Toward a Unified Security Testbed and Security Analytics Framework

Ravishankar K. Iyer, Zbigniew T. Kalbarczyk, Adam J. Slagell,
Phuong M. Cao, Eric C. Badger

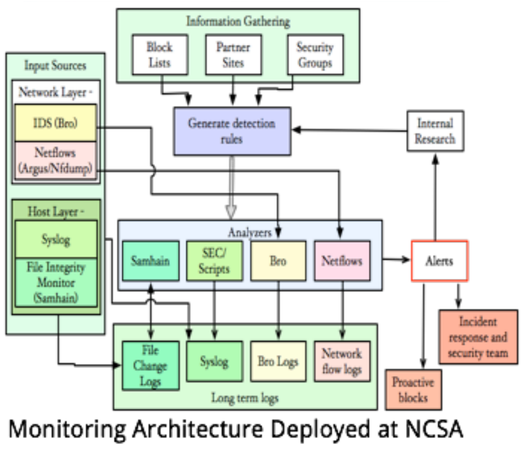
National Center for Supercomputing Applications

NCSA infrastructure servers mission-critical research and simulation

Attackers target NCSA for its powerful computing infrastructure and valuable data

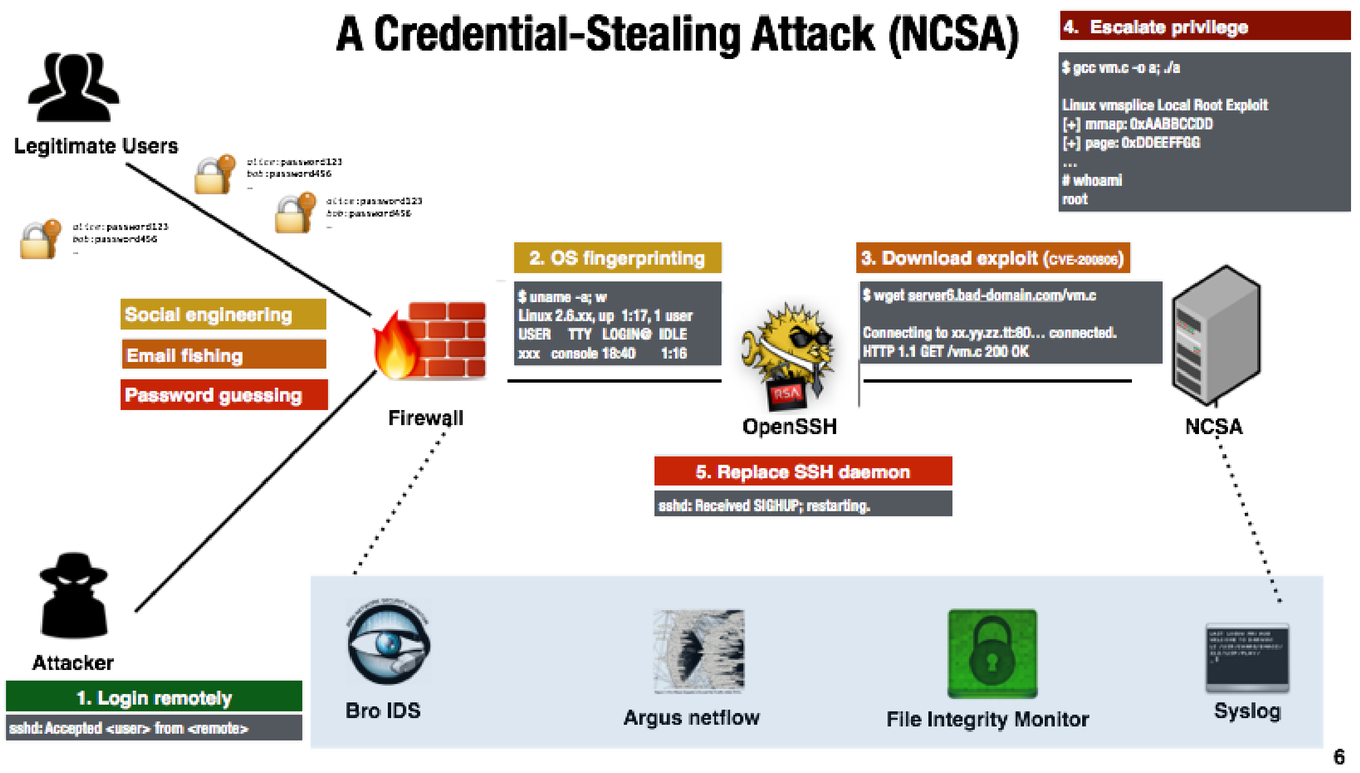
In the past 7 years (2008-2014), more than 160 incidents were observed

