Luuk Hendriks
B.Sc. Computer Science
M.Sc. Telematics (April 2014)

Now: Ph.D. student at DACS

(Graduation) project: SSHCure

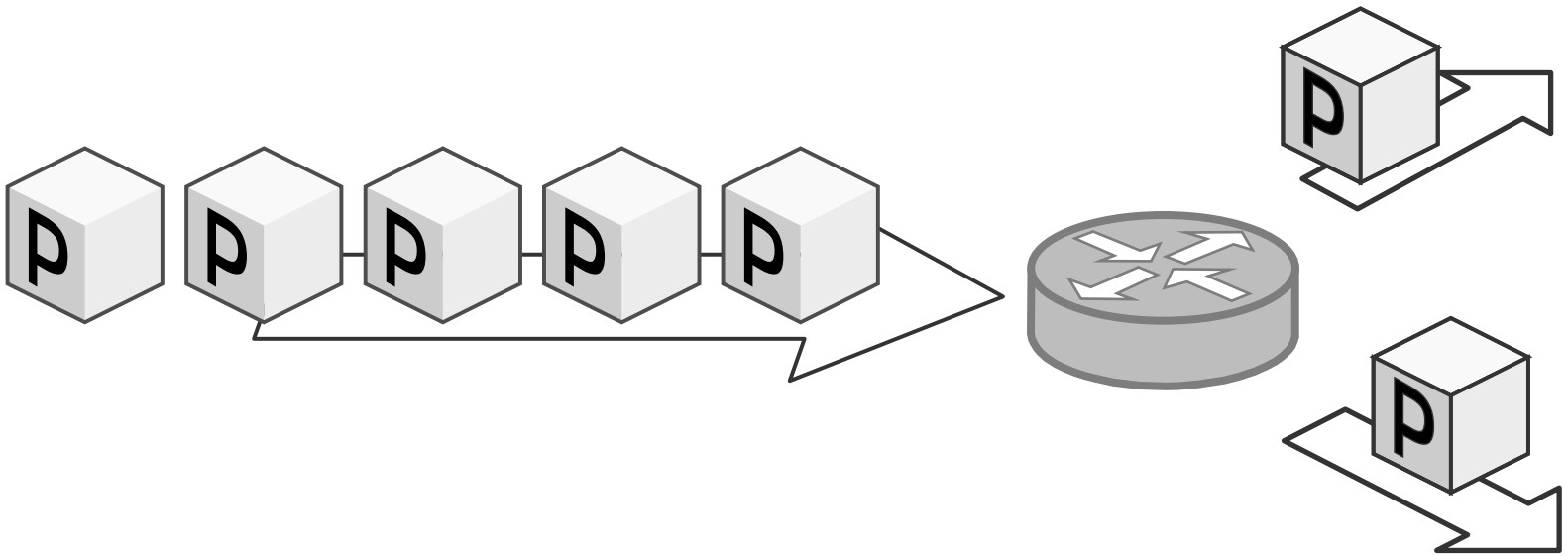
