Articulus

Detecting IP Hijacking Through Server Fingerprinting

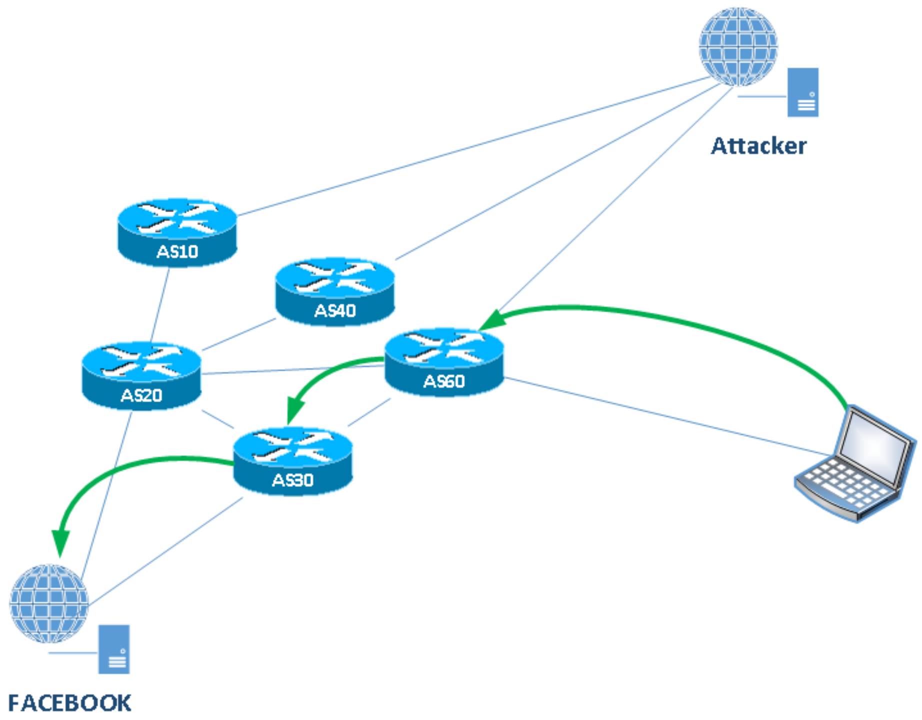
Research Question

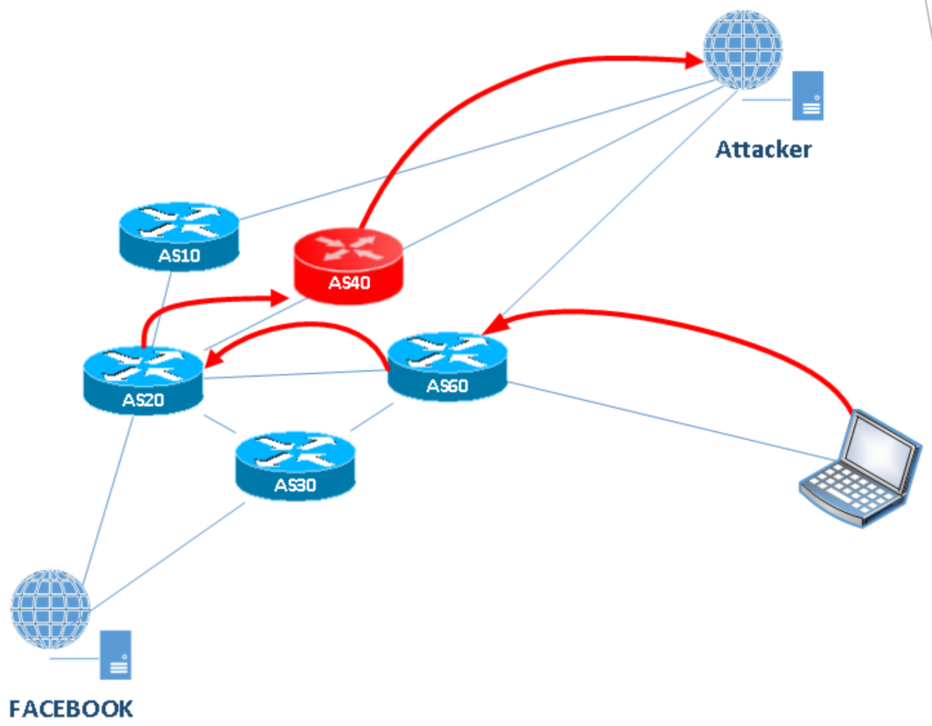
How can we detect BGP IP hijacking by probing the at–risk subnets to detect suspect change to hosts and subnets.

