

Hacking and Securing Network Monitoring Systems:

End-to-end walkthrough example on Ganglia

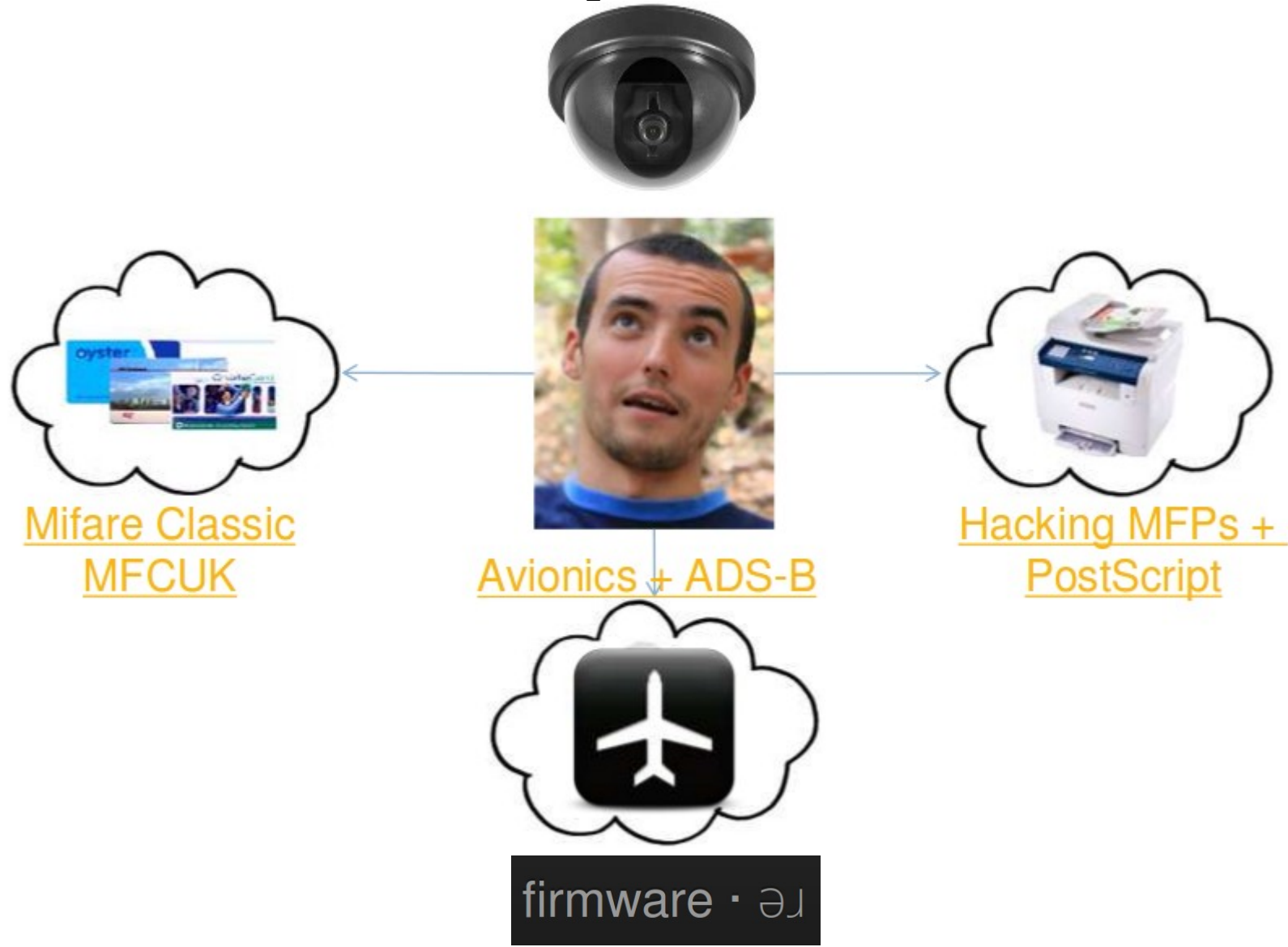
Andrei Costin

www.firmware.re

@costinandrei

#whoami

- Embedded security researcher, fresh Dr. :)



Agenda

- Introduction
- Overview of NMS
- Attack Lifecycle
- Pre-Attack
- Static Analysis
- Dynamic Analysis
- Vulnerability Analysis
- Exploit Development
- Conclusion

Introduction

What is Cloud Computing?

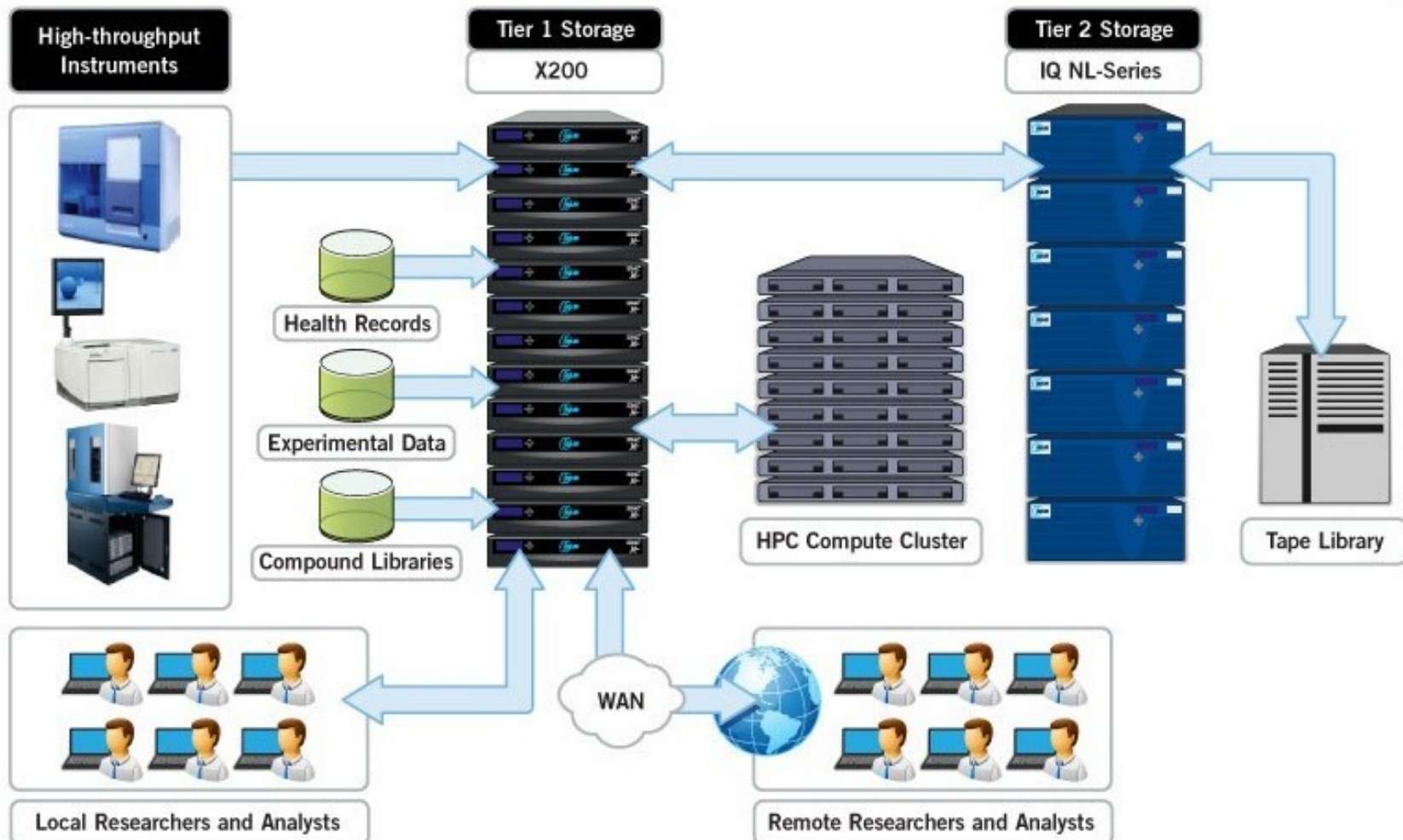
*"When broken down, cloud computing is a specialized distributed computing model. Building upon the desirable characteristics of **cluster, grid, utility**, and service-oriented computing, cloud computing introduces a unique complement of features to create a new computing paradigm"*

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

Introduction

What is HPC?

