An Overview of the Bro Intrusion Detection System

Brian L. Tierney, Vern Paxson, James Rothfuss
Lawrence Berkeley National Laboratory

Typical Approach:
Firewall with “default deny” policy

- A blocking router is a type of firewall
- Blocks individual services (ports) inbound and possibly outbound
- Blocks address ranges inbound and possibly outbound
LBNL approach:
IDS with Blocking Router

- IDS controls a blocking router
- IDS blocks dynamically when an intrusion attempt is detected or alerts upon suspicious activity
- Router blocks statically like a firewall
- “Intrusion Prevention”

LBNL Inbound (from Internet)
TCP Traffic

Number of TCP connection attempts per week, Jan 2000 to Aug 2004

- Total traffic
- Scanning traffic
- Legitimate traffic

Blaster worm released
**Bro’s Use at LBL**

- Operational 24×7 since 1996
- Monitors traffic for suspicious behavior or policy violations: incoming/outgoing/internal
- In conjunction with blocking routers, Bro acts as a dynamic and intelligent firewall
  - Blocks access from offending IP addresses
  - Blocks high risk ports
  - Blocks known high-risk activity
  - Terminates connections and/or sends alarms
- Very high performance: GigEther
- Award winning research
Bro Goals & Requirements (1995)

- Ability to monitor traffic in a very high performance environment
- Real-time detection and response
- Separation of mechanism from policy
- Ready extensibility of both mechanism and policy
- Resistant to evasion

How Bro Works

- Taps GigEther fiber link passively, sends up a copy of all network traffic.
• Kernel filters down high-volume stream via standard *libpcap* packet capture library.

• “Event engine” distills filtered stream into high-level, *policy-neutral* events reflecting underlying network activity
  - E.g. Connection-level:
    - connection attempt
    - connection finished
  - E.g. Application-level:
    - ftp request
    - http_reply
  - E.g. Activity-level:
    - login success
How Bro Works

• “Policy script” processes event stream, incorporates:
  – Context from past events
  – Site’s particular policies

• ... and takes action:
  • Records to disk
  • Generates alerts via syslog, paging, etc.
  • Executes programs as a form of response
Signature Engine

• Bro also includes a signature engine for matching specific patterns in packet streams:
  – Conceptually simple
  – Easy to share
  – Compatible with Snort (widely used freeware IDS)
    • E.g., can run on Snort’s default set of 2,500+ signatures

• As with other Bro analysis, signature matches generate events amenable to high-level policy script processing, rather than direct alerts

Examples of Bro’s Contextual Signatures (“Rules”)

• HTTP server attack
  – Snort signature: simple pattern matching on MS ISS attack
  – Bro rule: additional check to see if, e.g., host is running Apache ⇒ ignore alarm

• Error code checking
  – Snort signature: no checking of reply
  – Bro rule: Looks at return code for HTTP/FTP/SMTP,
    • signature match + error code = no alert

• Multi-stage attacks
  – Easy in Bro to express “signature A but only if followed by signature B” or “A unless followed by B”
  – Easy to express “generate alarms if given host triggers N or more signatures” or “triggers against N or more local hosts”

• Greatly reduces number of false positives!
Bro as a Tool for Network Analysis/Forensics

- Bro supports extensive long-term logging
- We have a record of every TCP connection in/out of LBNL going back to 1994
  - Time, size, duration, who, protocol, status
  - Plus specifics of apps analyzed by Bro:
    - Usernames, filenames, URLs
- Invaluable for forensic analysis
- Also invaluable for trending, retrospective analysis, longitudinal studies

Example: Bro dropping an IP source address

ISS Server attack:
Nov 5 00:04:07 140.138.148.222/2142 > cindy/http %63654: attack URI GET
/scripts/..%5c..%5cwinnt/system32/cmd.exe?
/c+copy+c:\winnt\system32\cmd.exe+c:\inetpub\scripts\script.exe, dropping

Policy: Drop this host:
Nov 5 00:04:07 AddressDropped dropping address 140.138.148.222 (attack URI /scripts/..%5c..%5cwinnt/system32/cmd.exe?/c+copy+c:\winnt\system32\cmd.exe+c:\inetpub\scripts\script.exe)
WU-FTP buffer overflow attack

Alarm:
Jan 21 01:31:56 ssl.hawera.de/1540 > obsidian/ftp #18 excessive filename: 00000000000000000000000000000000..[495].

Details from FTP log file:
Feb 21 00:53:15 #4733 clydesdale.cacc.ncsu.edu/2564 > obsidian.lbl.gov/ftp start
Feb 21 00:53:16 #4733 USER ftp/mozilla@ (logged in)
Feb 21 00:53:16 #4733 RNFR ./. (350 File exists, ready for destination name)
Feb 21 00:53:22 #4733 PWD (done)
Feb 21 00:53:22 #4733 CWD 00000000000000000000000000000000..[495] (unavail)
Feb 21 00:53:22 #4733 CWD ~/{.,.,.,.} (ok)

Sample Bro Alarms

Nov 16 03:31:23 AddressDropped low port trolling a213-22-132-227.netcabo.pt 258/tcp
Nov 16 06:25:23 SensitivePortmapperAccess rpc: cs4/917 > guacamole.cchem.berkeley.edu/portmap pm_dump: (done)
Nov 16 06:30:49 AddressScan 66.243.211.244 has scanned 10000 hosts (445/tcp)
Nov 16 06:30:50 SensitiveConnection hot: neutrino 200b > 147.8.137.149/telnet 463b 14.2s "root"
Nov 16 06:30:50 OutboundTFTP outbound TFTP: sip000d28083467.dhcp -> inoc-dba.pch.net
Nov 16 06:30:52 SensitiveConnection hot: 198.128.27.21 560b > 208.254.3.160/https 4202b 0.5s <IRC source sites>
Nov 16 06:30:53 WormPhoneHome worm phone-home signature mcr-88-4 -> 218.146.108.51/9900
Nov 16 06:30:56 FTP_Sensitive ftp: fun.ee/3766 > soling.cs.vu.nl/ftp #1537 RETR nfsshell.tar.gz (complete)
Nov 16 06:32:38 HTTP_SensitiveURI scan1/34462 > 198.128.27.212/http %988: GET /admin/file_manager.php?action=download&filename=./../../../../../etc/passwd <no reply>
Related Research

- Bro serves as platform for:
  - Developing new methods of analyzing high-level network activity
    - Detecting scans, "stepping stones", "backdoors"
  - "Independent state"
    - Sharing context between Bro’s across time & space
  - Efficient hardware to support intrusion detection
  - Investigating defenses against evasion
  - Hardware assist - "Shunting"

- Operation at LBNL produces ongoing bonanza of intrusion detection research data
  - Rich, challenging environment
New Project: Shunting

Bro vs. Bro-Lite

• Bro and Bro-Lite are the exact same set of software
  – All Bro-Lite work is going into the main Bro distribution

• Bro-Lite refers to a specific default policy configuration
• Bro-Lite is a project name
For more Information

- New Web site: http://www.bro-ids.org/
- Bro-Lite “alpha” release now available
  – http://www.bro-ids.org/alpha/
- Bro-Lite “beta” release coming soon
- Send email to bro@bro-ids.org