SSH Intrusion Detection

Detection based on three phases:
scan, brute-force, compromise

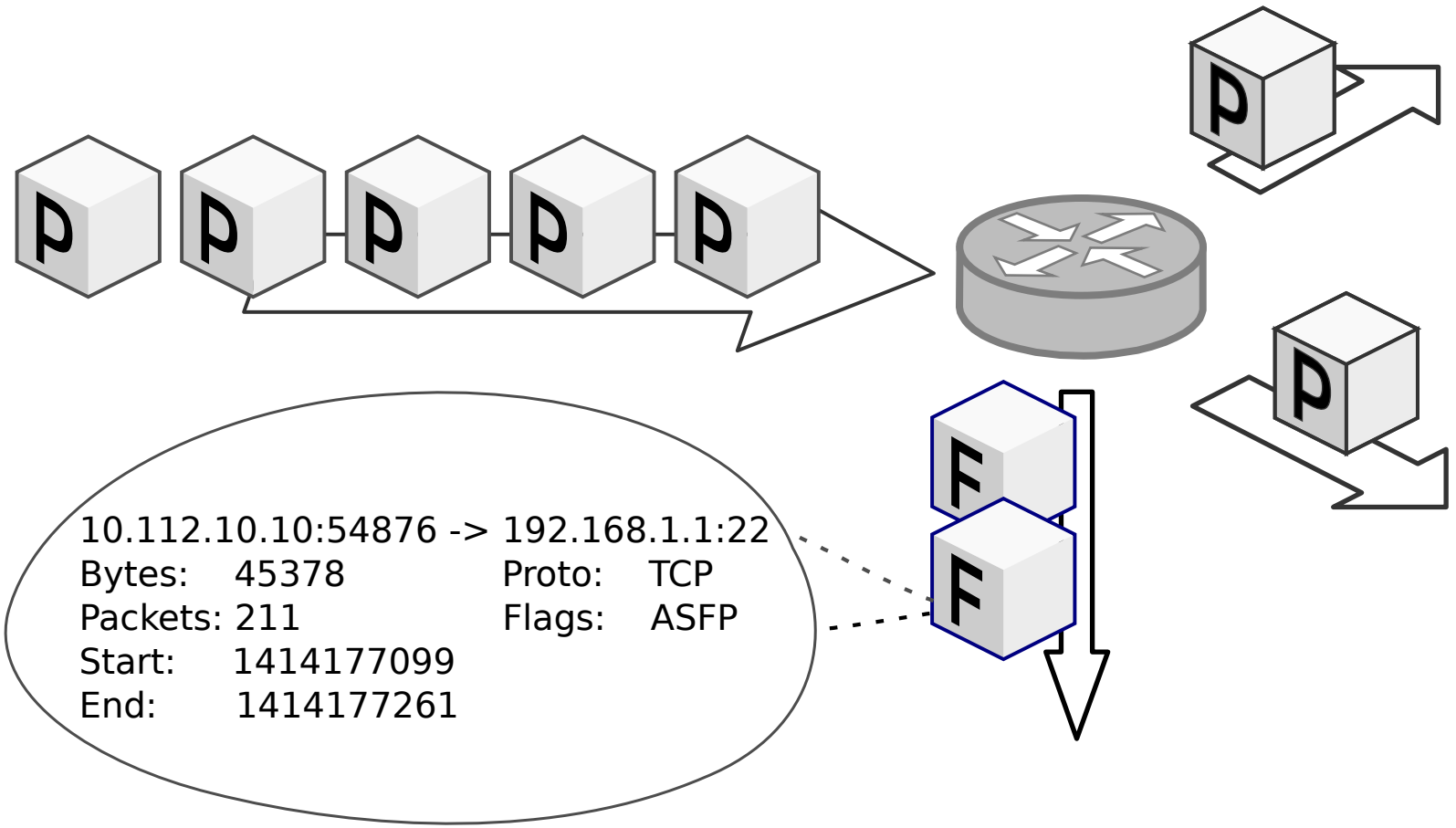
Network-level information for scalability

