All Your Cluster-Grids Are Belong to Us: Monitoring the (in)Security of Infrastructure Monitoring Systems

Andrei Costin

EURECOM, France

1st Workshop on Security & Privacy in the Cloud (SPC)

30 Sep 2015, Florence Italy

EURECOM
Sophia Antipolis

Agenda

- Introduction
- Overview of NMS
- Reconaissance
- Static+Dynamic Analysis
- Vulnerability Analysis
- Countermeasures
- Conclusion

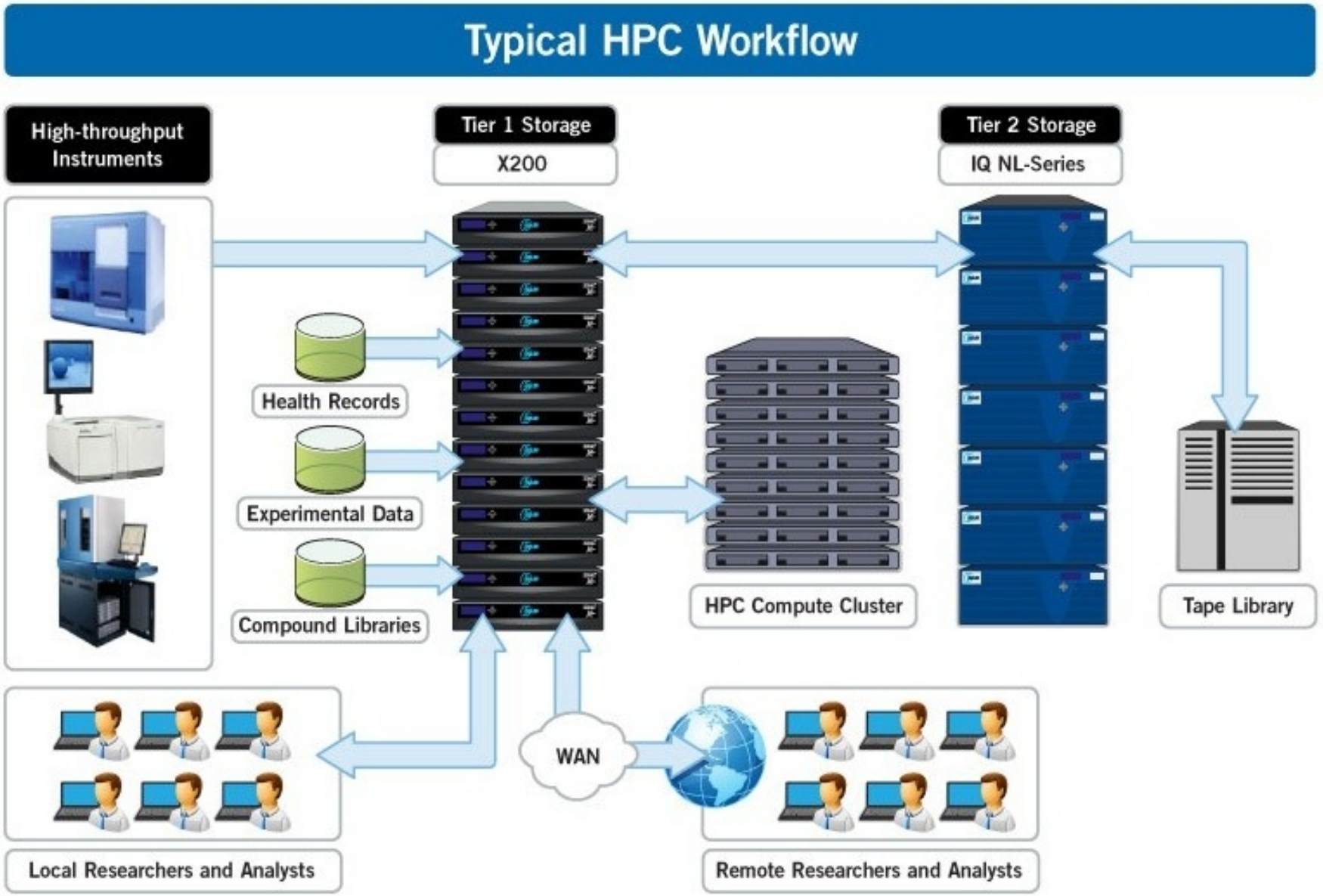
Introduction
What is Cloud Computing?

"When broken down, cloud computing is a specialized distributed computing model. Building upon the desirable characteristics of ***cluster, grid, utility****, [...] to create a new computing paradigm"*

J. Idziorek, Exploiting Cloud Utility Models for Profit and Ruin, 2012

EURECOM
Sophia Antipolis

Introduction
What is HPC?



Introduction
What is NMS?

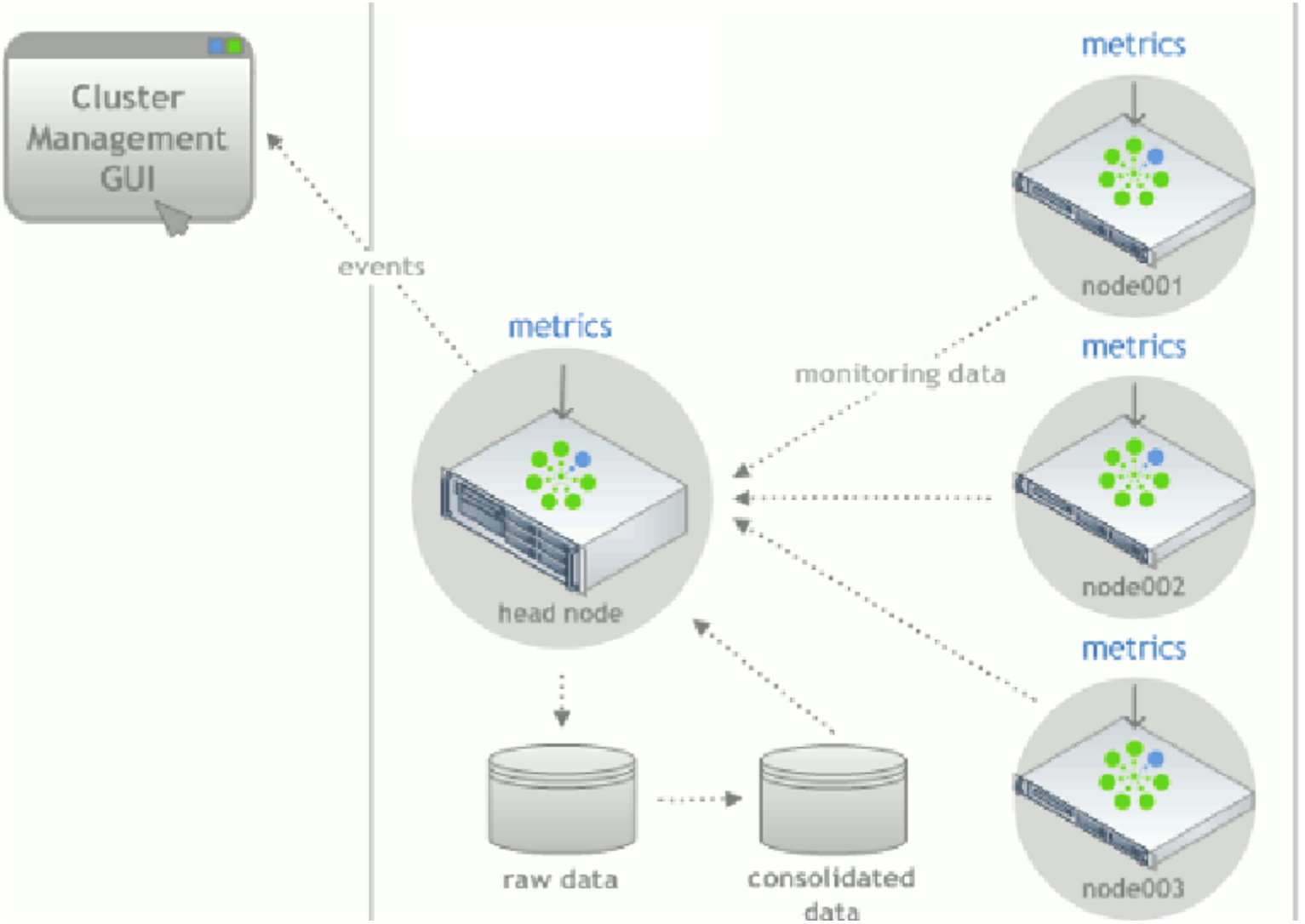
- NMS
  - Network Monitoring System
  - Monitoring systems for **infrastructure, servers and networks**

Introduction
What is NMS?

- NMS
  - Network Monitoring System
  - Monitoring systems for **infrastructure, servers and networks**

- Where used?
  - HPC=High-Performance Computing
    - Grids
    - Clusters
    - Federation of Clusters
  - Cloud

Introduction
What is NMS?



EURECOM
Sophia Antipolis

Overview of NMS
What are the tools?

Nagios

ZenOss
Open Source IT Management

CACTI/SNMP

ZABBIX

MONIT
Barking at daemons

OBSERVIUM
network management and monitoring

ARGUS
Monitoring Software

EURECOM
Sophia Antipolis

Overview of NMS
What are the tools?

- **Ganglia**

  ”a scalable distributed monitoring system for High-Performance Computing (HPC) systems such as clusters and grids”

Overview of NMS
What are the tools?

- **Ganglia**

  ”a scalable distributed monitoring system for High-Performance Computing (HPC) systems such as clusters and grids”

- **Cacti**

  ”a complete network graphing solution”

Overview of NMS
What are the tools?

