Chair of Network Architectures and Services
Department of Informatics
Technical University of Munich

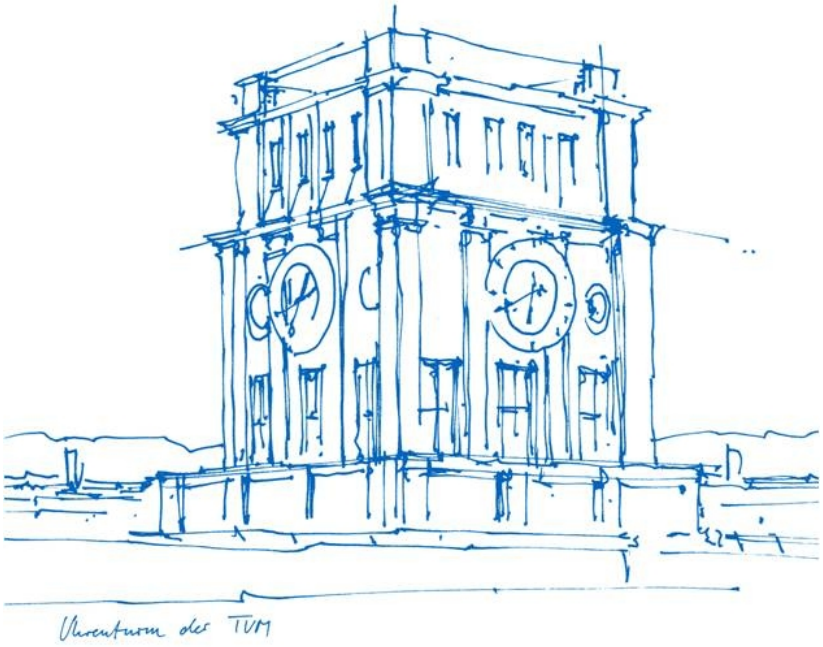
Detection of Amplifiers using Active Measurements

Hamza Zafar

Advisor(s): Simon Bauer, M. Sc.
Oliver Gasser, M. Sc.
Dipl.-Inform. Stefan Metzger
Supervisor: Prof. Dr.-Ing. Georg Carle

Technical University of Munich (TUM)
Department of Informatics
Chair of Network Architectures and Services

Garching, 08.04.2019

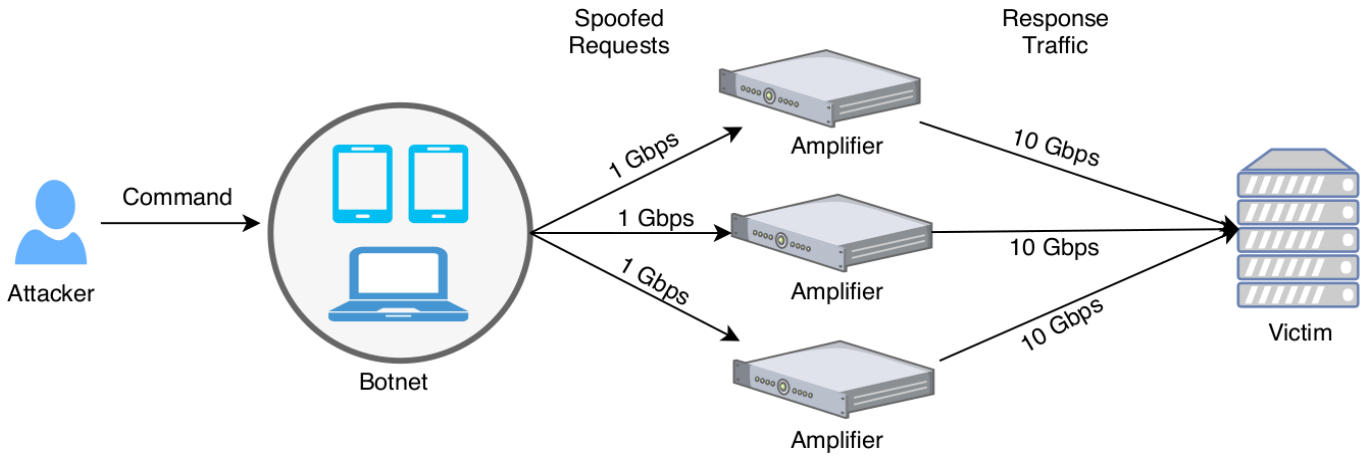


Agenda

- Introduction
- Framework
- Measurements
- Dashboards
- Conclusion

Introduction: Background

- **Distributed Reflective Denial-of-Service Attack (DRDoS)**



- Figure: DRDoS attack using a botnet.

- **Bandwidth Amplification Factor (BAF):**

$$BAF = \frac{len(Response\ payload)}{len(Request\ payload)}$$

- **Amplifier:**
  - Publicly available
  - Lacks authentication
  - Connection-less
  - BAF > 1

Introduction: Motivation

- **Terabit Attack Era**
  - GitHub reported 1.35 Tbps
  - Arbor Networks reported 1.7 Tbps
- **Abuse of IoT devices**
  - Mirai malware
- **Solution**
  - No IP address spoofing, no DRDoS attacks
  - Reduce the number of amplifiers
- **Our Contribution**
  - Framework to detect amplifiers using active network measurements

Introduction: Research Questions

- How to orchestrate network scans in a large network?
- How to conduct network scans ethically?
- Do amplifiers exhibit any characteristics?
- Does the bandwidth amplification factor (BAF) changes over time?
- Does the number of active amplifiers change over time?

Framework: Features

- **REST API**
  - Developed using Django REST Framework (DRF)

API Endpoint	Request Method	Description
/api/v1/scan	POST	create new scan
/api/v1/scan	GET	list scan names
/api/v1/scan/{name}	GET	get scan details
/api/v1/scan/{name}	PUT	update scan
/api/v1/scan/{name}	DELETE	remove scan
/api/v1/scan/{name}/result	GET	get latest scan result
/api/v1/scan/running	GET	list task-ids of running scanning jobs
/api/v1/scan/revoke/{task_id}	GET	revoke running job with the specified task_id

TABLE : REST API endpoints

- **CLI Client**
  - Increases usability

- **Scan Scheduling**
  - Periodically execute network scans
  - Celery Task Queue used

Framework: Features (cont.)

