistent CHANGES
- v0.7a90 Profiling, State Mgmt
- v0.7a175/0.8aX Signatures, SMTP, IPv6 support, User manual
- 0.8a37 Communication, Persistence, Namespaces, Log Rotation
- v0.8aX/0.9aX SSL/SMB STABLE releases, BroLite
- v1.0 BinPAC, IRC/RPC analyzers, 64-bit support, Sane version numbers
- v1.1/v1.2 *when* Stmt, Resource tuning, Broccoli, DPD
- v1.3 Ctor expressions, GeoIP, Conn Compressor
- v1.4 DHCP/BitTorrent, HTTP entities, NetFlow, Bro Lite Deprecated
- v1.5 BroControl
- Bro SDCI
- v2.0 User Experience
- v2.1 IPv6, Input Framew.
- v2.2 File Analysis, Summary Stats
- Bro Center
- v2.3 Performance, SNMP, Radius, SSL++

Bro History

Academic Publications

1995 1996 1997 1998 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014

- 1998: USENIX Paper
- 2000: Stepping Stone Detector
- 2003: Anonymizer, Active Mapping, Context Signat.
- 2004: TRW, State Mgmt., Independ. State
- 2005: Host Context, Time Machine, Enterprise Traffic
- 2006: BinPAC, DPD, 2nd Path
- 2007: Bro Cluster, Shunt
- 2008: Autotuning
- 2009: Parallel Prototype
- 2012: Input Framework
- 2013: SSL Trust Relationships
- 2014: Summary Stats, HILTI, DPI Concurrency, PLC Modeling

- Vern writes 1st line of code
- 1995: LBNL starts using Bro operationally
- 1996: v0.2, 1st CHANGES entry
- 1997: v0.4, HTTP analysis, Scan detector, IP fragments, Linux support
- 1998: v0.6, RegExps, Login analysis
- 1999: v0.7a48, Consistent CHANGES
- 2000: v0.7a90, Profiling, State Mgmt
- 2001: v0.7a175/0.8aX, Signatures, SMTP, IPv6 support, User manual
- 2002: 0.8a37, Communication, Persistence, Namespaces, Log Rotation
- 2003: v0.8aX/0.9aX, SSL/SMB, STABLE releases, BroLite
- 2004: v1.0, BinPAC, IRC/RPC analyzers, 64-bit support, Sane version numbers
- 2005: v1.1/v1.2, *when* Stmt, Resource tuning, Broccoli, DPD
- 2006: v1.3, Ctor expressions, GeoIP, Conn Compressor
- 2007: v1.4, DHCP/BitTorrent, HTTP entities, NetFlow, Bro Lite Deprecated
- 2008: v1.5, BroControl
- 2009: v2.0, User Experience
- 2010: Bro SDCI (NSF)
- 2011: v2.1, IPv6, Input Framew.
- 2012: v2.2, File Analysis, Summary Stats
- 2013: v2.3, Performance, SNMP, Radius, SSL++
- 2014: Bro Center (NSF)

Deployments

Installations across the US

Universities
Research Labs
Supercomputer Centers
Government Organizations
Fortune 50 Enterprises

Examples

Lawrence Berkeley National Lab
National Center for Supercomputing Applications
Indiana University
Carnegie Mellon
National Center for Atmospheric Research

... and many more sites I can't talk about.

Fully integrated into *Security Onion*

Popular security-oriented Linux distribution

Community

50/90/150 attendees at BroCon '12/'13/'14
60 organizations at BroCon '14
2,500 Twitter followers
800 mailing list subscribers
70 users average on IRC channel
10,000 downloads / version
from 150 countries
> 30,000 Onion downloads ('12)

Bro History

Academic Publications

1995 1996 1997 1998 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014

- 1998: USENIX Paper
- 2000: Stepping Stone Detector
- 2003: Anonymizer, Active Mapping, Context Signat.
- 2004: TRW, State Mgmt., Independ. State
- 2005: Host Context, Time Machine, Enterprise Traffic
- 2006: BinPAC, DPD, 2nd Path
- 2007: Bro Cluster, Shunt
- 2008: Autotuning
- 2009: Parallel Prototype
- 2012: Input Framework
- 2013: SSL Trust Relationships
- 2014: Summary Stats, HILTI, DPI Concurrency, PLC Modeling

