Open Science Grid

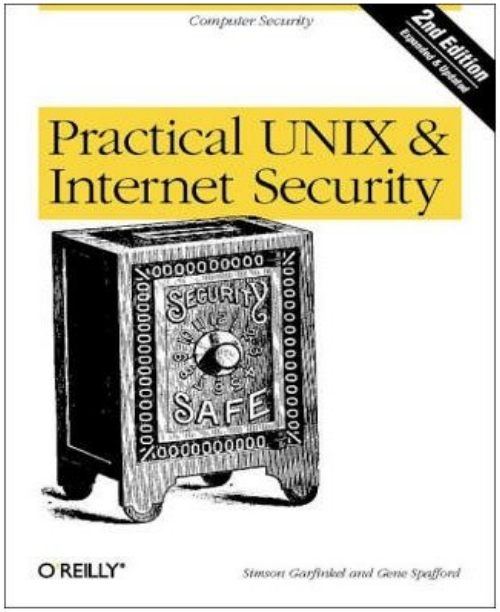
Incident Response Forensics and Review OSG Security Drill

OSG Site Administrators workshop
Indianapolis
August 6-7 2009

Anand Padmanabhan
UIUC

Open Science Grid

What you should already know



- If you have questions on Unix security please **ASK** the security team
- Ref: http://tldp.org/HOWTO/Security-HOWTO/
- Book: http://oreilly.com/catalog/9780596003234/

Figure taken from cover of O'Rielly publication book on security

Open Science Grid

What can you expect form this talk?

- We will take security drill as a example incident
  - Review security drill results from Tier1 sites
- We will discuss how to:
  - Respond during a security incident
  - Communicate with security team and how to respond to an incident
  - Ban a user DN from your site
  - Track jobs submitted by a user and kill them
  - Find the IP address the job is coming from
  - Basic forensics steps for incident response

Open Science Grid

Tier1 Security Drill - 2009

- Objectives
  - Make sure sufficient incident response procedure are in place
  - Ensure appropriate communication channels are available

Review of the job submitted during drill

- The job submitted to the tier 1 sites does the following
  - Scans /proc for process info
  - Downloads material from offsite with wget.
  - Repeatedly invokes another “bad program"
  - Looks for world-writable directories visible from where the job is running
  - Hides itself in any writable directory
  - Tries to add entries with cron and at
  - Reports data periodically to an offsite location (remote web server)
- If tomorrow we submitted such a job to your site will you be able to find and neutralize it?

Open Science Grid

What was expected of the sites

- Communication
- Containment
- Forensics

Open Science Grid

What was expected of the sites

- At a minimum, sites are expected to
  - Find the test process and kill them.
  - Ban the test user from submitting additional jobs.
  - Discover the incoming IP address of the test process.
  - Do an analysis of the network traffic (broader the better: there were bonus points).
  - Do an analysis of submitted binaries (there were bonus points).
- Email the security team with details when accomplishing each step.
- Instructions provided to the site can be found at
  - https://twiki.grid.iu.edu/bin/view/Security/SecurityDrillInstrSites

Question for the site admins here:
Do you know how to do these steps?

Open Science Grid

Communication

- OSG security requests the site admins to report all incidents affecting Grid machines.
  - If you are in doubt err on side of caution and let us know. We will work with you to figure out if this incident will impact the Grid.
  - https://twiki.grid.iu.edu/bin/view/Security/IncidentDiscoveryReporting
  - Doug already covered site responsibilities earlier
    - https://twiki.grid.iu.edu/bin/view/Documentation/SecuritySiteResponsibilities
- We ask for reporting incidents so that we can
  - Access the risk it poses to OSG at large
  - Notice any patterns in the attacks
  - Contain the spread of the incident/attack

Open Science Grid

Communication

- You can send us signed and encrypted emails if necessary
  - Instructions at:https://twiki.grid.iu.edu/bin/view/Security/SecureEmail
- We work with you to keep information confidential
  - We release to OSG site/VO security contacts only as much information as necessary to maintain security
  - You input will be sought before information is released
- Also always remember to contact your local cyber-security team when you notice an incident
- We had no reports in past 7 months. Why?

Open Science Grid

Banning Users

- This will prevent the user/DN for submitting new jobs to the sites
- Instructions for sites using Gums 1.2, 1.3 or edg-mkgridmap can be found at
  - https://twiki.grid.iu.edu/bin/view/Security/BanningUsersAtSite
- Notes:
  - Banning a user just prevents them from authorizing at your site anew. Jobs already running will still continue
  - If you do not have a single authorization tool like GUMS for all entry points in your site, you will have to ensure all entry points get updated.

Finding if user authenticated at the site

- Look at the various log files (e.g. gatekeeper, gsiftp, GUMS log)
  - An fairly exhaustive lists of log files can be found at: https://twiki.grid.iu.edu/bin/view/ReleaseDocumentation/ComputeElementLogFiles
- globus-gatekeeper.log will tell you if user authenticated through the particular gatekeeper
  - It will also tell you which IP address the offending user submitted his job from
- gums-service-admin.log will record the authentication decisions made by GUMS

Open Science Grid

Finding User Jobs

- Did the job go through the fork jobmanager or batch system
- Inspect the batch system to find the node the user job ran
  - For Condor
    - % condor_q -l job_id
    - % condor_q –l userid
  - For PBS
    - % qstat -f job_identifier
- Also review the batch system logs

Open Science Grid

Finding User Jobs

- Locate user processes
  - ps -u uid -U uid uwww
  - Remember to locate processes on both Computing Element (CE) and Worker Node (WN)
- Removing job from batch system
  - Condor: % condor_rm cluster_id
  - PBS: =% qdel job_id
- Kill suspicious processes associated with the user
- Remember to check your cron and at entries
  - The job submitted during the drill was adding entries to the cron and at, so that even if you kill your jobs, the “bad process” started to run again at some later time

