

JUNE 18-20, 2008

Audit and IDS Steve Grubb, Red Hat



Linux Audit and Intrusion Detection Systems

- Review audit system
- Learn a little about some threats
- Overview of IDMEF
- Introduction to prelude



Audit System's Uses

- Watch file accesses
- Monitor system calls
- Record commands run by user
- Record security events
- Search for events
- Run summary reports



Audit Requirements

Shall be able to record at least the following:

- Date and time of event, type of event, subject identity, and outcome
- Sensitivity labels of subjects and objects
- Be able to associate event with identity of user causing it
- All modifications to audit configuration and attempted access to logs
- All uses of authentication mechanisms
- Changes to any trusted database
- Attempts to import/export information
- Be able to include/exclude events based on user identity, subject/object labels, other attributes



Syscall Audit Rules

Follows the general form:

-a filter, action -S syscall -F field=value -k "rule-note"

Example to see opens by users that failed due to permission: -a exit,always -S open -F exit=-EACCES -F auid>=500 -F auid!=4294967295

-F can be one of: a0, a1, a2, a3, arch, auid, devmajor, dir, devminor, exit, user/group ids, filetype, inode, msgtype, object/subject context parts, path, perms, pid, ppid, or success.

"and" created by adding more "-F" name/value pairs. An "or" is created by adding a new rule.

Results are evaluated by the filter to decide if event is auditable



File System Audit Rules

File system audit rules take the general form of: -w /full/path-to-file -p wrxa -k "rule note"

Can also be expressed as syscall audit rule: -a exit,always -F path=/full/path-to-file -F perm=wrxa -k "rule note"

The perm field selects the syscalls that are involved in file writing, reading, execution, or attribute change.



Trusted Apps

- All entry point programs must set loginuid
- Apps that modify trusted databases were updated to send audit event records:
 - amtu, aide
 - at, vixie-cron
 - coreutils
 - dbus, glibc (nscd)
 - gdm, kdm, xdm.
 - openssh, pam, util-linux, vsftpd
 - passwd, shadow
 - nss



Pam IDS updates

pam_tally2

- Locks out an account for consecutive failed login attempts
- Sends ANOM_LOGIN_FAILURES

pam_access

- Used to forbid logins from certain locations, consoles, and accounts
- /etc/security/access.conf controls its config
- Sends ANOM_LOGIN_ACCT and ANOM_LOGIN_LOCATION

pam_time

- Used to forbid logins during non-business hours
- /etc/security/time.conf controls its config
- Sends ANOM_LOGIN_TIME

pam_limits

- Used to limit maximum concurrent sessions and other user restrictions
- /etc/security/limits.conf controls its config
- Sends ANOM_LOGIN_SESSIONS







ausearch results

type=PATH msg=audit(06/06/2008 14:15:19.373:3588) : item=1 name=/tmp/ svck4.tmp/svd8l.tmp inode=168834 dev=08:07 mode=file,600 ouid=sgrubb ogid=sgrubb rdev=00:00 obj=unconfined_u:object_r:user_tmp_t:s0

type=PATH msg=audit(06/06/2008 14:15:19.373:3588) : item=0 name=/tmp/ svck4.tmp/ inode=168794 dev=08:07 mode=dir,775 ouid=sgrubb ogid=sgrubb rdev=00:00 obj=unconfined_u:object_r:user_tmp_t:s0

type=CWD msg=audit(06/06/2008 14:15:19.373:3588) : cwd=/home/sgrubb

type=SYSCALL msg=audit(06/06/2008 14:15:19.373:3588) : arch=x86_64 syscall=unlink success=yes exit=0 a0=7fff66ec9340 a1=7fff66ec92a0 a2=14 a3=3e831eadc0 items=2 ppid=4030 pid=4041 auid=sgrubb uid=sgrubb gid=sgrubb euid=sgrubb suid=sgrubb fsuid=sgrubb egid=sgrubb sgid=sgrubb fsgid=sgrubb tty=(none) ses=1 comm=simpress.bin exe=/usr/lib64/openoffice.org/program/simpress.bin subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=delete



aureport results

Summary Report

Range of time in logs: 05/27/2008 09:28:34.600 - 06/07/2008 09:31:58.719 Selected time for report: 06/06/2008 00:00:00 - 06/07/2008 09:31:58.719 Number of changes in configuration: 113 Number of changes to accounts, groups, or roles: 0 Number of logins: 4 Number of failed logins: 0 Number of authentications: 17 Number of failed authentications: 0 Number of users: 2 Number of terminals: 13 Number of host names: 4 Number of executables: 115 Number of files: 41551 Number of AVC's 10 Number of MAC events: 8 Number of failed syscalls: 1284 Number of anomaly events: 3 Number of responses to anomaly events: 0 Number of crypto events: 0 Number of keys: 4 Number of process IDs: 1006 Number of events: 44470