- Vern writes 1st line of code
- LBNL starts using Bro operationally
- v0.2 1st CHANGES entry
- v0.4 HTTP analysis, Scan detector, IP fragments, Linux support
- v0.6 RegExps, Login analysis
- v0.7a48 Consistent CHANGES
- v0.7a90 Profiling, State Mgmt
- v0.7a175/0.8aX Signatures, SMTP, IPv6 support, User manual
- 0.8a37 Communication, Persistence, Namespaces, Log Rotation
- v0.8aX/0.9aX SSL/SMB, STABLE releases, BroLite
- v1.0 BinPAC, IRC/RPC analyzers, 64-bit support, Sane version numbers
- v1.1/v1.2 *when* Stmt, Resource tuning, Broccoli, DPD
- v1.3 Ctor expressions, GeoIP, Conn Compressor
- v1.4 DHCP/BitTorrent, HTTP entities, NetFlow, Bro Lite Deprecated
- v1.5 BroControl
- v2.0 User Experience
- Bro SDCI (NSF)
- v2.1 IPv6, Input Framew.
- v2.2 File Analysis, Summary Stats
- Bro Center (NSF)
- v2.3 Performance, SNMP, Radius, SSL++

Bro History

Academic Publications

1995 1996 1997 1998 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014

- 1998: USENIX Paper
- 2000: Stepping Stone Detector
- 2003: Anonymizer, Active Mapping, Context Signat.
- 2004: TRW, State Mgmt., Independ. State
- 2005: Host Context, Time Machine, Enterprise Traffic
- 2006: BinPAC, DPD, 2nd Path
- 2007: Bro Cluster, Shunt
- 2008: Autotuning
- 2009: Parallel Prototype
- 2012: Input Framework
- 2013: SSL Trust Relationships
- 2014: Summary Stats, HILTI, DPI Concurrency, PLC Modeling

- Vern writes 1st line of code
- LBNL starts using Bro operationally
- v0.2 1st CHANGES entry
- v0.4 HTTP analysis, Scan detector, IP fragments, Linux support
- v0.6 RegExps, Login analysis
- v0.7a48 Consistent CHANGES
- v0.7a90 Profiling, State Mgmt
- v0.7a175/0.8aX Signatures, SMTP, IPv6 support, User manual
- 0.8a37 Communication, Persistence, Namespaces, Log Rotation
- v0.8aX/0.9aX SSL/SMB, STABLE releases, BroLite
- v1.0 BinPAC, IRC/RPC analyzers, 64-bit support, Sane version numbers
- v1.1/v1.2 *when* Stmt, Resource tuning, Broccoli, DPD
- v1.3 Ctor expressions, GeoIP, Conn Compressor
- v1.4 DHCP/BitTorrent, HTTP entities, NetFlow, Bro Lite Deprecated
- v1.5 BroControl
- Bro SDCI
- v2.0 User Experience
- v2.1 IPv6, Input Framew.
- v2.2 File Analysis, Summary Stats
- Bro Center
- v2.3 Performance, SNMP, Radius, SSL++

The NSF Bro Center of Expertise

Promote Bro as a comprehensive, low-cost security capability for the NSF community.

http://nsf.bro.org

mailto:nsf@bro.org

The NSF Bro Center of Expertise

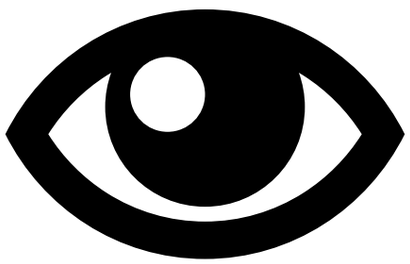
Promote Bro as a comprehensive, low-cost security capability for the NSF community.

http://nsf.bro.org

mailto:nsf@bro.org

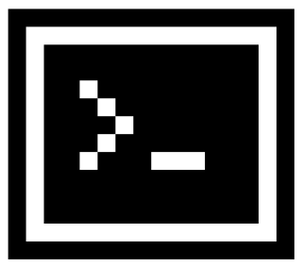
The NSF Bro Center of Expertise

Promote Bro as a comprehensive, low-cost security capability for the NSF community.