Behavioral analysis of **attack tools** in terms of **flows**

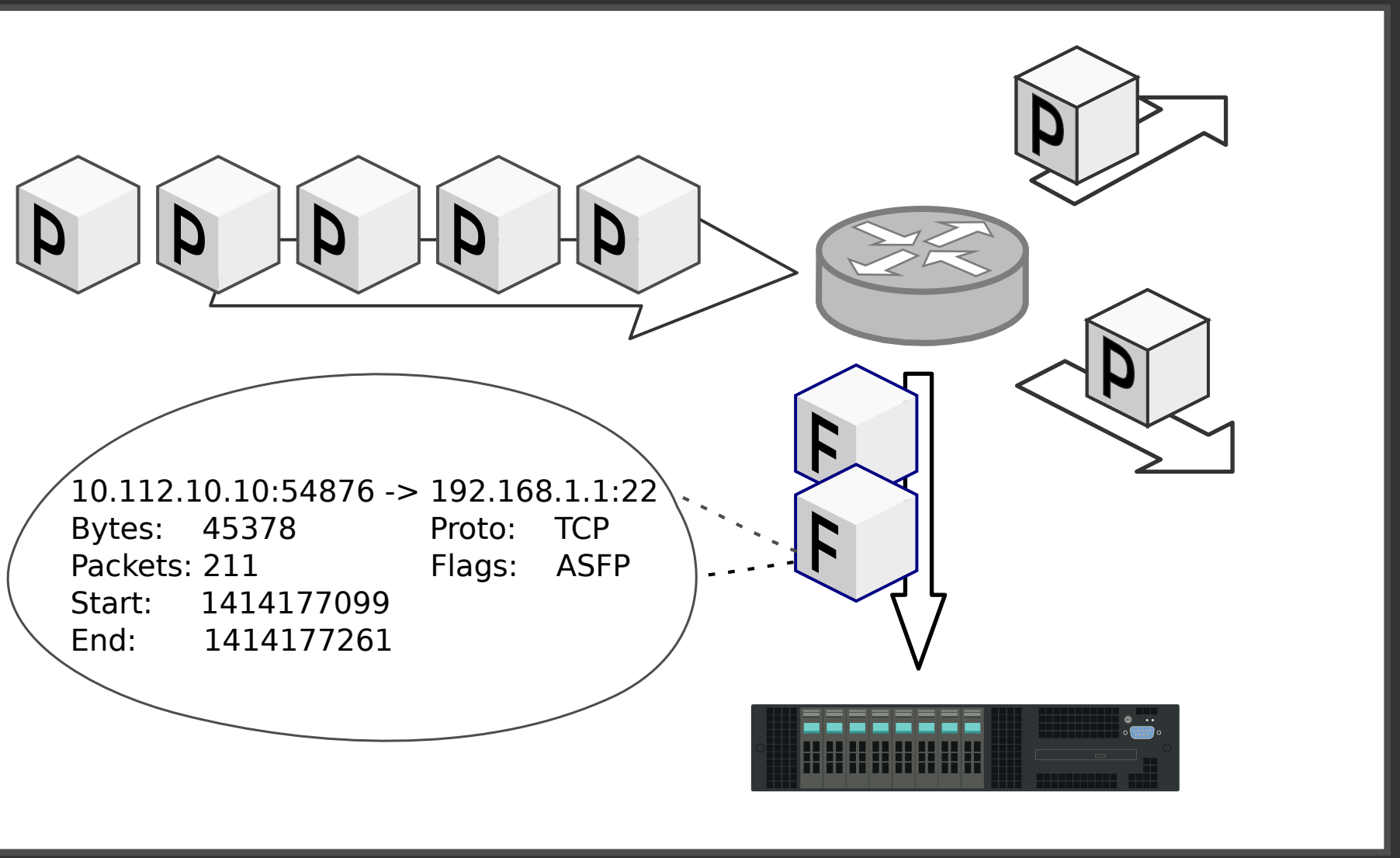
(Net)Flow 101



(Net)Flow 101

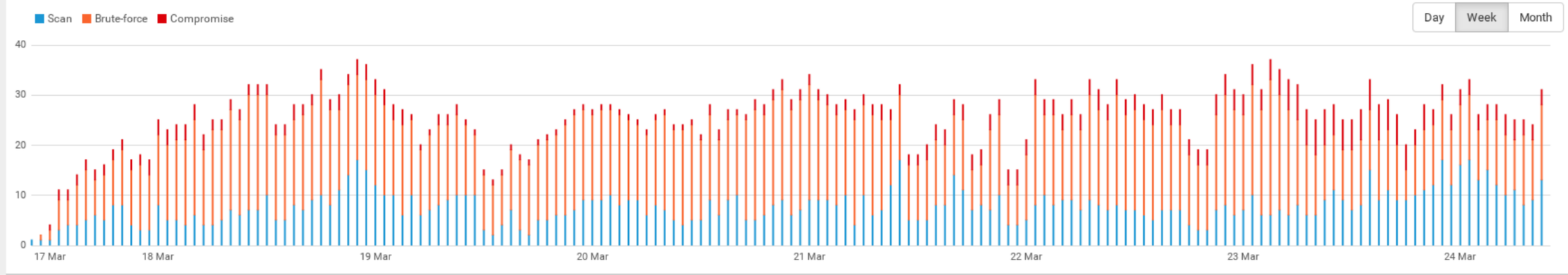

P
P
P
P
P
P
P
F
F
10.112.10.10:54876 -> 192.168.1.1:22
Bytes: 45378 Proto: TCP
Packets: 211 Flags: ASFP
Start: 1414177099
End: 1414177261