aureport --file

File Summary Report

total file

- 776 /usr/bin/
- 763 /usr/lib64/
- 690 /var/lib/PackageKit/
- 690 /var/lib/PackageKit/transactions.db-journal
- 670 /usr/include/linux/
- 366 /usr/share/mimelnk/application/
- 254 /usr/share/apps/katepart/syntax/
- 248 /usr/share/doc/HTML/en/kdelibs-apidocs/kio/bookmarks/html/
- 182 /dev/.udev/queue/
- 166 /var/run/hald/
- 166 /var/run/hald/acl-list
- 140 /usr/share/services/
- 108 /lib/modules/2.6.25.4-30.fc9.x86_64/kernel/drivers/ata/
- 41 /var/run/ConsoleKit/database~



Audit System Data Flow





Intrusion Goals





Network Intrusion Attack Tree



Steve Grubb, Red Hat



Privilege Escalation Attack Tree





audisp-prelude

- Audispd plugin that reads audit stream
- Identifies suspicious events
- Sends most interesting ones to prelude-manager
- Has 15 different configurable detections
- Has a test mode so that it can be checked
 - Takes input from stdin
 - Must be raw log format (ausearch –raw > ./test.log)
 - /sbin/audisp-prelude –test < ./audit-test.log | less



Audisp-prelude Detections

Controlled by /etc/audispd/audisp-prelude.conf detect avc – SE Linux AVCS detect logins – detects any login detect login fail max - detects output from pam tally2 detect login session max – detects output from pam limits detect login location – detects output from pam access detect login time – detects output from pam time detect abend – detects any abnormal terminations: segv, abort detect promiscuous – detects opening of promiscuous socket detect mac status – detects changes in SE LINUX configuration detect group auth – detects failures in group password auth detect_watched_acct - detects any login for account being watched detect watched file – detects access to file being watched detect watched_exec – detects execution of specific programs detect watched mk exe – detects the creation of executables



SE Linux records a program's behavioral model





Intrusion Goals & Detections





Network Intrusion Attack Tree & Detections



Steve Grubb, Red Hat





Privilege Escalation Attack Tree & Detections



Watched File, exec, mk_exe

- Requires special audit rules
 - -k ids-type-severity
 - Ids gets the attention of key processor
 - Type file, exec, or mkexe
 - Severity info, low, med, or hi

-a exit,always -F path=/full-path/file -F perm=wa -k ids-file-med -a exit,always -F path=/full-path/file -F perm=x -k ids-exec-med -a exit,always -S chmod -F dir=/home -F a1&0111 -F filetype=file -k ids-mkexe-hi



What to do with this info?

- Audit system is now an active component
- Have the ability to pick out events
- Hard to watch all machines
- Many events overwhelm people because hard to pick out what's important
- The key is central collection, escalation, and correlation



IDMEF

- Intrusion Detection Message Exchange Format
- Governed by IETF RFC 4765
- Describes XML format
 - What parameters are available
 - How to represent values
 - Network protocol
- Normalizes events so programs from different vendors, OS, and devices can in theory interoperate
- libprelude.so provides a complete and mature IDMEF library







Prelude

- Full featured Hybrid-IDS
- Has many sensors
- Has event aggregation
- Correlate many events
- Can alert in realtime
- Event notification popups





Hybrid IDS

- Host Based IDS not very prone to false positives
 - Event either happened or it didn't
 - You have full context of what the event means
- Network Based IDS can generate false positives
 - New protocols can look like attack
 - Can only report what it sees
 - Might not be able to decrypt some traffic
 - Limited context about what really happening
- Hybrid Mixes the two



Prelude Architecture





Prelude Sensors

- Audit
- Snortd
- Samhain
- OSSEC
- Nepenthes
- NuFW

- LML
 - Pam
 - Apache
 - Syslog
 - Arpwatch
 - Cisco equipment
 - Asterisk
 - Clamav
 - Nagios
 - Portsentry
 - Postfix
 - Sonicwall
 - Spamassassin
 - webmin



Libprelude communication

- Sensor must be registered to its manager
- Communication is encrypted
- Failover capability when cannot contact manager
- Relay events from manager to manager
- Reverse relay to keep DMZ secure



Visualize Alerts - Prewikka

- Apache based cgi-bin
- Has database of recent alerts
- Allows multiple users with different permissions
- Sort/select alerts by type, host, target, severity, sensor, and many more ways at the top of the columns.