- **E-mail notifications**
  - Notify about amplifiers and error messages

- **Network Scanner (Zmap)**
  - Horizontal scanner (one scan per protocol)
  - Fast network scanner *“/0 scans in under 45 minutes”*
  - Stateless
  - Randomized probes
  - IPv6 address space scanning

- **Visualization Dashboards**
  - Developed using *Grafana*
  - Home Dashboard: stats from all scans
  - Scan Dashboard: stats for a specific scan
  - Amplifier Dashboard: stats for a specific amplifier

Measurements

- **Address ranges:** TUM's public IPv4 addresses
- **Scanning frequency:** Twice a day
- **Scanning duration:** Two weeks (23.02.2019 – 06.03.2019)
- **No. of scanned addresses:** 130k
- **Scan execution time:** approx. 17 minutes

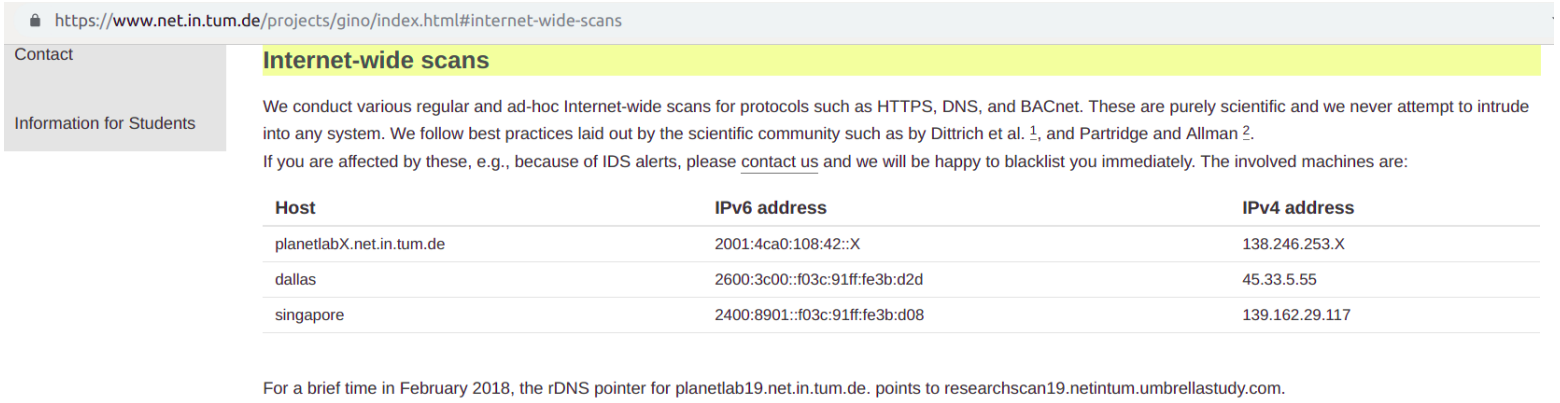
Protocol	Attack Vector
Chargen	get random ASCII characters
CLDAP	get list of users registered in a directory
DNS	DNS ANY query for google.com
Memcached	*stat items* command
NetBIOS	get NetBIOS name table
NTP	*monlist* command
QOTD	get random quote
RIPv1	get routing table
SNMP	get system description field using community string public
SSDP	discover packet for UPnP devices

TABLE: Overview of attack vectors used for detection of amplifiers.

Measurements: Ethical Considerations

- Validate probe packet
  - Don’t cause harm to the devices
  - Use Wireshark to validate packet structure
  - Optimally, deploy services and capture request packets

- Host a web page to express scanning intentions



- Maintain a blacklist

- Avoid saturating networks
  - Low packet rate (128 pps)
  - ZMap’s randomized probing

- Restricted access to scan results

Measurements: Results

- Amplifiers detected for 5 protocols
- NetBIOS, SNMP have the highest no. of amplifiers
- Amplifiers decrease during the weekend
- Amplifiers increase during the day

Protocol	Min	Max	Avg
NetBIOS	73	215	122
SNMP	23	27	25
SSDP	1	3	2
Chargen	2	2	2
DNS	1	1	1

Table: Min, Max and Avg. number of amplifiers

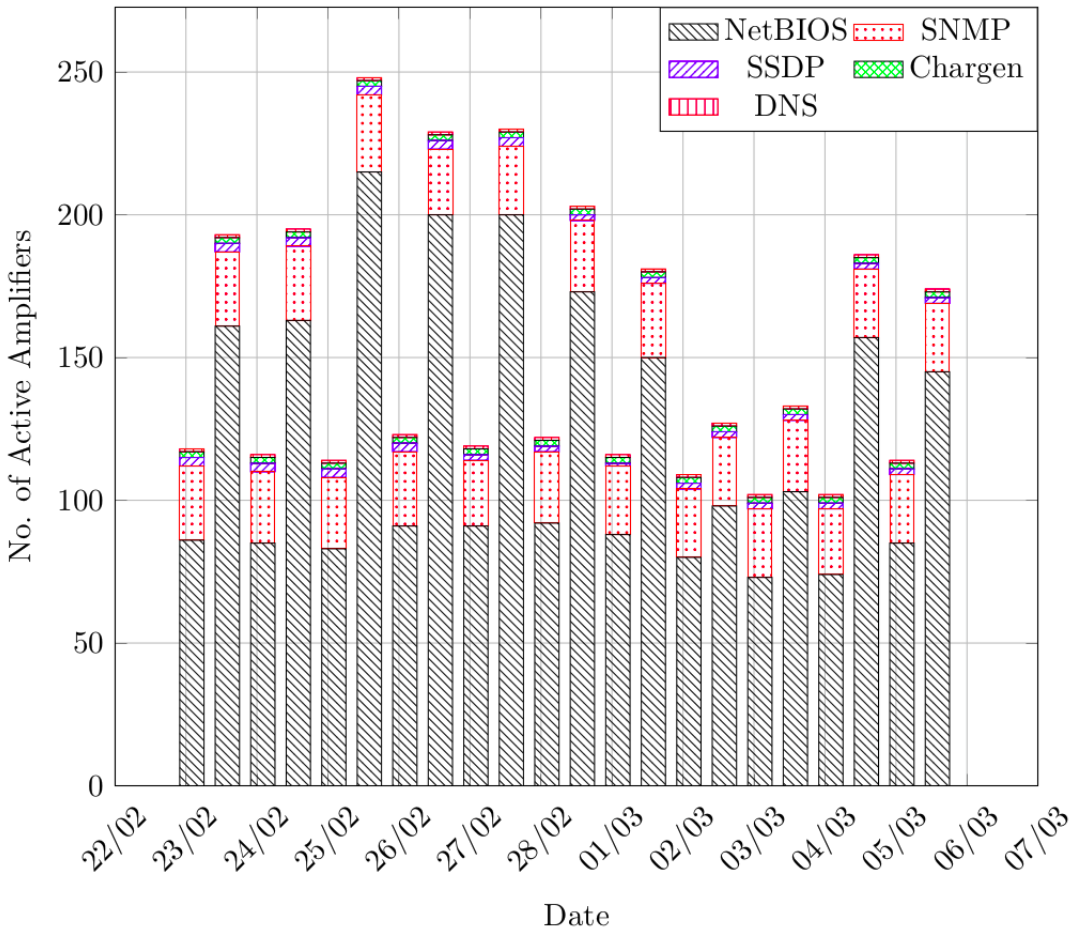


Figure: No. of active amplifiers detected over a period of two weeks

Measurements: NetBIOS Amplifiers

- Windows based protocol to allow applications to communicate on LAN
- Probe NetBIOS *nametable*
- Linux/Unix based machines found running NetBIOS
  - SAMBA suite
- Amplifiers belong to three subnets
- Subnet-1:
  - End user devices
- Subnet-2 & subnet-3:
  - Printers
  - Mail servers
  - LDAP servers

