Flow-based SSH Compromise Detection

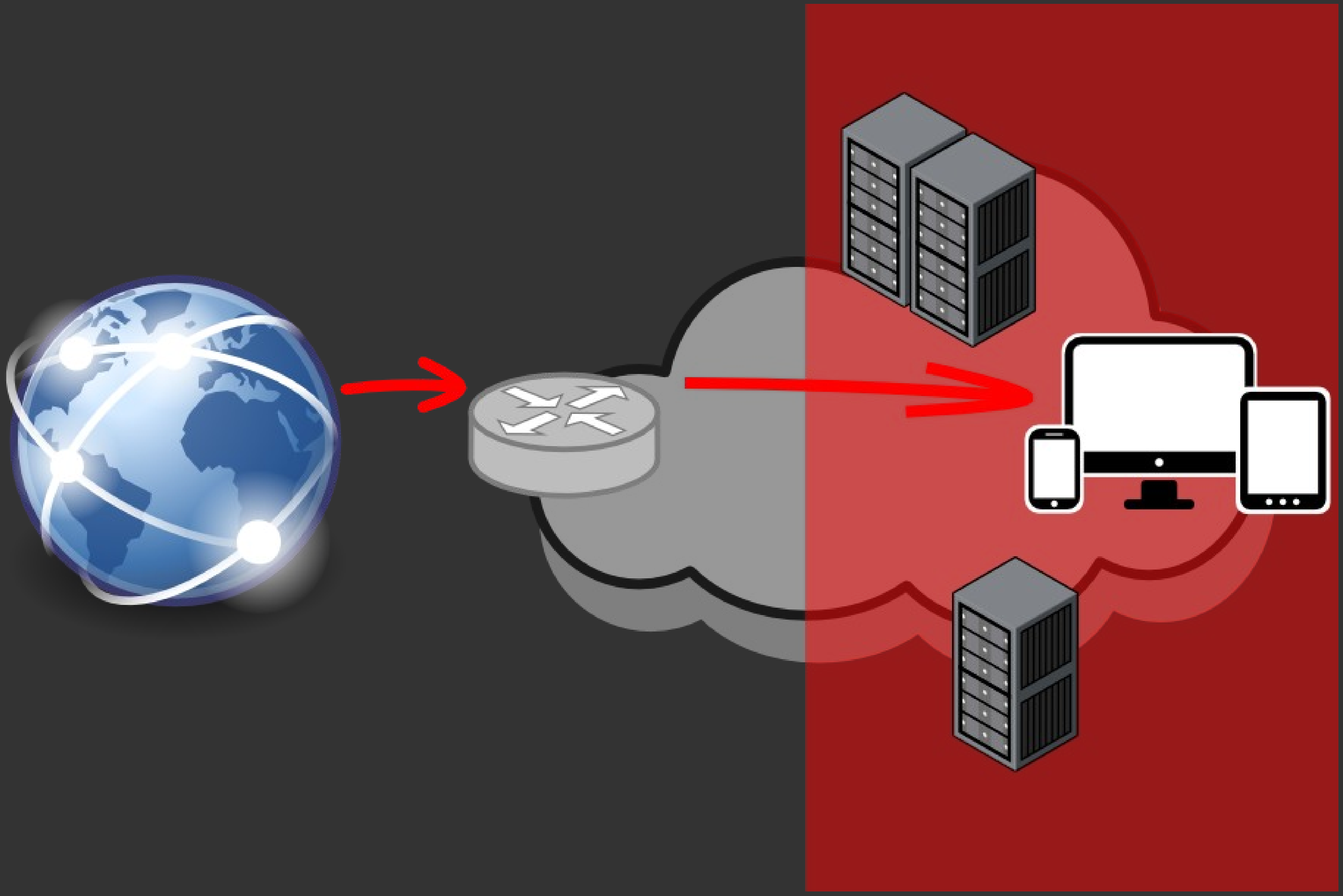
RIPE69 - London

Luuk Hendriks
Design and Analysis of Communication Systems

UNIVERSITY OF TWENTE.