<u>File Edit View History Bookmarks Tools Help</u>

Prewikka Demo

Prelude console

✓ Google

	Alerts	CorrelationAlerts	ToolAlerts		admin on saturday	07 june 2008 lo g	gout	
Events								
Agents		reports typesees	Source	Target	Sensor	Time		
Settings	(vendor-sp	ecific:1:1852, vendor-specific:u	rl) 74.6.22.126:44036/tcp	66.162.173.83:80/tcp	snort	13:56:31		
About	1 x <mark>MS-SQ</mark> 1 x MS-SQ	L Worm propagation attempt L version overflow attempt	89.222.153.113	66.162.173.81	snort	13:53:01		
	1 x <mark>MS-SQ</mark> 1 x MS-SQ	L Worm propagation attempt L version overflow attempt	61.128.186.202	66.162.173.80	snort	13:49:59		
	2 x User Au	uthentication (succeeded)	n/a	66.162.173.80	PAM (zeus.web-insights.net) 13:47:31 - 13:47			
	User login	(succeeded)	74.185.148.203:50095/tcp	zeus.web-insights.net:22/tcp 66.162.173.80:22/tcp Userld name: steve Process name: sshd (18821)	sshd (zeus.web-insights.net)	13:47:17		
	2 x MAC Vi 1 x MAC Vi 1 x Login (s	iolation (succeeded) iolation (failed) succeeded)	n/a	n/a	auditd	iditd 13:47:16 - 12:51:44		
	ICMP PING (vendor-sp	CyberKit 2.2 Windows ecific:1:483, vendor-specific:url	206.174.74.22:icmp	66.162.173.86:icmp snort		13:42:55		
	1 x MS-SQL Worm propagation attempt 1 x MS-SQL version overflow attempt ICMP PING CyberKit 2.2 Windows (vendor-specific:1:483, vendor-specific:url)		61.134.56.18	66.162.173.89	snort	13:33:15		
			219.248.253.239:icmp	<u>66.162.173.6</u> :icmp	<u>.162.173.6</u> ;icmp snort			
	WEB-MISC (vendor-sp	cobots.txt access ecific:1:1852, vendor-specific:u	rl) 193.47.80.42:42819/tcp	3.47.80.42:42819/tcp 66.162.173.83:80/tcp snort		13:22:41		
Filter	1 x <mark>MS-SQ</mark> 1 x MS-SQ	L Worm propagation attempt L version overflow attempt	61.132.223.14	66.162.173.88	snort	13:22:15		
Period 6 Hours ▼ Timezone Frontend localtime ▼	WEB-MISC (vendor-sp	cobots.txt access ecific:1:1852, vendor-specific:u	rl) 78.137.163.133:52670/tcp	66.162.173.83:80/tcp	snort	13:20:49		
Limit 50 By time (desce •	ICMP PING (vendor-sp	CyberKit 2.2 Windows ecific:1:483, vendor-specific:url	71.48.35.137:icmp	66.162.173.6:icmp	snort	13:12:47		
Apply Save	WEB-MISC (vendor-sp	c <mark>robots.txt access</mark> ecific:1:1852, vendor-specific:u	rl) 78.137.163.133:49707/tcp	66.162.173.89:80/tcp	snort	13:12:39		
2008-06-07 07:59:43 2008-06-07 13:59:43	1 x MS-SQ 1 x MS-SQ	L Worm propagation attempt L version overflow attempt	118.86.63.202	66.162.173.91	snort	13:07:44		
-04:00	1 x MS-SQ 1 x MS-SQ	L Worm propagation attempt L version overflow attempt	61.153.50.237	66.162.173.92	snort	12:33:06		
	ICMP PING (vendor-sp	CyberKit 2.2 Windows ecific:1:483, vendor-specific:url	222.235.168.223:icmp	66.162.173.6:icmp	snort	12:29:12		
1 50 (total:54)	1 x <mark>MS-SQ</mark> 1 x MS-SQ	L Worm propagation attempt L version overflow attempt	218.7.160.84	66.162.173.88	snort	12:20:05		