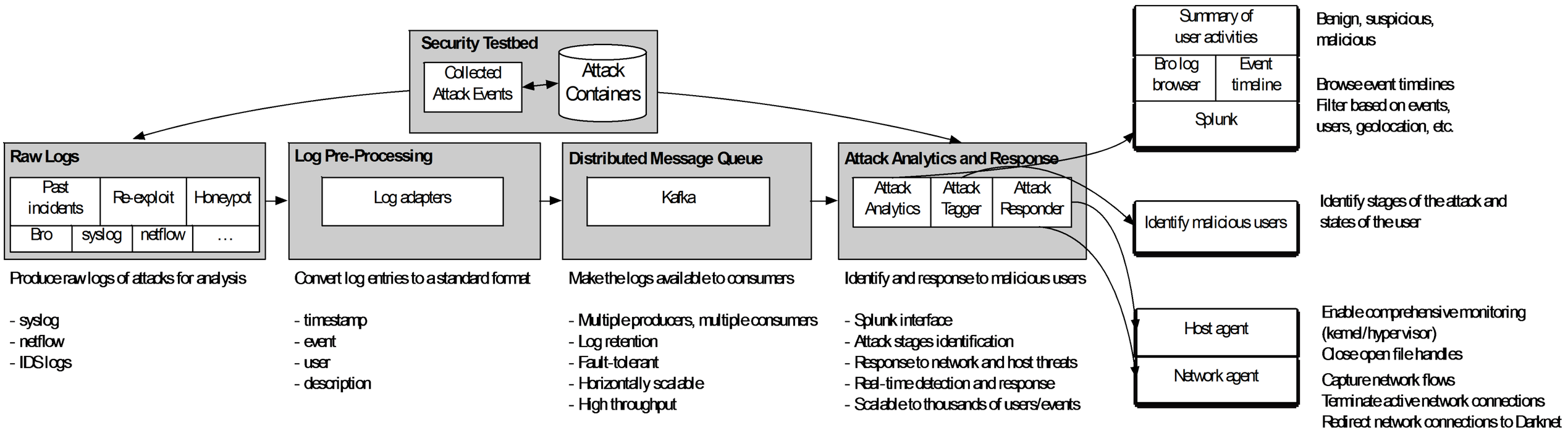
- Brute-force attacks
- Credential compromise
- Application compromise
- Abusing computing infrastructure
  - Send spam
  - Launch Denial of Service attacks.



Monitoring Architecture Deployed at NCSA

A Credential-Stealing Attack (NCSA)





Preliminary Performance Evaluation

Real-time log-aggregation

Kafka can transport logs in real-time and retain the logs in a predefined amount of time for further analysis.

In our prototype, a single Kafka container can ingest up to 45,000 events per second (100 bytes per event).

Our Kafka deployment can comfortably handle Bro notice logs, which is coming in the order of 500 messages per hour.

Real-time attack detection

AttackTagger can process each event in about 600ms. It scales linearly with the number of events because we used Gibbs sampling for approximate inference.

Conclusion and Future Work

What we did

A prototype for real-time security log aggregation and analytics, aimed to preempt intrusions.

An architecture of reproducible security attacks for education purpose and for providing attack data for AttackTagger model

Preliminary performance test showed that our prototype can handle security logs (e.g., Bro notice logs) in real-time.

Future work

Re-architect AttackTagger framework to handle streaming events

Add more types of attacks to our security testbed and call for community contributions.

http://hot-sos.org/

The Science of Security initiative is funded by the National Security Agency.