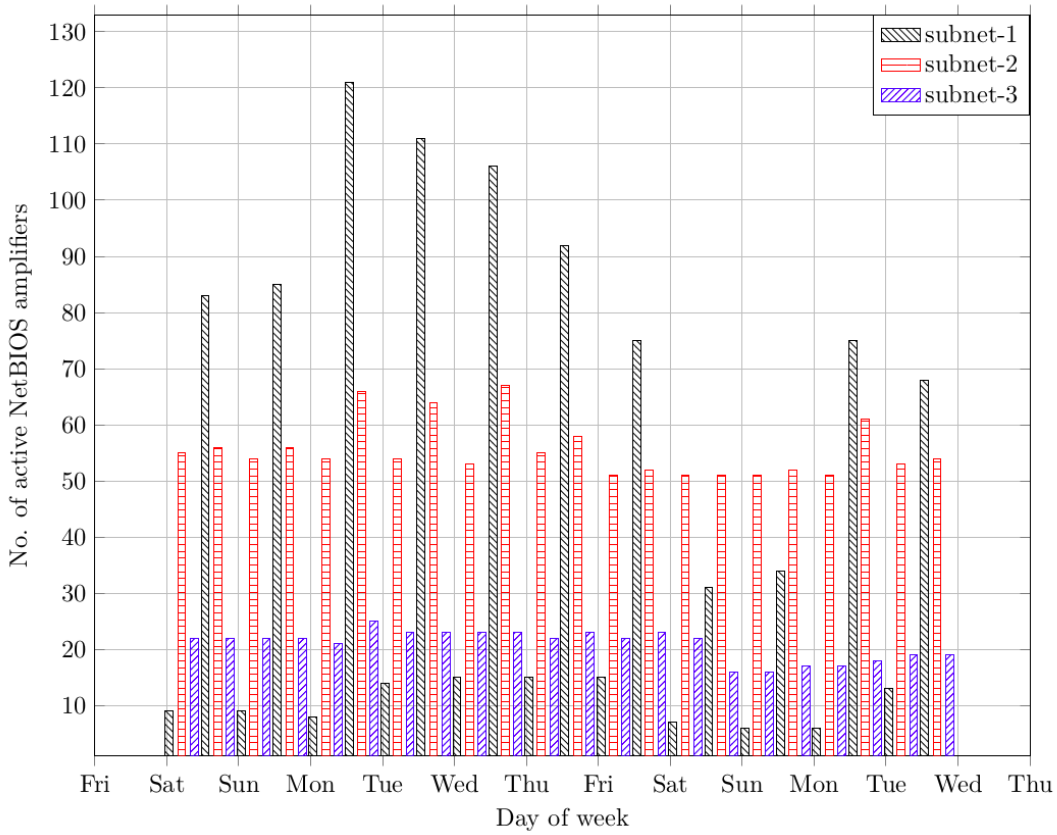


Figure: Number of active NetBIOS amplifiers in three subnets

Measurements: SNMP Amplifiers

- Simple Network Management Protocol (SNMP)
- Manage and monitor network devices
- Probe *system description* property

```
Samsung Samsung M262x 282x Series; V3.00.01.04 JAN-18-2012;
Engine V1.00.02 01-17-2013;NIC V6.01.01;S/N ZD2JB8GD2B00LSR
```

Figure: System description string received from a Samsung printer

- SNMP *GetRequest* vs. *GetBulkRequest*
- Majority of SNMP amplifiers are printers

Vendor	Device Type	Count
HP	Printer	11
Brother	Printer	4
Kyocera	Printer	3
Samsung	Printer	2
Lexmark	Printer	1
Epson	External print server	1
nTop	nBox Netflow hardware appliance	1
APC	Uninterruptible Power Supply (UPS)	1

TABLE: SNMP amplifier device types and vendors.

Measurements: SSDP Amplifiers

- Simple Service Discovery Protocol (SSDP)
- Discovery and advertisement of plug-and-play devices
- Probe SSDP discover request
- Two Samsung printers found

DNS Amplifiers

- Probe DNS *ANY* query for google.com
- One DNS open resolver found
- DNS resolver caches results
- BAF drops during weekend due to
- less records in resolver's cache

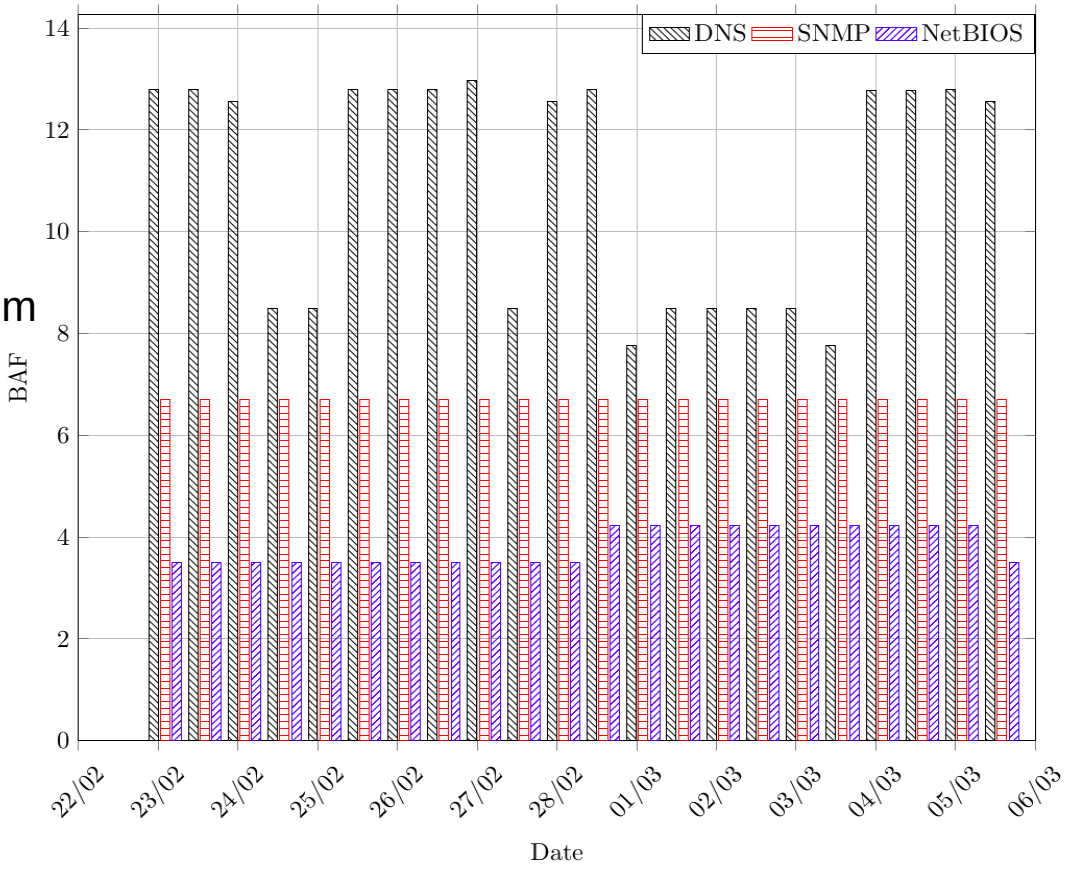


Figure: Change in BAF of amplifiers

Measurements: Chargen Amplifiers

- Legacy character generator protocol
- Testing and network debugging
- Highest BAF (74X)
- Two amplifiers
- Nmap scan reveals amplifiers are running:
  - Legacy protocols *Echo*, *Discard*
  - Outdated Sun Solaris 8 OS
- Sun Solaris 8 enables Chargen on system startup
- Sun management console found

