

Advanced Vulnerability Assessment Tool for Distributed Systems (AVAT)

Sándor Ács, Péter Kotcauer [acs.sandor, peter.kotcauer]@sztaki.mta.hu Miklos Kozlovszky kozlovszky.miklos@nik.uni-obuda.hu



- Motivations
- State-of-the-art
- OpenVAS
- Design and Implementation
- Vulnerability assessments results
- Conclusion and future work



Motivations

- Large scale resources
 - Supercomputing infrastructure, HPC centers, GRID/Cloud systems, etc.
 - Large impact if fails
- Homogeneous resources
 - Computational, networking, storage, middleware
 - Reusable break-in methods, large gain if successfull
- Lot of users/semi-open communities
 - Social networking issues
 - Weakest points



HP-SEE User Forum 2012 - Belgrade, Serbia 17th October 2012



- There are lot of potential security problems with distributed and shared systems:
 - Coming from the technology itself
 - Coming from site/softwarestack setup
 - Coming from end-user behavior
- General goal: Less vulnerable infrastructure (survive cyberattacks)
 - Protect user data
 - Eliminate malicious infrastructure (re)usage
- Our goal is to create a vulnerability assessment framework for distributed systems in order to decrease threats!

HP-SEE User Forum 2012 - Belgrade, Serbia 17th October 2012



Ó B

U

D

Α

Ι

E G Y

Ε

Т

Ε

Μ

DCI monitoring around the globe (General DCI monitoring tools)

- Grid monitoring tools
 - SFTs (Site Functionality Tests)
 - Nagios
 - Ganglia
 - Netmon
 - PerfSonar
 - GridView
 - RTM
 - ...
- Cloud Monitoring
 - Hyperic
 - Zenoss

. . .

- RevealCloud
- Rackspace Cloud Monitoring

Note: applications are often reused to monitor other DCIs

HP-SEE User Forum 2012 - Belgrade, Serbia 17th October 2012

¢		1	-		f	141.0.4	155	1	5	1	(Teil	N BE
100	-1	A12448	1 and	2			-	•	Ser -			i fii
1	- 4	~~~	1				100.000	10.0	25-		19	16.1
	1 J	11.11		0.000		h					1	
		le si de ser de de	A HAR	1		5	-	TO CODE		1		
100												
100	24	Yspectrus	Fandhoon			Saingune		Det.	-			
100								1.000		1	-	-
	1	SEE-GRID	ALGIS	DI PHY	SCL	or phy	100.00 XX	0	r <u>O</u>	98	28	2
100	2	SEE-GRID	AEG	\$92.RC	wii	gid01.m	ab by easy	0	K 🔂	88	- 12	2
	3	SEE GRID	AEGISE	1.11.15	LIDA	grad01.+2	We make at	01	K gh	28	24	2
1.00	4	SEE-GRID	AD	IS84 K	G	cluster1.c	ah hg ac s	74 01	K OL	52	ok	0
1000	5	SEE GRID	AEGE	SISSET	BG	11029 ett	Dig at yo	0	K Ok	08	01	0
	6	SEE GRID	AL	OI IND	IA	profesh	ni minne	d 0	K ok	ck	ak	0
	7	SEE-GRID	-	-02.FD	-	and state	for surf a		IT OR	crit	14	-
		SET CRID			iir. It	101 mil	and drawn			-	100	
XC-		SEL GRAD	HO.			COLUMN IN			10	100	100	-
21C	,	SEE GRID	HA.	02-1411	<u>.</u>	git ett s	man mb		OR OF	28	- 98	62
	10	SEE-GRID	BA	O.EIF	84	n00.grid	etformed	1 I.I.I	10 R 218	218	- 24	12
UterALL	11	SEE GRID	BABAPMESA BG01-DP		grid01_perfuneabs er002.ipp.acad.bg			к 🔬	1	-	2	
	12	SEE GRID					g 0	K <u>ak</u>	24	at	9	
	13	SEE-GRID	B	BG02-IM		ce001 unites bas bg			K Oh	68	62	0
	14	SEE GRID	BG	04 ACA	D	(e02 gr	decedby	0	K Ok	28	ok	2
HINSOL.		111	2 34	14		-	994	17 101	-	43.8 9	1 10	
e01)		LEE.	5 . 4	8				45 55	-	108.5 0	a 23	2.4
4			1. 1.							17.3 4		
		Marid.	1 1							2.7 44		1.08
		The second			54					23,7.8	8 24	
						a second			and the second second			



DCI monitoring around the globe (Security monitoring tools)