<u>F</u> ile <u>E</u> dit <u>V</u> iew Hi <u>s</u> tory <u>B</u> ookmar	rks <u>T</u> ools	s <u>H</u> elp										4
🜪 🔶 - 🎜 🔕 🕓 餐 http	p://www.w	veb-insi	ghts.net/pi	rewikka	?view=alert	_summary&d	origin=ale	ert_listing&m	essageid=c4	7303fc-5 ☆ 🗸	G~ Google	٢
Prewikka Demo	rts	orrela	tionAlert	e T	oolAlerts					admin or		console
Events		onea	tionAlert		oolAlei ts	_	_	_	_	ciumin oi	r saturday or june 2000	logout
Agents	ert											
Settings Crea	ate time				De	etect time			Analyzer tim	10		
About 200	8-06-07 13	3:47:16.4	4765 -04:00		20	08-06-07 12:5	1:44 -04:0	0	2008-06-07	7 13:47:16.45014 -04	4:00	
Mes	ssageID											
c47	303fc-34b9	9-11dd-89	Əba									
Text	t .	Severity	Completion	Type D)escription							
MA	C lation	low	failed	other A	o program has	tried to access kness in the pro	something	that is not allow	ved in the MAC	oolicy. This could indi	cate an attacker trying	onsole logout
	Analyzer	r #1 —					J					
	-											
	Model	Name	Analyze	rid	0.025	Version	Class	Manufacturer		oom/ogrubb/oudit/		onsole logout
	auditu	auuitu	200402	2047390	5935	1.7.4	HID3	Red Hat, http	people.redital.	com/sgrubb/audiv		
	Linux 2.6.24	system 4.7-92.fcl	8									
	Process				Proces	s Dath				Process DID		
	audisp-prel	lude			/sbin/au	udisp-prelude				1428		
	Analyz	er Pat	h (1 not s	shown) —							
	-				-							
So	ource(0)											
Nor	de name											
zeu	S											
	er category											
арр	lication			Туре			Name	N	lumber		Tty	
				origin	nal-user		unset	4	294967295		(none)	

RED HAT SUMMIT

<u>F</u> ile <u>E</u> dit <u>V</u> iew Hi <u>s</u> tory <u>B</u> ookmarks <u>T</u>	ools <u>H</u> elp					0
ቀ 🗼 ~ 😂 🔕 🕓 餐 http://ww	w.web-insights.net/prewikka?vi	ew=alert_summary∨	igin=alert_listing&m	nessageid=c47303fc-3 🎡	✓ Google	٩
Prewikka Demo	CorrelationAlerts To	olAlerts		adm	Prelude c	onsole
Events		1	I	· · -		
Agents Derati	.6.24.7-92.fc8					
Settings	-	Drococc Deth		Dresses DID		
About	-prelude	/sbin/audisp-prelude		1428		
Anal Source Node name zeus User catego application	yzer Path (1 not shown) - (0)	user	Name N unset 4	Process PID 1428 1428 Number Tly 4294967295 (none) Process PID 18808		
Process		Process Path		Process PID		
prewikka.cg	ji	/usr/bin/python		18808		
Node name	(0) •					
Zeus						
Additio	nal data					
Meaning	Value					
AVC Text	node=zeus type=AVC msg=audit(1 /prewikka.cgi" dev=md1 ino=51577	212857504.511:1471): avc: 0 scontext=system_u:system_	lenied { ioctl } for pid=18 r:httpd_t:s0 tcontext=sys	808 comm="prewikka.cgi" path stem_u:object_r:httpd_prewikka	="/usr/share/prewikka/cgi-bin _script_exec_t:s0 tclass=file	
Audit event serial #	1471					



	Alerts C	orrelation/	Alerts Tool	Alerts				ad	min on saturday 07 j	une 2008	log		
Events	_										1		
Agents	Alert												
Settings	Create time	Create time					alyzer time						
About	2008-06-07 13	:53:01.805515 -	04:00	2008-06-07	13:53:01.804	4435 -04:00	20	2008-06-07 13:53:01.805644 -04:00					
	MessagelD	MassagelD											
	9289e670-34b	a-11dd-bea4											
						I							
	Text	n overflow att	ompt			Ident	Severity	Type	Description				
	MS-SQL Versio	on over now at t	empt			1.2050	IOW	other	wise activity				
	Origin	Origin				Name M			Meaning				
	vendor-specific	vendor-specific				1:2050 S			Snort Signature ID				
	vendor-specific	vendor-specific				url							
	vendor-specific			2002-0649									
	bugtragid	bugtraqid				5310							
	- Analyzer	r Analyzer #1											
	Model	Name	Analyzerid	d		Version	Class	Manufacturer					
	Snort	snort	2035257361705	5394		2.8.1	NIDS	http://www.snort.org					
	Operating S	Operating System											
	Linux 2.6.24	1.7-92.fc8											
	Process)				- 11				
					18457								
	- Analyza	or Doth (1 r	ot shown)										
	Analyz	a Path (1 f	iot shown) —										