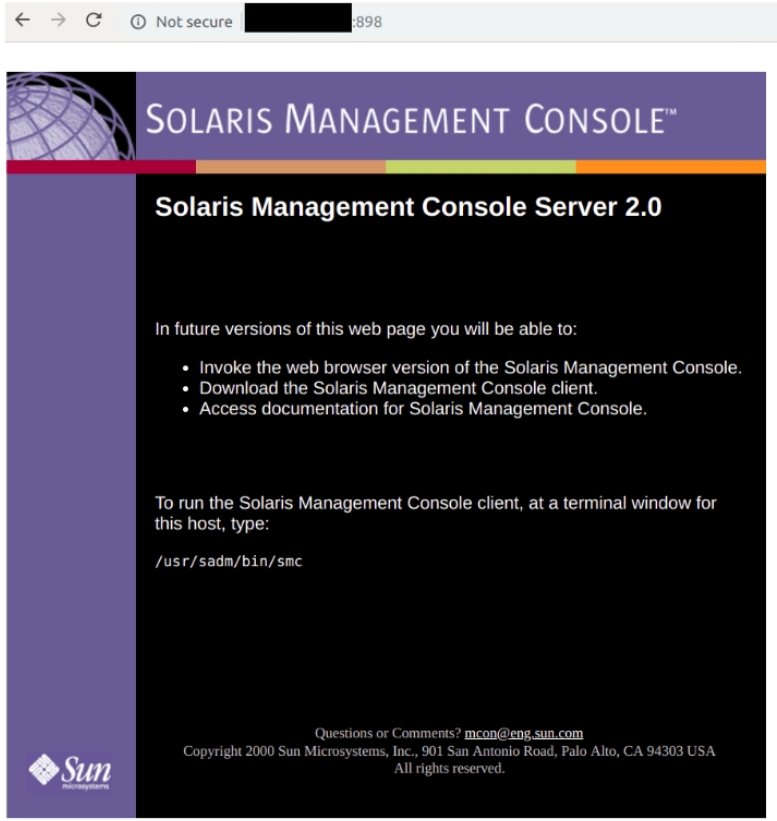


Figure: Sun Management Console

Measurements

- Bandwidth Amplification Factor of amplifiers:

Protocol	Amplifiers	BAF		
		all	50%	10%
NetBIOS	145	3.24	4.06	4.91
SNMP	24	3.02	4.15	6.47
SSDP	2	14.86	19.7	19.7
Chargen	2	74	74	74
DNS	1	12.56	12.56	12.56

Table: BAF per protocol recorded from the last scanning iteration, all shows the average BAF of all amplifiers, 50% and 10% shows the average BAF of 50% and 10% of the worst amplifiers, respectively.

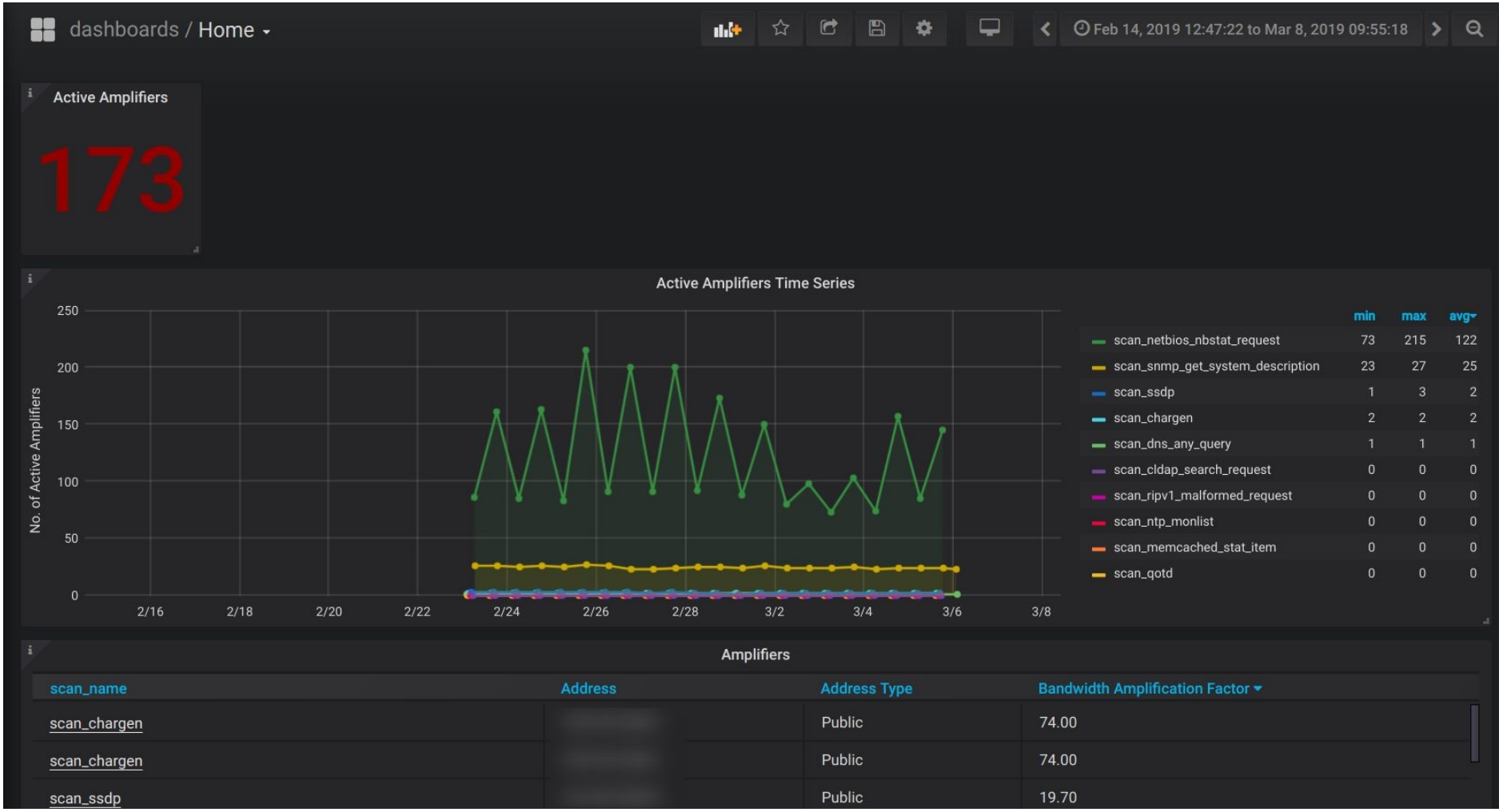
- 9 devices found with multiple amplification vulnerabilities