Conventional SSH intrusion detection relies on **end-hosts**

Detection capabilities are limited, **overloading operators**



On our campus network, we see
100 attacks a day

A backbone network can easily reach
1000 attacks a day

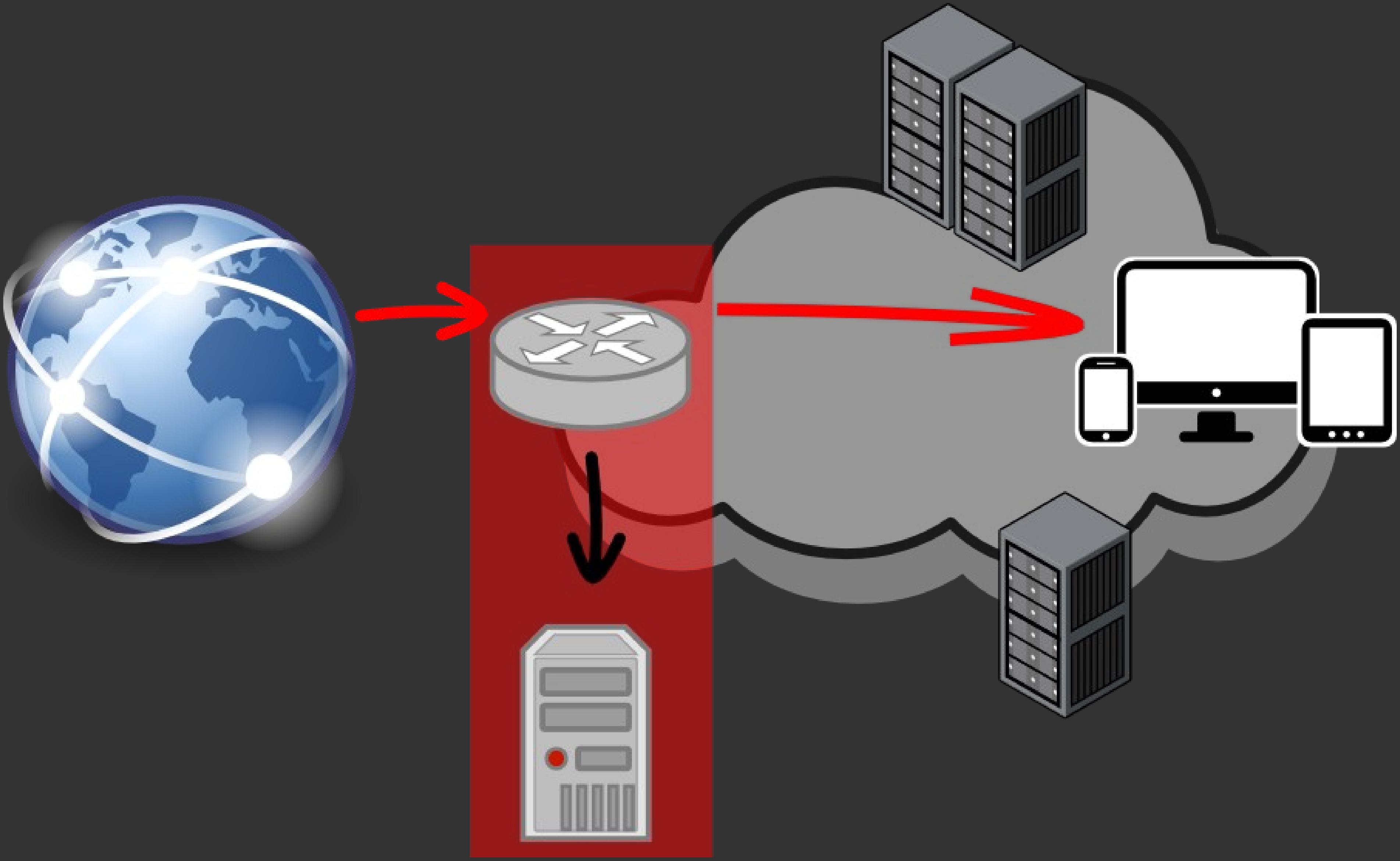
Proper detection:

- is needed
- will drive network operators nuts

Our flow-based approach enables to

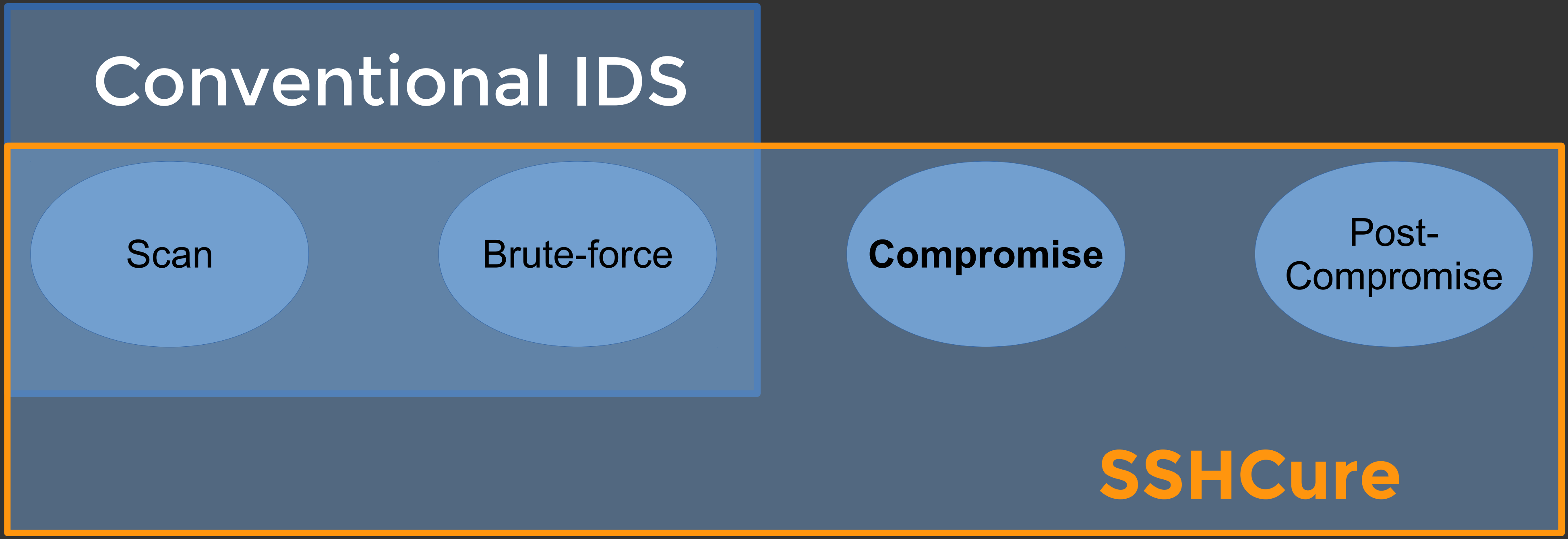
cover an entire network

making it scalable and easy to deploy



Conventional intrusion detection systems detect attacks

We do **compromise detection**
All flow-based



Conventional IDS

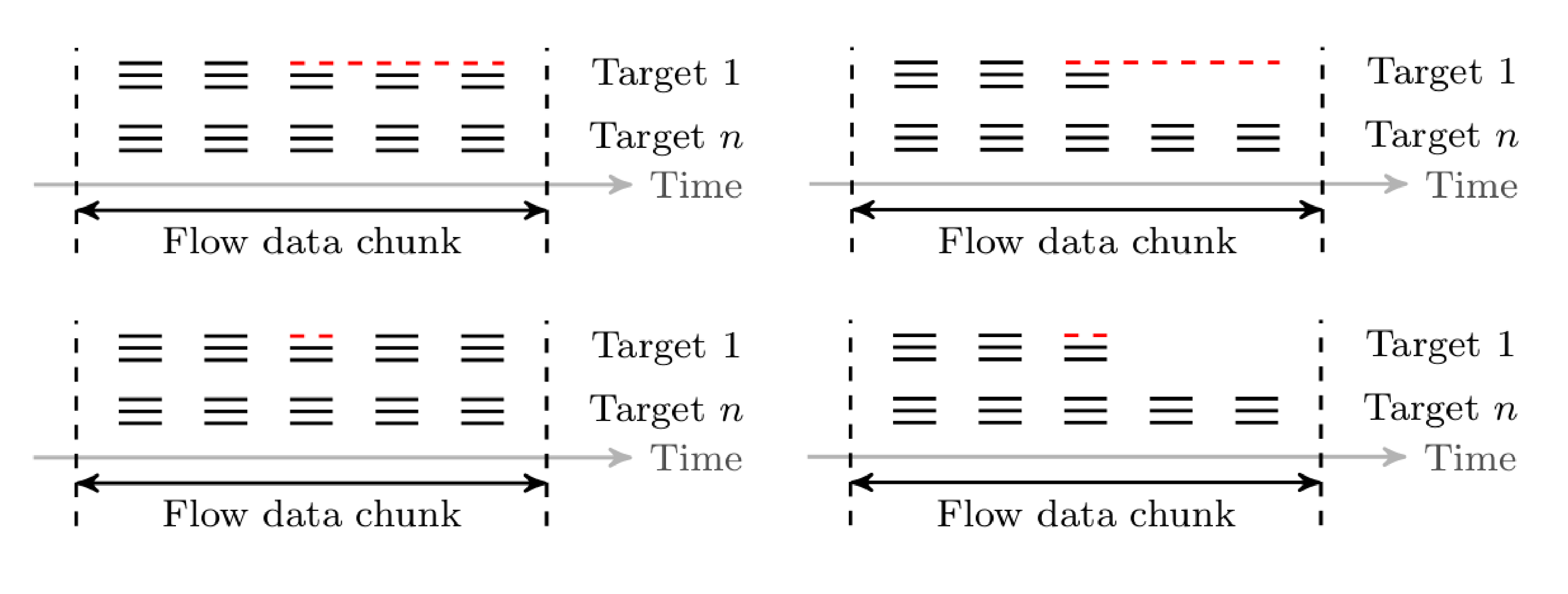
Scan

Brute-force

Compromise

Post-Compromise

SSHCure



“SSH Compromise Detection using NetFlow/IPFIX”