Typical HPC Workflow



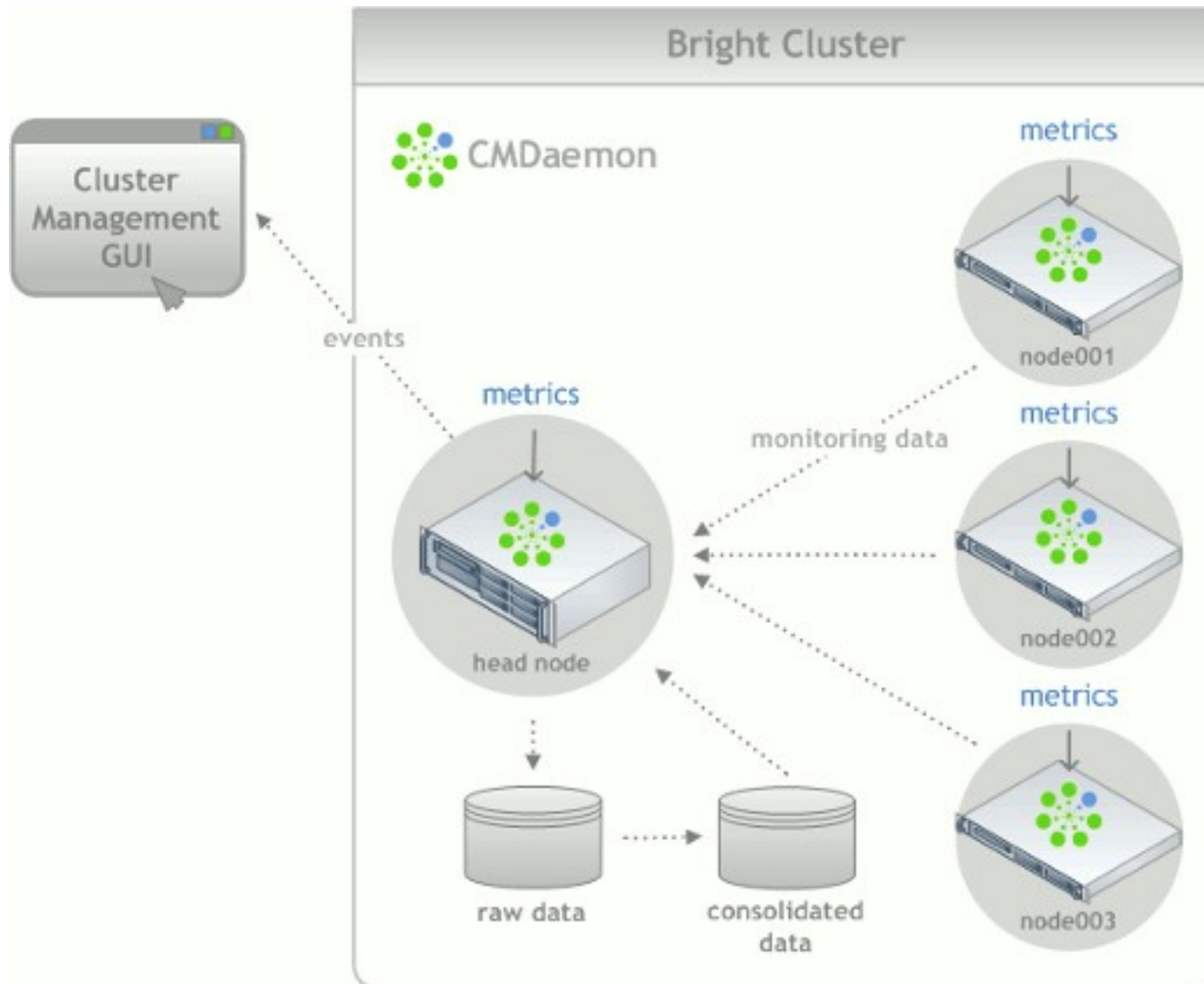
Introduction

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?



Overview of NMS

What are the tools?



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"

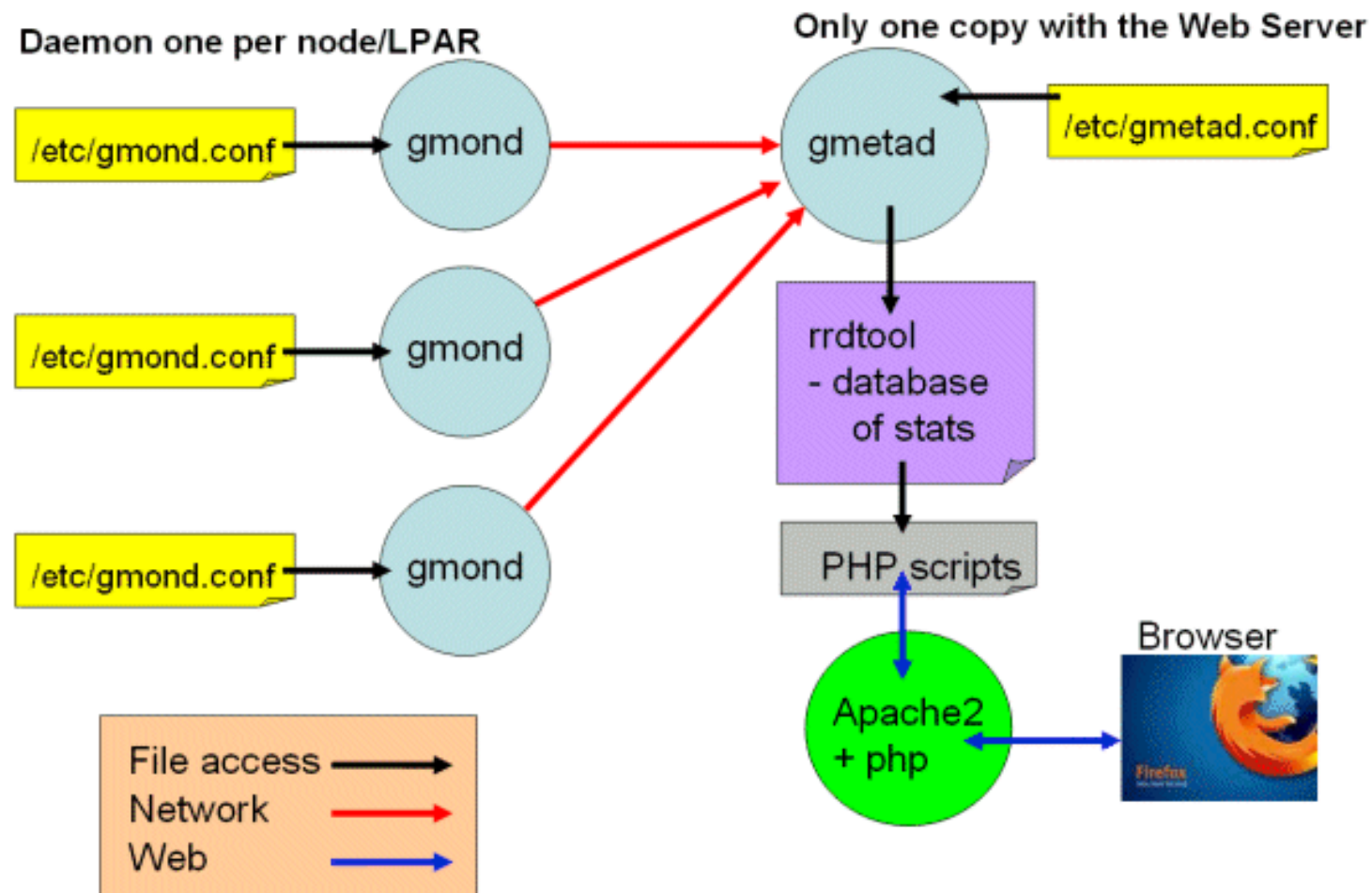
- **Observium**

"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?

Ganglia Data Flow



Overview of NMS

How they work?

- **Hands-On**
 - **exercise_setup.txt**
 - Check Ganglia installation
 - Check Ganglia info leak

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](#)
[Oinetia](#)



[Cummins](#)
[freescape](#)
[Sandia National Laboratories](#)
[Rocketcalc](#)
[Yale](#)
[Deutsches Elektronen-Synchrotron](#)
[bp](#)
[Nortel](#)
[LexisNexis](#)
[Landmark](#)
[SARA](#)
[Bellsouth](#)
[University of Pisa, Italy](#)
[X-ISS](#)
[Tennessee 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.](#)
[GlobeExplorer](#)
[John Deere](#)
[Xilinx](#)
[Freddie Mac](#)
[jeteye](#)
[Tokyo Institute of Technology](#)
[Purdue University](#)
[Stanford](#)
and **thousands** of other people just ask
[Google](#).

Attack Lifecycle

First step?

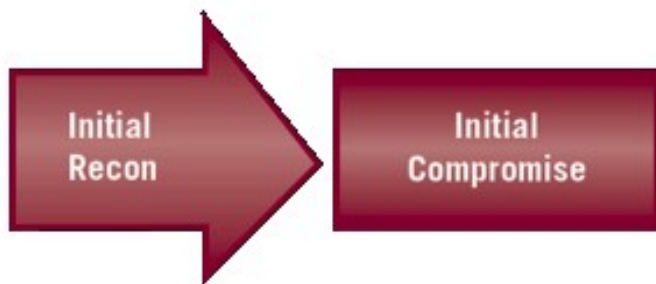
Attack Lifecycle

First step?