Pos.	Protocol Combination	Count
1	NetBIOS, SNMP	7
2	NetBIOS, SSDP	1
3	NetBIOS, SSDP, SNMP	1

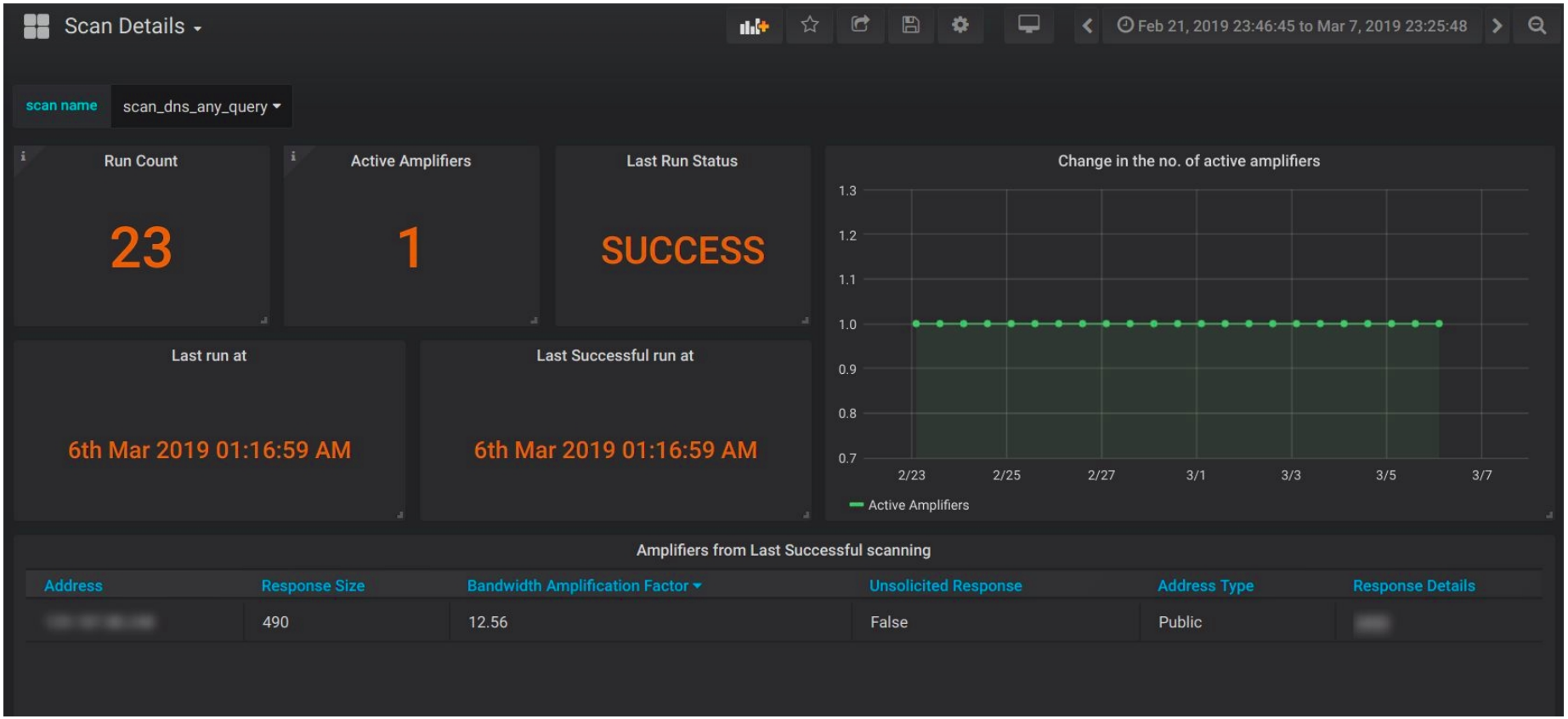
Table: Combination of vulnerable protocols detected in amplifiers