R. Hofstede, L. Hendriks, A. Sperotto, A. Pras
In:
ACM SIGCOMM Computer Communication Review
#44, Oktober 2014

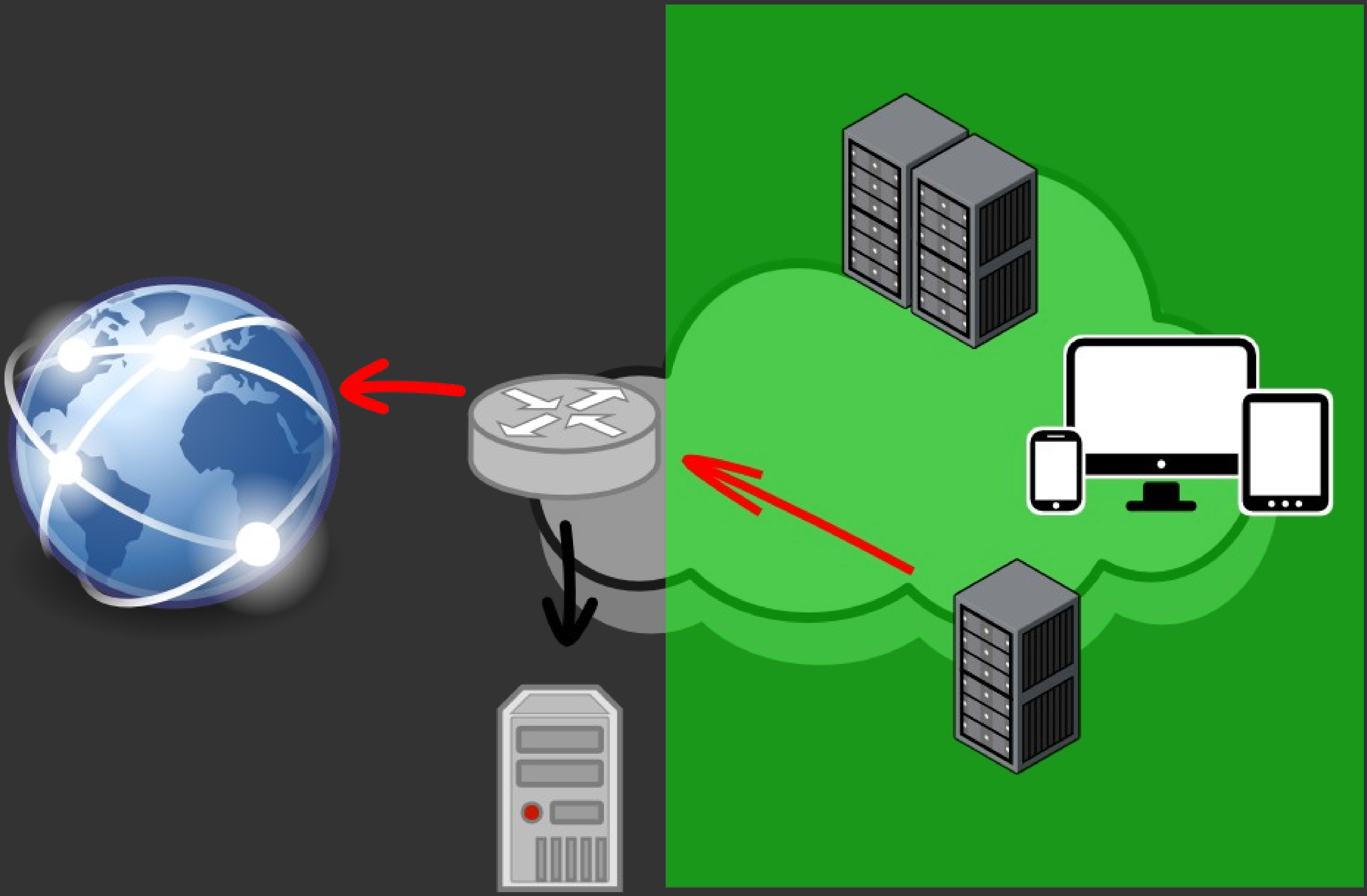
Results show accuracies
close to 100%

Validation done using ~100 machines
(servers, desktops, honeypots)
configured by different adminstrators

Datasets available!
http://www.simpleweb.org/wiki/SSH_datasets

“Our rule no. 1:
it's not about what comes into your network, it's about ***what goes out****.”*