(Net)Flow 101


10.112.10.10:54876 -> 192.168.1.1:22
Bytes: 45378
Proto: TCP
Packets: 211
Flags: ASFP
Start: 1414177099
End: 1414177261

Dashboard
Incoming
Outgoing

Attacks



Incoming attacks

Phases	Active	Attacker	Start time	Targets
		[redacted]	Tue. Mar 24, 2015 05:00	177
		[redacted]	Mon. Mar 23, 2015 20:58	149
		[redacted]	Mon. Mar 23, 2015 01:10	181
		[redacted]	Sun. Mar 22, 2015 17:01	178
		[redacted]	Sun. Mar 22, 2015 11:08	187

Top targets - Compromise

Target	Attacks	Compromises
[redacted]	317	11
[redacted]	273	9
[redacted]	186	7
[redacted]	266	6
[redacted]	285	5

Outgoing attacks

Phases	Active	Attacker	Start time	Targets
		[redacted]	Tue. Mar 24, 2015 00:10	1
		[redacted]	Mon. Mar 23, 2015 13:51	1
		[redacted]	Mon. Mar 23, 2015 12:29	1
		[redacted]	Mon. Mar 23, 2015 10:01	1
		[redacted]	Mon. Mar 23, 2015 01:41	1

Top targets - Brute-force

Target	Attacks	Compromises
[redacted]	461	6
[redacted]	451	325
[redacted]	445	322
[redacted]	429	322
[redacted]	427	322

Search
Status
About

SSHCURE Flow-based intrusion detection for SSH

UNIVERSITY OF TWENTE.

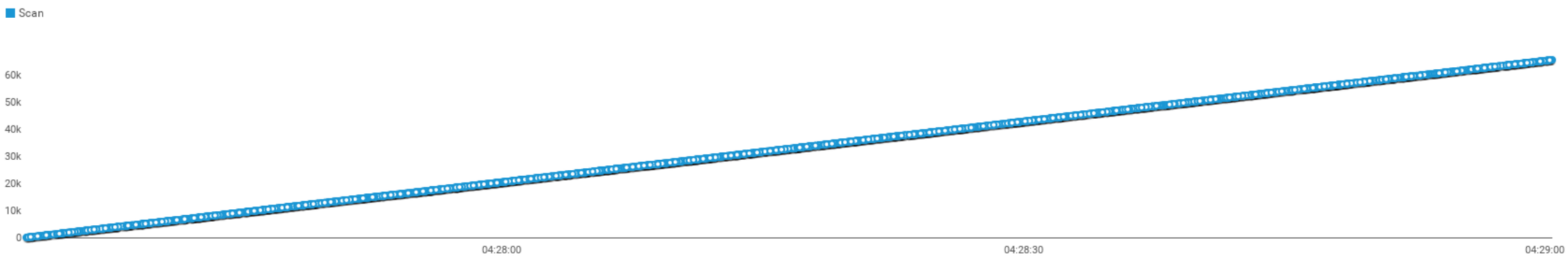
- Dashboard
- Incoming
- Outgoing
- Search
- Status
- About

Incoming attacks

Phases	Active	Attacker	Start time	Targets
			Tue. Mar 24, 2015 04:31	97
			Tue. Mar 24, 2015 04:27	65531
			Tue. Mar 24, 2015 04:26	57085
			Tue. Mar 24, 2015 04:25	195
			Tue. Mar 24, 2015 04:25	22

Attack details of

Attacker
Phases
Start time Tue. Mar 24, 2015 03:27
End time Tue. Mar 24, 2015 03:29
Blacklisted
Total packets 67.79 K
Total bytes 3.12 M
Total flows 67.01 K



Targets

Phases	Blocked	Target	Flow data
			Select a target from the overview on the left

Dashboard
Incoming
Outgoing

Incoming attacks

Phases	Active	Attacker	Start time	Targets
		[redacted]	Tue. Mar 24, 2015 04:31	97
		[redacted]	Tue. Mar 24, 2015 04:27	65531
		[redacted]	Tue. Mar 24, 2015 04:26	57085
		[redacted]	Tue. Mar 24, 2015 04:25	195
		[redacted]	Tue. Mar 24, 2015 04:25	22