- **Ganglia**

  ”a scalable distributed monitoring system for High-Performance Computing (HPC) systems such as clusters and grids”

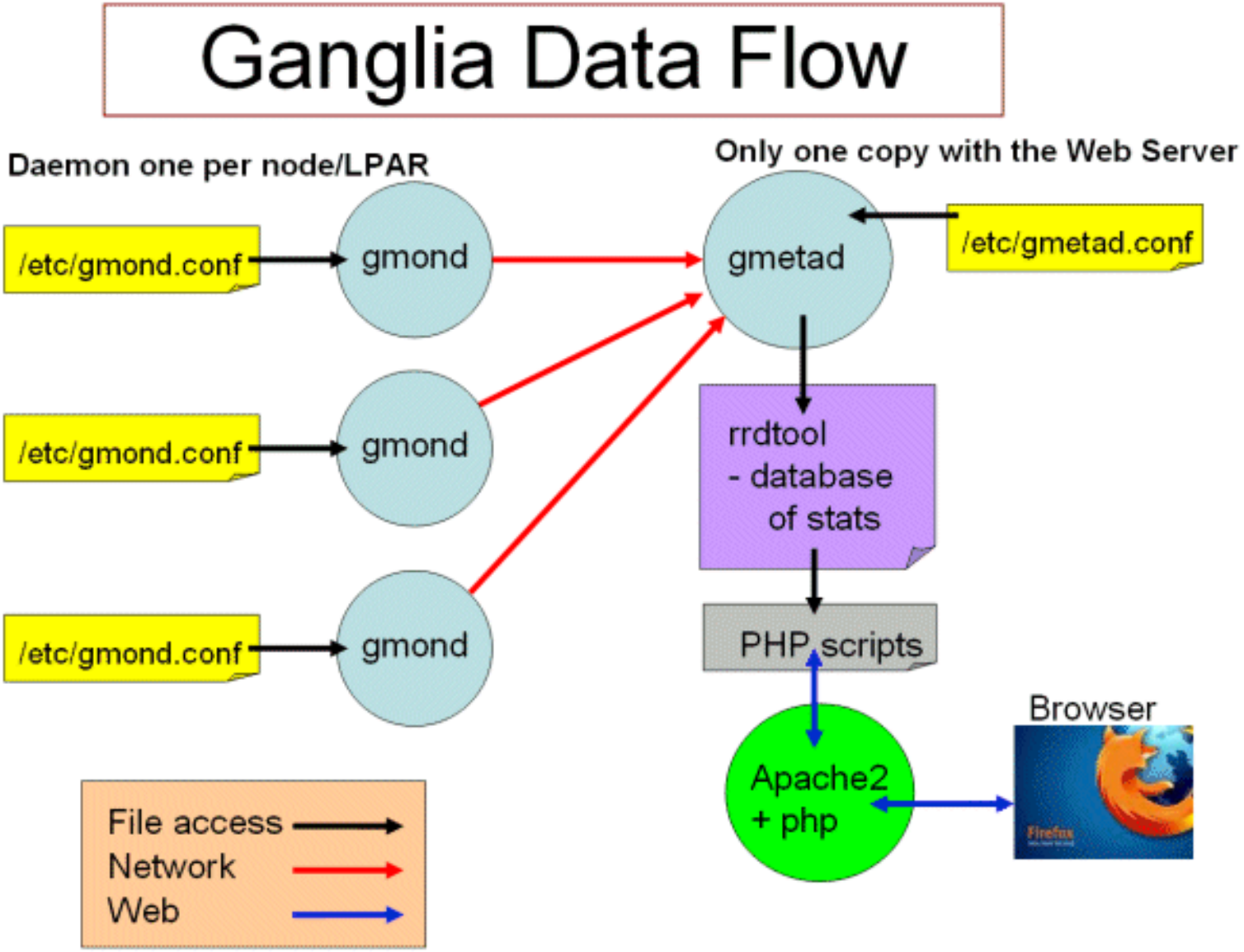
- **Cacti**

  ”a complete network graphing solution”

- **Observium**

  ”an autodiscovering network monitoring platform supporting a wide range of hardware platforms and operating systems including Cisco, Windows, Linux, HP, Juniper, Dell, FreeBSD, Brocade, Netscaler, NetApp and many more. Observium seeks to provide a powerful yet simple and intuitive interface to the health and status of your network”

Overview of NMS
How they work?



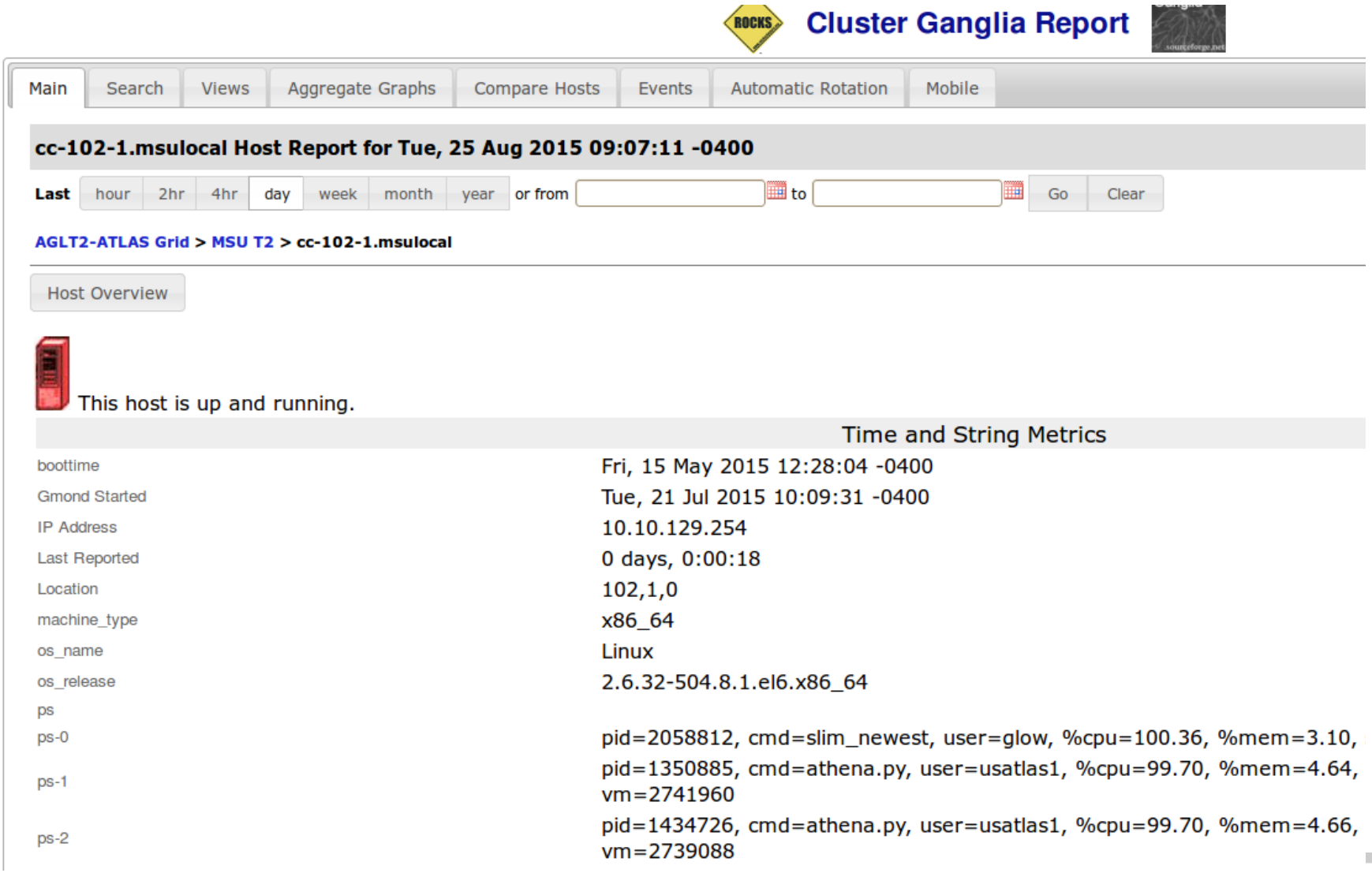
EURECOM
Sophia Antipolis

Overview of NMS
Who uses them?

WHO USES GANGLIA?

Berkeley (the birthplace of ganglia)
Twitter
flickr
last.fm
OpenX
Monetate
San Diego Supercomputing Center (contributed great code to the project)
Massachusetts Institute of Technology (MIT)
National Aeronautics and Space Administration (NASA)
National Institutes of Health (NIH)
Reuters
Internet Archive
Industrial Light & Magic
Wikipedia (check it out!)
Virginia Tech (built the fastest supercomputer at any academic institution in the world using ganglia)
Etsy
Pandora
Dow Chemical
Motorola
Harvard
D.E. Shaw
Lucent
CERN
Cisco
Sun (thanks for recommending ganglia for Grid Infrastructure!)
HP
Microsoft
Dell (thanks for the hardware donation!)
Cray
Boeing
Lockheed-Martin
GE Global Research
Cadence Design Systems
nVidia
Duke University
Bank of America
Queensland University of Technology
Georgetown University
UOL.com
PriceGrabber.com
Ticket Master
Qinetiq
Cummins
freescale
Sandia National Laboratories
Rocketcalc
Yale
Deutsches Elektronen-Synchrotron
bp
Nortel
LexisNexis
Landmark
SARA
Bellsouth
University of Pisa, Italy
X-ISS
Tennesee Tech University
Princeton
The Moving Picture Company
University of Michigan
Universite De Sherbrook
The Royal Bank of Scotland
U.S. Air Force
Celgene
Groundwork
Brookhaven National Laboratory
N.E.C.
GlobeXplorer
John Deere
Xilinx
Freddie Mac
jeteye
Tokyo Institute of Technology
Purdue University
Stanford
and **thousands** of other people just ask Google.

Information Leakage
What is leaked?



Cluster Ganglia Report

Main | Search | Views | Aggregate Graphs | Compare Hosts | Events | Automatic Rotation | Mobile

cc-102-1.msulocal Host Report for Tue, 25 Aug 2015 09:07:11 -0400

Last | hour | 2hr | 4hr | day | week | month | year | or from [ ] to [ ] Go Clear

AGLT2-ATLAS Grid > MSU T2 > cc-102-1.msulocal

Host Overview

This host is up and running.