File Edit View History Bookmarks Tools Help http://www.web-insights.net/prewikka?view=alert_summary&origin=alert_listing&messageid=9289e670-G~ Google \sim Prewikka Demo Prelude console **CorrelationAlerts ToolAlerts** Alerts admin on saturday 07 june 2008 logout Events Source(0) Agents Node name (resolved) Node address Port Protocol ip version Settings 89.222.153.113 89.222.153.113 3067 4 udp About Target(0) Node address Port Protocol Node name (resolved) ip version 66.162.173.81 66.162.173.81 1434 4 udp Additional data Meaning Value snort rule sid 2050 snort_rule_rev 12 **Network centric information** IP Version Header length TOS Length ld DF lp offset TTL Protocol Checksum Source address Target address R F M 4 5 0 404 44437 0 56 17 61568 89.222.153.113 66.162.173.81 UDP Source port Target port Length Checksum 3067 1434 384 17933 Payload Payload 0000: 0010: 0020: 0030: 0040: 0050: 0060: 01 dc c9 b0 42 eb 0e 01 01 01 01 01 01 01 70 aeв.....р. 0070: 42 01 70 ac 42 90 90 90 90 90 90 90 90 68 dc c9 B.p.B....h.. :0300 b0 42 b8 01 01 01 01 31 c9 b1 18 50 c2 fd 35 01 .B....1...P...5. 0090: 01 01 05 50 89 e5 51 68 2e 64 6c 6c 68 65 6c 33 ...P..Qh.dllhe13 00a0: 32 68 6b 65 72 6e 51 68 6f 75 6e 74 68 69 63 6b 2hkernQhounthick 00b0: 43 68 47 65 74 54 66 b9 6c 6c 51 68 33 32 2e 64 ChGetTf.110h32.d 00c0: 68 77 73 32 5f 66 b9 65 74 51 68 73 6f 63 6b 66 hws2 f.etQhsockf 00d0: b9 74 6f 51 68 73 65 6e 64 be 18 10 ae 42 8d 45 .toQhsend....B.E



File Edit View History Bookmarks Tools Help ✓ G ✓ Google 🛛 🔇 🔇 🥳 http://www.web-insights.net/prewikka?view=sensor_listing Q \sim Prewikka Demo Prelude console Agents **Heartbeats** admin on saturday 07 june 2008 logout Events Node location n/a Agents Settings Node name n/a Linux 2.6.24.7-92.fc8 Total: 4 About Delete Name Model Version Class Last heartbeat Status auditd auditd 1.7.4 HIDS 2008-06-07 14:05:32 -04:00 Online prelude-Iml Prelude LML 0.9.12.2 Log Analyzer 2008-06-07 14:05:46 -04:00 Online prelude-manager Prelude Manager 0.9.12.1 Concentrator 2008-06-07 14:05:50 -04:00 Online snort Snort 2.8.1 NIDS 2008-06-07 13:58:50 -04:00 Online

Alerts Heartbeats Delete



Future Directions

- Add Brouette
 - Offers real-time alerts via libnotify
- Add mod_security2 log format parsing for LML
 - This is the biggest hole in HIDS capability now
- Add more sensors
 - Rogue DHCP detection
 - Integrate passive asset detection
- Add more detections for auditd sensor
 - Changing uid
 - Account changes
 - Test Failures (amtu, aide, RBAC, sectool)
 - Crypto failures



Future Directions

Correlation when Engine is ready

- Provide framework for higher level analysis
- Reconstruct sequence of events
- Detect Targets, Protocols, Tools, etc
- Adapt Severity Rating
- Allow filtering to suppress false positive
- Improve accuracy by scoring alerts
- Reactive Countermeasure

Visualization tools

• PIG – Prelude IDMEF Grapher



Nessus Scan

Prelude IDMEF Grapher

<u>Fi</u>le <u>H</u>elp





Future Directions

There are weaknesses in the IDMEF spec

- Seems to have been designed from snort's PoV
- No way to express some HIDS concepts
 - Roles are not in spec
 - No concept of sensitivity
 - In the case of promiscuous socket target is network
 - Not allowed to say results were indeterminate
 - Data Source Identifier should be in spec
 - Can't say source of attack is a service or program
 - Access of shadow -is maore than just a FILE attack, its an attack on the credentials

Seems like a new spec is in order to fix these deficiencies



Questions ?

HOWTO http://people.redhat.com/sgrubb/audit/prelude.txt

Audit Info http://people.redhat.com/sgrubb/audit

Mail sgrubb@redhat.com