(Slightly) related work

- BGPmon
- Cyclops by UCLA
- Uptrends SSL monitoring
- Unnamed Eric & Mick tool

The problem

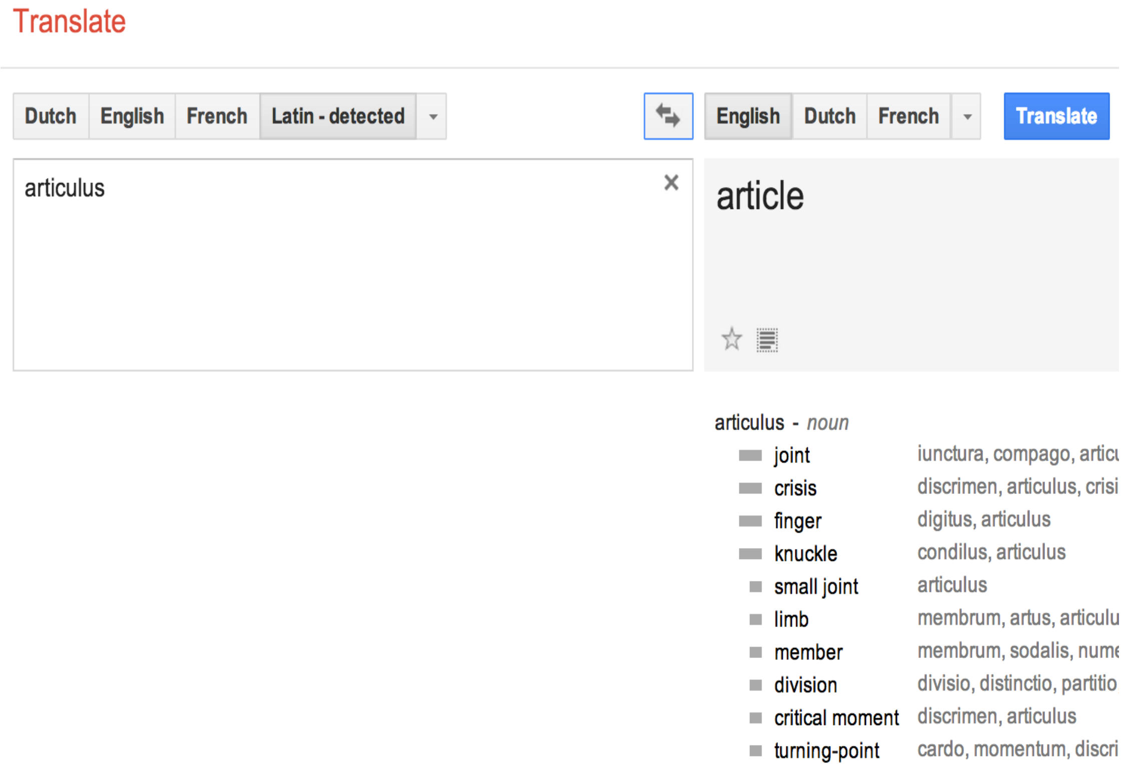

Attacker
AS10
AS40
AS20
AS60
AS30
FACEBOOK


Attacker
AS10
AS40
AS20
AS60
AS30
FACEBOOK

What are the possibilities

- Man-in-the-middle attacks
- Downgrade attacks
- False information

Articulus



articulus

article

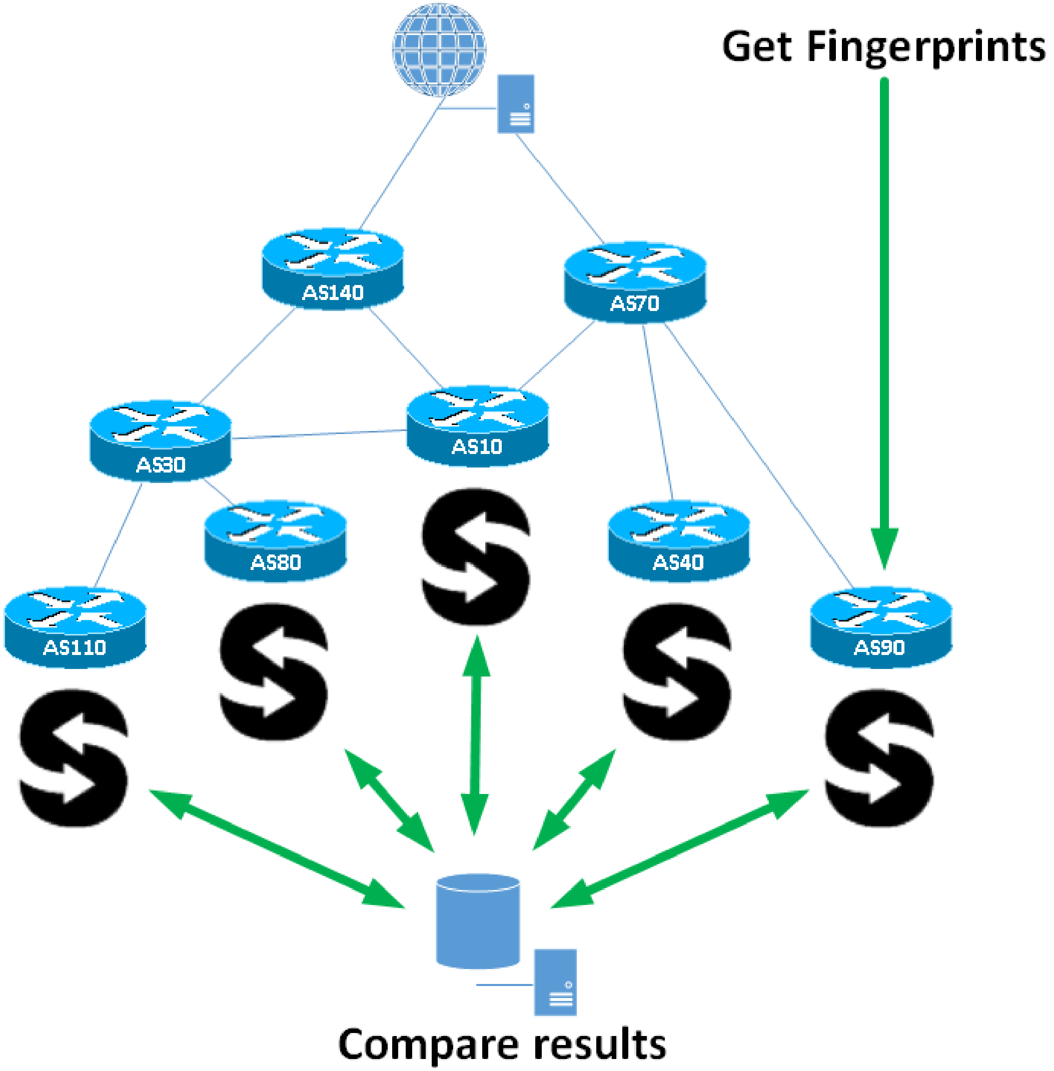
articulus - *noun*

joint	iunctura, compago, articu
crisis	discrimen, articulus, crisi
finger	digitus, articulus
knuckle	condilus, articulus
small joint	articulus
limb	membrum, artus, articulu
member	membrum, sodalis, nume
division	divisio, distinctio, partitio
critical moment	discrimen, articulus
turning-point	cardo, momentum, discri

Terminology

- Sentinel
  - Globally spread out
  - Executes fingers
- Node
  - At-risk host in need of protection
- Server
  - Command & control server
  - Result comparison
- Fingers
  - Commands executed on Sentinels

Our solution



Fingerprinting

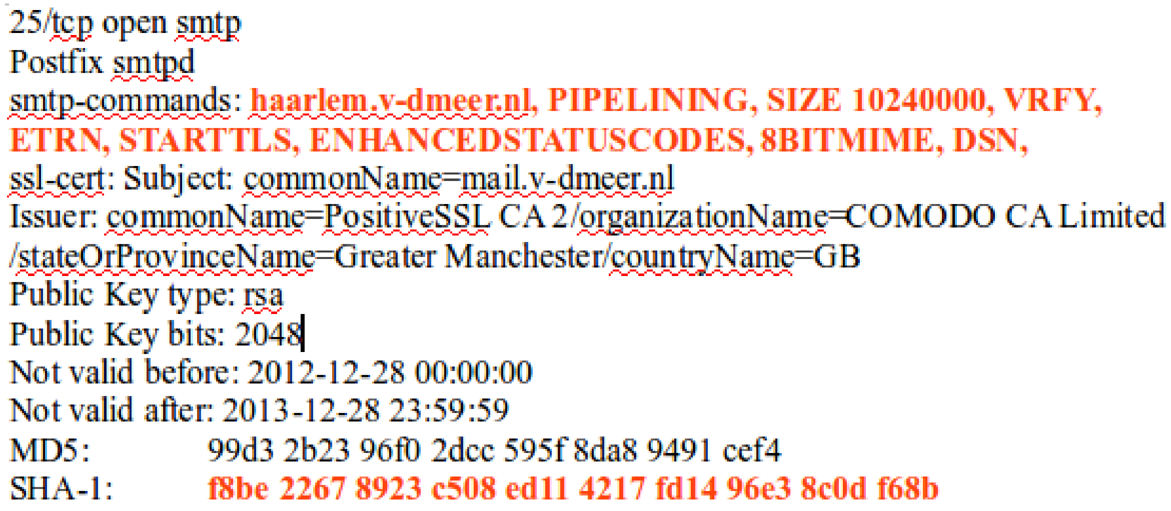
- Identifying software used
- Identifying software version used
- Identifying specific host characteristics

Fingerprinting - DNS

- Response only
- DNS censorship/hijacking detection.

Fingerprinting - Mail services

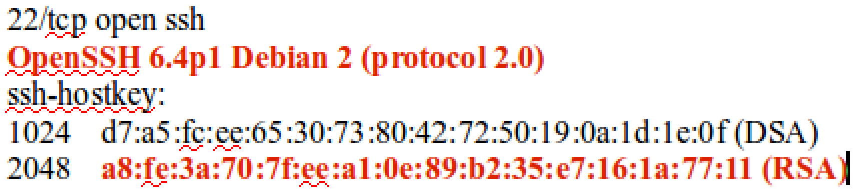
- SMTP / IMAP / POP
- STARTTLS



```
25/tcp open smtp
Postfix smtpd
smtp-commands: haarlem.v-dmeer.nl, PIPELINING, SIZE 10240000, VRFY,
ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
ssl-cert: Subject: commonName=mail.v-dmeer.nl
Issuer: commonName=PositiveSSL CA 2/organizationName=COMODO CA Limited
/stateOrProvinceName=Greater Manchester/countryName=GB
Public Key type: rsa
Public Key bits: 2048
Not valid before: 2012-12-28 00:00:00
Not valid after: 2013-12-28 23:59:59
MD5:         99d3 2b23 96f0 2dcc 595f 8da8 9491 cef4
SHA-1:       f8be 2267 8923 c508 ed11 4217 fd14 96e3 8c0d f68b
```