Time and String Metrics	
boottime	Fri, 15 May 2015 12:28:04 -0400
Gmond Started	Tue, 21 Jul 2015 10:09:31 -0400
IP Address	10.10.129.254
Last Reported	0 days, 0:00:18
Location	102,1,0
machine_type	x86_64
os_name	Linux
os_release	2.6.32-504.8.1.el6.x86_64
ps	
ps-0	pid=2058812, cmd=slim_newest, user=glow, %cpu=100.36, %mem=3.10,
ps-1	pid=1350885, cmd=athena.py, user=usatlas1, %cpu=99.70, %mem=4.64, vm=2741960
ps-2	pid=1434726, cmd=athena.py, user=usatlas1, %cpu=99.70, %mem=4.66, vm=2739088

Information Leakage Attack-Enabler

- **OS Details**
  - CVEs for Kernel
- NIST NVD, CVEdetails

Linux » Linux Kernel : All Versions

Sort Results By : Version Descending Version Ascending Number of Vulnerabilities Descending Num

Total number of versions found = 1772 Page : 1 (This Page) 2 3 4 5 6 7 8 9 10 11 1

Version	Language	Update	Edition	Number of Vulnerabilities	
2.6.0				489	Version Details Vulnerabilities
2.6.1				478	Version Details Vulnerabilities
2.6.2				465	Version Details Vulnerabilities
2.6.10				465	Version Details Vulnerabilities
2.6.11				457	Version Details Vulnerabilities

Information Leakage Attack-Enabler

- **OS Details**
  - CVEs for Kernel
- Linux Kernel 2.6.32

Linux » Linux Kernel » 2.6.32 RC4 : Vulnerability Statistics

Vulnerabilities (**182**) Related Metasploit Modules (Cpe Name:*cpe:/o:linux:linux_kernel:2.6.32:rc4*)

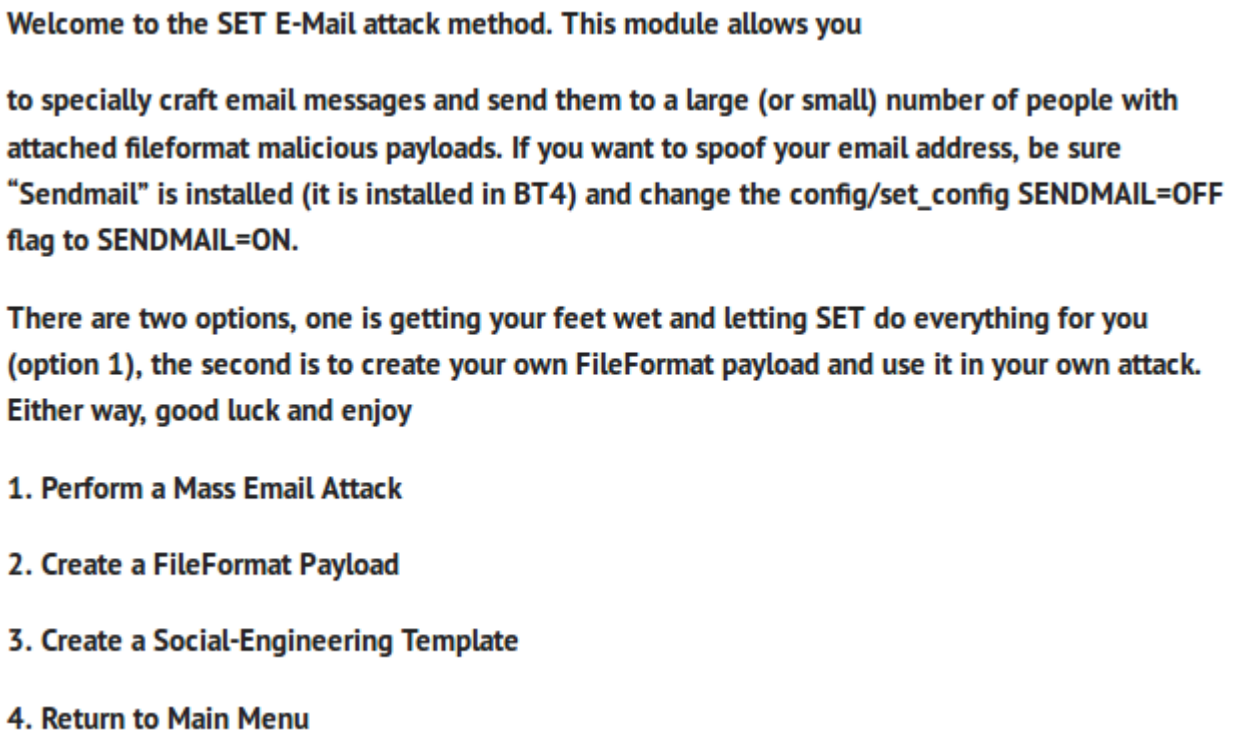
Vulnerability Feeds & Widgets

Vulnerability Trends Over Time

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2009	14	11		3	1						1	4			
2010	75	37		9	4					4	25	7			3
2011	69	50		16	6					1	20	8			1
2012	4	3								1					
2013	12	7		3	1					2	1	2			
2014	1	1													
2015	7	2			1					2	1	1			
Total	182	111		31	13					10	48	22			4
% Of All		61.0	0.0	17.0	7.1	0.0	0.0	0.0	0.0	5.5	26.4	12.1	0.0	0.0	

Information Leakage Attack-Enabler

- **Usernames**
  - Login Bruteforce
  - Social Engineering Emails (e.g., phishing, drive-by)
- Social Engineering Toolkit (SET)



EURECOM
Sophia Antipolis

Information Leakage Attack-Enabler

- **Commands, Resource Usage**
  - Mimicry and Blending Attacks

- How?
  - Learn normal system status/behaviour – *Xn*
  - When in malicious state *Xm*, stick as close as possibly to the legitimate state *Xn*

$$A(Xm) = \text{argmin } d(Xm, Xn), \text{ s.t., } d(Xm, Xn) < D$$

EURECOM
Sophia Antipolis

Reconaissance Types

- Active
  - Tools: NMAP, AMAP, Nessus
  - Pros: +/- accurate, wide range of info
  - Cons: noisy, triggers IPS/IDS

Reconaissance Types

- Active
  - Tools: NMAP, AMAP, Nessus
  - Pros: +/- accurate, wide range of info
  - Cons: noisy, triggers IPS/IDS

- **Passive**
  - **Search dorks: Google, Shodan**
  - Attack: Information Leakage and non-Authorization

Reconaissance
Passive

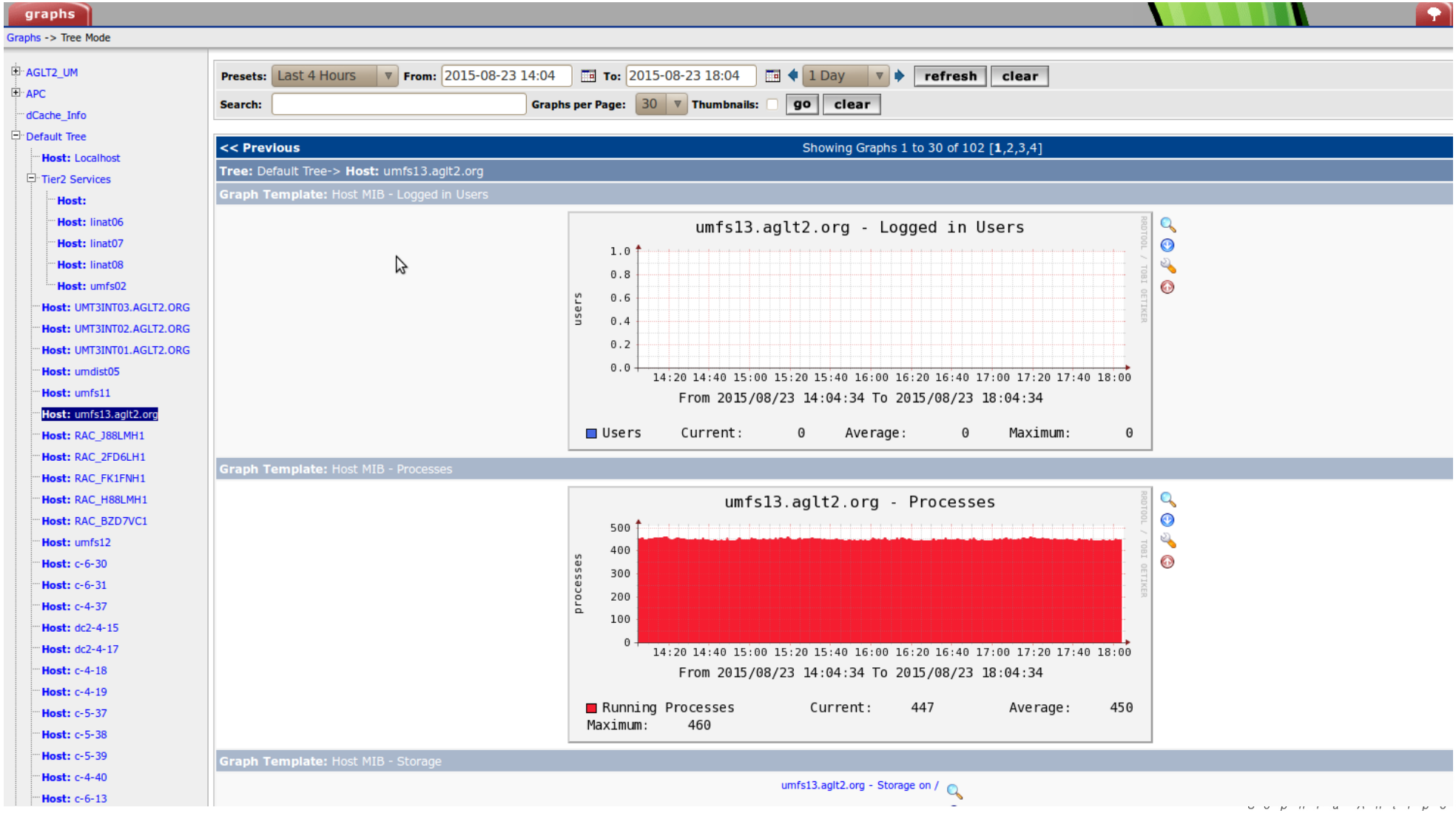
- Google dorks – Ganglia
  - intitle:"Cluster Report"
  - intitle:"Grid Report"
  - intitle:"Node View"
  - intitle:"Host Report"
  - intitle:"Ganglia:: "
  - "Ganglia Web Frontend version 2.0.0"

Reconaissance
Passive

- Google dorks – Cacti
  - inurl:"/cacti/graph_view.php"
  - intitle:"cacti" inurl:"graph_view.php"

