Intrusion Detection Systems

Evan Misshula

emisshula@qc.cuny.edu

How old is hacking?

- In 1972, the US Air Force was worried about computer security problems.
  - https://www.sans.org/reading-room/whitepapers/detection/history-evolution-intrusion-detection-344
- A variety of private IDS but..
- In 1998, Marty Roesch released the first version of Snort.
- In 1999, Snort 1.5 with logging and packet analysis
- In 2000, Michael Davis ported it to Windows

Chokepoint

- One flaw of IDS is that it requires all trafic to go through a sensor
- This creates a chokepoint
- Prior to Snort 3.0 this meant a single thread (like python)

Evolution of Network Processing

- Since 1998 networks have gone from 100 Mps to 1 Gig …
- Now to 40 Gig and moving 100 Gig
- Sensor CPU are not able to keep up with exponential growth

Parallel or distributed computing

- Need to distribute over
  - sensors
  - more cpus or GPU's

Data is not information

- one single port scan can generate:
  - an alarm for each port
  - 65,000+
- This is not useful

Architecture alternatives

- host based
- Each machine on the net screens its own traffic
- detection power grows with network

Management problems

- patching, maintenance
- automatic denials
- high volume of alerts
- large user interaction
  - scalable security == user education
  - need to scale security team (personell)

Snort Architecture

- relies on LibPcap
- available on Windows, Mac and Linux
- not efficient enough for high volume networks
- packets are delivered to pre-processors
  - every packet goes through each one to check for obfuscated attack

Configuration impacts performance

- The more checks the worse the performance
- Snort uses a "first match" to exit and improve
- malicious traffic is routed to an output plugin

Suricata

- 1st release in 2009
- Funded by Navy and Homeland Security
- Non-profit "Open Information Security Foundation"
- Native multi-threading (not in Snort)
- Alert and event filtering limits (not in Snort)
- subnet IP reputation
- CUDA to accelerate pattern recognition

Bro

- scientific environments
- Project of Berkley and Lawrence Livermore
- Based on Bash scripts
- Vern Paxson, 1995
- Event driven not signatures
- Can blacklist an IP or even shut down a host based on event
- Bro's scripting language is called Bro

Snort performance

- Pre 3.0 single process
- Sits on top of libpcap which is also single process
- No built in load balancing
- Changing to AFPackent
- Hard coded small buffer size

How to scale Snort

- LibPcap 1.0
- PFRing high throughput kernel module providing load balancing
- Threaded New API (TNAPI) and a compatible NIC
  - Can get to 10 Gigs per second
  - Custom hardware from 2K USD to 25K USD

Suricata

- native multithreading
- normalizes traffic only once/Snort on a per instance basis
- sent to worker thread for payload inspection
- Snort greater volume with the same accuracy (Elbin and Rowe, 2013)

Suricata captures

- High performance
  - `AF_Packet` or `PF_Ring`
- Standard
  - PCAP or NFlog
- IPS
  - netfilter ipfw
- cards
  - Endace, Napatech and Tilera

Suricata new features

- IP reputation
- multi-threading
- IPv6
- GeoIP Lookup

Performance gains are contested

They've produced a clone of Snort that performs worse at taxpayer's expense. ~ Martin Roesch

Bro

- Script decions to drop, sample, throttle or redirect packets
- Mac, FreeBSD and Linux only
- Steep learning curve

Bro architecture

- supports libpcap and `PF_Ring ZC`
- worker architecture
- no native load balancers but there are commercial add ons (cPacket)
- one core for every 80 Mbps of traffic
- manager recieves notifications and writes alerts

Bro vs Snort

- Bro does not just drop traffic
  - send emails, page staff, terminate a connection
- Snort2Bro can convert Snort and Suricata rules to Bro
- Can act based on commercial services
  - hash registries, Team Cymru's Malware Hash Registry

Overflow

- When processing limits are reached
  - packets are dropped
  - false negatives

Best practice

Defense in depth is the coordinated use of multiple security countermeasures to protect the integrity of the information assets in an enterprise ~ Margret Rouse

- Layer security platforms
- Suricata and Bro for >10 Gps networks

Bro in depth

References

https://www.sans.org/reading-room/whitepapers/intrusion/open-source-ids-high-performance-shootout-35772
https://www.youtube.com/watch?v=ZwrPBEilF9g
http://calhoun.nps.edu/bitstream/handle/10945/36465/Rowe_Finding_Realistic.sequence=1

Created by Evan Misshula.