Individual Advice

Training Material, Guidelines, Best Practices



Development, Maintenance

`http://nsf.bro.org` `mailto:nsf@bro.org`

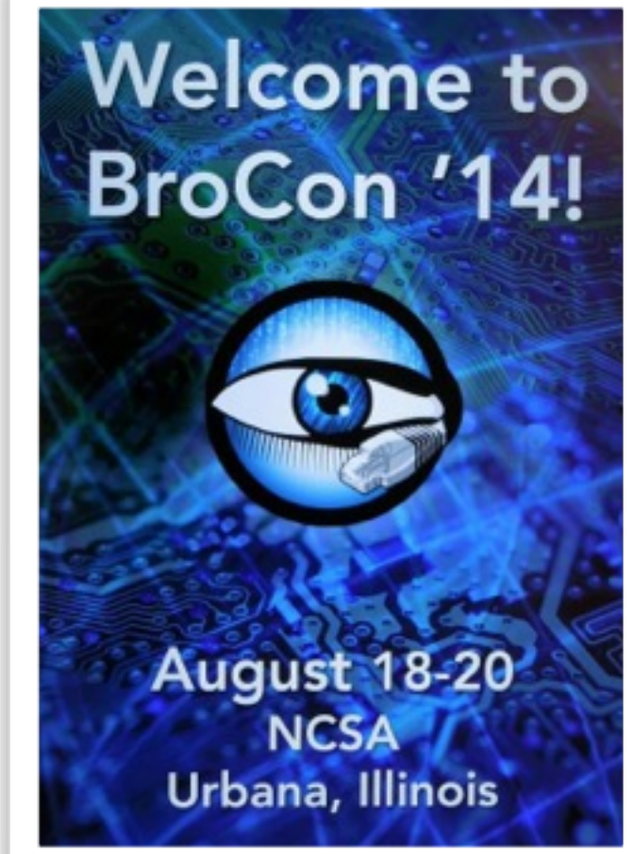
Center Team

Located at *International Computer Science Institute*, Berkeley, CA; and the *National Center for Supercomputing Applications,* Urbana-Champaign, IL.

Events

BroCon 2014.

2.5 days, 150 attendees, 4 corporate sponsors.
Presentations, training, demos.



Bro Workshops.

NSF Cybersecurity Summits '13 & '14.
DOE NSM Meeting, June '14.

In Planing.

Advanced Workshop at ICSI.
BroCon '15 (East coast, tentatively).
Co-organize BoFs/demos at Internet2 & Supercomputing.

Current Engagements & Collaborations

Individual Advice.

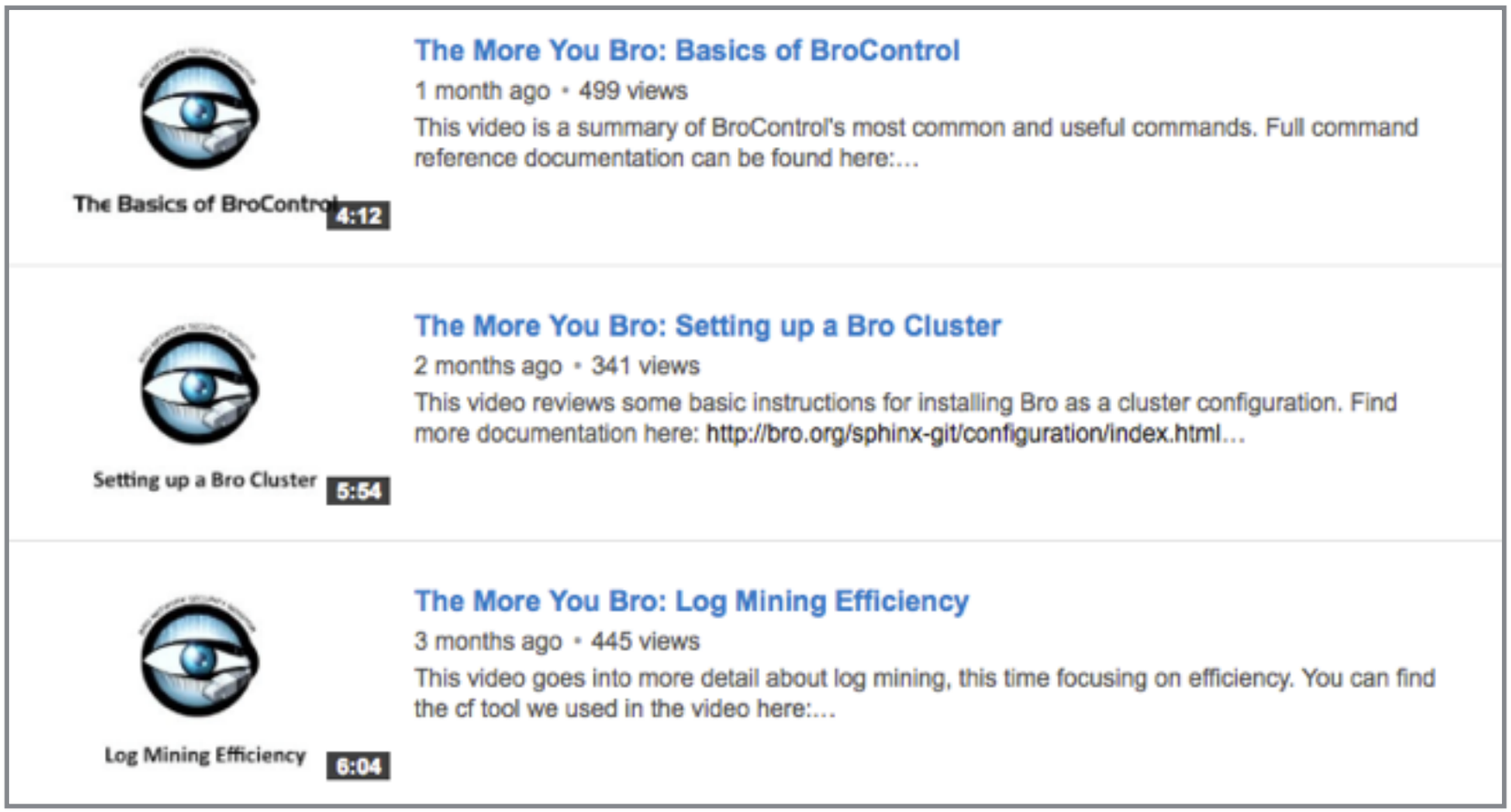
Universities, NSF MREFs, K-12 schools.