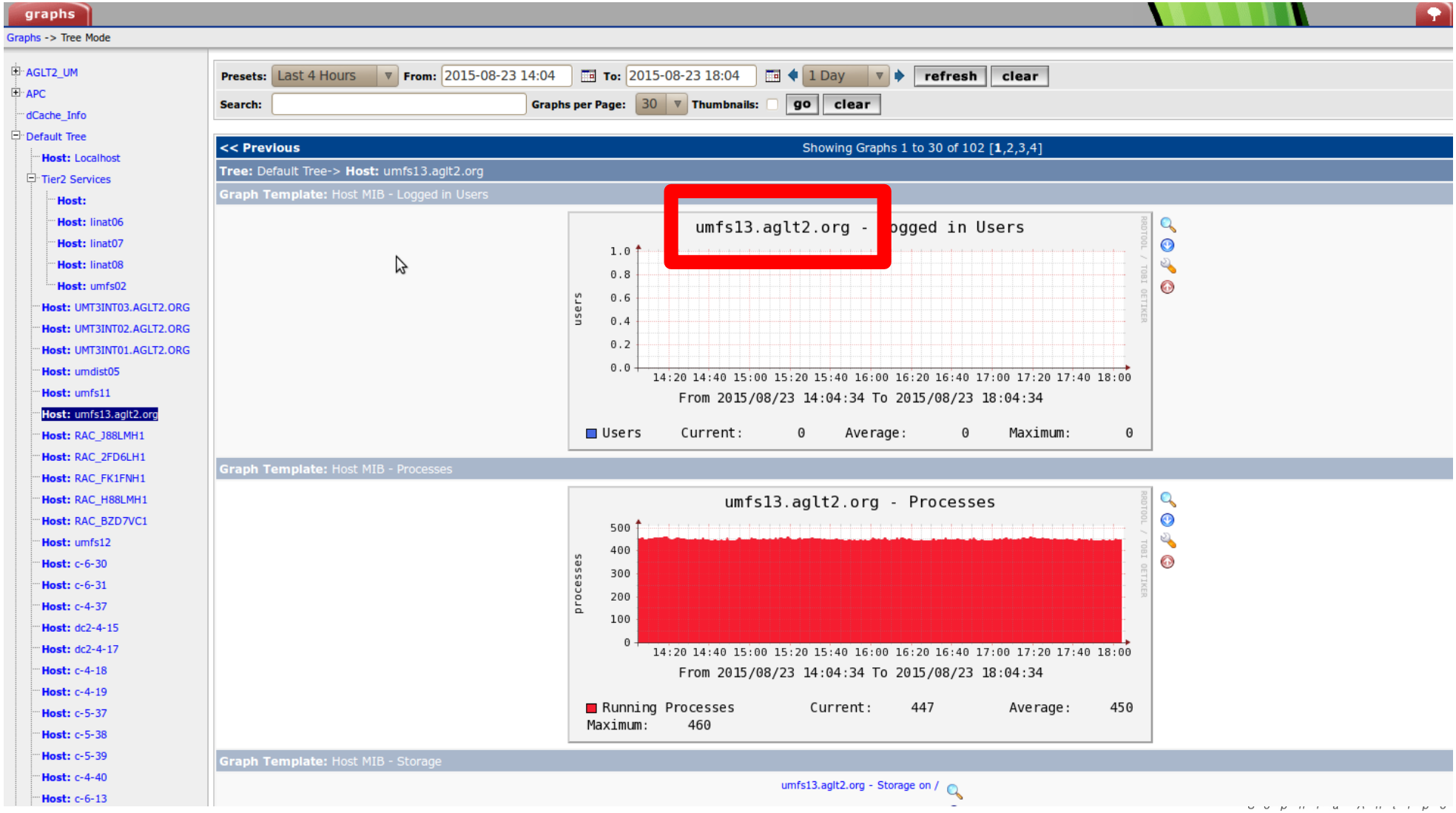
Reconaissance
Passive

- Google dorks – Cacti



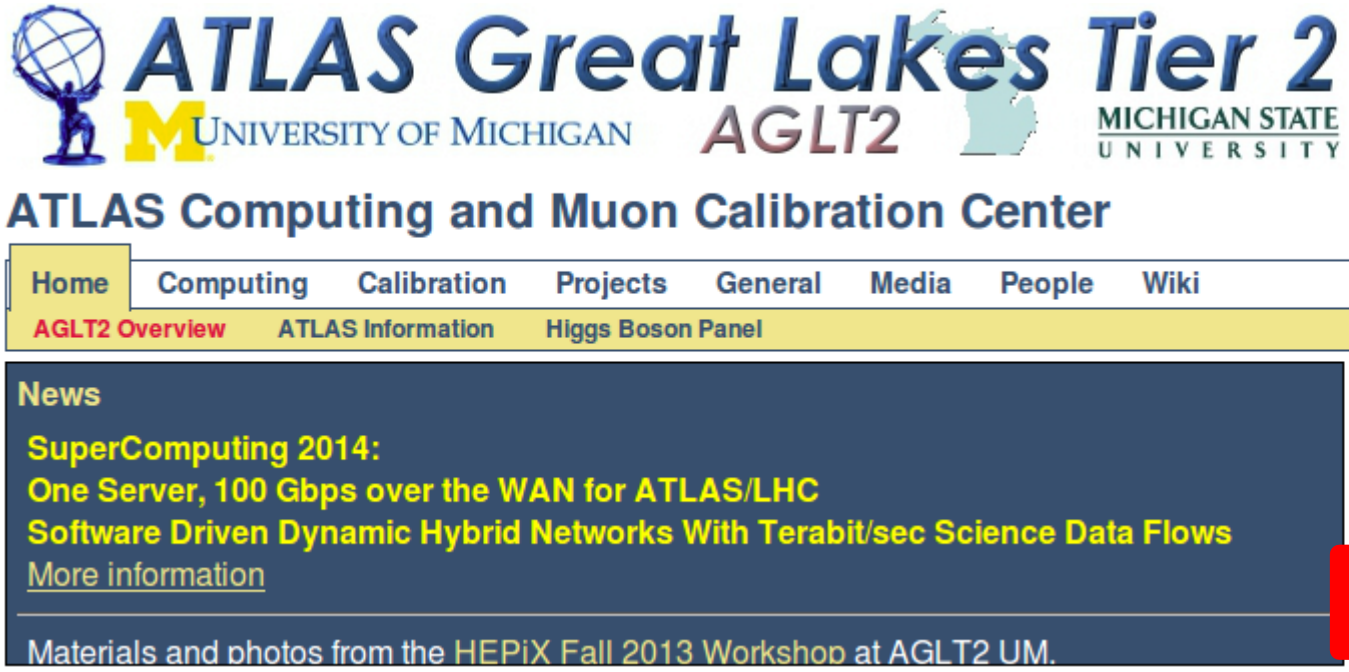
Reconaissance
Passive and **Recursive**

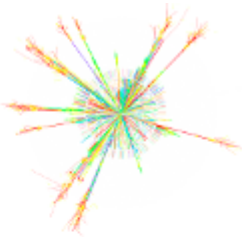
- Google dorks – Cacti → Ganglia



Reconaissance
Passive and **Recursive**

- Google dorks – Cacti → Ganglia
  - www.aglt2.org

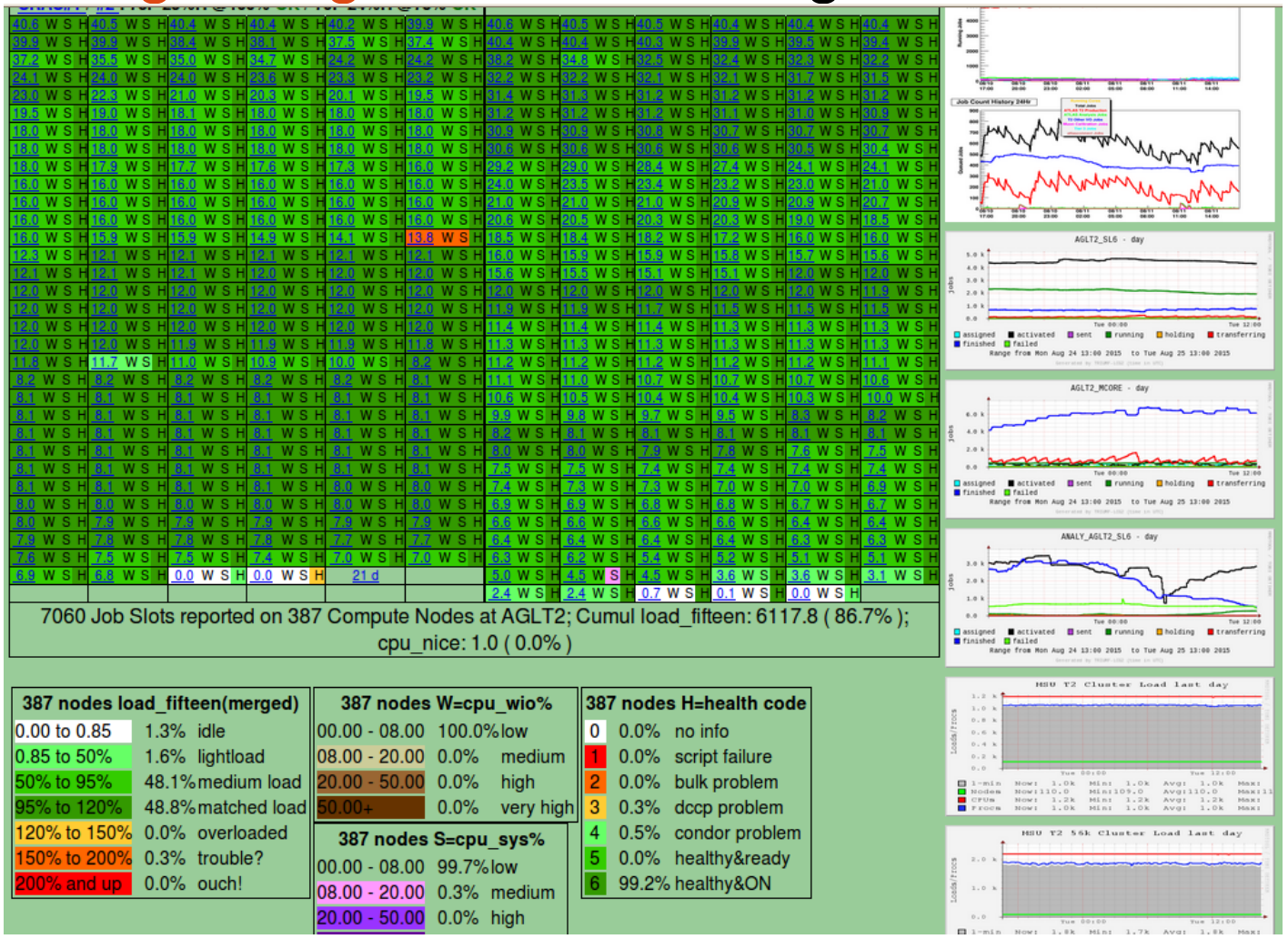




EURECOM
Sophia Antipolis

Reconaissance
Passive and **Recursive**

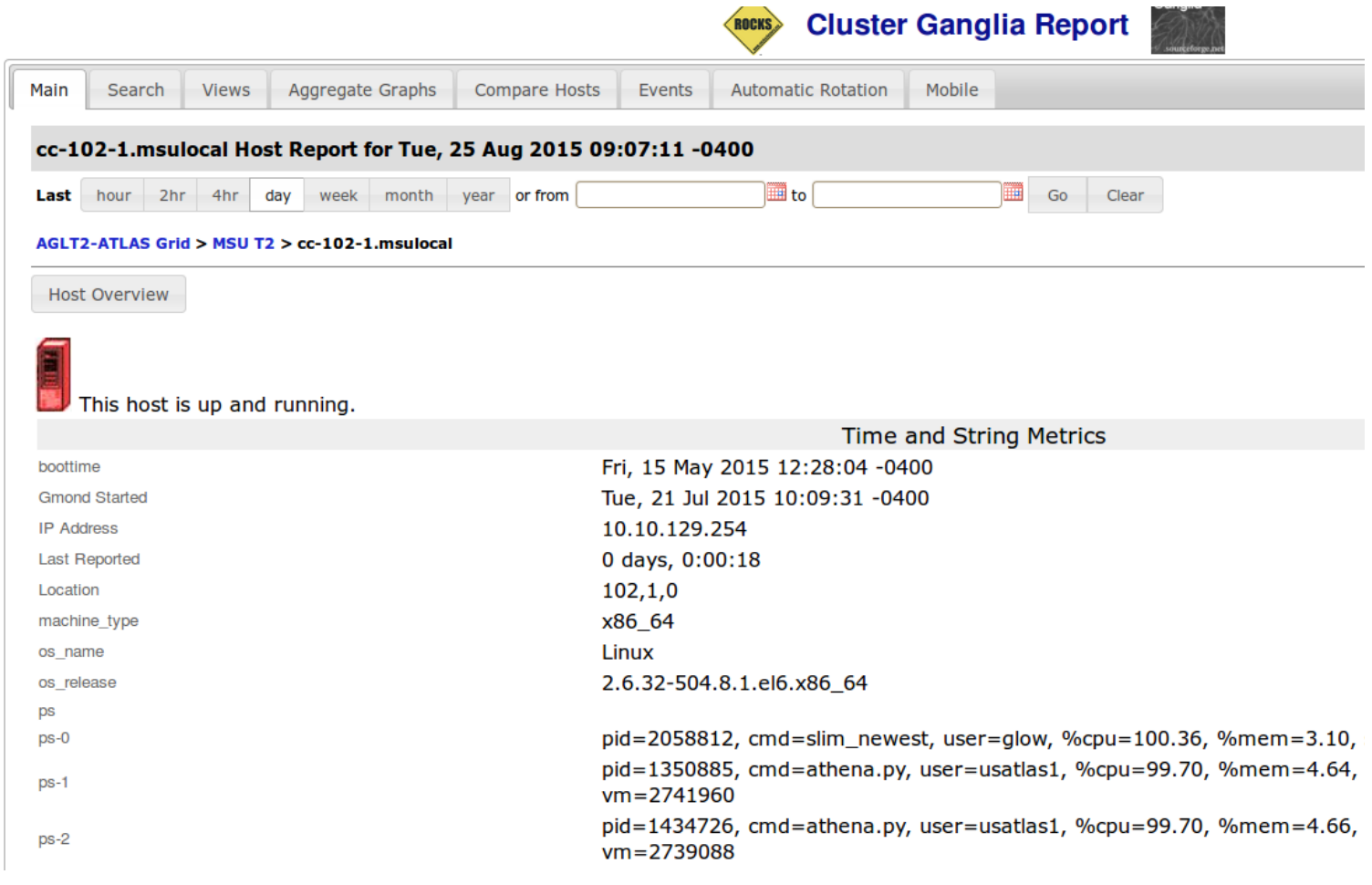
- Google dorks – Cacti → Ganglia
  - www.aglt2.org Job Status Page



EURECOM
Sophia Antipolis

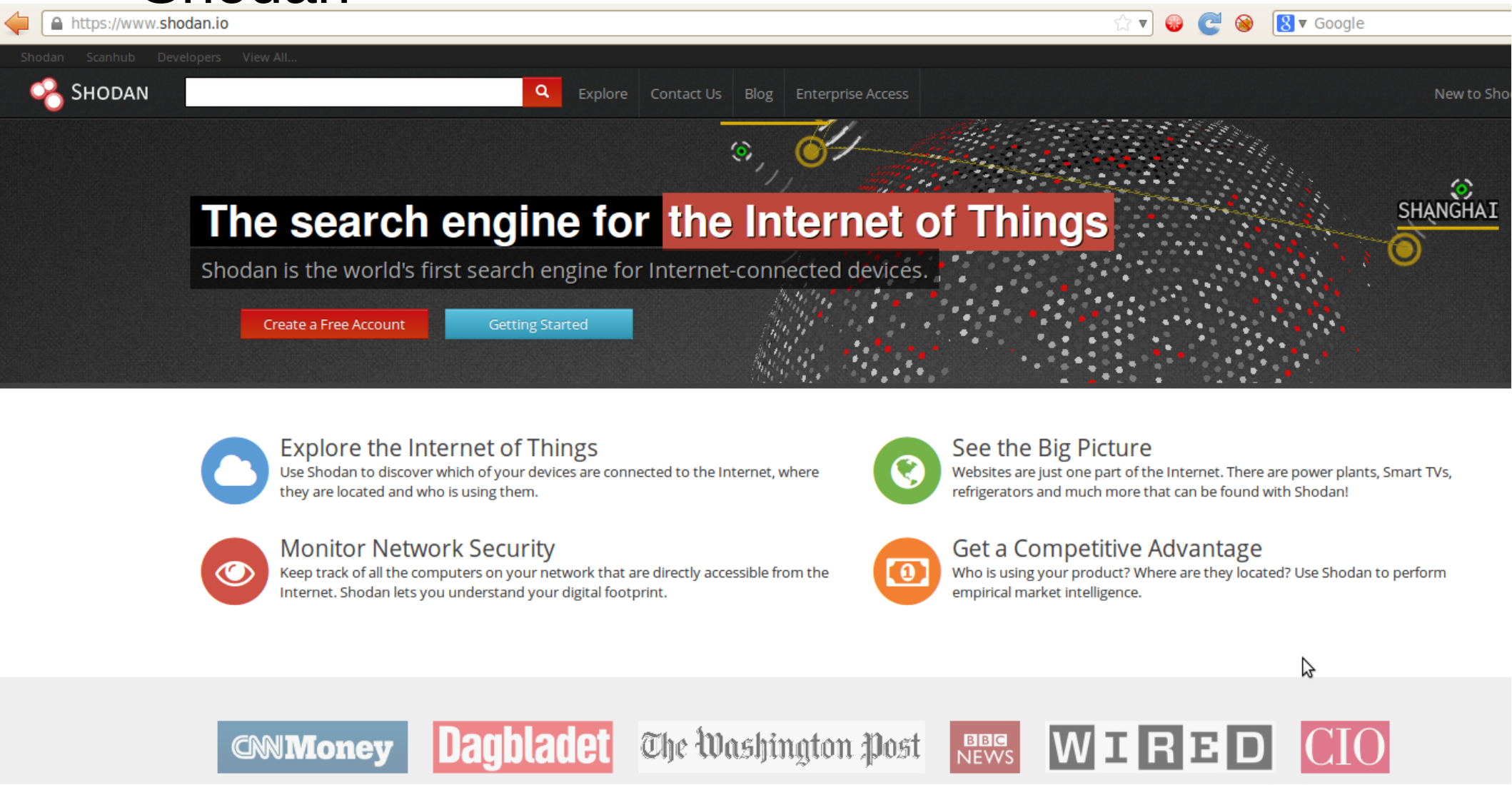
Reconaissance
Passive and **Recursive**

- Google dorks – Cacti → Ganglia
  - **From Cacti reached also to Ganglia!**



Reconaissance
Passive

- Shodan



Reconaissance Results

- Exposed web interfaces
  - **364** Ganglia
    - **~43K** nodes (web info leak)
    - ~1370 clusters
    - ~490 grids
  - 5K Cacti and 2K Observium

Reconaissance Results

- Exposed web interfaces
  - **364** Ganglia
    - **~43K** nodes (web info leak)
    - ~1370 clusters
    - ~490 grids
  - 5K Cacti and 2K Observium
- Exposed daemons
  - **~40K** publicly exposed Ganglia gmond nodes (XML Info Leak)

Reconaissance Results

TABLE I
DISTRIBUTION AND COUNTS OF UNIQUE HOSTS, SPLIT BY GANGLIA'S MODULE AND COUNTRY OF HOSTS' IP.