Initial
Recon

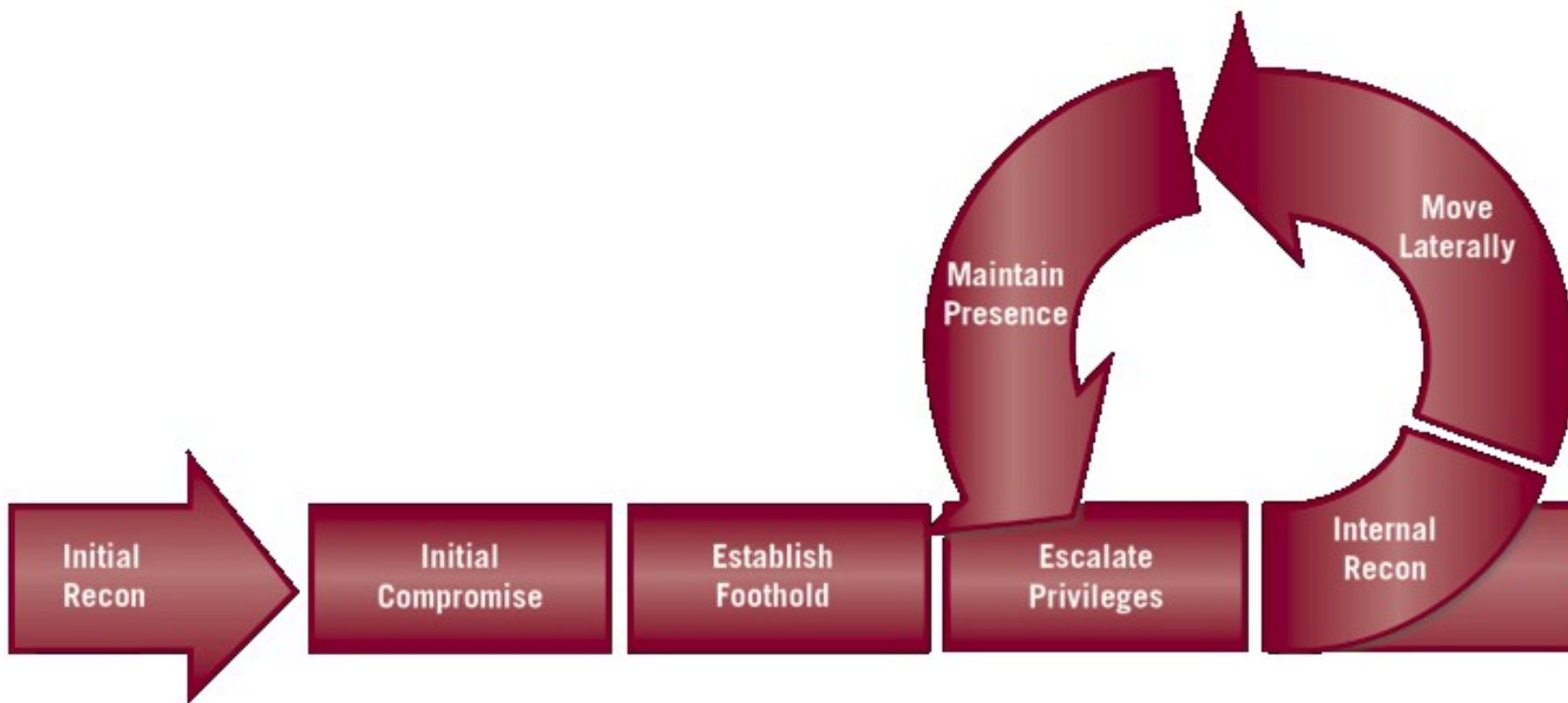
Attack Lifecycle



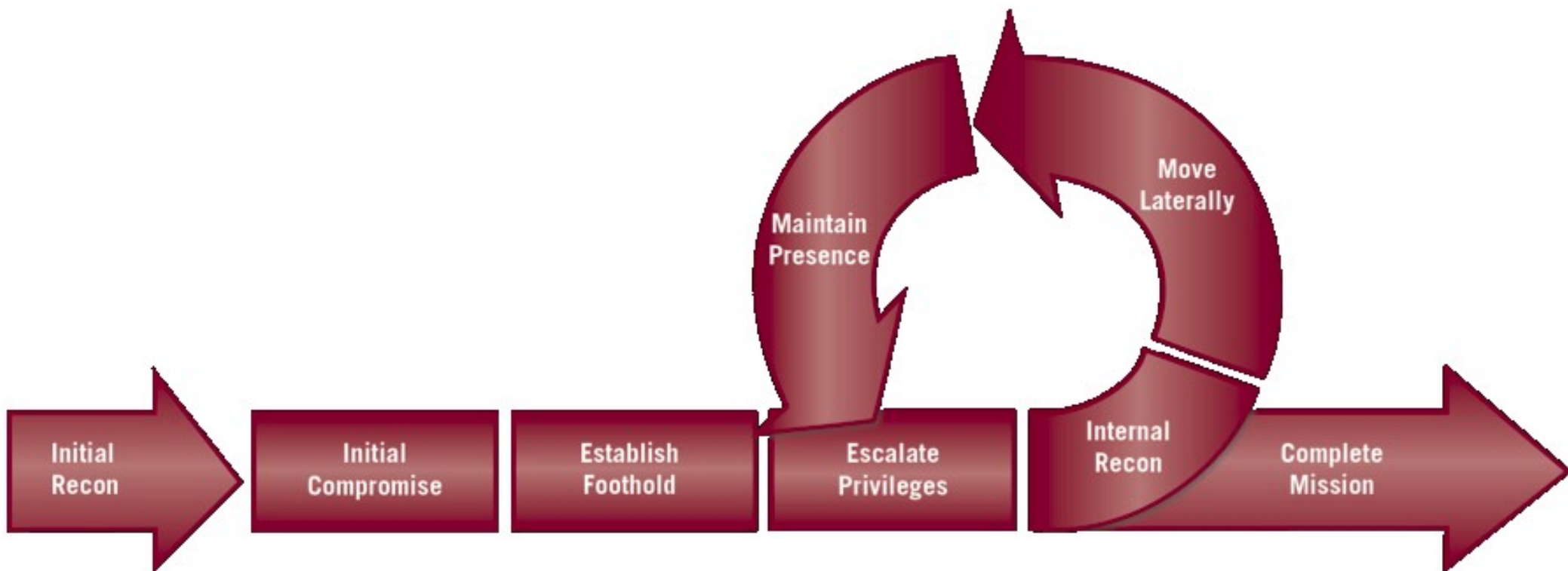
Attack Lifecycle



Attack Lifecycle



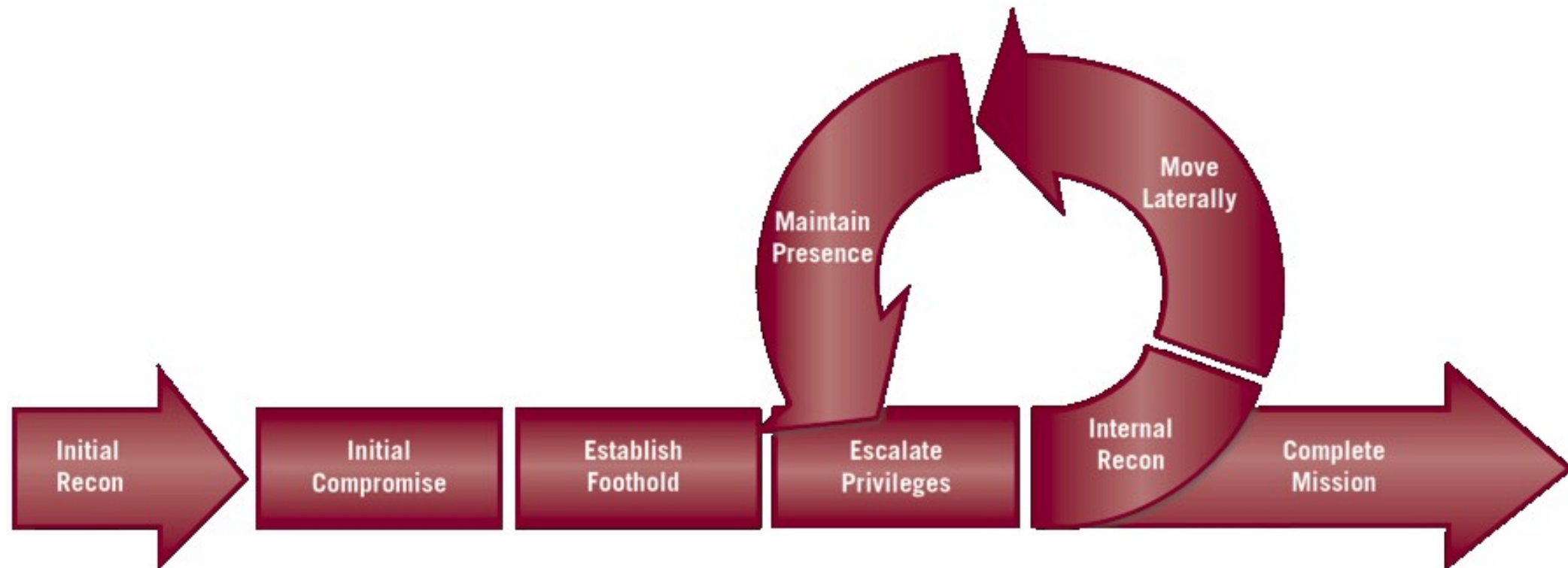
Attack Lifecycle



Attack Lifecycle

Attack Types on NMS

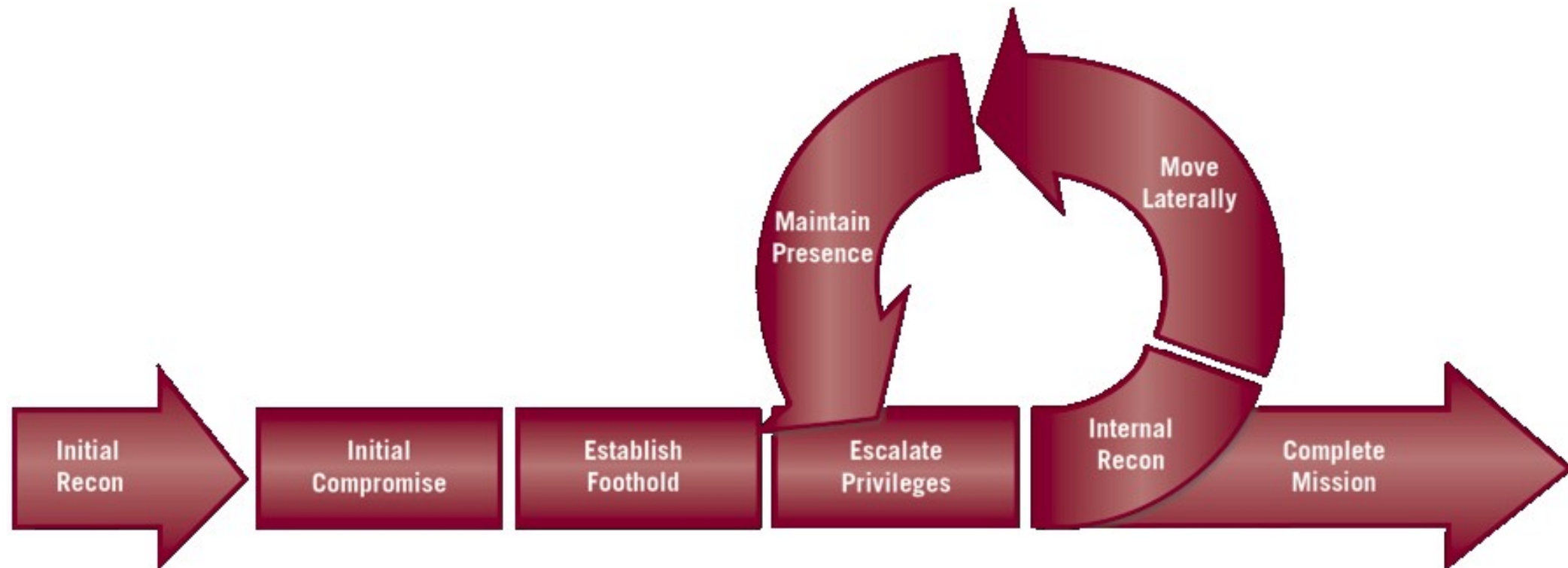
- Information Leakage
 - IP Address, OS/SW/HW Details, Users, Commands
 - Active/Passive Scans, **Use Info Leak**
 - Phase: **Initial Recon and Internal Recon**



Attack Lifecycle

Attack Types on NMS

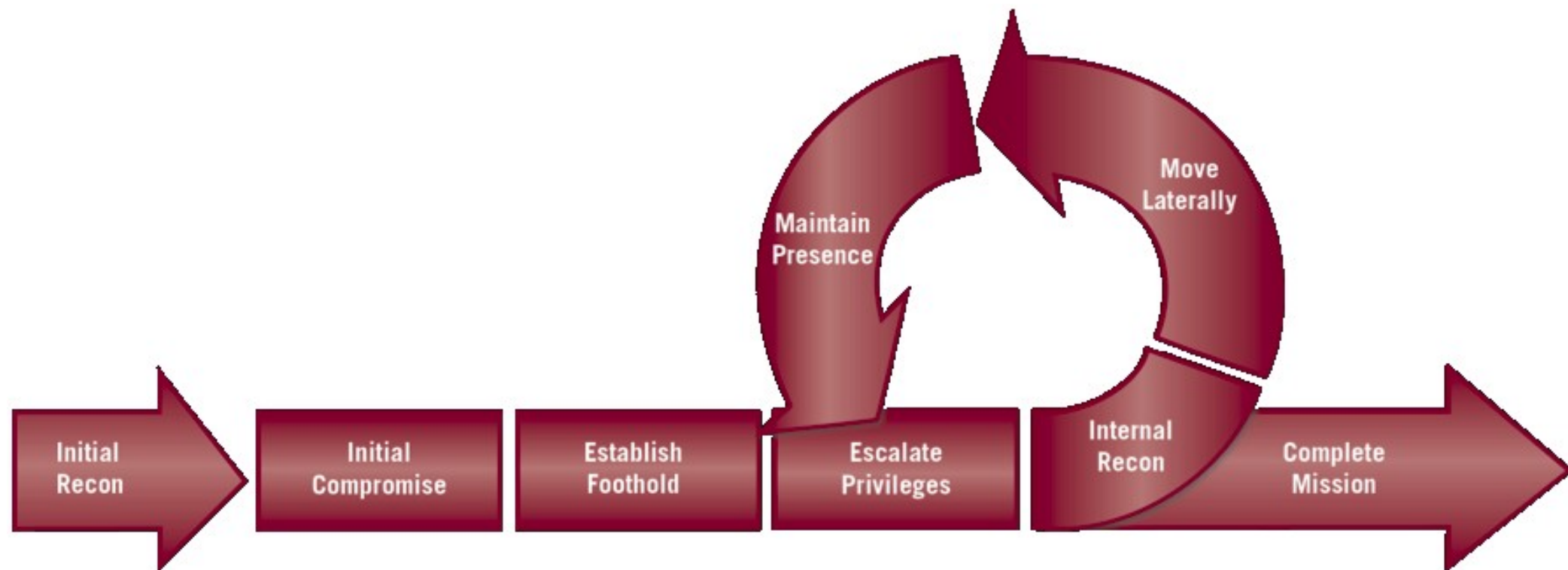
- Web-Application Security
 - XSS, SQLi, Remote Cmd/Code Execution (RCE)
 - Use Static/Dynamic Analysis, **Use Vuln Analysis**
 - Phase: **Initial Compromise/Establish Foothold**



Attack Lifecycle

Attack Types on NMS

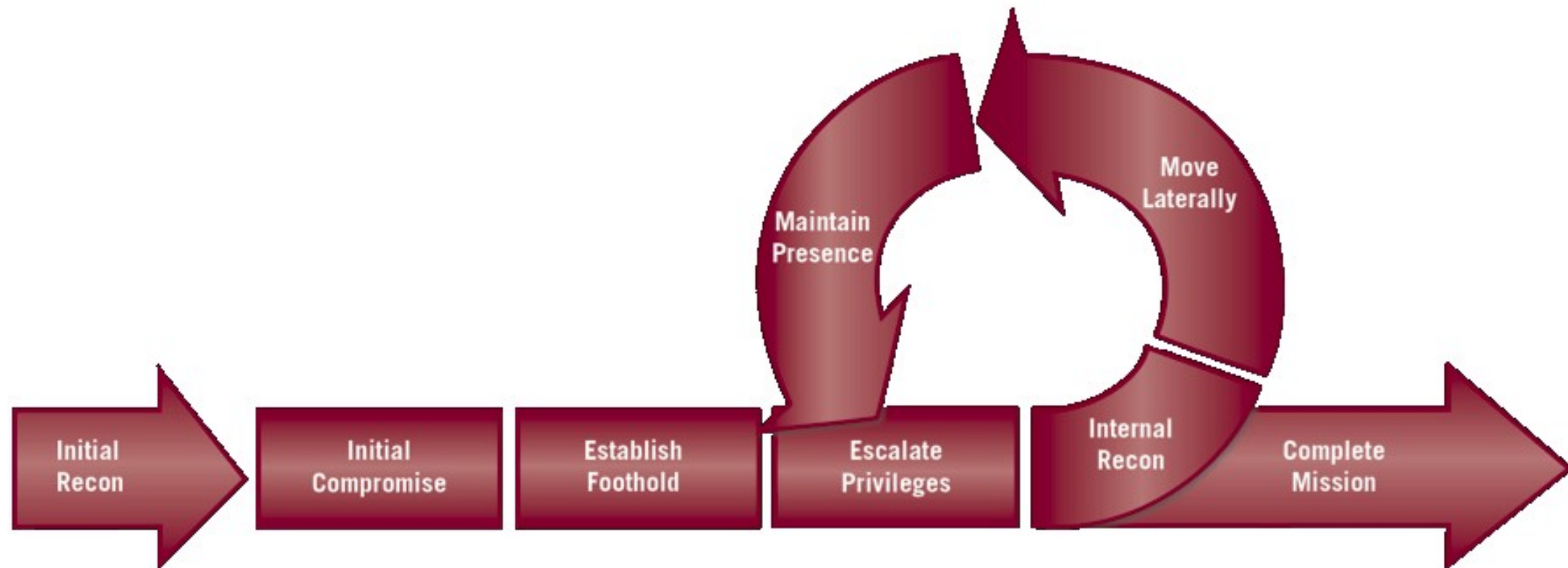
- Classic Attacks
 - Buffer Overflows, Kernel Exploits
 - CVEs for Old Kernels, **Use Info Leak**
 - Phase: **Escalate Privileges/Move Laterally**



Attack Lifecycle

Attack Types on NMS

- Mimicry/Blended Attacks
 - ResourceUsage/Communication/Process Mimicry
 - Evade IDS and Anomaly Detection, **Use Info Leak**
 - Phase: **Maintain Presence**



Information Leakage Attack-Enabler

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

Welcome to the SET E-Mail attack method. This module allows you

to specially craft email messages and send them to a large (or small) number of people with attached fileformat malicious payloads. If you want to spoof your email address, be sure "Sendmail" is installed (it is installed in BT4) and change the config/set_config SENDMAIL=OFF flag to SENDMAIL=ON.