Fingerprinting – Secure Shell

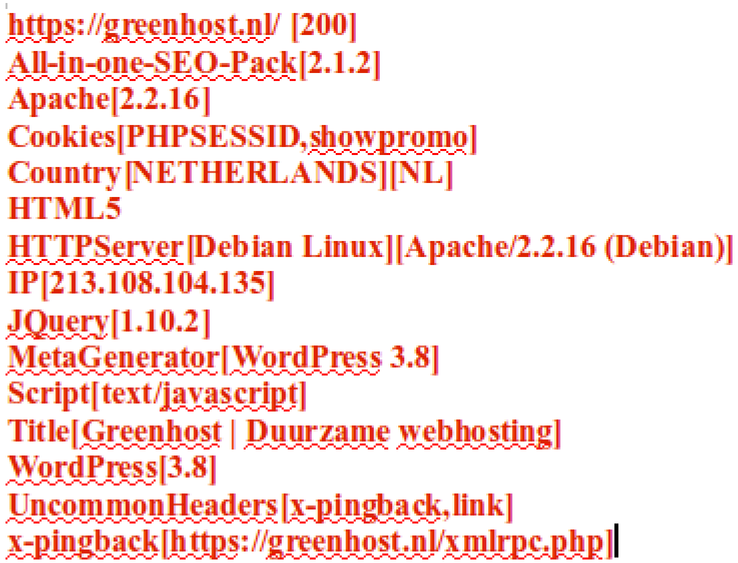
- RSA Fingerprint
- OpenSSH version
- Distribution



```
22/tcp open ssh
OpenSSH 6.4p1 Debian 2 (protocol 2.0)
ssh-hostkey:
1024   d7:a5:fc:ee:65:30:73:80:42:72:50:19:0a:1d:1e:0f (DSA)
2048   a8:fe:3a:70:7f:ee:a1:0e:89:b2:35:e7:16:1a:77:11 (RSA)
```

Fingerprinting - Webservices

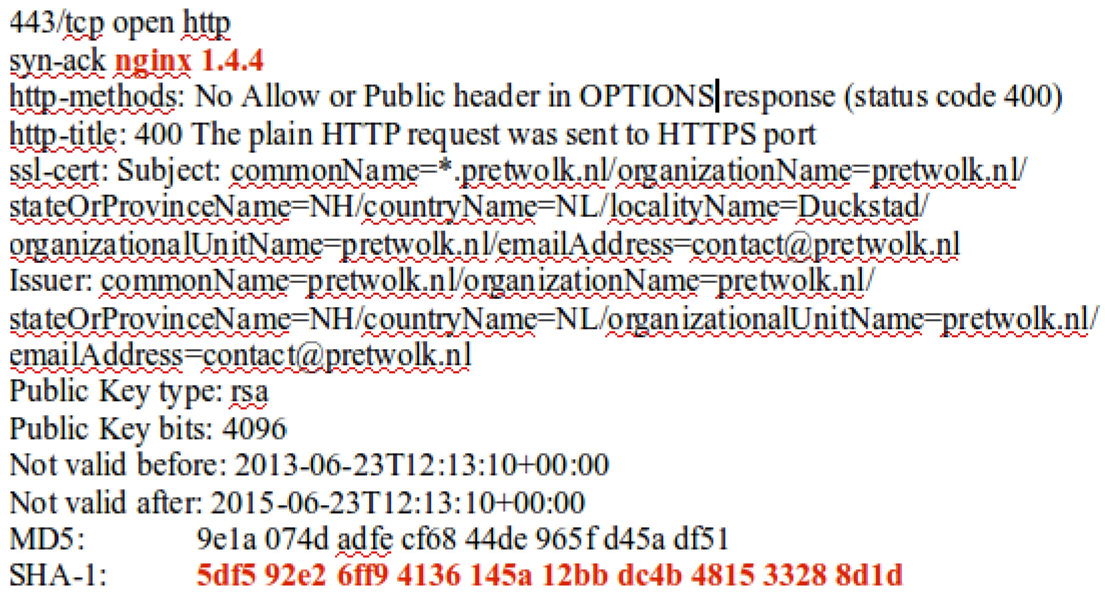
- WordPress 3.8
- Apache 2.2.16
- JQuery 1.10.2



```
https://greenhost.nl/ [200]
All-in-one-SEO-Pack[2.1.2]
Apache[2.2.16]
Cookies[PHPSESSID,showpromo]
Country[NETHERLANDS][NL]
HTML5
HTTPServer[Debian Linux][Apache/2.2.16 (Debian)]
IP[213.108.104.135]
JQuery[1.10.2]
MetaGenerator[WordPress 3.8]
Script[text/javascript]
Title[Greenhost | Duurzame webhosting]
WordPress[3.8]
UncommonHeaders[x-pingback,link]
x-pingback[https://greenhost.nl/xmlrpc.php]
```

Fingerprinting – Sercure Webservices

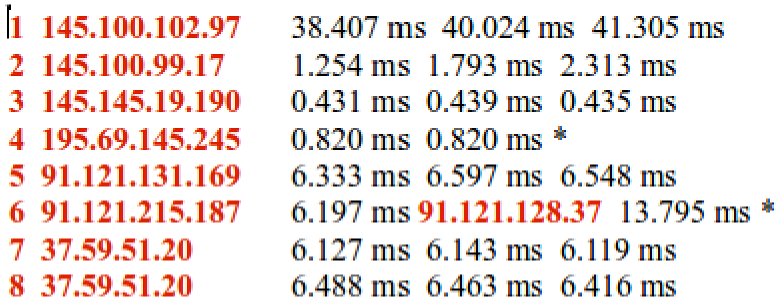
- Nginx 1.4.4
- SHA-1 of certificate



```
443/tcp open http
syn-ack nginx 1.4.4
http-methods: No Allow or Public header in OPTIONS response (status code 400)
http-title: 400 The plain HTTP request was sent to HTTPS port
ssl-cert: Subject: commonName=*.pretwolk.nl/organizationName=pretwolk.nl/
stateOrProvinceName=NH/countryName=NL/localityName=Duckstad/
organizationalUnitName=pretwolk.nl/emailAddress=contact@pretwolk.nl
Issuer: commonName=pretwolk.nl/organizationName=pretwolk.nl/
stateOrProvinceName=NH/countryName=NL/organizationalUnitName=pretwolk.nl/
emailAddress=contact@pretwolk.nl
Public Key type: rsa
Public Key bits: 4096
Not valid before: 2013-06-23T12:13:10+00:00
Not valid after: 2015-06-23T12:13:10+00:00
MD5:        9e1a 074d adfe cf68 44de 965f d45a df51
SHA-1:      5df5 92e2 6ff9 4136 145a 12bb dc4b 4815 3328 8d1d
```

Fingerprinting - Traceroute

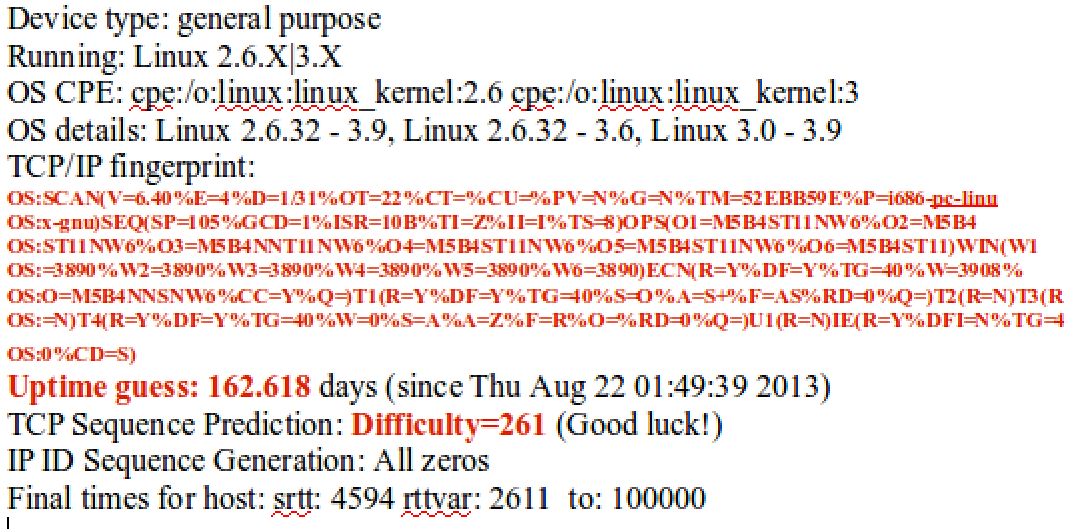
- ICMP / UDP / TCP port 80



```
1  145.100.102.97     38.407 ms  40.024 ms  41.305 ms
2  145.100.99.17      1.254 ms  1.793 ms  2.313 ms
3  145.145.19.190     0.431 ms  0.439 ms  0.435 ms
4  195.69.145.245     0.820 ms  0.820 ms *
5  91.121.131.169     6.333 ms  6.597 ms  6.548 ms
6  91.121.215.187     6.197 ms 91.121.128.37  13.795 ms *
7  37.59.51.20        6.127 ms  6.143 ms  6.119 ms
8  37.59.51.20        6.488 ms  6.463 ms  6.416 ms
```