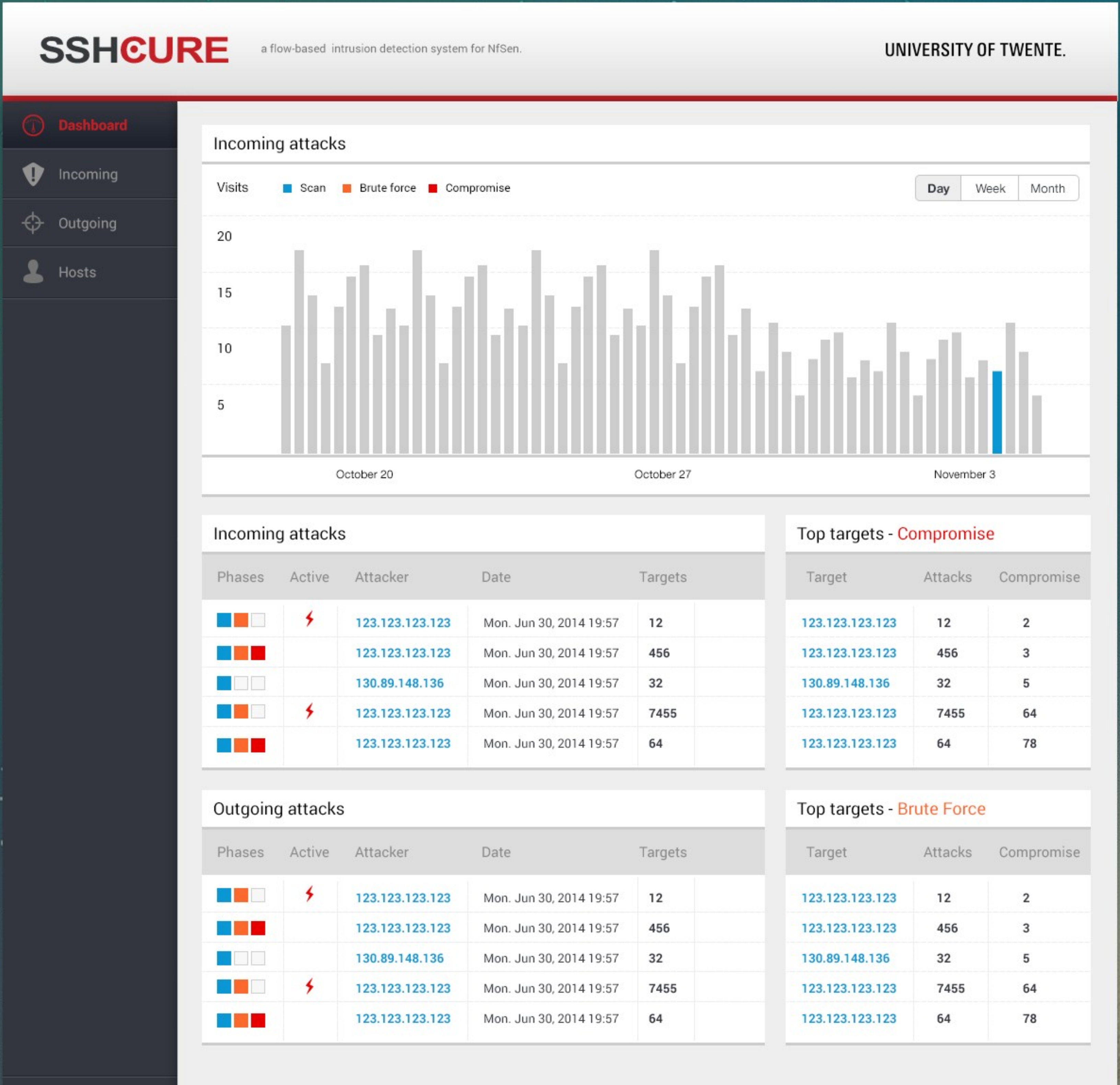
- NREN operator



Summarizing, network-based compromise detection … :

- is possible and **accurate**
- detects attacks **going to** and **coming from** your network
- is scalable and **easy to deploy**

SSHCURE



Incoming attacks

Incoming attacks

Phases	Active	Attacker	Date	Targets
🟦🟧⬜	⚡	123.123.123.123	Mon. Jun 30, 2014 19:57	12