Collaborations.

CTSC	Outreach & training, security reviews.
ESnet	SDN, Science DMZ security.
RIT	Teaching Community.

Teaching Bro - Material

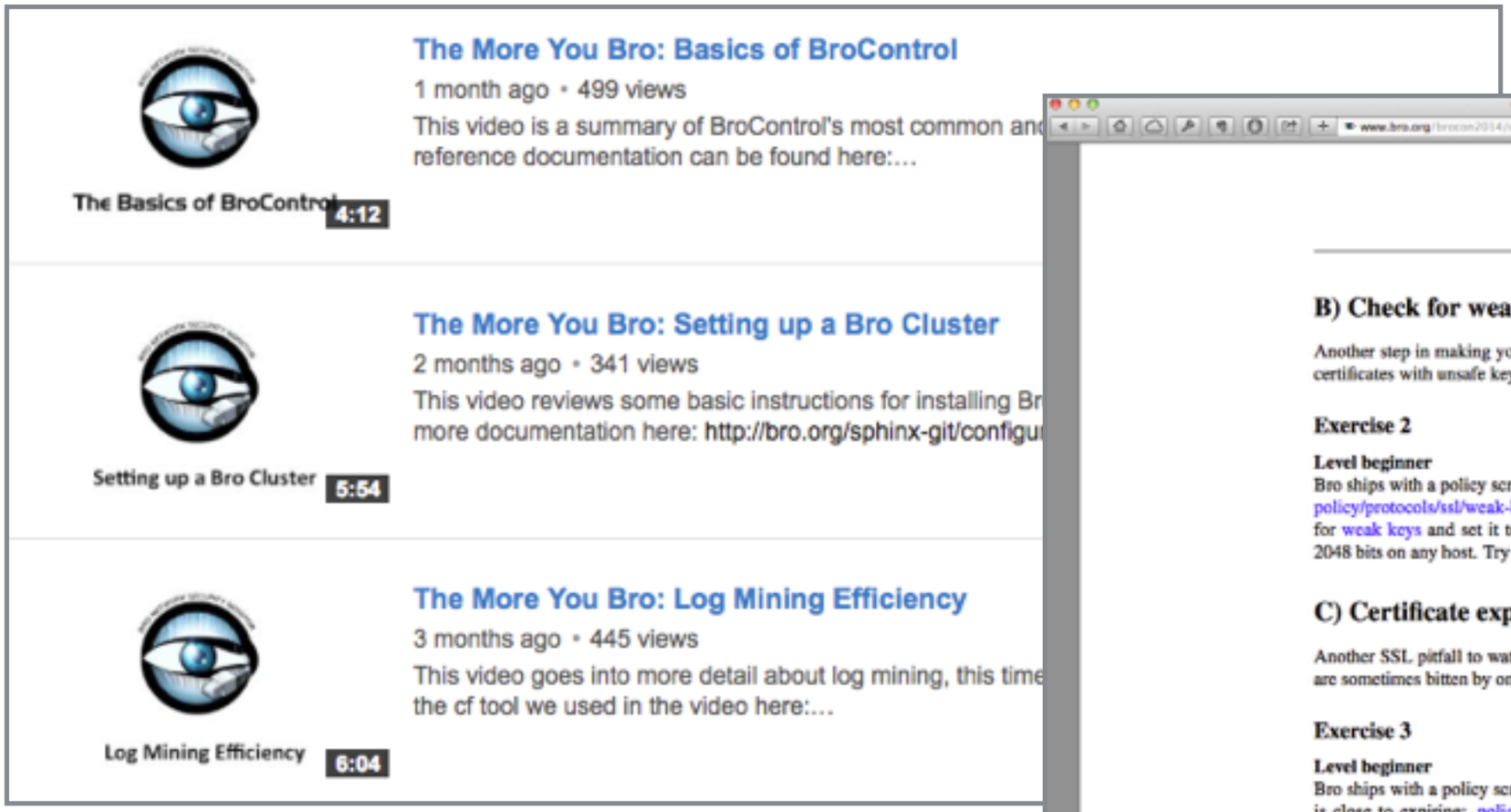