There are two options, one is getting your feet wet and letting SET do everything for you (option 1), the second is to create your own FileFormat payload and use it in your own attack. Either way, good luck and enjoy

1. Perform a Mass Email Attack
2. Create a FileFormat Payload
3. Create a Social-Engineering Template
4. Return to Main Menu

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

- **Commands, Resource Usage**
 - Mimicry and Blending Attacks
- How?
 - Learn normal system status/behaviour – X_n
 - When in malicious state X_m , stick as close as possibly to the legitimate state X_n

$$A(X_m) = \operatorname{argmin} d(X_m, X_n), \text{ s.t., } d(X_m, X_n) < D$$

Reconnaissance 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**

Reconnaissance

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"

Reconnaissance

Passive

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

Reconnaissance

Passive

- Google dorks – Ganglia – **Romania**
 - intitle:"Cluster Report" **site:.ro**
 - intitle:"Grid Report" **site:.ro**
 - intitle:"Node View" **site:.ro**
 - intitle:"Host Report" **site:.ro**
 - intitle:"Ganglia:: " **site:.ro**
 - "Ganglia Web Frontend version 2.0.0"

Reconnaissance Passive

- Google dorks – Ganglia – Romania

planckgrid.spacescience.ro/ganglia/?c=ISS-Planck&h=planckgrid.local&m=load_one&r=hour&s=by name&hc=4&mc=2

This host is up and running.

Time and String Metrics	
boottime	Thu, 09 Apr 2015 12:07:06 +0300
Gmond Started	Mon, 03 Aug 2015 17:17:54 +0300
IP Address	172.16.6.1
Last Reported	0 days, 0:00:14
Location	0,0,0
machine_type	x86_64
os_name	Linux
os_release	2.6.32-431.11.2.el6.x86_64
ps	
ps-0	pid=4610, cmd=VBoxHeadless, user=lonel, %cpu=3.28, %mem=2.62, size=28, data=21872, shared=11
ps-1	pid=28073, cmd=gmetad, user=nobody, %cpu=3.28, %mem=0.00, size=68, data=1884, shared=11
ps-10	pid=6, cmd=watchdog/0, user=root, %cpu=0.00, %mem=0.00, size=0, data=0, shared=0, vm=0
ps-11	pid=7, cmd=migration/1, user=root, %cpu=0.00, %mem=0.00, size=0, data=0, shared=0, vm=0
ps-12	pid=8, cmd=migration/1, user=root, %cpu=0.00, %mem=0.00, size=0, data=0, shared=0, vm=0
ps-13	pid=9, cmd=ksoftirqd/1, user=root, %cpu=0.00, %mem=0.00, size=0, data=0, shared=0, vm=0
ps-14	pid=10, cmd=watchdog/1, user=root, %cpu=0.00, %mem=0.00, size=0, data=0, shared=0, vm=0
ps-15	pid=11, cmd=migration/2, user=root, %cpu=0.00, %mem=0.00, size=0, data=0, shared=0, vm=0
ps-16	pid=12, cmd=migration/2, user=root, %cpu=0.00, %mem=0.00, size=0, data=0, shared=0, vm=0
ps-17	pid=13, cmd=ksoftirqd/2, user=root, %cpu=0.00, %mem=0.00, size=0, data=0, shared=0, vm=0
ps-18	pid=14, cmd=watchdog/2, user=root, %cpu=0.00, %mem=0.00, size=0, data=0, shared=0, vm=0
ps-19	pid=15, cmd=migration/3, user=root, %cpu=0.00, %mem=0.00, size=0, data=0, shared=0, vm=0
ps-2	pid=3315, cmd=gmond, user=nobody, %cpu=2.63, %mem=0.02, size=152, data=11224, shared=3
ps-20	pid=16, cmd=migration/3, user=root, %cpu=0.00, %mem=0.00, size=0, data=0, shared=0, vm=0
ps-21	pid=17, cmd=ksoftirqd/3, user=root, %cpu=0.00, %mem=0.00, size=0, data=0, shared=0, vm=0
ps-22	pid=18, cmd=watchdog/3, user=root, %cpu=0.00, %mem=0.00, size=0, data=0, shared=0, vm=0
ps-23	pid=19, cmd=migration/4, user=root, %cpu=0.00, %mem=0.00, size=0, data=0, shared=0, vm=0
ps-3	pid=2662, cmd=kondemand/14, user=root, %cpu=0.66, %mem=0.00, size=0, data=0, shared=0, vm=0
ps-4	pid=3307, cmd=snmpd, user=root, %cpu=0.66, %mem=0.01, size=28, data=3708, shared=976, vn