🟦🟧🟥		123.123.123.123	Mon. Jun 30, 2014 19:57	456
🟦⬜⬜		130.89.148.136	Mon. Jun 30, 2014 19:57	32
🟦🟧⬜	⚡	123.123.123.123	Mon. Jun 30, 2014 19:57	7455
🟦🟧🟥		123.123.123.123	Mon. Jun 30, 2014 19:57	64

Top targets - Compromise

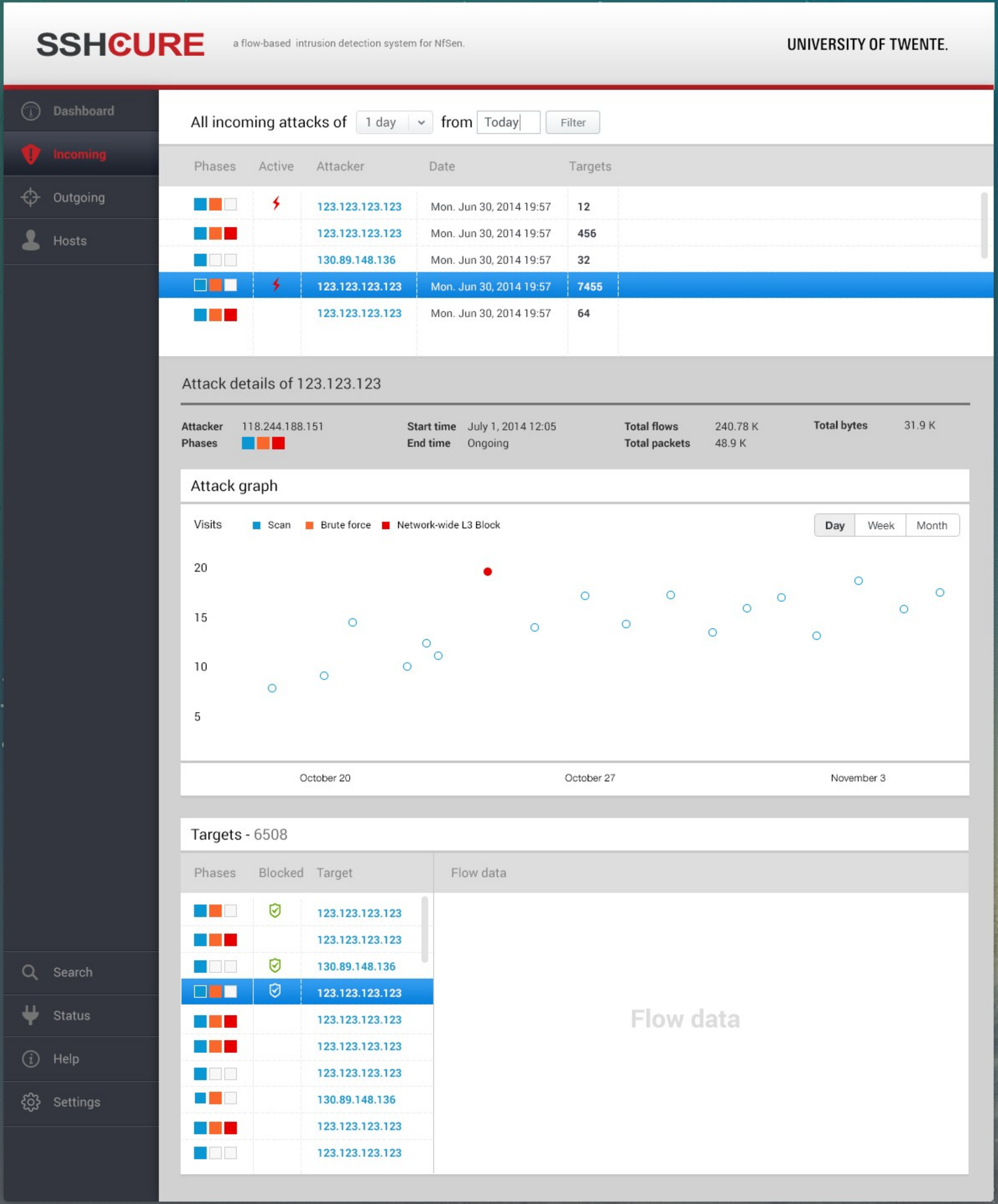
Target	Attacks	Compromise
123.123.123.123	12	2
123.123.123.123	456	3
130.89.148.136	32	5
123.123.123.123	7455	64
123.123.123.123	64	78