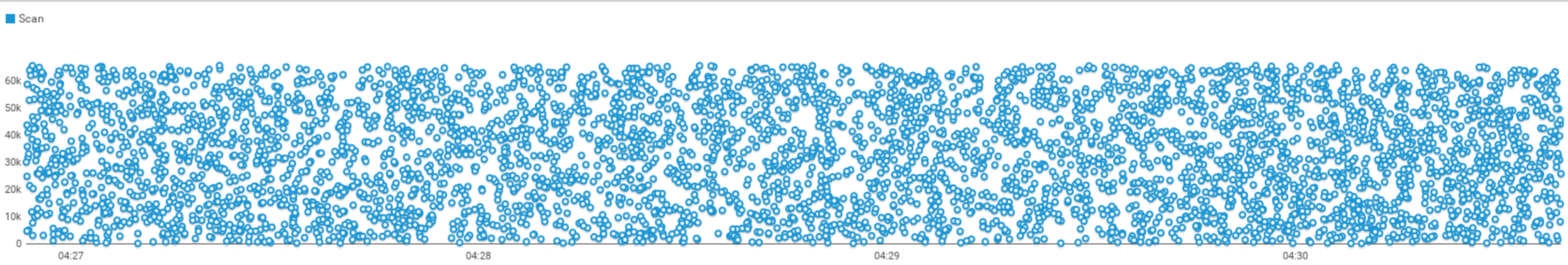
Attack details of [redacted]

Attacker [redacted]
Phases

Start time Tue. Mar 24, 2015 03:26
End time Tue. Mar 24, 2015 03:30

Blacklisted
Total packets 59.03 K

Total bytes 2.72 M
Total flows 58.37 K



Targets

Phases	Blocked	Target	Flow data
[redacted]			

Select a target from the overview on the left

Search
Status
About

SSHCURE Flow-based intrusion detection for SSH

UNIVERSITY OF TWENTE.

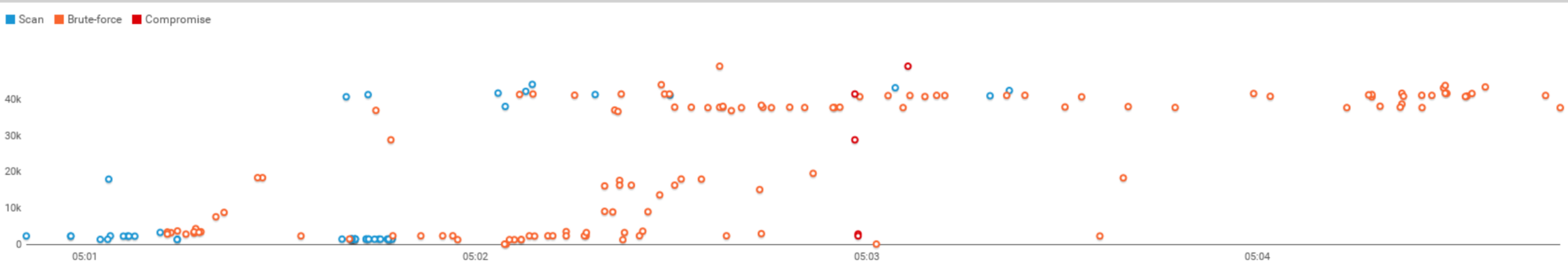
- Dashboard
- Incoming
- Outgoing
- Search
- Status
- About

Incoming attacks

Phases	Active	Attacker	Start time	Targets
■■■		[redacted]	Tue. Mar 24, 2015 05:00	177
■■		[redacted]	Tue. Mar 24, 2015 05:00	4
■■		[redacted]	Tue. Mar 24, 2015 05:00	2
■		[redacted]	Tue. Mar 24, 2015 04:54	218
■		[redacted]	Tue. Mar 24, 2015 04:43	16644

Attack details of [redacted]

Attacker	[redacted]	**Start time**	Tue. Mar 24, 2015 04:00	**Blacklisted**		**Total bytes**	25.88 M
Phases	■■■	**End time**	Tue. Mar 24, 2015 04:04	**Total packets**	191.47 K	**Total flows**	12.25 K



Targets

Phases	Blocked	Target	Flow data
■■■		[redacted]	*Select a target from the overview on the left*
■■		[redacted]	
■■		[redacted]	
■		[redacted]	
■		[redacted]	
■■		[redacted]	
■■		[redacted]	