- Commercial vulnerability assessment tools
 - Qualys
 - Nessus
- Open vulnerability assessment tools
 - OpenVAS
 - Nexpose
 - Pakiti
 - EGI Pakiti
 - EGI Security Dashboard
 - GSSVA
 - SZTAKI solution some years ago used for SEE-GRID-SCI
 - Pakiti based
 - Only software stack investigation









- Mostly non-DCI compliant (or limited)
 - Non job-aware (job creation?)
 - Submission problems (middleware dependencies)
 - Result retrieval
 - Working in user space (how, and how not)
 - port opening for communication
- Service-like operation is limited
 - Hierarchical authentication schemes
 - available mostly in commercial solutions
 - Periodical monitoring
 - Alarming schemes
 - "Security sampling" solutions
 - Try not disturb the normal business



- The core of the **AVAT** (*Advanced Vulnerability Assessment Tool for Distributed Systems*) is based on Open Vulnerability Assessment System (OpenVAS) framework.
- OpenVAS:
 - It collects several services and tools to provide a vulnerability scanning and vulnerability management solution.
 - Free software (most components are licensed under the GPL).
 - External NVT (*Network Vulnerability Test*) repository.



Ó

Β

U D

Α

Ι

E G Y

Ε

Т

Ε

 \mathbf{M}

- OpenVAS Server: about 30 MB (packed
- OpenVAS Server: about 300 MB (unpacked)
- Working in user space after some tricks
- Communication via ssl/https
- Server and client on the same host
 - Localhost 127.0.0.0 range can be used
- Client output: html file
- One vulnerability assessment = 1 html result file
- Needs to collect, harmonize and visualize
- Server + client are running on worker nodes (but only computing elements are addressable)
- No direct submission is possible (use brokering services if available)



Ó B

U D

Α

Ι

Design and Implementation (1)

- During the investigation, we have used:
 - ARC middleware for the centers of the HP-SEE infrastructure
 - gLite middleware for the SEEGRID VO.









Submit test jobs. Start the testjob and download NVT updates. Send back the result of the vulnerability scan to the UI.



- How does the testjob work?
 - 1. Download the precompiled OpenVAS server, client and libs.
 - 2. Set up the environment (export path of binaries and libraries).
 - 3. Update NVTs.
 - 4. Start the OpenVAS server.
 - 5. Connect the client to the server and scan the current machine.
 - 6. Create a result file from the output of the vulnerability assessment.



Results of the vulnerability assessments

- Some examples:
 - results0.html
 - results1.html
 - results2.html
 - results3.html



follow the recommended steps and procedures to eradicate

	Scan Details
Hosts which were alive and responding during test	1
Number of security holes	4
Number of security warnings	1
Number of security notes	18
Number of false positives	0

	Host L		
Host(s)	Possible Issue		
127.0.0.1	Security hole(s)		

Analysis of Ho					
Address of Host	Port/Service	Issue regarding Port			
127.0.0.1	ssh (22/tcp)	Security warning(s)			
127.0.0.1	smtp (25/tcp)	Security hole(s)			
127.0.0.1	sunrpc (111/tcp)	Security note(s)			
127.0.0.1	ipp (631/tcp)	Security note(s)			
127.0.0.1	etlservicemgr (9001/tcp)	No Information			
127.0.0.1	dynamid (9002/tcp)	No Information			
127.0.0.1	otp (9390/tcp)	Security note(s)			
127.0.0.1	sunrpc (111/udp)	Security note(s)			
127.0.0.1	general/tcp	Security note(s)			
127.0.0.1	ntp (123/udp)	Security hole(s)			
127.0.0.1	general/HOST-T	No Information			
127.0.0.1	general/CPE-T	No Information			

HP-SEE User Forum 2012 - Belgrade, Serbia 17th October 2012



- AVAT can cover broad range of security issues (based on OpenVAS)
- AVAT can provide unified vulnerability assessment for multimiddleware DCIs (Transparent interoperability issue resolution)
- Our solution is fully compliant with the available DCI solutions (ARC and gLite so far) extension is "easy"
- Service-like DCI vulnerability assessment is feasible and could help to create more secure infrastructure (support system administrators)
- Sampling (statistical selection) can be effectively used for DCI vulnerability assessments
- Vulnerability assessment was done on some parts of the HP-SEE and SEE-GRID-SCI infrastructure
 - HP-SEE: investigated 4 HPC Centers, 1 center has 4 vulnerabilities (total 4, avg. 1/center)
 - SEEGRID: investigated 16 sites, 12 sites has vulnerabilities (total 52, avg. 3.25/site)
 - Most of the issues can be fixed with updates.



Thank you for the attention!

Questions?

HP-SEE User Forum 2012 - Belgrade, Serbia 17th October 2012