Fingerprinting – TCP/IP

- Uptime Guess
- TCP characteristics
- TCP Sequence difficulty



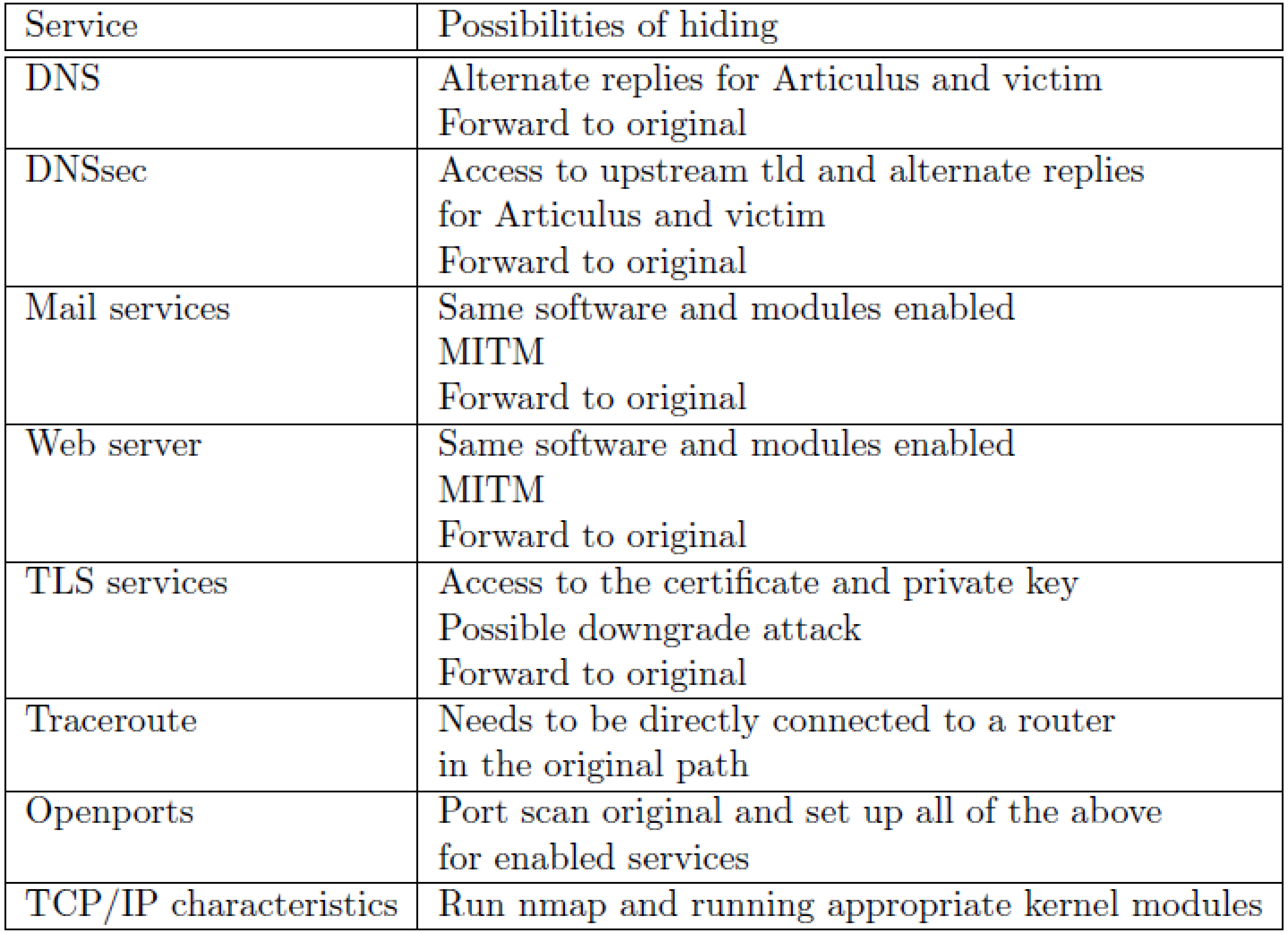
```
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.9, Linux 2.6.32 - 3.6, Linux 3.0 - 3.9
TCP/IP fingerprint:
OS:SCAN(V=6.40%E=4%D=1/31%OT=22%CT=%CU=%PV=N%G=N%TM=52EBB59E%P=i686-pc-linu
OS:x-gnu)SEQ(SP=105%GCD=1%ISR=10B%TI=Z%II=I%TS=8)OPS(O1=M5B4ST11NW6%O2=M5B4
OS:ST11NW6%O3=M5B4NNT11NW6%O4=M5B4ST11NW6%O5=M5B4ST11NW6%O6=M5B4ST11)WIN(W1
OS:=3890%W2=3890%W3=3890%W4=3890%W5=3890%W6=3890)ECN(R=Y%DF=Y%TG=40%W=3908%
OS:O=M5B4NNSNW6%CC=Y%Q=)T1(R=Y%DF=Y%TG=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R
OS:=N)T4(R=Y%DF=Y%TG=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)U1(R=N)IE(R=Y%DFI=N%TG=4

OS:0%CD=S)
Uptime guess: 162.618 days (since Thu Aug 22 01:49:39 2013)
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: All zeros
Final times for host: srtt: 4594 rttvar: 2611  to: 100000
```

Reporting

- Three levels
  - Paranoid
  - System administrator
  - User
- Alerts
  - Email
  - SMS

Fingerprinting – Avoiding detection



Service	Possibilities of hiding
DNS	Alternate replies for Articulus and victim Forward to original
DNSsec	Access to upstream tld and alternate replies for Articulus and victim Forward to original
Mail services	Same software and modules enabled MITM Forward to original
Web server	Same software and modules enabled MITM Forward to original
TLS services	Access to the certificate and private key Possible downgrade attack Forward to original
Traceroute	Needs to be directly connected to a router in the original path
Openports	Port scan original and set up all of the above for enabled services
TCP/IP characteristics	Run nmap and running appropriate kernel modules