Visualization Dashboards Demo

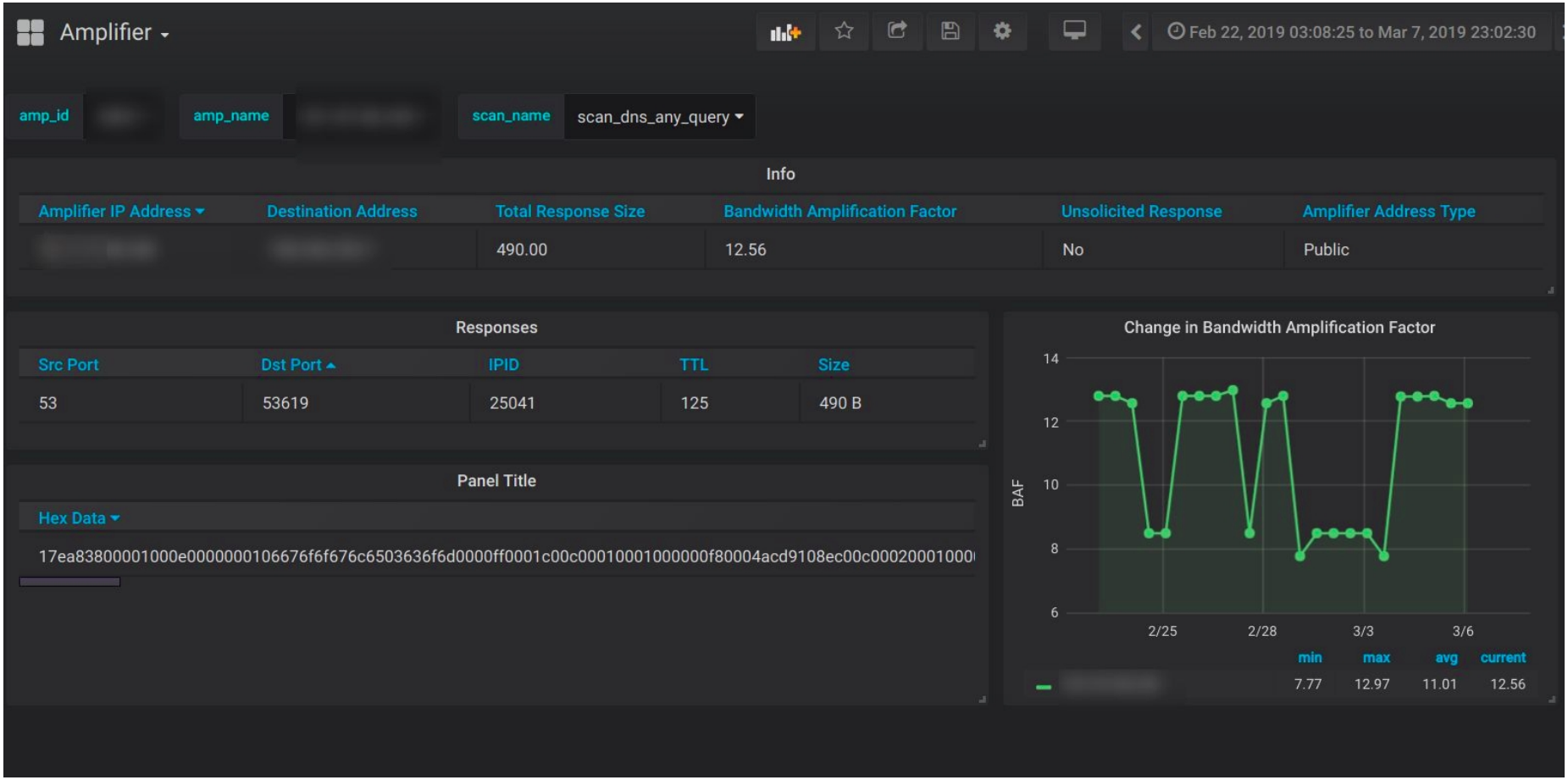
Framework: Home Dashboard



Framework: Scan Dashboard



Framework: Amplifier Dashboard



Conclusion

- Extensible framework for amplifier detection using active measurements
- Evaluation by executing scans ethically in Munich Scientific Network
- Number of amplifiers and BAF varies with time
- Misconfigurations exposes devices
- Internet wide scans in future could be a source of interesting insights

Backup Slides

Framework: REST API

- **REST architecture style**
  - Client-server *“separation of concerns”*
  - Uniform Interface

- **Django REST Framework (DRF)**
  - Python based
  - Opensource
  - Pluggable components
  - Field validations (IP address format, port range)

- CLI Client
  - Constructs and sends request
  - Increases usability

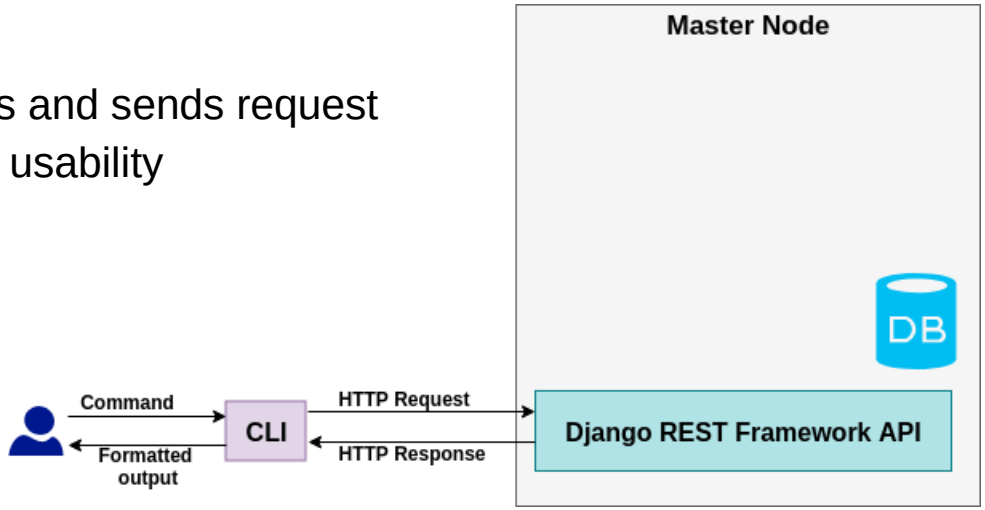


Figure: Framework architecture

Framework: Scan Scheduling

- **Scan Scheduling**
  - Periodically execute network scans
- **Celery**
  - Task Queue
  - Asynchronous execution of long running tasks
  - Publisher-Subscriber model
- **Celery beat scheduler**
  - Keeps track of scans
  - Triggers task execution
- **Celery worker**
  - Executes tasks
  - Stores results in database

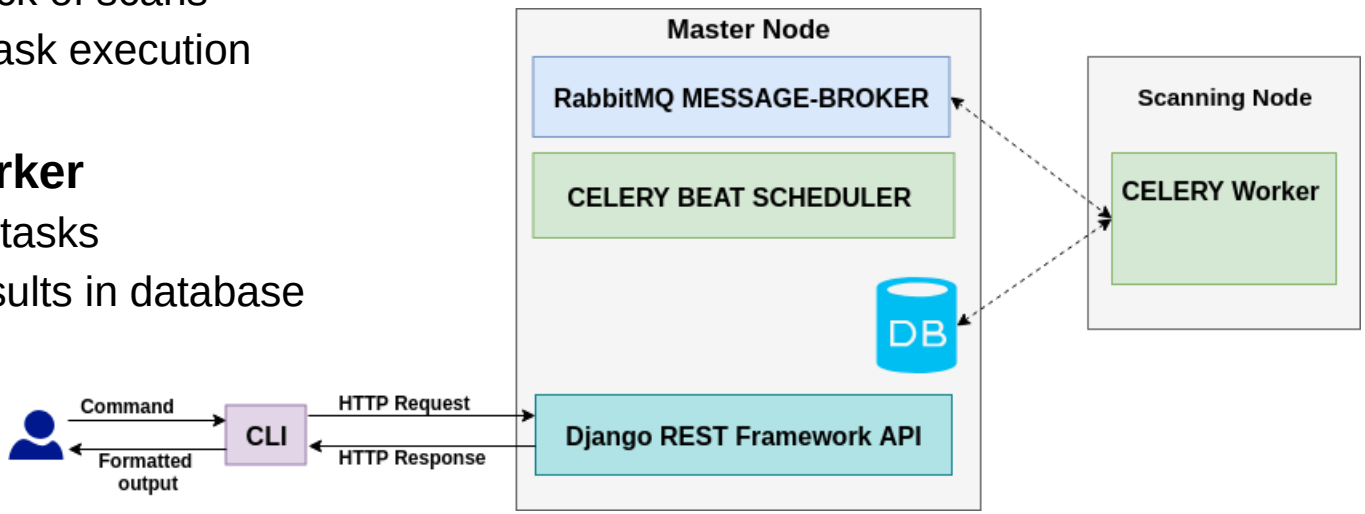


Figure: Framework architecture

Framework: Network Scanner

- **Network Scanner**
  - Horizontal vs. vertical scanning technique
- **ZMap**
  - Fast network scanner *“/0 scans in under 45 minutes”*
  - Stateless
  - Decouples sending probes and receiving responses
  - Bypasses the TCP/IP stack
  - Randomized probes
  - IPv6 address space scanning
  - Blacklist feature
- **One scan per protocol**

