Making Intrusion Detection Systems Interactive and Collaborative

Scott Campbell scottc@nersc.gov
Stephen Chan sychan@lbl.gov
Lawrence Berkeley Lab
NERSC
Networking and Security Team
Motivations

• Open Source Intrusion Detection Systems
  – Typically controlled by text configuration files
  – Non-interactive

• Security Monitoring and Response
  – Collaborative Activity
  – Hard to teach/train
Solution

• Prototyped a solution using Bro
  – Bro is a stateful Network Intrusion Detection System
  – Developed at Lawrence Berkeley Lab
  – In production since 1996

• BroShell
  – Interactive, command line interface to Bro
  – Query for IDS internal state, information about hosts
  – Set policy dynamically, add or remove state information about hosts
• Jabber Bot interface to BroShell
  – Collaborative interface to Bro
    • Multiple users can observe and interact with BroShell simultaneously
    • Allows newbies to observe for training purposes
    • Chat logs can provide history/audit function
    • Many to many mapping between people and applications
  – Compatible with popular IM clients
[7:44 AM] `sychanbot` has entered the room.
[7:44 AM] `sychan` has entered the room.
[7:42 AM] `<sychanbot>` Hey there! I ignore anything that isn't prefixed by `@bro`
[7:44 AM] `<sychan>` `@bro ping`
[7:44 AM] `<sychanbot>` Executing: `./broshell.sh ping`
[7:44 AM] `<sychanbot>` pong event from 127.0.0.1: seq=1, time=0.001505/1.002159 s
[7:44 AM] `<sychan>` `@bro show cpu`
[7:44 AM] `<sychanbot>` Executing: `./broshell.sh show cpu`
[7:44 AM] `<sychanbot>` total CPU time/total clock time: 0.000448
[7:45 AM] `<sychan>` I'm happily ignored!
Links, references, whatnot

- Bro web site

- Documents on BroShell
  - [http://www.nersc.gov/~scottc/software/bro/broshell.html](http://www.nersc.gov/~scottc/software/bro/broshell.html)

- Paper on Work Practices of Sys Admins