Country (iso2 code)	**Ganglia Gmond**	**Ganglia Web Frontend**
US	51%	32%
CN	10%	4%
KR	8%	8%
ES	6%	3%
FR	4%	3%
TW	3%	7%
DE	3%	3%
IT	$\approx$ 1%	3%
CH	$\ll$ 1%	5%
Others	14%	32%
Total (count)	39553	364

Reconaissance Results

- 43K nodes on 364 Ganglia Web Interfaces

EURECOM
Sophia Antipolis

Reconaissance Results

- 43K nodes on 364 Ganglia Web Interfaces
- 120 main kernel versions
  - 411 kernel sub-versions

Reconaissance Results

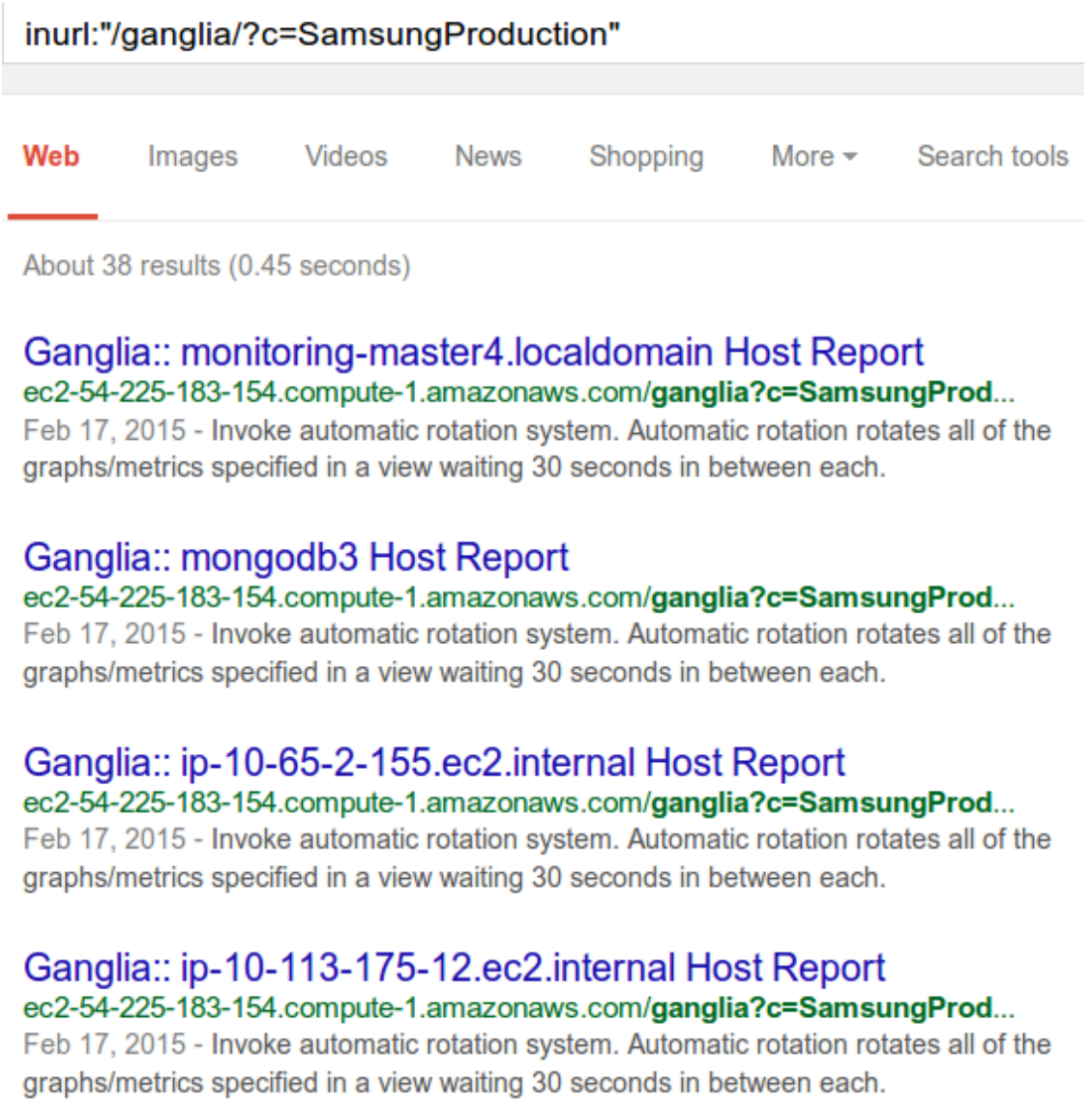
- 43K nodes on 364 Ganglia Web Interfaces
- 120 main kernel versions
  - 411 kernel sub-versions
- Kernel version 2.6.32 most popular
  - Runs on 38% of the 43K hosts
  - Hundreds of vulnerabilities in all 2.6.32 kernels (according to CVEdetails)

Reconaissance Results

- 43K nodes on 364 Ganglia Web Interfaces
- 120 main kernel versions
  - 411 kernel sub-versions
- Kernel version 2.6.32 most popular
  - Runs on 38% of the 43K hosts
  - Hundreds of vulnerabilities in all 2.6.32 kernels (according to CVEdetails)
- **Secured** kernels
  - *grsecurity* on 9 hosts (only!)
  - *hardened-sources* on 6 hosts (only!)

Reconaissance Results

- *amzn* kernels on 45 hosts (~0.1%)



Reconaissance Results

- 364 Ganglia Web Frontends
- Only 42 (i.e., 11.5%) run HTTPS
- Only 16 (i.e., 4.4%) run **trusted*** HTTPS
  - *Did not perform tests of weak/flawed HTTPS implementations

EURECOM
Sophia Antipolis

Static and Dynamic Analysis

- Static analysis
  - *”Static analysis is the process of testing an application by examining its source code, byte code or application binaries for conditions leading to a security vulnerability, without actually running it.”*
- Tools
  - We use RIPS for Ganglia **Web** Frontend (**PHP**)
  - More tools

Static and Dynamic Analysis

- Dynamic analysis
  - *”Dynamic analysis is the process of testing the application by running it.”*
- Tools
  - We use Arachni Scanner for Ganglia **Web** Frontend

Static and Dynamic Analysis

- Analysis data
  - 25 Ganglia versions (static + dynamic)
    - 4 JobMonarch plugin versions (static only)
  - 35 Cacti versions (static only)
  - 1 Observium version (static only)

Static Analysis

- Ganglia
  - Between 87 and 145 total reports per version
  - Between 43 and 92 **XSS** reports per version

Static Analysis

- Ganglia
  - Between 87 and 145 total reports per version
  - Between 43 and 92 **XSS** reports per version
- Cacti
  - Between 189 and 400 total reports per version
  - Between 92 and 265 **XSS** reports per version

Static Analysis

- Ganglia
  - Between 87 and 145 total reports per version
  - Between 43 and 92 **XSS** reports per version
- Cacti
  - Between 189 and 400 total reports per version
  - Between 92 and 265 **XSS** reports per version
- Observium
  - 82 total reports per version
  - 52 **XSS** reports per version

Static Analysis

- Ganglia
  - Between 87 and 145 total reports per version
  - Between 43 and 92 **XSS** reports per version
- Cacti
  - Between 189 and 400 total reports per version
  - Between 92 and 265 **XSS** reports per version
- Observium
  - 82 total reports per version
  - 52 **XSS** reports per version
- Some totals
  - 7553 **XSS** reports
  - Manual triage and confirmation does not scale!

Static Analysis

Version / Vulnerability Type	CE	HTRS	CI	HI	PFC	UNS	SQLI	LDAPI	FI	FM	FD	XSS	TOTAL/version
cacti-0.8	0	68	2	0	21	5	0	0	0	1	0	92	189
cacti-0.8.1	0	68	2	0	21	5	0	0	0	1	0	95	192
cacti-0.8.2	0	68	2	0	21	5	0	0	0	1	0	95	192
cacti-0.8.2a	0	68	2	0	21	5	0	0	0	1	0	95	192
cacti-0.8.3	0	70	2	0	21	5	0	0	0	1	0	102	201
cacti-0.8.3a	0	70	2	0	21	5	0	0	0	1	0	102	201
cacti-0.8.4	0	75	4	0	23	5	0	0	0	1	2	98	208
cacti-0.8.5	0	78	4	0	26	5	0	0	0	1	2	113	229
cacti-0.8.5a	0	78	4	0	23	5	0	0	0	1	2	116	229
cacti-0.8.6	2	78	5	1	25	7	0	0	1	7	5	160	291
cacti-0.8.6a	2	78	5	1	25	7	0	0	1	7	6	161	293
cacti-0.8.6b	2	78	5	1	25	7	0	0	1	7	4	161	291
cacti-0.8.6c	2	78	5	1	25	7	0	0	1	7	5	161	292
cacti-0.8.6d	2	78	5	1	25	7	0	0	1	7	5	160	291
cacti-0.8.6e	2	78	5	1	25	7	0	0	1	7	5	179	310
cacti-0.8.6f	2	78	6	1	25	7	0	0	1	7	5	180	312
cacti-0.8.6g	2	78	6	1	27	7	0	0	1	8	5	179	314
cacti-0.8.6h	2	78	6	1	29	7	0	0	1	8	5	190	327
cacti-0.8.6i	2	78	5	1	29	7	0	0	1	7	5	261	396
cacti-0.8.6j	2	78	5	1	29	7	0	0	1	7	5	265	400
cacti-0.8.6k	2	78	5	1	29	7	0	0	1	7	5	234	369
cacti-0.8.7	2	78	3	1	30	10	0	1	1	7	5	205	343
cacti-0.8.7a	2	78	3	1	30	10	0	1	1	7	5	205	343
cacti-0.8.7b	2	78	3	1	30	10	0	1	1	7	5	154	292
cacti-0.8.7c	2	78	3	1	31	11	0	1	1	10	3	202	343
cacti-0.8.7d	2	78	3	1	31	11	0	1	1	10	3	206	347
cacti-0.8.7e	2	78	3	1	31	11	0	1	1	10	3	208	349
cacti-0.8.7g	2	77	2	1	29	11	0	0	1	8	3	141	275
cacti-0.8.7h	33	75	2	1	1	11	0	0	1	8	3	159	294
cacti-0.8.7i	33	75	2	1	1	11	0	0	1	8	3	159	294
cacti-0.8.7i-PIA-3.1	38	76	2	1	1	11	0	0	2	8	3	169	311
cacti-0.8.8	36	76	2	1	1	11	0	0	2	8	3	169	309
cacti-0.8.8a	36	76	2	1	1	11	0	0	2	8	3	169	309
cacti-0.8.8b	36	76	2	1	1	11	0	0	2	8	3	169	309
cacti-0.8.8c	36	77	2	1	1	11	0	0	2	8	3	204	345
ganglia_jobmonarch-1.0	0	0	1	0	3	2	0	0	0	0	0	1	7
ganglia_jobmonarch-1.1	0	0	1	0	3	2	0	0	0	0	0	1	7
ganglia_jobmonarch-1.1.1	0	0	1	0	3	2	0	0	0	0	0	1	7
ganglia_jobmonarch-1.1.2	0	0	1	0	3	2	0	0	0	0	0	1	7
ganglia-web-3.4.1	0	3	1	1	2	14	0	0	0	16	14	89	140
ganglia-web-3.4.2	0	3	1	1	2	14	0	0	0	16	14	90	141
ganglia-web-3.5.0	0	3	1	1	2	14	0	0	0	16	15	87	139
ganglia-web-3.5.10	0	3	1	1	2	13	0	0	0	13	11	43	87
ganglia-web-3.5.1	0	3	1	1	2	15	0	0	0	16	16	89	143
ganglia-web-3.5.11	0	3	3	1	2	13	0	0	0	12	12	46	92
ganglia-web-3.5.12	0	3	3	1	2	13	0	0	0	12	12	46	92
ganglia-web-3.5.2	0	3	1	1	2	15	0	0	0	16	15	90	143
ganglia-web-3.5.3	0	3	1	1	2	15	0	0	0	16	15	92	145
ganglia-web-3.5.4	0	3	1	1	2	15	0	0	0	16	15	92	145
ganglia-web-3.5.7	0	3	1	1	2	15	0	0	0	16	12	60	110
ganglia-web-3.5.8	0	3	1	1	2	13	0	0	0	13	11	43	87
ganglia-web-3.6.2	0	2	2	1	2	17	0	0	0	12	11	47	94
gweb-2.0.0	0	3	1	1	2	5	0	0	0	7	8	69	96
gweb-2.1.1	0	3	3	1	2	5	0	0	0	9	10	74	107
gweb-2.1.2	0	3	3	1	2	5	0	0	0	10	10	74	108
gweb-2.1.3	0	3	3	1	2	5	0	0	0	10	10	74	108
gweb-2.1.5	0	3	1	1	2	5	0	0	0	8	8	72	100
gweb-2.1.6	0	3	3	1	2	5	0	0	0	9	10	76	109
gweb-2.1.7	0	3	3	1	2	5	0	0	0	9	10	76	109
gweb-2.1.8	0	3	1	1	2	6	0	0	0	13	10	75	111
gweb-2.2.0	0	3	1	1	2	12	0	0	0	20	12	92	143
gweb-3.3.0	0	3	1	1	2	13	0	0	0	18	15	92	145
gweb-3.3.1	0	3	1	1	2	13	0	0	0	18	14	92	144
observium	0	1	2	0	3	3	4	0	9	5	4	51	82
TOTAL/vulnerability	286	2727	166	50	798	556	4	6	40	536	408	7553	-