Video Tutorials



`http://www.youtube.com/user/BroPlatform`

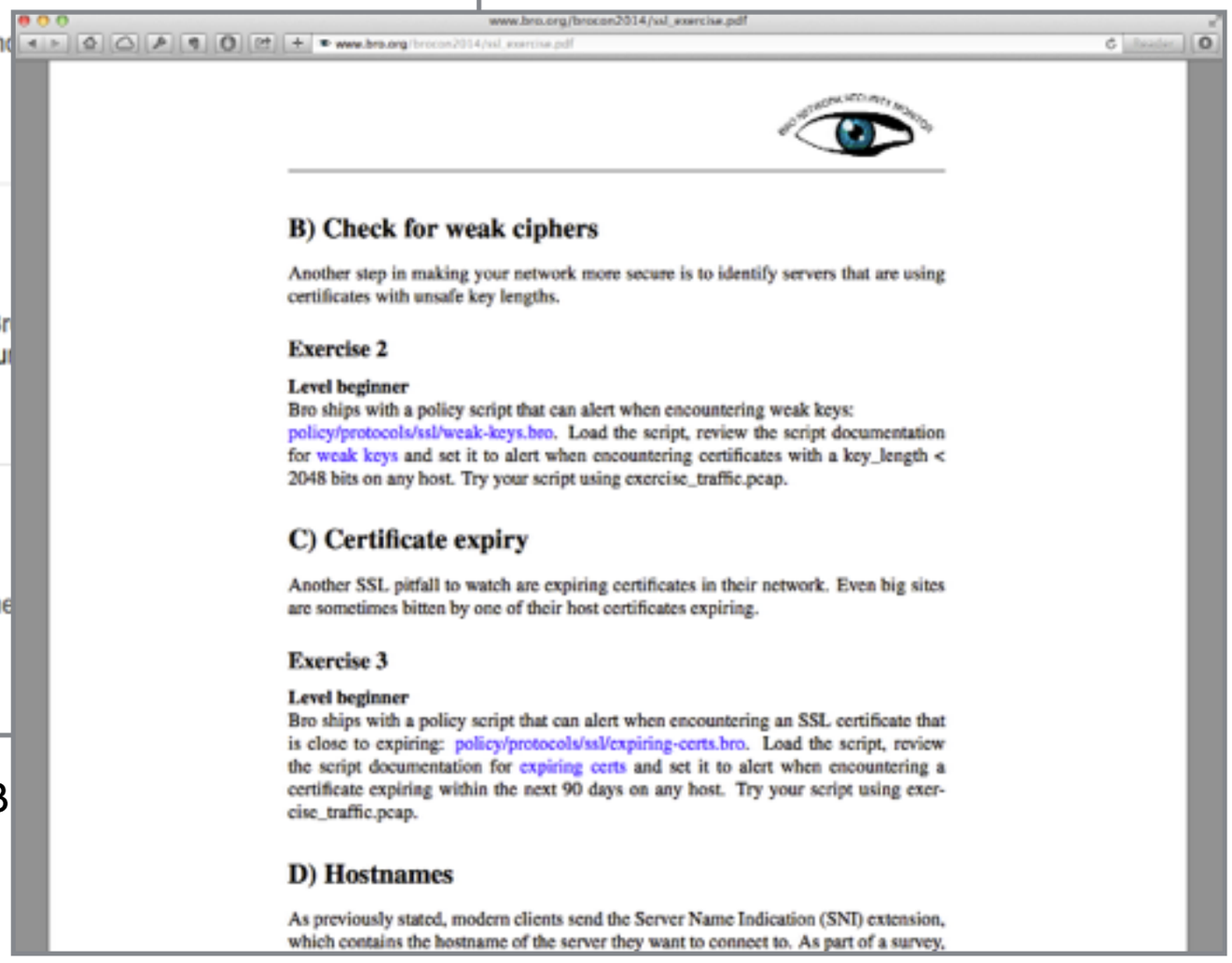
Teaching Bro - Material

Video Tutorials



http://www.youtube.com/user/B