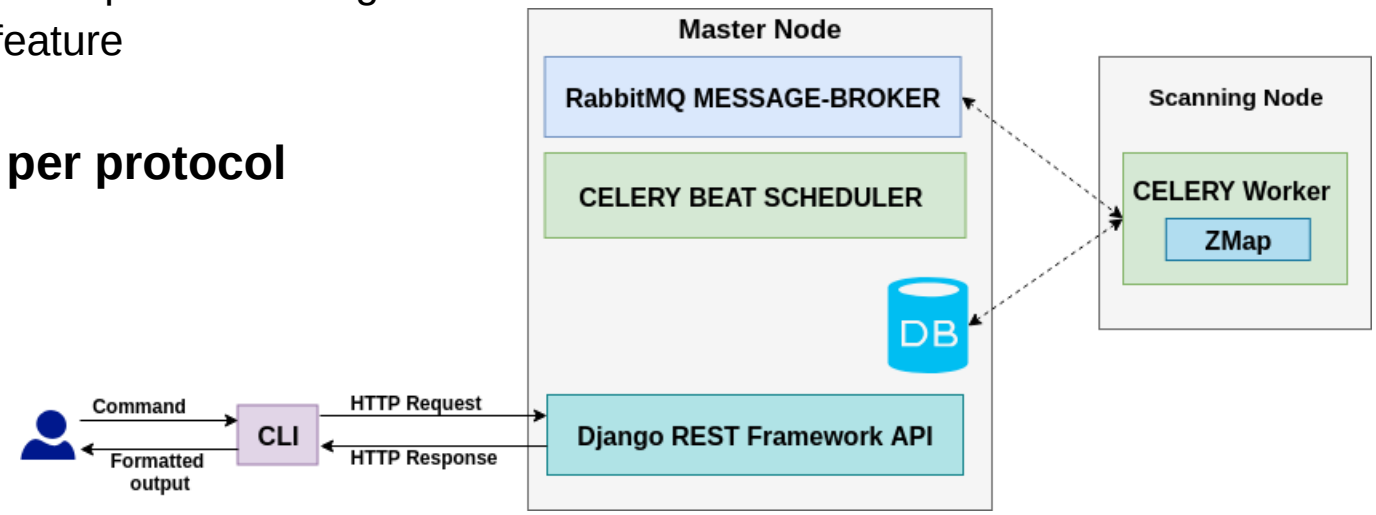
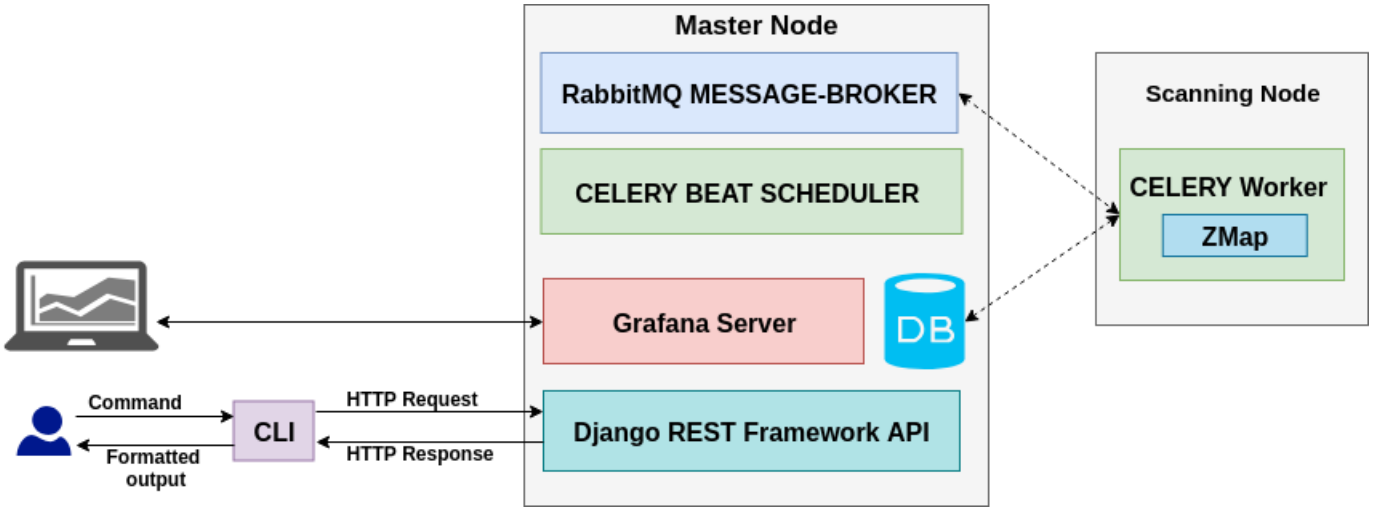


Figure: Framework architecture

Framework: Visualization

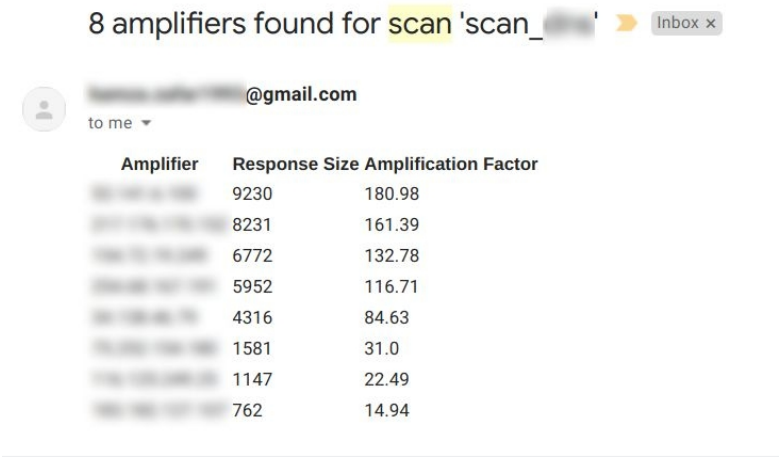
- **Grafana – Data visualization framework**
  - Opensource
  - Support for several databases
  - Tables, graphs, heat-maps etc. to visualize data

- **Home Dashboard:** stats from all scans
- **Scan Dashboard:** stats for a specific scan
- **Amplifier Dashboard:** stats for a specific amplifier



Framework: Notifications

- **E-mail notifications**
  - Sent when the scan completes or fails
  - Helps in tackling operational challenges of the framework