EURECOM
Sophia Antipolis

Static and Dynamic Analysis

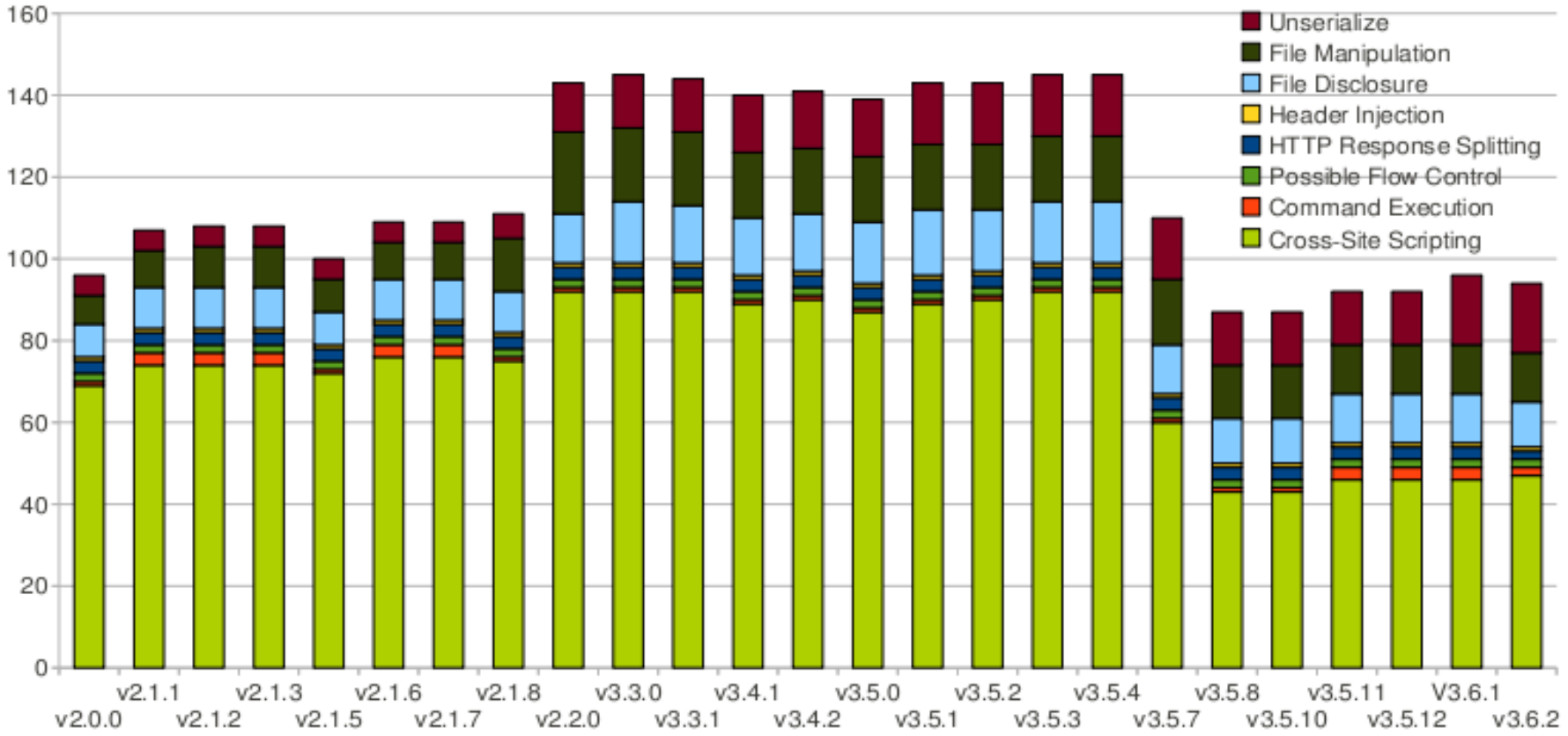


Fig. 1. Vulnerabilities in Ganglia Web Frontend found statically with RIPS. Distribution by Ganglia's version and vulnerability type.

EURECOM
Sophia Antipolis

Static and Dynamic Analysis

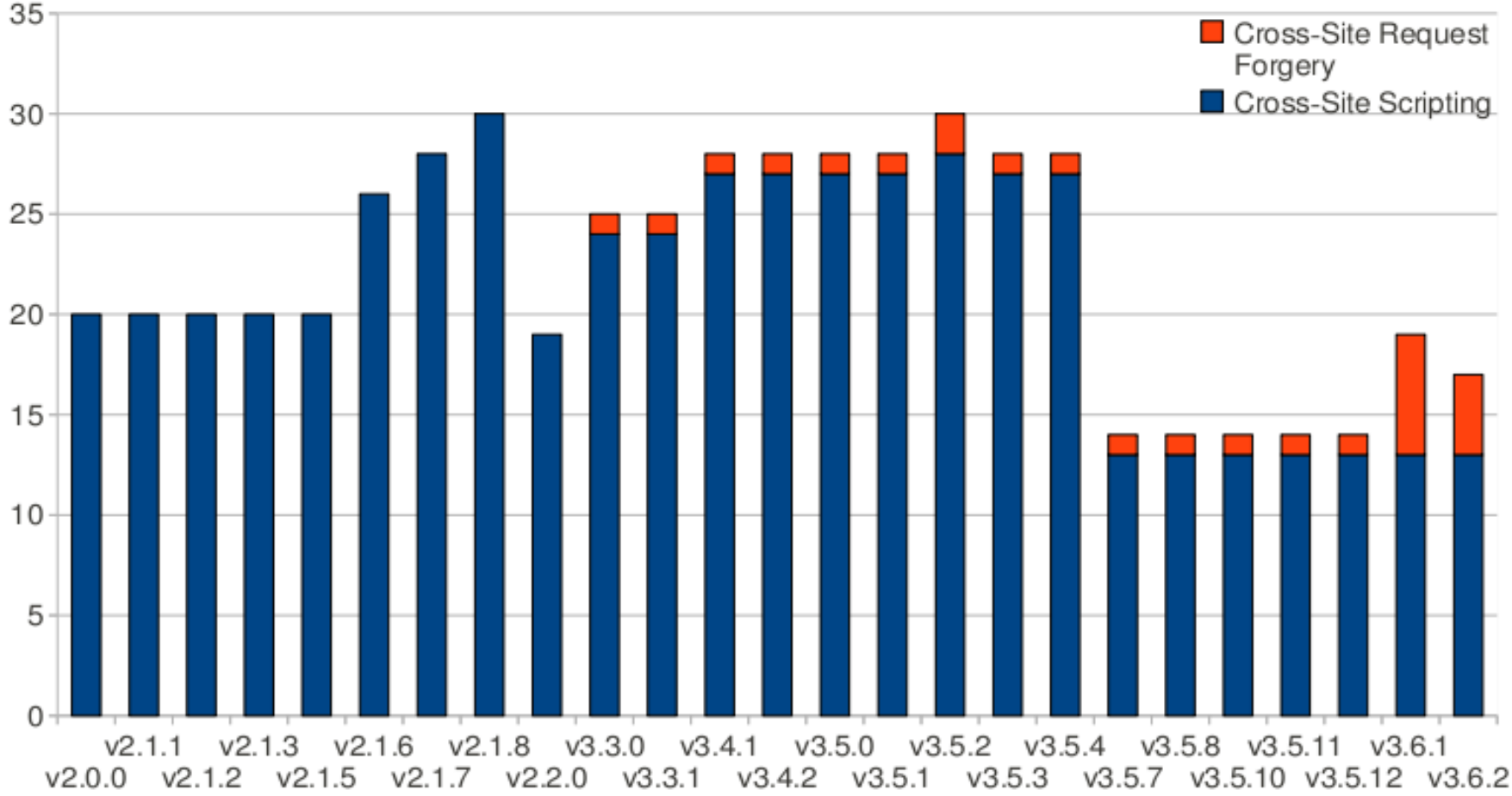


Fig. 2. Vulnerabilities in Ganglia Web Frontend found dynamically with Arachni. Distribution by Ganglia's version and vulnerability type.