Comparing Fingerprints

- All output saved
- RegEx fingerprint
- Compare result to previous result

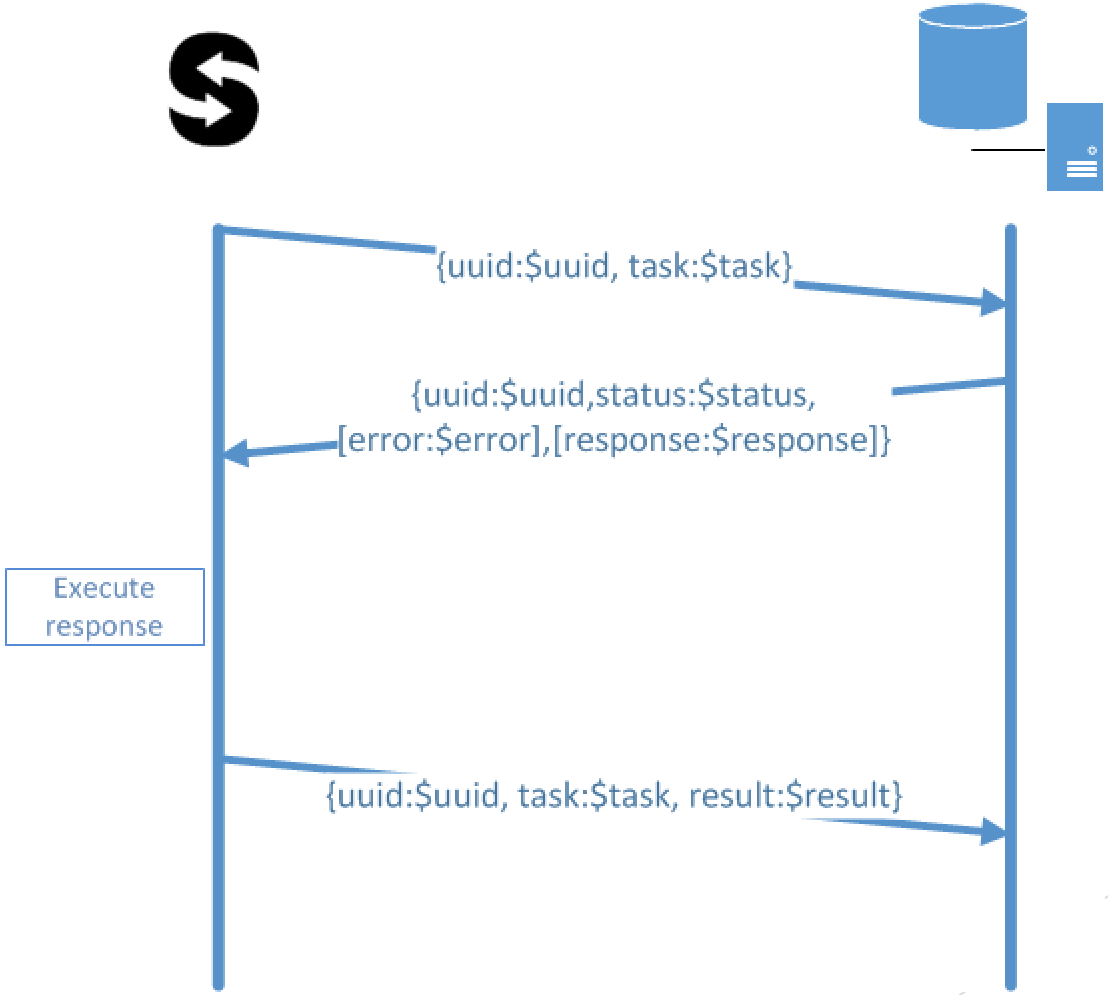
Technical details

- Command and Control server
  - Python API
  - Only works for approved UUID’s
  - HTTPS webserver with Python support (Apache, Nginx, …)
  - MySQL database (MariaDB should work as well)

- Sentinels
  - Python
  - Hardcoded server and certificate (-pinning)
  - POST requests to C&C API
  - Generates UUID
  - Parallel command execution

Technical details

- Secure
- Lightweight
- Scalable


{uuid:$uuid, task:$task}
{uuid:$uuid,status:$status,
[error:$error],[response:$response]}
Execute response
{uuid:$uuid, task:$task, result:$result}

Modular setup

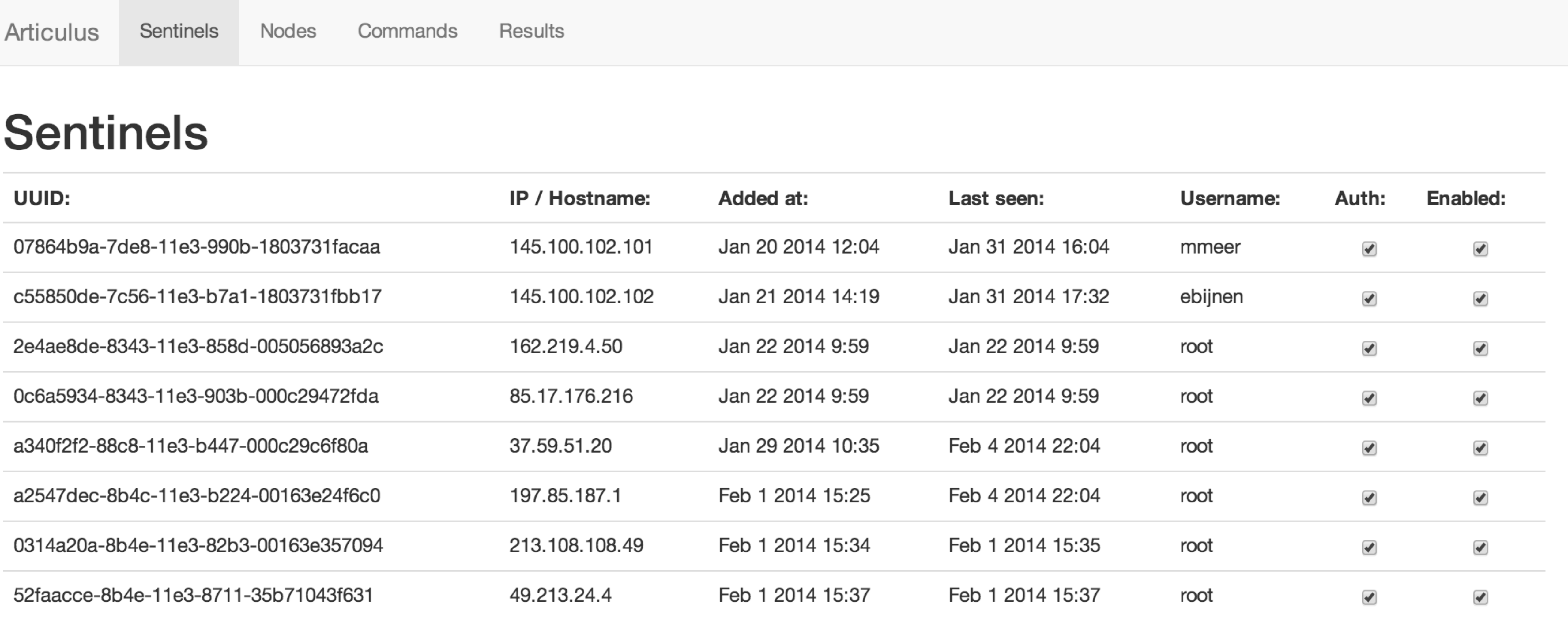
- Add commands for execution on the fly
  - Sentinel needs commands to be installed though
- Add nodes dynamically
- IPv4 and IPv6 support

DEMO

- http://sne.pretwolk.nl:81

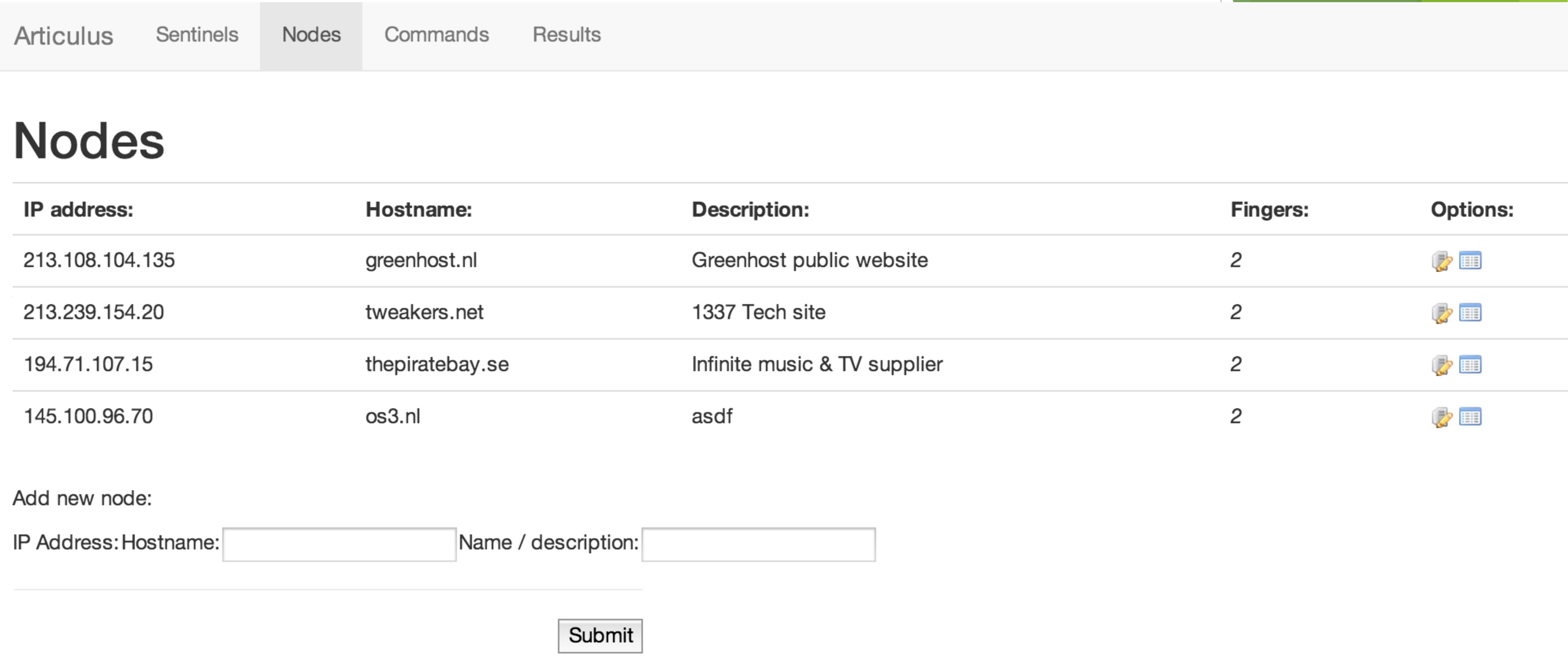
Thank you for your attention

- Are there any questions?