Open Science Grid

Collecting network flows

- Contact your institutions network security team
  - Ask from for netflows from the users IP address and the network flows of the affected machines
  - You should have already contacted your local security team by this time and they should be able to guide you
- Most institutions will have network experts who will be able to provide this data

Open Science Grid

Analyzing submitted binaries

- You would be able to retrieve the execute directory maintained by globus and batch system
  - You should find binary/script and condor files/proxy
- Executable can be analyzed using
  - 'ldd' to review what libraries it is linked against
  - 'strings' command to review binary file
    - Look for hostnames, email addresses, usernames, passwords, and other clues
  - Sometimes looking at stdout and stderr associated with the job provides valuable information

Open Science Grid

Analyzing network traffic

- Does the job have any open files or ports?
  - Use lsof and/or netstat
    - % lsof -u uid -P
    - % netstat -ap
- Contact your institutions network security team to collect netflows
  - Ask from for netflows from the users IP address and the network traffic to/from the affected machines.
- Most institutions will have network experts who will be able to provide netflows

Open Science Grid

Note on Privilege Escalation

- If the attacker succeeds in escalating the privileges by installing rootkits, the simple forensic techniques we have discussed here will be insufficient to diagnose the problem
  - Once an attacker has root access we can no longer rely on the commands we run on the node.
  - Run host and network based intrution detector tools.
  - Review network traffic flows.
  - Contact your institutions cybersecurity experts.
  - Detailed discussion on topics regarding root level compromise is outside the scope of this talk.

Open Science Grid

How did Tier 1 sites do?

Open Science Grid

Grading Criteria

- Communications
  - Site sends an immediate response to the security team confirming they received the notification.
  - Site promptly sends updates to the the security team until the drill is over.
  - Site gives detailed information over their actions and findings
- Containment
  - Site is able to find all the test process and kill it.
  - Site is able to ban the offending uid
  - Bonus Point: fast response time

Open Science Grid

Grading Criteria

- Forensics
  - Site can tell which IP address the attacker was coming from
  - Site is able to do an analysis of network traffic -- find that process has been sending data to the monitoring web server
  - Site is able to do an analysis of submitted binaries -- can roughly understand what the binary is supposed to do, can find out interesting strings in the binary
- Bonus points will be given to sites accomplishing more than outlined expectations.

Open Science Grid

Results

Roc	OSG	Security	Sevice	Challenge	5/18/2009	Evaluation Form	
Site	BNL						
Time of Alert	5/11/2009 10:07:09	Done	Target	Actual	Score	Notes	Bonus
			(Hours)	(Hours)	%		[Points]
Communication							
	Acknowledge/Heads-up report to CSIRT list	1	4	0.18	100	Prompt email acknowledgement	4.77
	Alert to VO Manager	1	24	0.23	100	Emails cc'ed to GoC	4.95
	Verify notification of the responsible CA	1	144	0.23	100	Emails cc'ed to GoC	4.99
	Final report to CSIRT list	1	144	9.2	100	No Formal Final report but detailed and comprehensive analysis in emails	4.68
	Average score for Communication				**100**		19.39
Containment							
	Found Jobs and killed them	1	4	0.88	100	Jobs killed in appropriate fashion	3.9
	Suspended the user at the Site	1	4	0.88	100	User ban installed	3.9
	Average score for Containment				**100**		7.8
Forensics							
	Discovery of initiating site (UI) and contact with thaSite's CSIRT	1	24	0.18	100		4.96
	Analysis of network traffic	1	48	9.2	100	Collected and sent netflows analysis - 1) incoming IP determined 2) rooier IP determined 3) determined uploads	4.04
	Analysis of the submitted binaries	1	48	3.5	100	Detailed Binary analysis - determined malware action (find ro directories, at and cron process, cain and abel, strings)	4.63
	Average score for Forensics				**100**		13.63

Drill was conducted and results were compiled by Aashish Sharma

Open Science Grid

Results

Roc	OSG	Securi	Sevice	Challeng	5/18/20(	Evaluation Form	
Site	FNAL						
Time of Alert	5/18/2009 10:34:45	Done	Target (Hours)	Actual (Hours)	Score %	Notes	Bonus [Points]
Communication							
	Acknowledge/Heads-up report to CSIRT list	1	4	0.08	100	Acknowledgement with in 5 mins of Initial notification	4.9
	Alert to VO Manager	1	24	0.08	100	Emails cc'ed to GoC	4.98
	Verify notification of the responsible CA	1	144	0.08	100	Emails cc'ed to GoC	4.99
	Final report to CSIRT list	1	144	4.25	100	No Formal Final Report but email communication was sequentail and comprensible	4.85
	Average score for Communication				**100**		19.72
Containment							
	Found Jobs and killed them	1	4	0.5	100	Jobs killed in appropriate fashion	4.37
	Suspended the user at the Site	1	4	0.08	100	User ban installed	4.9
	Average score for Containment				**100**		9.27
Forensics							
	Discovery of initiating site (UI) and contact with thaSite's CSIRT	1	24	0.08	100		4.98
	Analysis of network traffic	1	48	1.5	100	Collected and sent netflows analysis	4.84
	Analysis of the submitted binaries	1	48	4.25	100	Detailed Binary analysis	4.55
	Average score for Forensics				**100**		14.37

Drill was conducted and results were compiled by Aashish Sharma

Open Science Grid

Who can expect the drill next

- It will be Tier2's turn shortly to be exposed to a similar drill.

Questions?