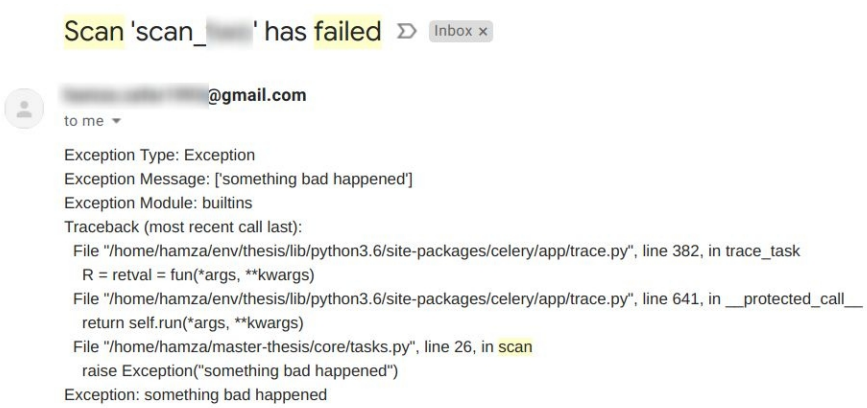


8 amplifiers found for scan 'scan_[redacted]' Inbox ×

[redacted]@gmail.com
to me

Amplifier	Response Size	Amplification Factor
[redacted]	9230	180.98
[redacted]	8231	161.39
[redacted]	6772	132.78
[redacted]	5952	116.71
[redacted]	4316	84.63
[redacted]	1581	31.0
[redacted]	1147	22.49
[redacted]	762	14.94

Figure: Amplifiers found notification



Scan 'scan_[redacted]' has failed Inbox ×

[redacted]@gmail.com
to me

```
Exception Type: Exception
Exception Message: ['something bad happened']
Exception Module: builtins
Traceback (most recent call last):
  File "/home/hamza/env/thesis/lib/python3.6/site-packages/celery/app/trace.py", line 382, in trace_task
    R = retval = fun(*args, **kwargs)
  File "/home/hamza/env/thesis/lib/python3.6/site-packages/celery/app/trace.py", line 641, in __protected_call__
    return self.run(*args, **kwargs)
  File "/home/hamza/master-thesis/core/tasks.py", line 26, in scan
    raise Exception("something bad happened")
Exception: something bad happened
```

Figure: Error notification

Measurements

- TUM's public IPv4 address ranges scanned
- 10 UDP-based protocols assessed for amplification abuse
- PlanetLab static IP addresses used for scanning nodes
- Scans executed twice a day

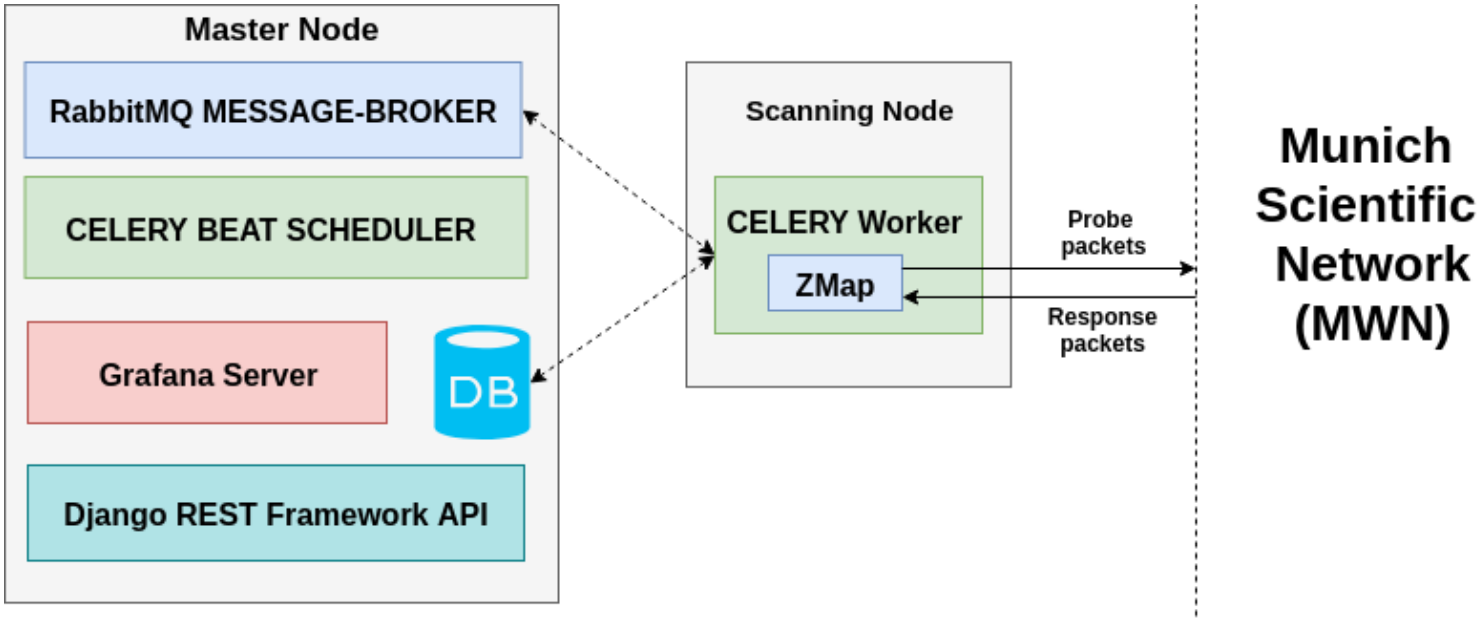


Figure: Scanning setup

Mitigation Strategies

- Prevent IP address spoofing

- Prevent public access to devices
  - SNMP, SSDP, NetBIOS are strictly designed for usage in LAN
  - Protect DNS resolvers

- Use latest operating systems and protocol versions
  - Sun Solaris 8's support was discontinued in March 2012
  - SNMPv3 provides username, password based authentication
  - UDP interface is disabled in latest memcached versions
  - NTP's monlist command is disabled in latest releases

- Secure service configuration
  - SNMP "*public*" passphrase on printers should be changed

- Protocol hardening
  - DNS: switch to TCP if the response size exceeds a threshold

Related Work

- Amplification Hell: Revisiting Network Protocols for DDoS Abuse [1]
  - Scanned the internet for amplifiers, we scanned a university network
  - Described a passive approach for amplifier detection (BAF=5 and traffic=10MB)
  - Response size from the Chargen amplifiers is 74 bytes
  - Scanned only SNMPv2, we scanned SNMPv1 and v2 devices
  - DNS average BAF 28.7, we observed 12.56
  - SSDP average BAF 30.7, we observed 14.86

- Hell of a Handshake: Abusing TCP for Reflective Amplification DDoS Attacks [2]
  - TCP stacks re-transmit the SYN-ACK packet to victim
  - No amplification attack reported based on the TCP amplifiers

- *OpenResolverProject.org* and *OpenNTPProject.org*
  - Scan internet for DNS and NTP amplifiers
  - Limited to two protocols and IPv4 addresses

[1] Christian Rossow. “Amplification Hell: Revisiting Network Protocols for DdoS Abuse”. In: In Proceedings of the 2014 Network and Distributed System Security Symposium, NDSS. 2014.

[2] Marc Kuhrer and Thomas Hupperich and Christian Rossow and Thorsten Holz, “Hell of a Handshake: Abusing TCP for Reflective Amplification DDoS Attacks”, In Proceedings of the 2014 USENIX Workshop on Offensive Technologies WOOT’ 14