Sentinels

UUID:	IP / Hostname:	Added at:	Last seen:	Username:	Auth:	Enabled:
07864b9a-7de8-11e3-990b-1803731facaa	145.100.102.101	Jan 20 2014 12:04	Jan 31 2014 16:04	mmeer	☑	☑
c55850de-7c56-11e3-b7a1-1803731fbb17	145.100.102.102	Jan 21 2014 14:19	Jan 31 2014 17:32	ebijnen	☑	☑
2e4ae8de-8343-11e3-858d-005056893a2c	162.219.4.50	Jan 22 2014 9:59	Jan 22 2014 9:59	root	☑	☑
0c6a5934-8343-11e3-903b-000c29472fda	85.17.176.216	Jan 22 2014 9:59	Jan 22 2014 9:59	root	☑	☑
a340f2f2-88c8-11e3-b447-000c29c6f80a	37.59.51.20	Jan 29 2014 10:35	Feb 4 2014 22:04	root	☑	☑
a2547dec-8b4c-11e3-b224-00163e24f6c0	197.85.187.1	Feb 1 2014 15:25	Feb 4 2014 22:04	root	☑	☑
0314a20a-8b4e-11e3-82b3-00163e357094	213.108.108.49	Feb 1 2014 15:34	Feb 1 2014 15:35	root	☑	☑
52faacce-8b4e-11e3-8711-35b71043f631	49.213.24.4	Feb 1 2014 15:37	Feb 1 2014 15:37	root	☑	☑

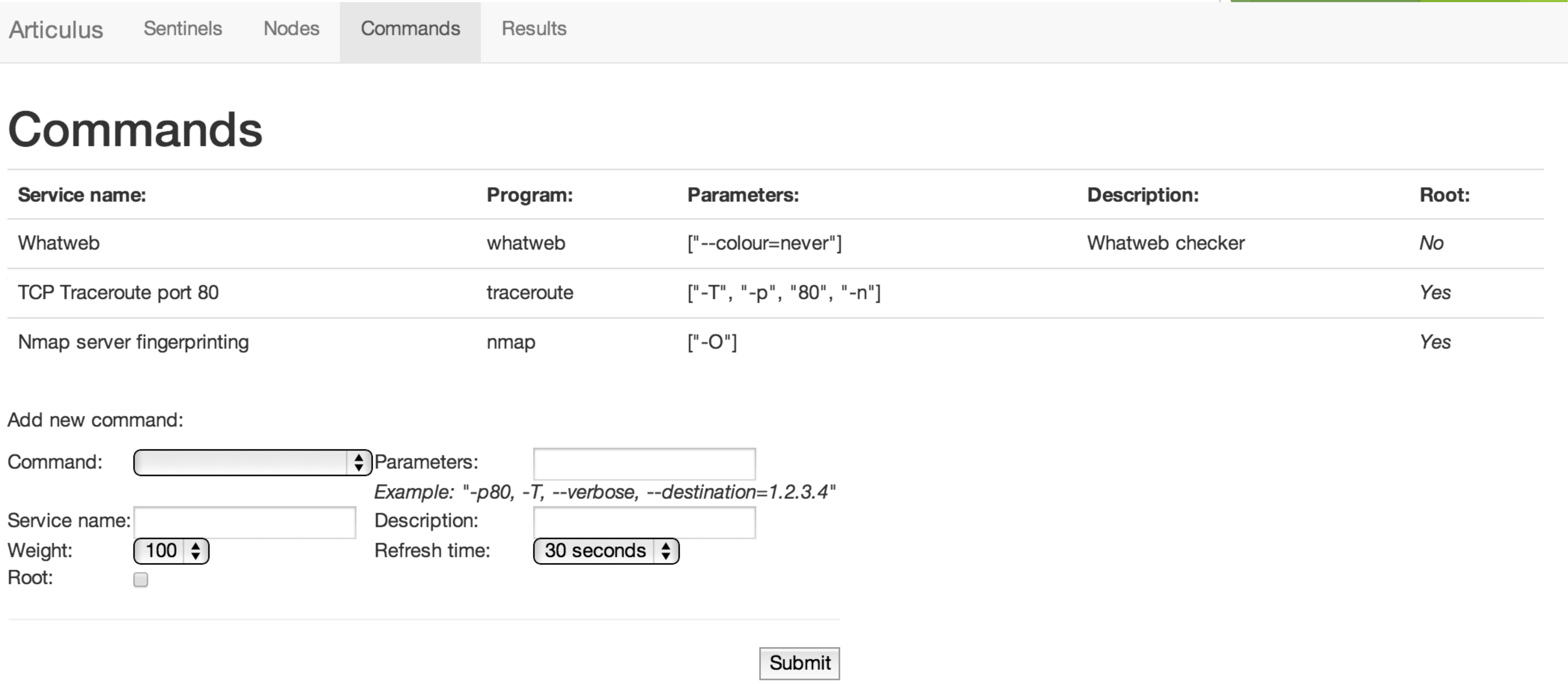


Nodes

IP address:	Hostname:	Description:	Fingers:	Options:
213.108.104.135	greenhost.nl	Greenhost public website	2	✎ ▦
213.239.154.20	tweakers.net	1337 Tech site	2	✎ ▦
194.71.107.15	thepiratebay.se	Infinite music & TV supplier	2	✎ ▦
145.100.96.70	os3.nl	asdf	2	✎ ▦

Add new node:

IP Address: Hostname: □ Name / description: □

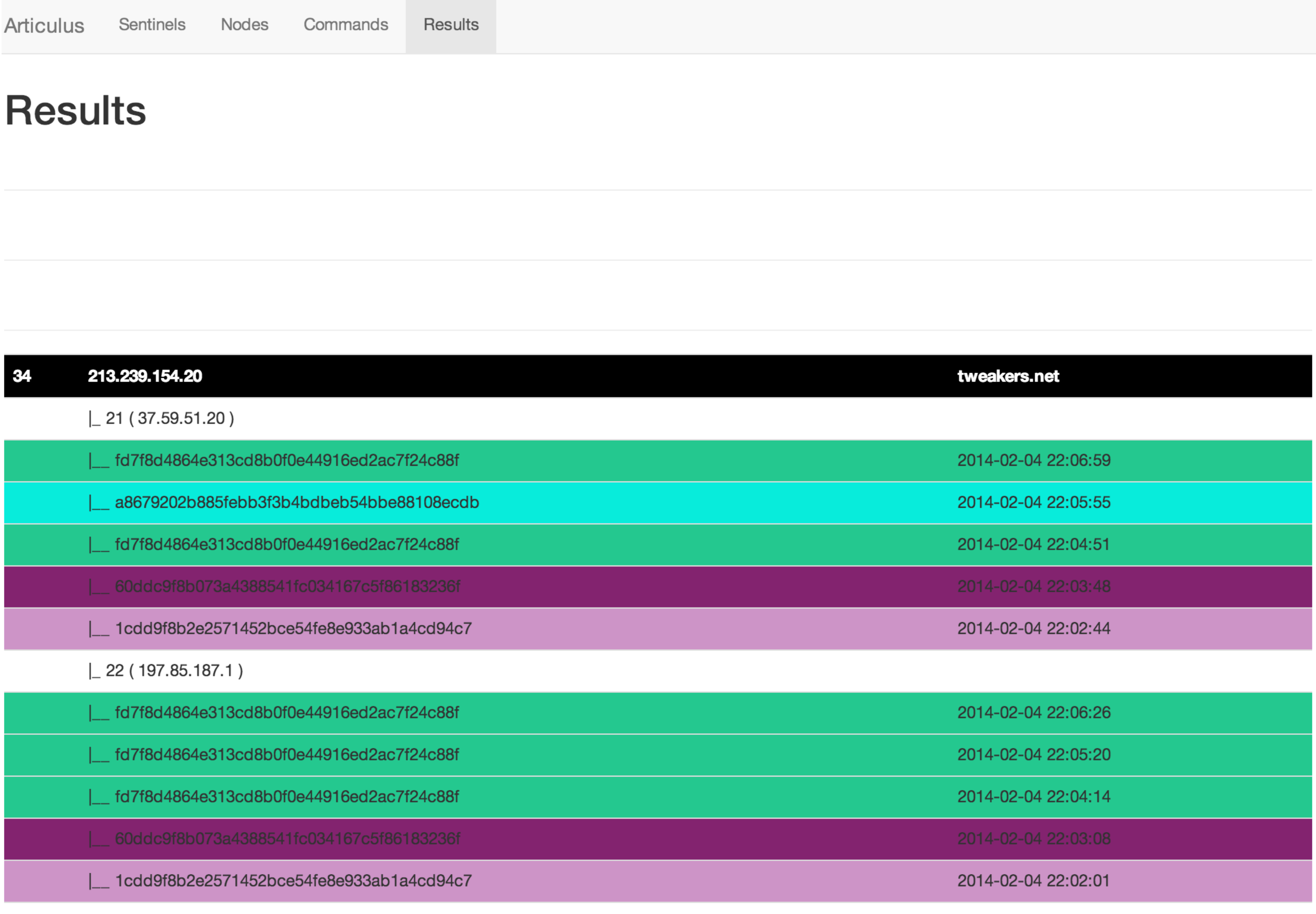


Commands

Service name:	Program:	Parameters:	Description:	Root:
Whatweb	whatweb	["--colour=never"]	Whatweb checker	*No*
TCP Traceroute port 80	traceroute	["-T", "-p", "80", "-n"]		*Yes*
Nmap server fingerprinting	nmap	["-O"]		*Yes*

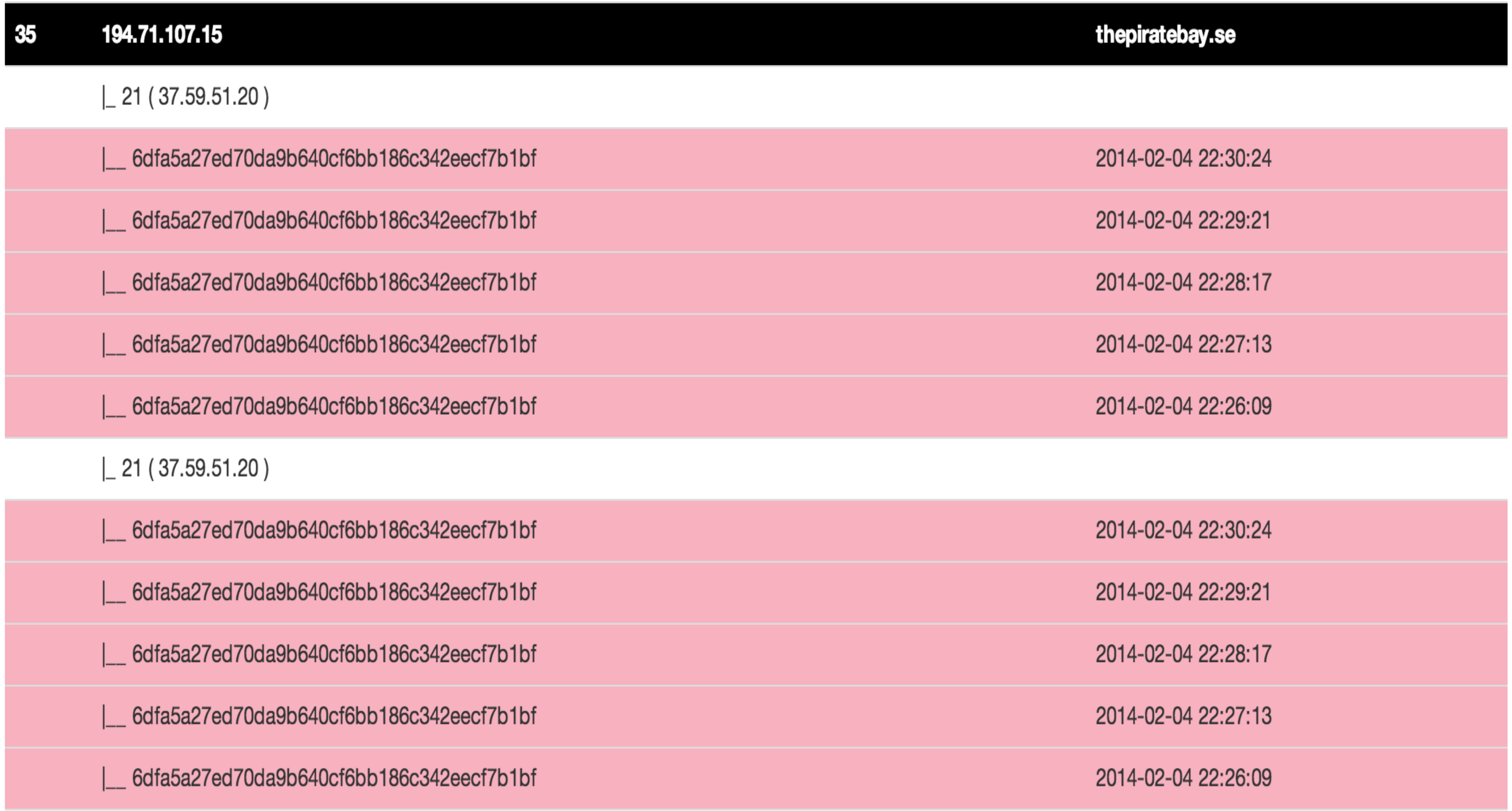
Add new command:

Command:		Parameters:	
		Example: "-p80, -T, --verbose, --destination=1.2.3.4"	
Service name:		Description:	
Weight:	100	Refresh time:	30 seconds
Root:	□		