Static and Dynamic Analysis

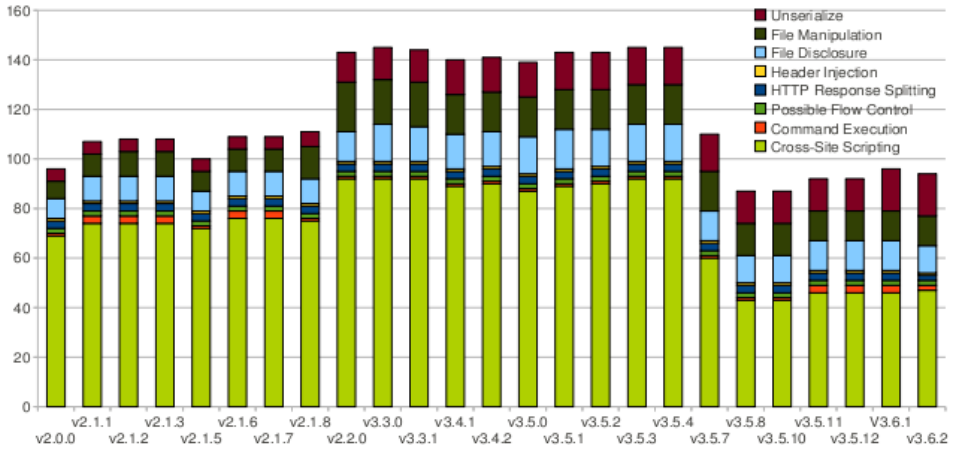


Fig. 1. Vulnerabilities in Ganglia Web Frontend found statically with RIPS. Distribution by Ganglia's version and vulnerability type.

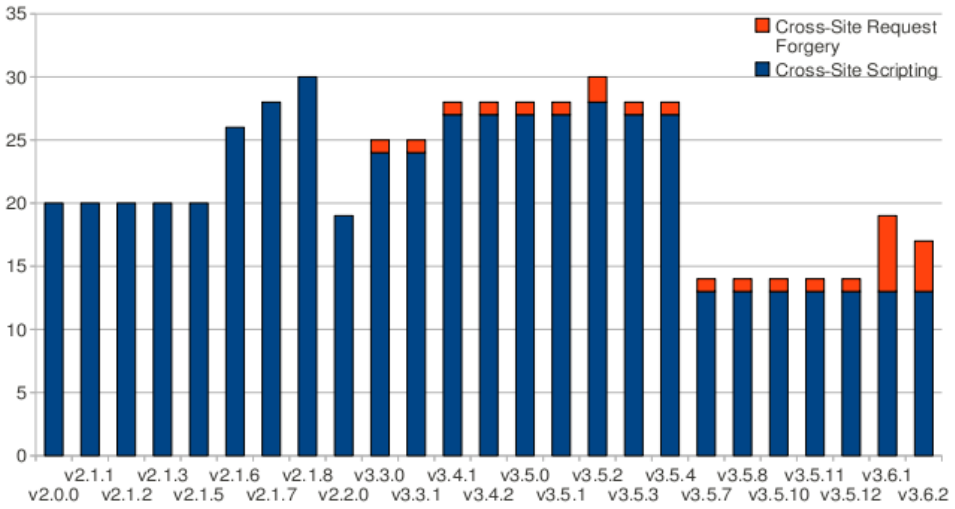


Fig. 2. Vulnerabilities found dynamically with Arachni. Distribution by Ganglia's version and vulnerability type.

EURECOM
Sophia Antipolis

Static and Dynamic Analysis

- 364 Ganglia Web Interfaces
  - 193 of them (i.e., 53%) run Ganglia Web ver < **3.5.1**

CVE-2012-3448

Name	CVE-2012-3448
Description	Unspecified vulnerability in Ganglia Web before 3.5.1 allows remote attackers to execute arbitrary PHP code via unknown attack vectors.
Source	CVE (at NVD; oss-sec, fulldisc, OSVDB, EDB, Metasploit, Red Hat, Ubuntu, Gentoo, SuSE, Mageia, more)
References	DSA-2610-1
NVD severity	high (attack range: remote)
Debian Bugs	683584

Static and Dynamic Analysis

- 364 Ganglia Web Interfaces
  - 193 of them (i.e., 53%) run Ganglia Web ver < **3.5.1**

CVE-2012-3448

Name	CVE-2012-3448
Description	Unspecified vulnerability in Ganglia Web before 3.5.1 allows remote attackers to execute arbitrary PHP code via unknown attack vectors.
Source	CVE (at NVD; oss-sec, fulldisc, OSVDB, EDB, Metasploit, Red Hat, Ubuntu, Gentoo, SuSE, Mageia, more)
References	DSA-2610-1
NVD severity	high (attack range: remote)
Debian Bugs	683584

Vulnerability Analysis

- CVE-2012-3448

e/cloudsec/ganglia-web/ganglia-web-3.5.0/graph.php
183 Encoding: UTF-8 Line end style: Unix

```
if ( ! isset($graph_config) ) {
    if ( ($graph == "metric") &&
         isset($_GET['title']) &&
         $_GET['title'] !== '')
      $metrictitle = sanitize($_GET['title']);
  $php_report_file = $conf['graphdir'] . "/" . $graph . ".php";
  $json_report_file = $conf['graphdir'] . "/" . $graph . ".json";
  if(_is_file(_$php_report_file)_){


    include_once $php_report_file;
    $graph_function = "graph_${graph}";
    if (isset($graph_arguments))
      eval('$graph_function($rrdtool_graph,' . $graph_arguments . ');');
    else
      $graph_function( $rrdtool_graph );  // Pass by reference call, $rrdtool_graph modified inplace
  } else if ( is_file( $json_report_file ) ) {
    $graph_config = json_decode( file_get_contents( $json_report_file ), TRUE );

    # We need to add hostname and clustername if it's not specified
```

B: /home/cloudsec/ganglia-web/ganglia-web-3.5.1/graph.php
Top line 490 Encoding: UTF-8 Line end style: Unix

```
    if ( ! isset($graph_config) ) {
        if ( ($graph == "metric") &&
             isset($_GET['title']) &&
             $_GET['title'] !== '')
          $metrictitle = sanitize($_GET['title']);
      $php_report_file = $conf['graphdir'] . "/" . $graph . ".php";
      $json_report_file = $conf['graphdir'] . "/" . $graph . ".json";

      # Check for path traversal issues by making sure real path is actually in graphdir

      if( is_file( $php_report_file ) and dirname(realpath($php_report_file)) ==  $conf['graphdir'] ) {
        include_once $php_report_file;
        $graph_function = "graph_${graph}";
        #if (isset($graph_arguments))
        #  eval('$graph_function($rrdtool_graph,' . $graph_arguments . ');');
        #else
        $graph_function( $rrdtool_graph );  // Pass by reference call, $rrdtool_graph modified inplace
      } else if ( is_file( $json_report_file )and_dirname(realpath($json_report_file))==__$conf['graphdi
        $graph_config = json_decode( file_get_contents( $json_report_file ), TRUE );

        # We need to add hostname and clustername if it's not specified
```

EURECOM
Sophia Antipolis

Vulnerability Analysis

- CVE-2012-3448
- Exploit DB 38030

Ganglia Web Frontend < 3.5.1 - PHP Code Execution

EDB-ID: 38030	**CVE:** 2012-3448	**OSVDB-ID:** 84240
Verified: ✖	**Author:** Andrei Costin	**Published:** 2015-08-31
Download Exploit: Source Raw	**Download Vulnerable App:**	

« Previous Exploit

```
<?php
/*

##############################################################################
#
# Author     : Andrei Costin (andrei theATsign firmware theDOTsign ro)
# Desc       : CVE-2012-3448 PoC
# Details    : This PoC will create a dummy file in the /tmp folder and
#              will copy /etc/passwd to /tmp.
#              To modify the attack payload, modify the code below.\
# Setup      : Ubuntu Linux 14.04 LTS x86 with Ganglia Web Frontend 3.5.0
#
##############################################################################

1. Assuming that ganglia is installed on the target machine at this path:
/var/www/html/ganglia/

2. Assuming the attacker has minimal access to the target machine and
can write to "/tmp". There are several methods where a remote attacker can
also trigger daemons or other system processes to create files in "/tmp"
whose content is (partially) controlled by the remote attacker.
```

EURECOM
Sophia Antipolis

Countermeasures

- Periodic upgrade to latest versions
  - Need better coding practices for NMS
  - Manual patching where applicable

Countermeasures

- Periodic upgrade to latest versions
  - Need better coding practices for NMS
  - Manual patching where applicable
- Password protect
  - E.g., basic HTTP authentication

Countermeasures

- Periodic upgrade to latest versions
  - Need better coding practices for NMS
  - Manual patching where applicable
- Password protect
  - E.g., basic HTTP authentication
- HTTPS
  - Not self-signed certificates!

Contributions

- First to systematically analyze at large scale the risks and vulnerabilities posed by the use of web monitoring tools

Contributions

- First to systematically analyze at large scale the risks and vulnerabilities posed by the use of web monitoring tools

- Collected and analyzed the internal details of networks and systems of a large number of grid and cluster environments
  - Investigated the risks of such data being openly available to the large public

Conclusions

- Large number of NMS web interfaces publicly exposed
  - Too many run obsolete exploitable versions (~53%)
  - Too few run proper HTTPS (~4.4%)

Conclusions

- Large number of NMS web interfaces publicly exposed
  - Too many run obsolete exploitable versions (~53%)
  - Too few run proper HTTPS (~4.4%)
- Big amount of infrastructure details publicly exposed
  - More than 40K nodes

Conclusions

- Large number of NMS web interfaces publicly exposed
  - Too many run obsolete exploitable versions (~53%)
  - Too few run proper HTTPS (~4.4%)
- Big amount of infrastructure details publicly exposed
  - More than 40K nodes
- Many vulnerabilities reported in NMS tools

Conclusions

- Large number of NMS web interfaces publicly exposed
  - Too many run obsolete exploitable versions (~53%)
  - Too few run proper HTTPS (~4.4%)
- Big amount of infrastructure details publicly exposed
  - More than 40K nodes
- Many vulnerabilities reported in NMS tools
- Privacy and security of cloud monitoring is not yet completely sufficient

EURECOM
Sophia Antipolis

Reference

- *A. Costin, "All your cluster-grids are belong to us: Monitoring the (in)security of infrastructure monitoring systems", Proceedings of the 1st IEEE Workshop on Security and Privacy in the Cloud (SPC), Florence Italy, September 2015.*

Thank You!

Questions?

{name.surname}@eurecom.fr