Exercises

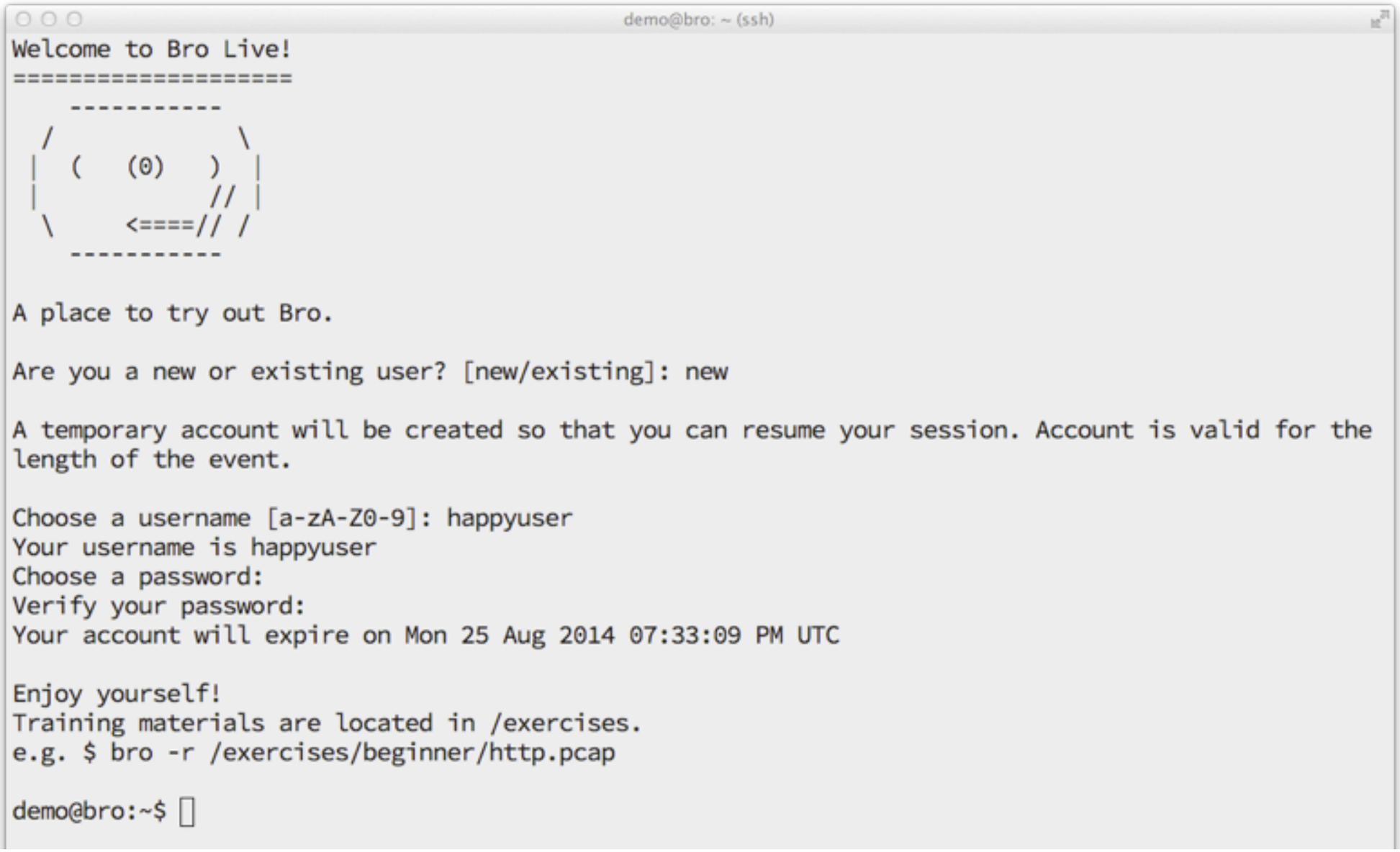


Teaching Bro - Infrastructure

`live.bro.org` SSH into a virtual Bro environment.

Teaching Bro - Infrastructure