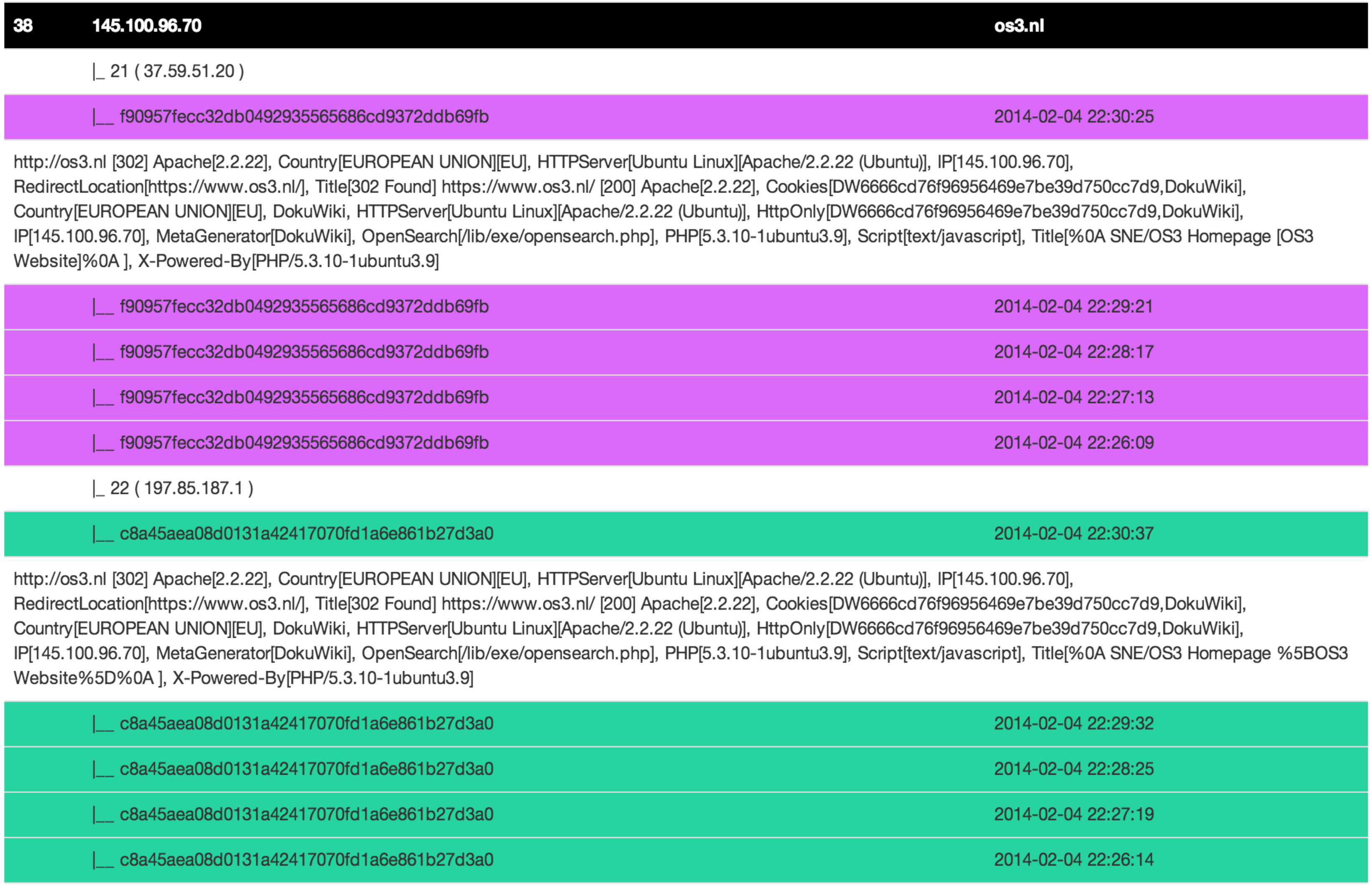


Results

34	213.239.154.20	tweakers.net
	|_ 21 (37.59.51.20)	
	|__ fd7f8d4864e313cd8b0f0e44916ed2ac7f24c88f	2014-02-04 22:06:59
	|__ a8679202b885febb3f3b4bdbeb54bbe88108ecdb	2014-02-04 22:05:55
	|__ fd7f8d4864e313cd8b0f0e44916ed2ac7f24c88f	2014-02-04 22:04:51
	|__ 60ddc9f8b073a4388541fc034167c5f86183236f	2014-02-04 22:03:48
	|__ 1cdd9f8b2e2571452bce54fe8e933ab1a4cd94c7	2014-02-04 22:02:44
	|_ 22 (197.85.187.1)	
	|__ fd7f8d4864e313cd8b0f0e44916ed2ac7f24c88f	2014-02-04 22:06:26
	|__ fd7f8d4864e313cd8b0f0e44916ed2ac7f24c88f	2014-02-04 22:05:20
	|__ fd7f8d4864e313cd8b0f0e44916ed2ac7f24c88f	2014-02-04 22:04:14
	|__ 60ddc9f8b073a4388541fc034167c5f86183236f	2014-02-04 22:03:08
	|__ 1cdd9f8b2e2571452bce54fe8e933ab1a4cd94c7	2014-02-04 22:02:01



35	194.71.107.15	thepiratebay.se
	|_ 21 (37.59.51.20)	
	|__ 6dfa5a27ed70da9b640cf6bb186c342eecf7b1bf	2014-02-04 22:30:24
	|__ 6dfa5a27ed70da9b640cf6bb186c342eecf7b1bf	2014-02-04 22:29:21
	|__ 6dfa5a27ed70da9b640cf6bb186c342eecf7b1bf	2014-02-04 22:28:17
	|__ 6dfa5a27ed70da9b640cf6bb186c342eecf7b1bf	2014-02-04 22:27:13
	|__ 6dfa5a27ed70da9b640cf6bb186c342eecf7b1bf	2014-02-04 22:26:09
	|_ 21 (37.59.51.20)	
	|__ 6dfa5a27ed70da9b640cf6bb186c342eecf7b1bf	2014-02-04 22:30:24
	|__ 6dfa5a27ed70da9b640cf6bb186c342eecf7b1bf	2014-02-04 22:29:21
	|__ 6dfa5a27ed70da9b640cf6bb186c342eecf7b1bf	2014-02-04 22:28:17
	|__ 6dfa5a27ed70da9b640cf6bb186c342eecf7b1bf	2014-02-04 22:27:13
	|__ 6dfa5a27ed70da9b640cf6bb186c342eecf7b1bf	2014-02-04 22:26:09



38	145.100.96.70	os3.nl
	|_ 21 (37.59.51.20)	
	|__ f90957fecc32db0492935565686cd9372ddb69fb	2014-02-04 22:30:25
http://os3.nl [302] Apache[2.2.22], Country[EUROPEAN UNION][EU], HTTPServer[Ubuntu Linux][Apache/2.2.22 (Ubuntu)], IP[145.100.96.70], RedirectLocation[https://www.os3.nl/], Title[302 Found] https://www.os3.nl/ [200] Apache[2.2.22], Cookies[DW6666cd76f96956469e7be39d750cc7d9,DokuWiki], Country[EUROPEAN UNION][EU], DokuWiki, HTTPServer[Ubuntu Linux][Apache/2.2.22 (Ubuntu)], HttpOnly[DW6666cd76f96956469e7be39d750cc7d9,DokuWiki], IP[145.100.96.70], MetaGenerator[DokuWiki], OpenSearch[/lib/exe/opensearch.php], PHP[5.3.10-1ubuntu3.9], Script[text/javascript], Title[%0A SNE/OS3 Homepage [OS3 Website]%0A], X-Powered-By[PHP/5.3.10-1ubuntu3.9]		
	|__ f90957fecc32db0492935565686cd9372ddb69fb	2014-02-04 22:29:21
	|__ f90957fecc32db0492935565686cd9372ddb69fb	2014-02-04 22:28:17
	|__ f90957fecc32db0492935565686cd9372ddb69fb	2014-02-04 22:27:13
	|__ f90957fecc32db0492935565686cd9372ddb69fb	2014-02-04 22:26:09
	|_ 22 (197.85.187.1)	
	|__ c8a45aea08d0131a42417070fd1a6e861b27d3a0	2014-02-04 22:30:37
http://os3.nl [302] Apache[2.2.22], Country[EUROPEAN UNION][EU], HTTPServer[Ubuntu Linux][Apache/2.2.22 (Ubuntu)], IP[145.100.96.70], RedirectLocation[https://www.os3.nl/], Title[302 Found] https://www.os3.nl/ [200] Apache[2.2.22], Cookies[DW6666cd76f96956469e7be39d750cc7d9,DokuWiki], Country[EUROPEAN UNION][EU], DokuWiki, HTTPServer[Ubuntu Linux][Apache/2.2.22 (Ubuntu)], HttpOnly[DW6666cd76f96956469e7be39d750cc7d9,DokuWiki], IP[145.100.96.70], MetaGenerator[DokuWiki], OpenSearch[/lib/exe/opensearch.php], PHP[5.3.10-1ubuntu3.9], Script[text/javascript], Title[%0A SNE/OS3 Homepage %5BOS3 Website%5D%0A], X-Powered-By[PHP/5.3.10-1ubuntu3.9]		
	|__ c8a45aea08d0131a42417070fd1a6e861b27d3a0	2014-02-04 22:29:32
	|__ c8a45aea08d0131a42417070fd1a6e861b27d3a0	2014-02-04 22:28:25
	|__ c8a45aea08d0131a42417070fd1a6e861b27d3a0	2014-02-04 22:27:19
	|__ c8a45aea08d0131a42417070fd1a6e861b27d3a0	2014-02-04 22:26:14

Thank you for your attention

- Are there any questions?