進階軟體資安:
雲端VIS防禦系統
防禦流程與結果

Step1:監控虛擬機

- 用 strace、qemu-monitor 來對 VM 做動態資料的蒐集、比對與建模(VM 的惡意行為模式)， strace 就相當於是對一個 VM 作黑箱檢測， 從 VM 對 Host 要求使用的 system call 做記錄及分析， qemu-monitor 可觀察 VM 的整體硬體狀態是否有異常， 或是被不當使用。

Step2:建立惡意虛擬機行為(system call)資料庫

- 1.監控惡意虛擬機從攻擊到入侵成功的system log分佈
- 2.利用機器學習方式(GHSOM)，分類惡意虛擬機與正常機器的system log，並寫下安全性的過濾設定

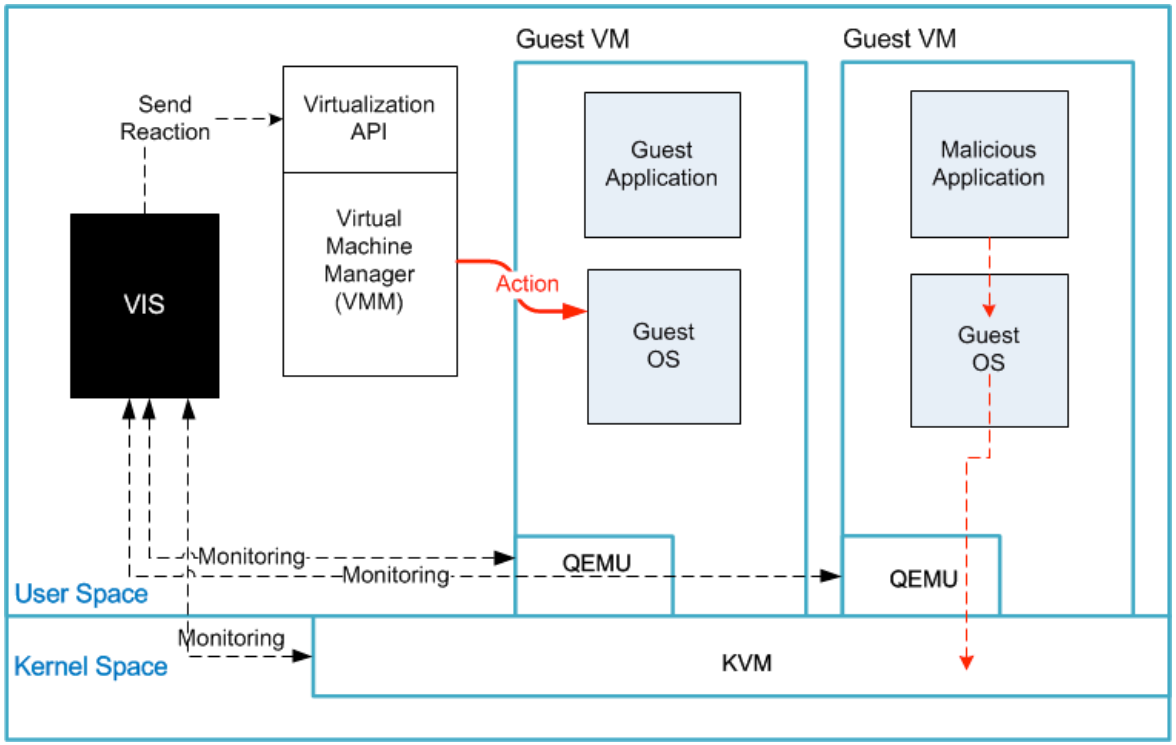
Step 3:檢查異常

- Behavior Checker 會從 Policy DB 載入 system call 安全性的過濾設定機制都存在 Introspection module 裡面,
- 而 Behavior Checker 即時的比對 VM 行為。

Step 4:異常處理

- 如果檢測到異常時， Behavior Checker元件 會傳送 “domain [shutdown]” 或是 “domain[destroy]” 這樣的訊息出去以銷燬或是將惡意的 VM 關機。
- 但在別一方面， VM 的虛擬硬碟，並不會立刻被刪除。
- 它會被 offline-migrate 到 sandbox Host上面去做檢測。 進一步分析更多資訊。
- 經由 VIS 的監控，我們可以追綜與比對 VM的行為。

监控程序


Guest VM
Guest VM
Send
Reaction
Virtualization
API
Guest
Application
Malicious
Application
Virtual
Machine
Manager
(VMM)
VIS
Action
Guest
OS
Guest
OS
Monitoring
Monitoring
QEMU
QEMU
User Space
Monitoring
Kernel Space
KVM