`live.bro.org` SSH into a virtual Bro environment.

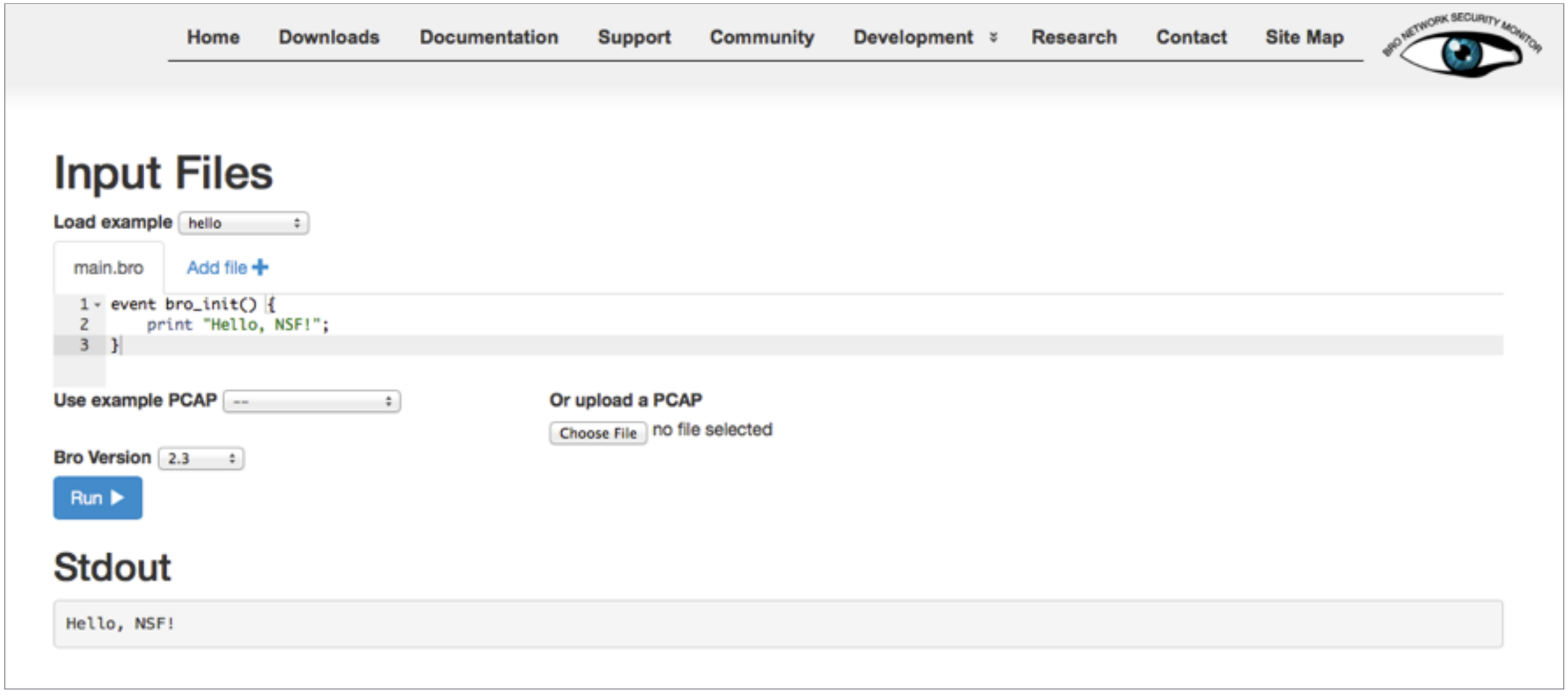


Teaching Bro - Infrastructure

`try.bro.org` A web-based Bro sandbox.