Outgoing attacks

Phases	Active	Attacker	Date	Targets
🟦🟧⬜	⚡	123.123.123.123	Mon. Jun 30, 2014 19:57	12
🟦🟧🟥		123.123.123.123	Mon. Jun 30, 2014 19:57	456
🟦⬜⬜		130.89.148.136	Mon. Jun 30, 2014 19:57	32
🟦🟧⬜	⚡	123.123.123.123	Mon. Jun 30, 2014 19:57	7455
🟦🟧🟥		123.123.123.123	Mon. Jun 30, 2014 19:57	64

Top targets - Brute Force

Target	Attacks	Compromise
123.123.123.123	12	2
123.123.123.123	456	3
130.89.148.136	32	5
123.123.123.123	7455	64
123.123.123.123	64	78



SSHCURE a flow-based intrusion detection system for NfSen.

UNIVERSITY OF TWENTE.

All incoming attacks of 1 day from Today Filter

Phases	Active	Attacker	Date	Targets
🟦🟧⬜	⚡	123.123.123.123	Mon. Jun 30, 2014 19:57	12
🟦🟧🟥		123.123.123.123	Mon. Jun 30, 2014 19:57	456
🟦⬜⬜		130.89.148.136	Mon. Jun 30, 2014 19:57	32
⬜🟧⬜	⚡	123.123.123.123	Mon. Jun 30, 2014 19:57	7455
🟦🟧🟥		123.123.123.123	Mon. Jun 30, 2014 19:57	64

Attack details of 123.123.123

Attacker	118.244.188.151	Start time	July 1, 2014 12:05	Total flows	240.78 K	Total bytes	31.9 K
Phases	🟦🟧🟥	End time	Ongoing	Total packets	48.9 K		

Attack graph

Targets - 6508

Phases	Blocked	Target
🟦🟧⬜	🛡	123.123.123.123
🟦🟧🟥		123.123.123.123
🟦⬜⬜	🛡	130.89.148.136
⬜🟧⬜	🛡	123.123.123.123
🟦🟧🟥		123.123.123.123
🟦🟧🟥		123.123.123.123
🟦⬜⬜		123.123.123.123
🟦🟧⬜		130.89.148.136
🟦🟧🟥		123.123.123.123
🟦⬜⬜		123.123.123.123

Flow data

Flow data

- NfSen plugin
- Guided installation
- *nix and BSD
- Ongoing development and support

http://github.com/sshcure

3.0 release Very Soon™ !

Flow-based
SSH Compromise Detection

As presented at RIPE69, London

Luuk Hendriks
luuk.hendriks@utwente.nl
IRC/GitHub: DRiKE (#sshcure on freenode)