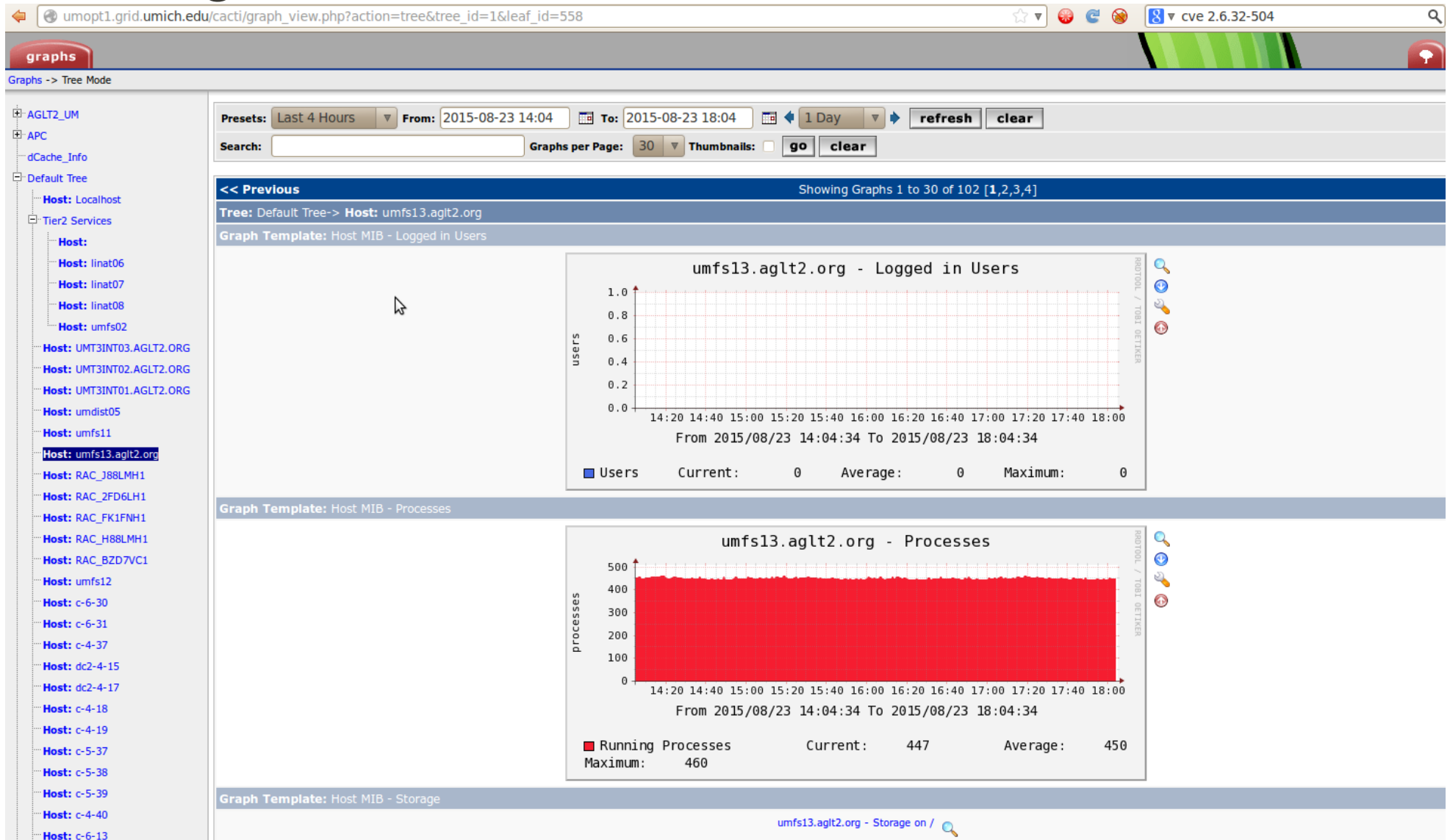
Reconnaissance

Passive

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

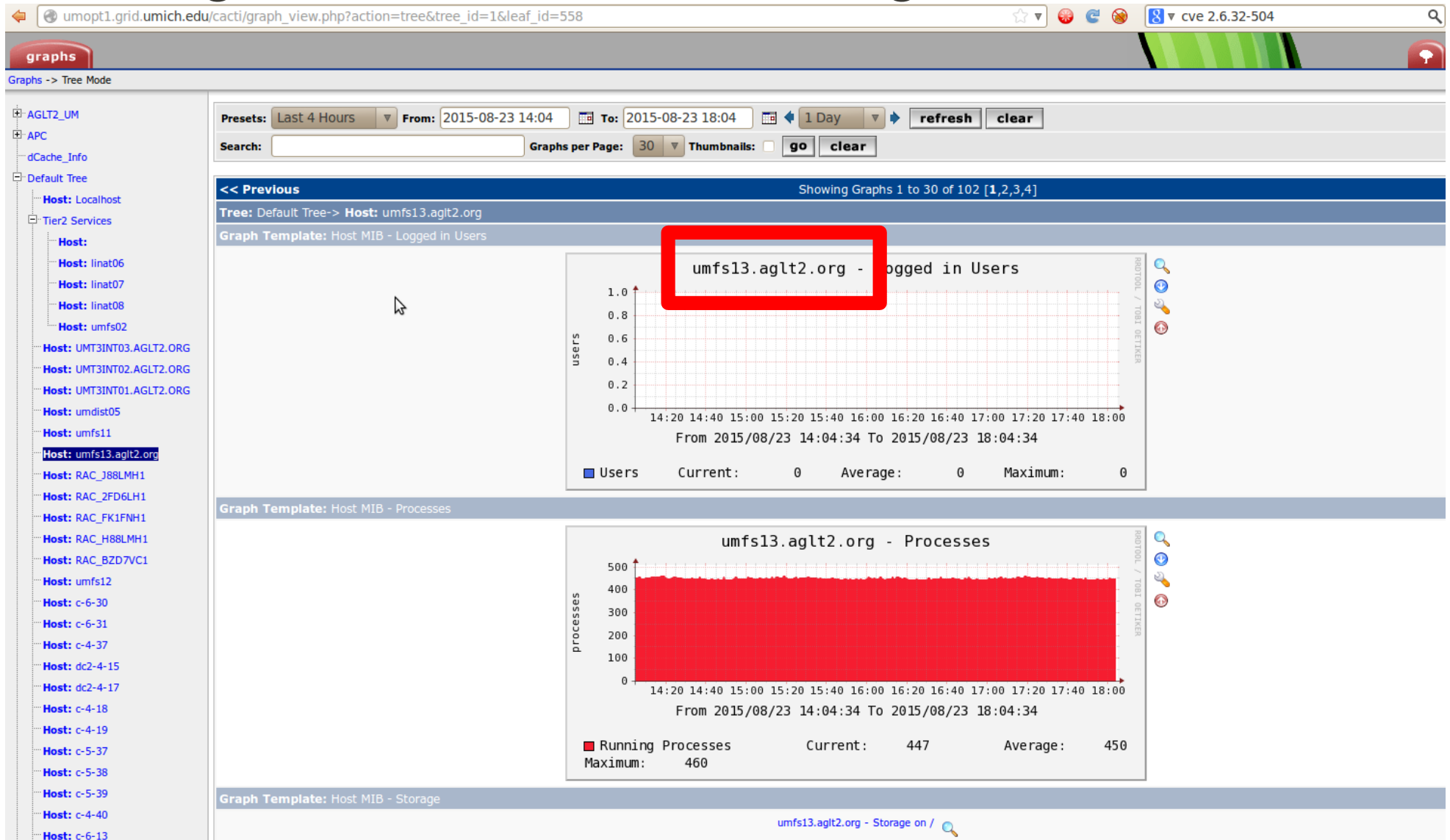
Reconnaissance Passive

- Google dorks – Cacti



Reconnaissance Passive and Recursive

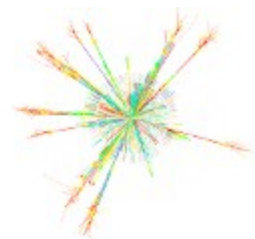
- Google dorks – Cacti → Ganglia



Reconnaissance

Passive and Recursive

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



ATLAS Computing and Muon Calibration Center

[Home](#) [Computing](#) [Calibration](#) [Projects](#) [General](#) [Media](#) [People](#) [Wiki](#)

[Simulated black hole event in ATLAS](#) [More Images](#)

[AGLT2 Overview](#) [ATLAS Information](#) [Higgs Boson Panel](#)

News

SuperComputing 2014:
One Server, 100 Gbps over the WAN for ATLAS/LHC
Software Driven Dynamic Hybrid Networks With Terabit/sec Science Data Flows
[More information](#)

Materials and photos from the HEPiX Fall 2013 Workshop at AGLT2 UM.

Current Statistics

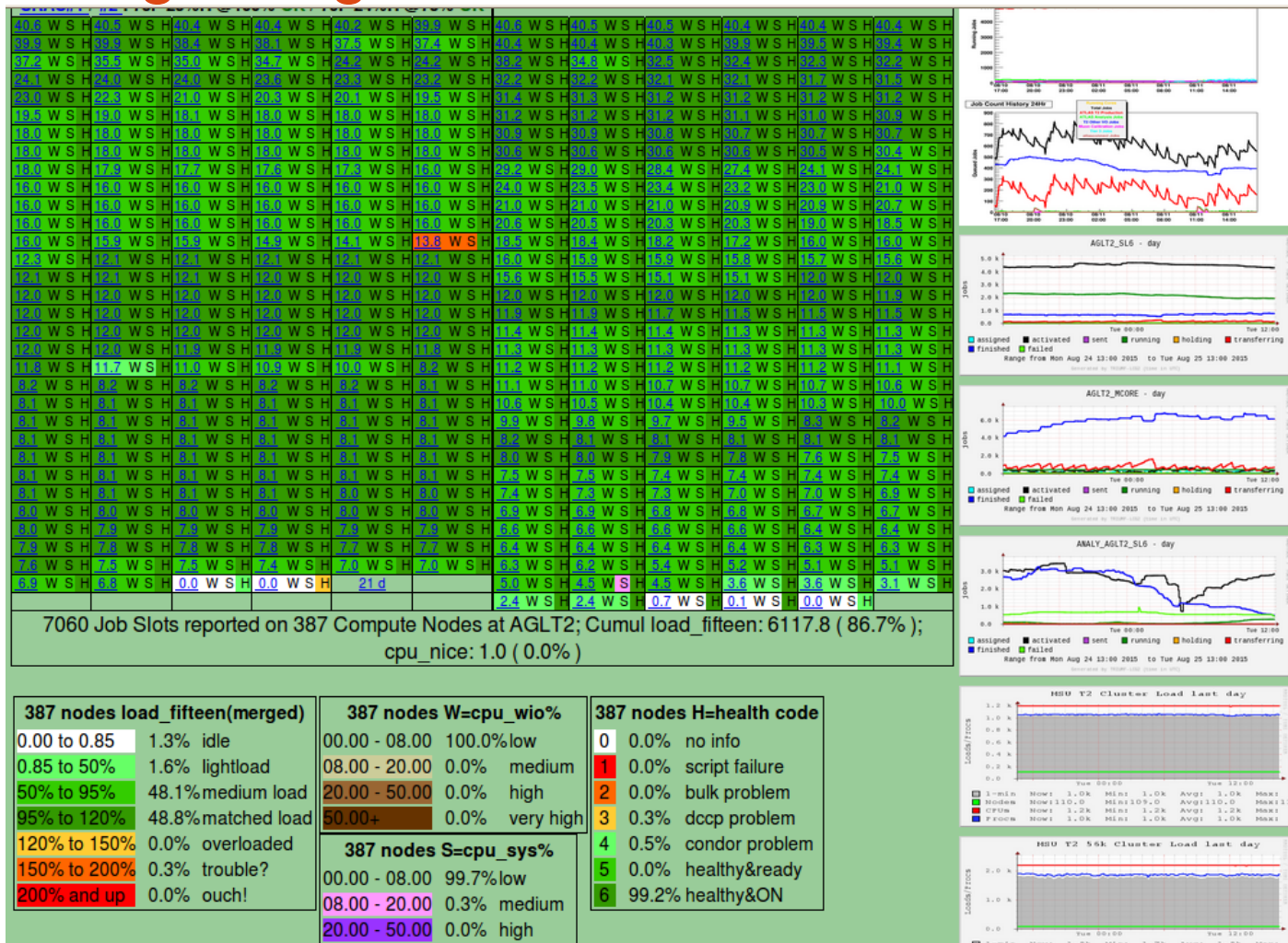
We have 3567 Condor jobs (2944 running on 6066 cores, 614 idle, 9 held)
Total Slots 3163, Cores 6826

[Job status page](#)

Reconnaissance

Passive and Recursive

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



Reconnaissance

Passive and Recursive

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

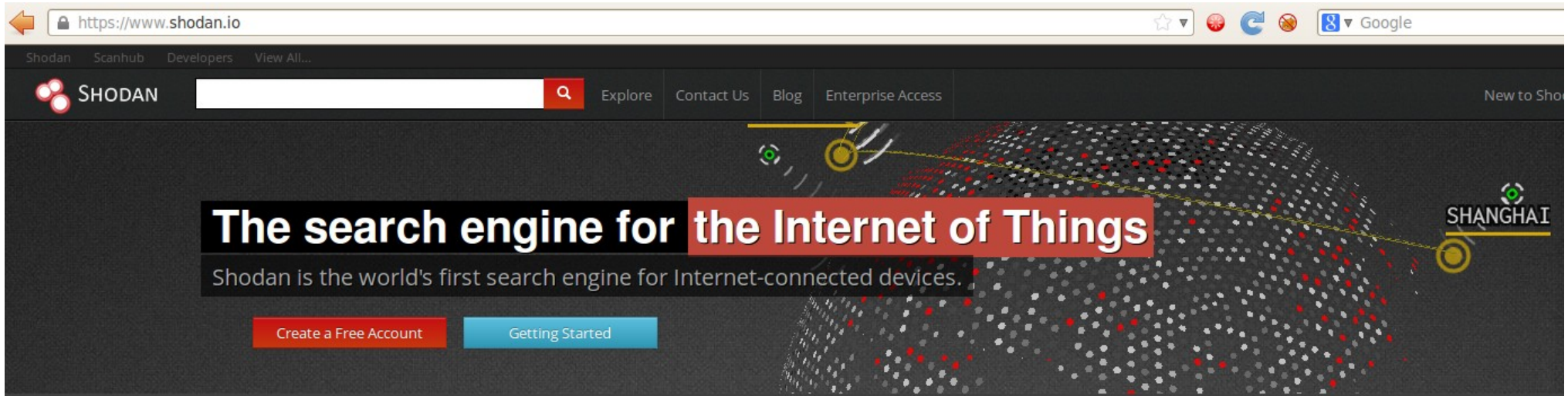


The screenshot shows the Ganglia web interface in a browser. The address bar displays the URL: `ganglia-um.aglt2.org/ganglia/?r=day&cs=&ce=&m=load_fifteen&s=by+name&c=MSU+T2&h=cc-102-1.msulocal&host_regex=&max_graphs=0`. The page title is "Cluster Ganglia Report". The navigation bar includes tabs: Main, Search, Views, Aggregate Graphs, Compare Hosts, Events, Automatic Rotation, and Mobile. The main content area shows a "Host Report for Tue, 25 Aug 2015 09:07:11 -0400" for the host "cc-102-1.msulocal". Below the report title, there are filters for "Last" (hour, 2hr, 4hr, day, week, month, year) and a date range selector. The breadcrumb trail is "AGLT2-ATLAS Grid > MSU T2 > cc-102-1.msulocal". The "Host Overview" section shows a red status icon and the text "This host is up and running." Below this, the "Time and String Metrics" table lists various system metrics.