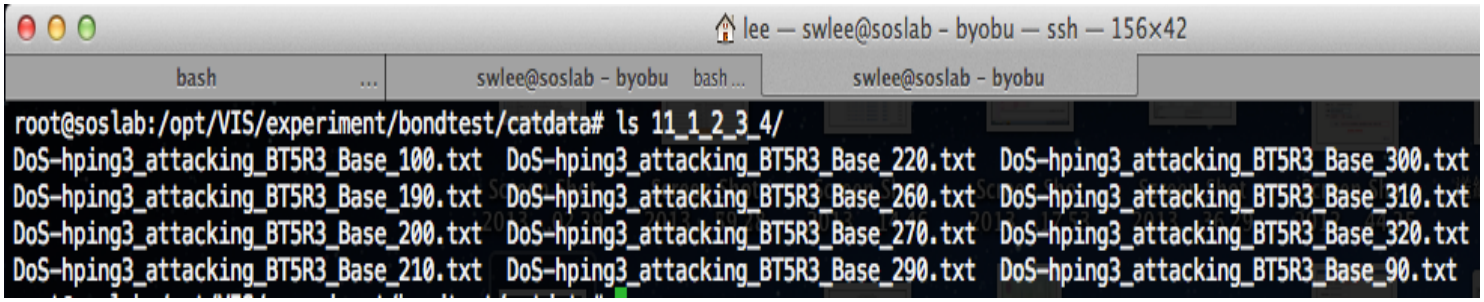
目前可偵測的攻擊

- 1. CVE-2013-0422
- 2. CVE-2013-0431
- 3. DoS-hping3
- 4. MS12-020
- 5. SET-Web-Java-Applet
- 6. SE_Firefox_xpi

惡意虛擬器防禦rule設置

- Step 1:偵測攻擊方的system call資料
- Step 2:攻擊system call資料的分類
- Step 3: 將顯著能判斷出攻擊者的system call資訊設置為rule(可能會有多個rule)
- Step 4:測試rule, 並判斷和rule接近的VM為惡意的VM(if失敗=>試試其他的rule)

Step 2:攻擊system call資料的分類



這是由Gothem所分類出惡意虛擬機的system call集合,可以由上圖清楚看出這一類皆為Dos-attacking

Step 3: 將顯著能判斷出攻擊者的system call資訊設置為rule(可能會有多個rule)

Hacker VM									
Attack(Valun. Number)	Period 0	Period 1	Period 2	Period 3	Period 4	Period 5	Period 6	Period 7	Period 8
CVE-2013-0422	Do nothing	Setting Attack	Attacking	Screenshot	sysinfo	ps	migrate	keylog	shell
		Rule 18_2 (3), 23(1), 60_1(1)	Rule 18_2 (2), 22_4(1), 23(7), 39_2(1), 61_2(1)	Rule 42_4(1)	Rule 36(1)	Rule 36(1)	23(1)	Rule 55(1)	Rule 18_2 (4), 42_3(1)
CVE-2013-0431	Do nothing	Setting Attack	Attacking	Screenshot	sysinfo	ps	migrate	keylog	shell
		Rule 18_2 (4)	Rule 18_2 (3),23(2), 42_3(1)	Rule 18_2 (1)	Rule 18_2 (1)	Rule 42_4(1)	Rule 39_2(1), 55(1)	Rule 18_2 (1), 61_1(1)	Rule 18_2 (2), 22_4(1), 55(1)
DoS-hping3	Do nothing	Attacking							
		Rule 11 (12)							
MS12-020	Do nothing	Setting Attack	Attacking						
			Rule 18_2 (1), 55(1)						
SET-Web-Java-Applet	Do nothing	Setting Attack	Attacking	shell	tasklist	kill	keylog(keystroke)		
		Rule 18_2 (3), 60_1(1)	Rule 18_2 (2), 36(1)	Rule 36(1)	Rule 18_2 (1)	Rule 18_2 (1), 55(1), 57_2(1)	Rule 18_2 (2), 58_1(1), 58_2(1)		
SE_Firefox_xpi	Do nothing	Setting Attack	Attacking	Screenshot	sysinfo	ps	migrate	keylog	shell
		Rule 46_4(1), 48_2(1)	Rule 18_2 (1), 46_2(1), 60_4(1)	Rule 36(1)	Rule 36(1)		Rule 23(1),36(1)		

Rule 和 System call 的對應

Attackes (Hacker)													
	Bond	select	select_err	recvmsg	recvmsg_err	read	read_err	write	write_err	rt_sigaction	rt_sigaction_err	ioctl	ioctl_err
Rule 11	627.687 5	2269.0833	0	647.8333333	0	38453.08	1551.1666	22411.7	0	469.4166666	66667	0	631.5
Rule 23	81.523437	2603.1666	0	631.5833333	0	3118.416	1084.4166	2667.08	0	1047	0	693.5	0
Rule 18_2	81.470703	2355.6562	0	624.40625	0	2651.375	905.625	2929.59	0	881.75	0	554.625	0
		sendto	sendto_err	recvfrom	recvfrom_err	futex	futex_err	timer_se	timer_sett	timer_gettime	timer_gettime_e	wait4	wait4_err
Rule 11		0	97.6666666	0	99.25	0	2768.75	469.5	0	476.5833333	0	547.5833	0
Rule 23		112.33333	0	119.0833333	0	66.5	10.583333	1050	83333333	0	1230.5	0	0
Rule 18_2		40.40625	0	70.9375	0	82	12.65625	884.78	12500000	0	1114.25	0	0

Step 4:測試rule, 並判斷和rule接近的VM為惡意的VM(if失敗=>試試其他的rule)

Attacks (Hacker)	CVE-2013-0422(JAVA)	CVE-2013-0431(JAVA)	DoS-hping3	MS12-020	SET-Web-Java-Applet	SE_Firefox_xpi
Rule 11			V			
Rule 23	V	V				
Rule 18_2	V	V		V	V	V

以相同的方式找出被入侵的虛擬機

Compromised (Victim)	CVE-2013-0422(JAVA)	CVE-2013-0431(JAVA)	DoS-hping3	MS12-020	SET-Web-Java-Applet	SE_Firefox_xpi
Rule 65_4	V	V				
Rule 47_2		V				
Rule 33			V			