Flow-based monitoring of honeypots

Martin Husák, Martin Drašar

Institute of Computer Science
Masaryk University
Brno, Czech Republic

24.5.2013

Motivation

Honeypots

- Traps set to detect attacks
- Network traffic is monitored
- Various host-based data are available

How can honeypots help the network security?

- What are the targets of attack?
- What are the intentions of attacker?
- What are the possible counteractions?

Used technologies

Honeypots

- Both high-interaction and low-interaction
- Various services opened – SSH, SMTP, HTTP...
- Gathering of credentials from authentication attempts

NetFlow

- Flow-based network monitoring
- Widely used at Masaryk University
- NetFlow collector NfSen

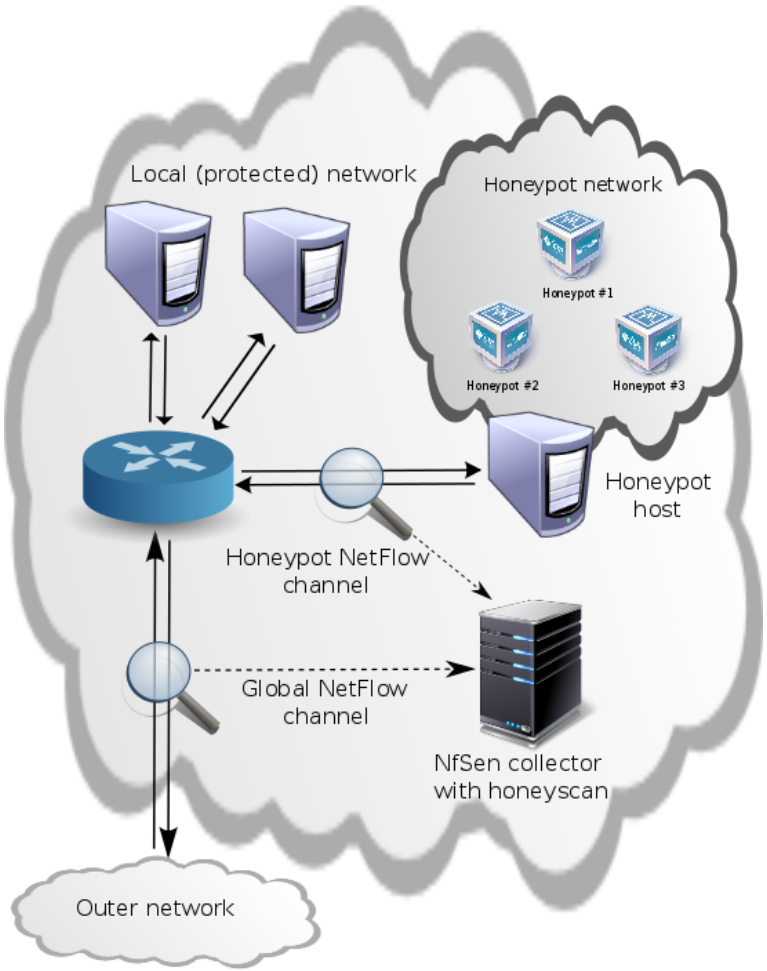
Honeyscan

- Plugin for NfSen
- Monitoring of honeypots
- Incident detection and reporting

Setup

Deployed at Masaryk University

- Up to 320 million flows a day
- 10–20 thousand flows destined to honeypots



Incident detection

Three types of incidents are detected and reported:

- Type 1: Access to honeypots from protected network
- Type 2: Massive access to honeypots and protected network
- Type 3: Authentication attempt against honeypot

Types 2 and 3 are reported only if the attacker has accessed a host in production network apart from honeypots.

Results

In Q1 2013 we have detected and reported:

1,100 security incidents caused by 830 unique IPs

- Type 1: 13, 13 unique IPs
- Type 2: 989, 738 unique IPs
- Type 3: 98, 84 unique IPs

15,749 authentication attempts

- SSH: 10,387
- POP3: 4,719
- FTP: 643

Future work

Network funnel

- Alternative to RTBH (Remotely-Triggered Black Hole)
- Suspicious traffic is routed to honeypot segment

Spam traps

- Mail servers or mail server emulators on honeypots
- Dealing with spam as with the authentication attempts

Conclusions

- Both network-based and host-based data are used for incident detection.
- Incident detection method is complementory to existing tools.
- Tool for network monitoring of honeypots was developed as a plugin for NfSen.
- Plugin Honeyscan is deployed in Masaryk University network.

Q&A

Flow-based monitoring of honeypots

Martin Husák
husakm@ics.muni.cz

Martin Drašar
drasar@ics.muni.cz

Institute of Computer Science
Masaryk University
Brno, Czech Republic

References

NfSen – NetFlow Sensor, http://nfsen.sourceforge.net/

CSIRT-MU, http://www.muni.cz/csirt

Honeyscan – honeypot monitoring plugin,
http://www.muni.cz/ics/services/csirt/tools/honeyscan