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

Reconnaissance Passive

- Shodan



Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.



See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!



Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.



Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

CNNMoney

Dagbladet

The Washington Post

BBC NEWS

WIRED

CIO

firmware · 01

Reconnaissance Passive

- Shodan – Ganglia – Romania

The screenshot shows the Shodan search engine interface. The search bar contains the query "port:8649 country:RO". The results are categorized into several sections:

- TOP COUNTRIES:** A world map with Romania highlighted. Below it, a table shows "Romania" with 31 results.
- TOP CITIES:** A table listing cities in Romania: Bucharest (3), Constanta (2), Sibiu (1), Cluj-napoca (1), and Alexandria (1).
- TOP ORGANIZATIONS:** A table listing organizations: Ringier Print SRL (8), RCS & RDS Business (6), 2K Telecom SRL (6), SC Distinct New Media SRL (3), and Euoweb Romania SA (2).
- TOP OPERATING SYSTEMS:** A table listing operating systems: Linux 2.6.x (1).
- TOP PRODUCTS:** A table listing products: Ganglia XML Grid monitor (19) and OpenSSH (3).

The main results section shows three entries:

- 82.76.58.35:** 82-76-58-35.rdsnet.ro, Linux 2.6.x, RCS & RDS Business. Added on 2015-11-09 12:08:37 GMT. Location: Romania, Bucharest. Details: HTTP/1.0 403 Forbidden, Server: Icecast 2.4.1, Date: Mon, 09 Nov 2015 12:08:35 GMT, Content-Type: text/plain; charset=utf-8, Cache-Control: no-cache, Expires: Mon, 26 Jul 1997 05:00:00 GMT, Pragma: no-cache. Note: Icecast connection limit reached.
- 86.122.20.112:** RCS & RDS Residential. Added on 2015-11-04 16:00:30 GMT. Location: Romania, Alexandria. Details: 220 RBfilms FTP server ready.
- 91.216.152.45:** Ringier Print SRL. Added on 2015-11-04 07:13:04 GMT. Location: Romania. Details: XML output showing Ganglia XML structure.
- 91.216.152.51:** Ringier Print SRL. Added on 2015-11-04 00:19:10 GMT. Location: Romania. Details: XML output showing Ganglia XML structure.

Reconnaissance Passive

- **Hands-on**

- **exercise_recon_dorks.txt**
- How to create a "search dork"
- *intext:"Ganglia Web Backend (gmetad) version 3.6.0"*
 - About **507,000 results** (0.58 seconds) ~ **Nodes**

- **Hands-on**

- **exercise_recon_apis.txt**
- Automate, using search APIs to collect data
- Parse data
- NOTE: at the end, if time permits

Reconnaissance Results

- Exposed web interfaces
 - **364** Ganglia
 - **~43K** nodes (web info leak)
 - ~1370 clusters
 - ~490 grids
 - 5K Cacti (~80% password protected)
 - 2K Observium (~80% password protected)
- Exposed daemons
 - **~40K** publicly exposed Ganglia gmond nodes (XML Info Leak)

Reconnaissance 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	≈ 1%	3%
CH	≪ 1%	5%
Others	14%	32%
Total (count)	39553	364

Reconnaissance Results

- 43K nodes on 364 Ganglia Web Interfaces
- 120 main kernel versions
 - 411 kernel sub-versions
- Kernel version 2.6.32
 - Runs on 38% of the 43K hosts
 - Summarizes 1600 vulnerabilities
- "Secured" kernels
 - *grsecurity* on 9 hosts (only!)
 - *hardened-sources* on 6 hosts (only!)

Reconnaissance Results

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

inurl:"/ganglia/?c=SamsungProduction"

Web

Images

Videos

News

Shopping

More ▾

Search tools

About 38 results (0.45 seconds)

Ganglia:: monitoring-master4.localdomain Host Report

[ec2-54-225-183-154.compute-1.amazonaws.com/ganglia?c=SamsungProd...](#)

Feb 17, 2015 - Invoke automatic rotation system. Automatic rotation rotates all of the graphs/metrics specified in a view waiting 30 seconds in between each.

Ganglia:: mongodb3 Host Report

[ec2-54-225-183-154.compute-1.amazonaws.com/ganglia?c=SamsungProd...](#)

Feb 17, 2015 - Invoke automatic rotation system. Automatic rotation rotates all of the graphs/metrics specified in a view waiting 30 seconds in between each.

Ganglia:: ip-10-65-2-155.ec2.internal Host Report

[ec2-54-225-183-154.compute-1.amazonaws.com/ganglia?c=SamsungProd...](#)

Feb 17, 2015 - Invoke automatic rotation system. Automatic rotation rotates all of the graphs/metrics specified in a view waiting 30 seconds in between each.

Ganglia:: ip-10-113-175-12.ec2.internal Host Report

[ec2-54-225-183-154.compute-1.amazonaws.com/ganglia?c=SamsungProd...](#)

Feb 17, 2015 - Invoke automatic rotation system. Automatic rotation rotates all of the graphs/metrics specified in a view waiting 30 seconds in between each.

Compromise + Foothold

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 Ganga Web Frontend (**PHP**)
 - **More tools**

Compromise + Foothold

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

Compromise + Foothold

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)

Compromise + Foothold

Static and Dynamic Analysis

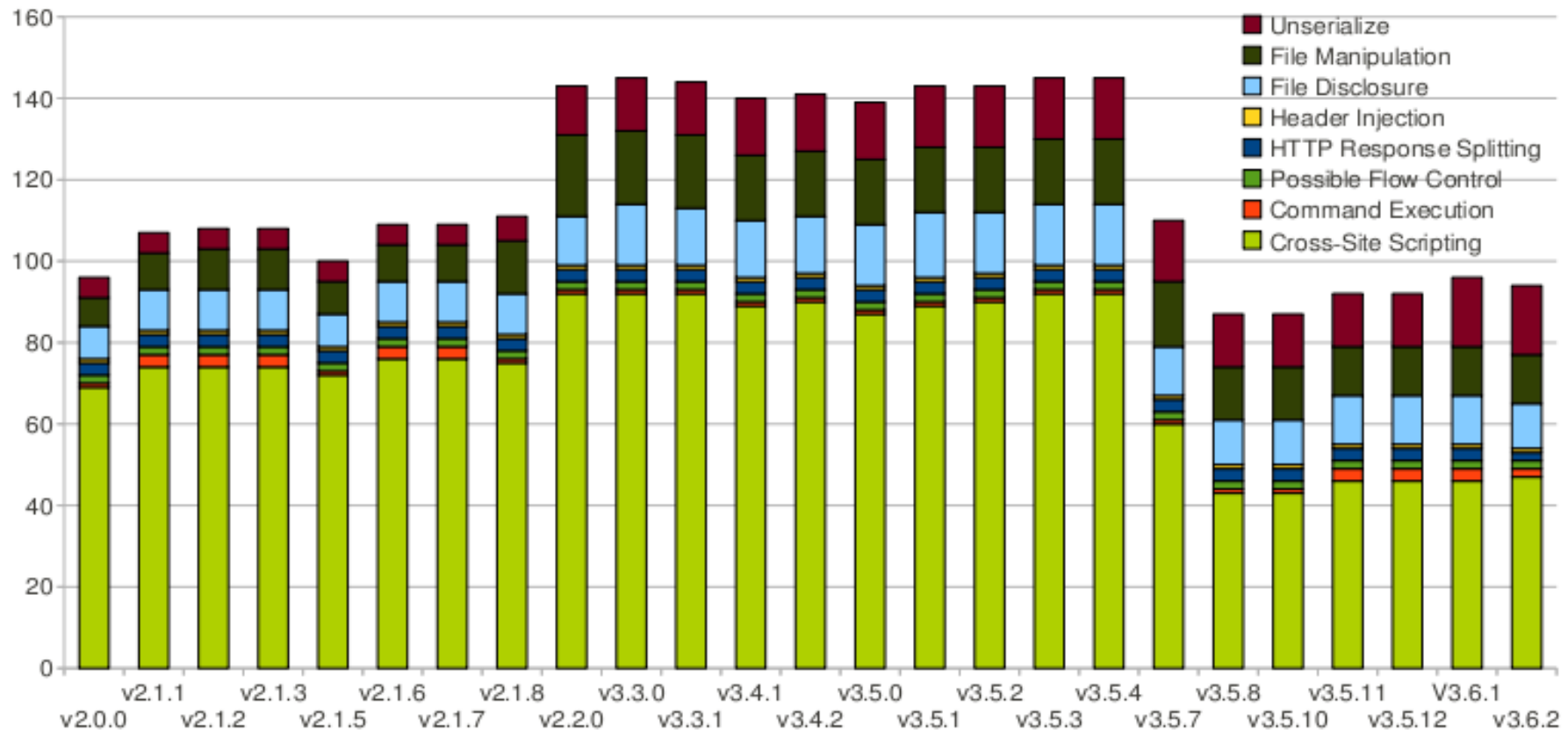


Fig. 1. Vulnerabilities in Ganglia Web Frontend found statically with RIPS. Distribution by Ganglia's version and vulnerability type.