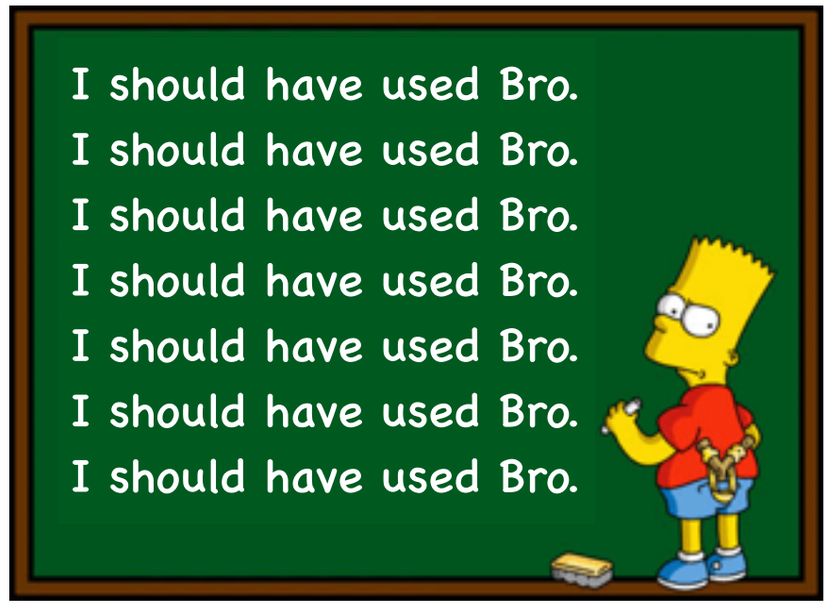
Teaching Bro - Infrastructure

`try.bro.org` A web-based Bro sandbox.



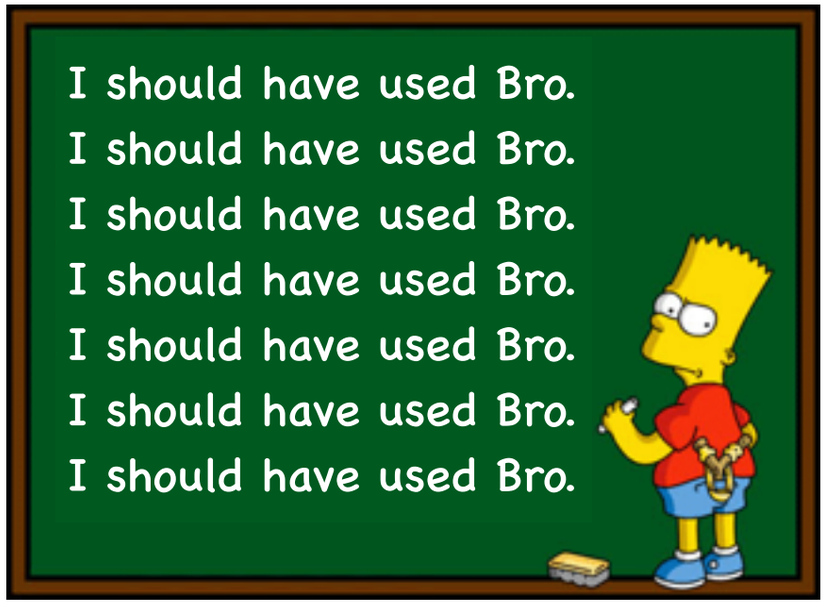
The Bro Teaching Community

People are learning Bro—and they are using Bro to learn.



The Bro Teaching Community

People are learning Bro—and they are using Bro to learn.



Kick-start community of educators teaching (with) Bro.

Exchange experiences, methods, & material.

We provide logistics and technical advice.

Weekly calls, mailing list, repository with seed material, access to team

Our initial solicitation met broad interest.

Universities & colleges, corporate IT, government organizations.

The Center is promoting Bro as a comprehensive, low-cost security capability for the NSF community.

The Bro Project	**Bro Center of Expertise**
www.bro.org	nsf.bro.org
info@bro.org	nsf@bro.org

Twitter	@Bro_IDS
Facebook	TheBroPlatform

The Center is promoting Bro as a comprehensive, low-cost security capability for the NSF community.

The Bro Project	**Bro Center of Expertise**
www.bro.org	nsf.bro.org
info@bro.org	nsf@bro.org
Twitter	@Bro_IDS
Facebook	TheBroPlatform