Compromise + Foothold

Static and Dynamic Analysis

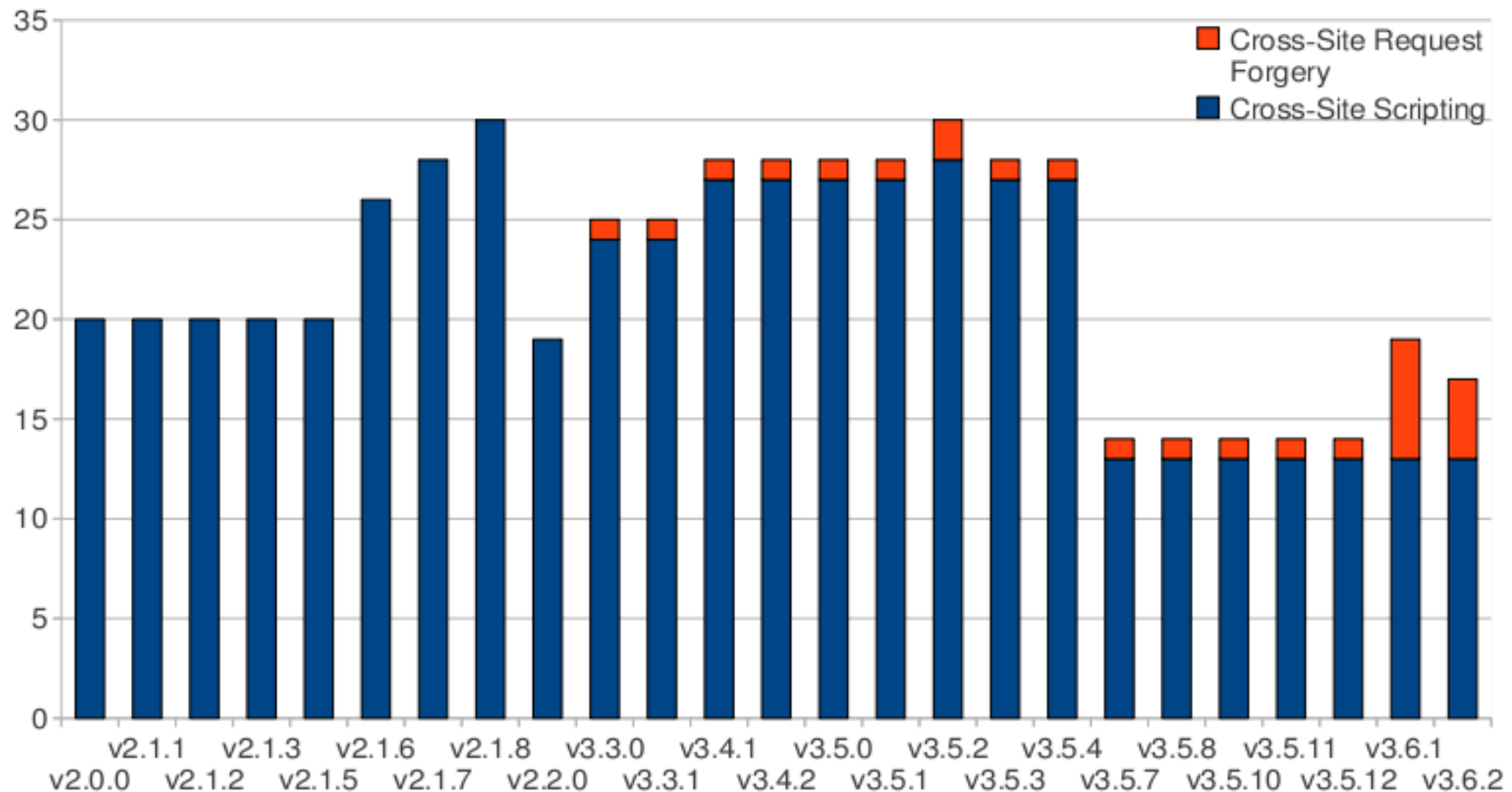


Fig. 2. Vulnerabilities in Ganglia Web Frontend found dynamically with Arachni. Distribution by Ganglia's version and vulnerability type.

Compromise + Foothold

Static and Dynamic Analysis

- **Hands-on**
 - Perform static analysis
 - **exercise_static_analysis.txt**
- **Hands-on**
 - Perform dynamic analysis
 - **exercise_dynamic_analysis.txt**
- Compare the two types of analysis

Compromise + Foothold

Static and Dynamic Analysis

- Ganglia 364
 - 193 hosts (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

Compromise + Foothold

Static and Dynamic Analysis

- Ganglia 364
 - 193 hosts (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 , Mandriva , more)
References	DSA-2610-1
NVD severity	high (attack range: remote)
Debian Bugs	683584

Compromise + Foothold Vulnerability Analysis

- CVE-2012-3448

a/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['graphdir'] ) {
        $graph_config = json_decode( file_get_contents( $json_report_file ), TRUE );

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

Compromise + Foothold VulnAnalysis + ExploitDev

- **Hands-on**
 - **exercise_vuln_analysis.txt**

Compromise + Foothold VulnAnalysis + ExploitDev

- **ExploitDB 38030** CVE-2012-3448

[Home](#)[Exploits](#)[Shellcode](#)[Papers](#)[Google Hacking Database](#)[Submit](#)[Search](#)

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: Download

[« Previous Exploit](#)[Next Exploit »](#)

```
1  <?php
2  /*
3
4  #####
5  #
6  # Author      : Andrei Costin (andrei theATsign firmware theDOTsign re)
7  # Desc        : CVE-2012-3448 PoC
8  # Details     : This PoC will create a dummy file in the /tmp folder and
9  #              will copy /etc/passwd to /tmp.
10 #              To modify the attack payload, modify the code below.\
11 # Setup       : Ubuntu Linux 14.04 LTS x86 with Ganglia Web Frontend 3.5.0
12 #
13 #####
14
15 1. Assuming that ganglia is installed on the target machine at this path:
16 /var/www/html/ganglia/
17
18 2. Assuming the attacker has minimal access to the target machine and
19 can write to "/tmp". There are several methods where a remote attacker can
20 also trigger daemons or other system processes to create files in "/tmp"
21 whose content is (partially) controlled by the remote attacker.
22
```

Countermeasures

- Password protect
 - **Hands-on**
 - `exercise_basic_auth.txt`
- HTTPS
 - **Hands-on Exercise**
 - `exercise_https.txt`
- HTTPS Caveats
 - From 364 Ganglia Web Frontends
 - Only 42 (i.e., 11.5%) run HTTPS
 - Only 16 (i.e., 39%) run ***"trusted"*** HTTPS

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.

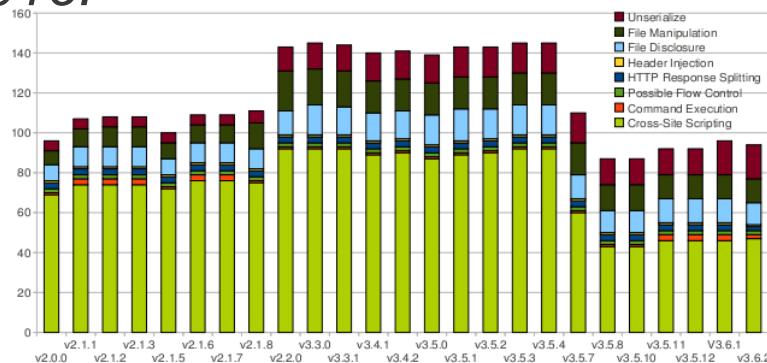


Fig. 1. Vulnerabilities in Ganglia Web Frontend found statically with RIPS. Distribution by Ganglia's version and vulnerability type.

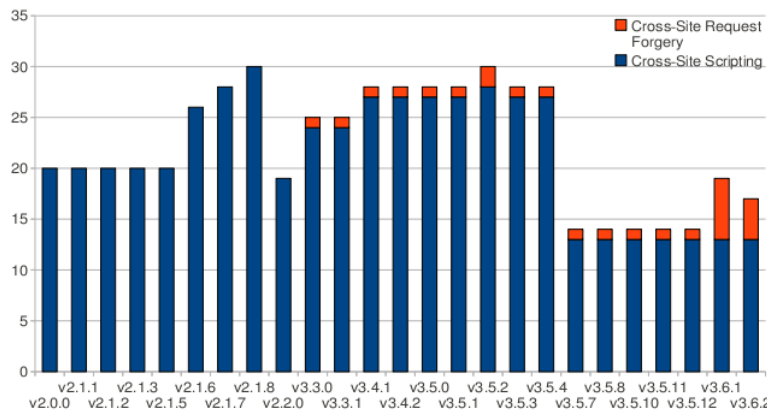


Fig. 2. Vulnerabilities found dynamically with Arachni. Distribution by Ganglia's version and vulnerability type.

The End
Thank You!
Questions?

{name}@firmware.re
@costinandrei