

An Introduction to Virtual Machine Introspection

Mike Nielsen

mike.nielsen@adventiumlabs.com

April 18, 2015

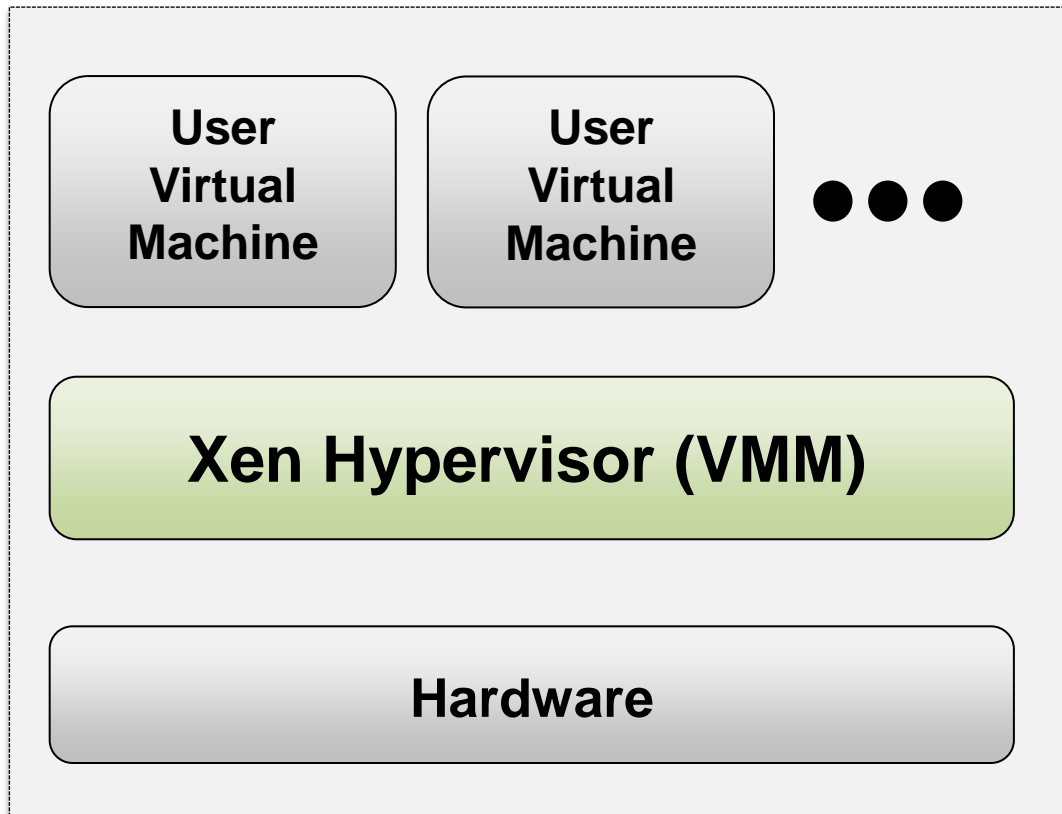
Introduction

- Introduction to virtualization and Xen
- Motivation for agentless VM introspection with an emphasis on security
- Uses of agentless VM introspection in the context of security
- Challenges to agentless VM introspection
- Examples of existing agentless VM introspection technology

Virtualization Background

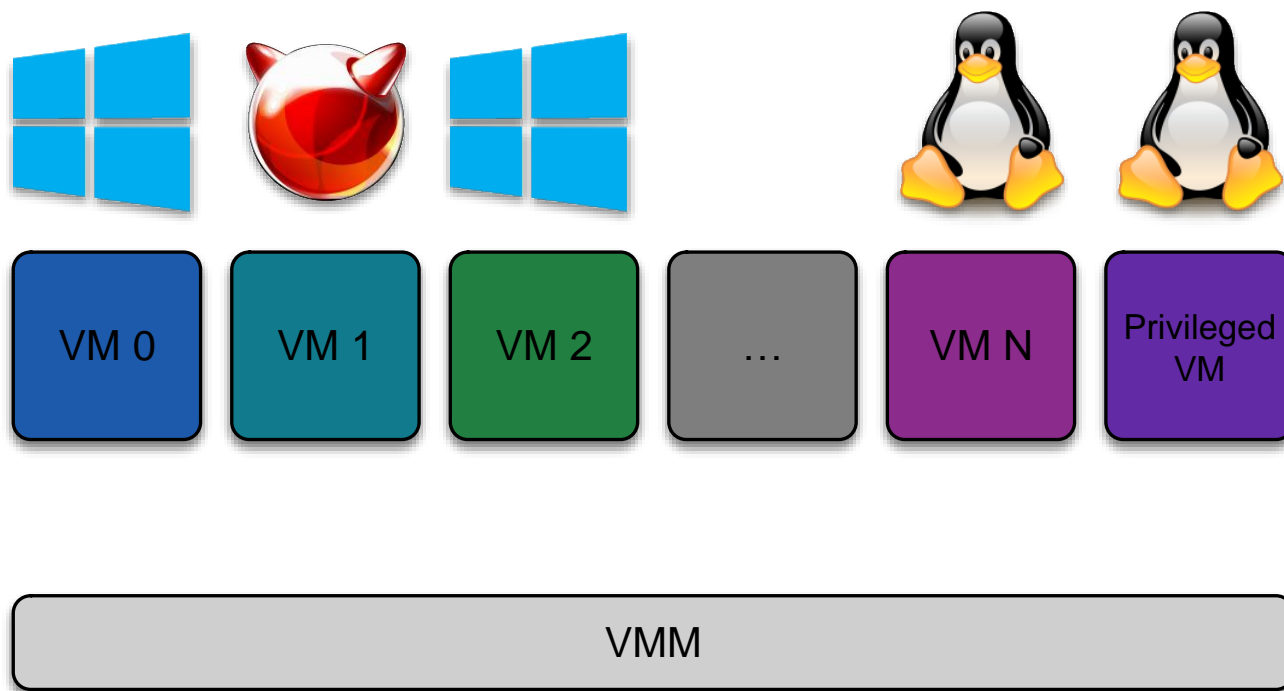
- Virtualization allows running many virtual machines (VMs) on a single host.
- A virtual Machine Monitor (VMM) creates and manages VMs. A VMM is also called a “hypervisor”.
- Examples of VMMs:
 - KVM
 - Microsoft Hyper-V
 - VMware ESXi
 - Xen

Xen Overview



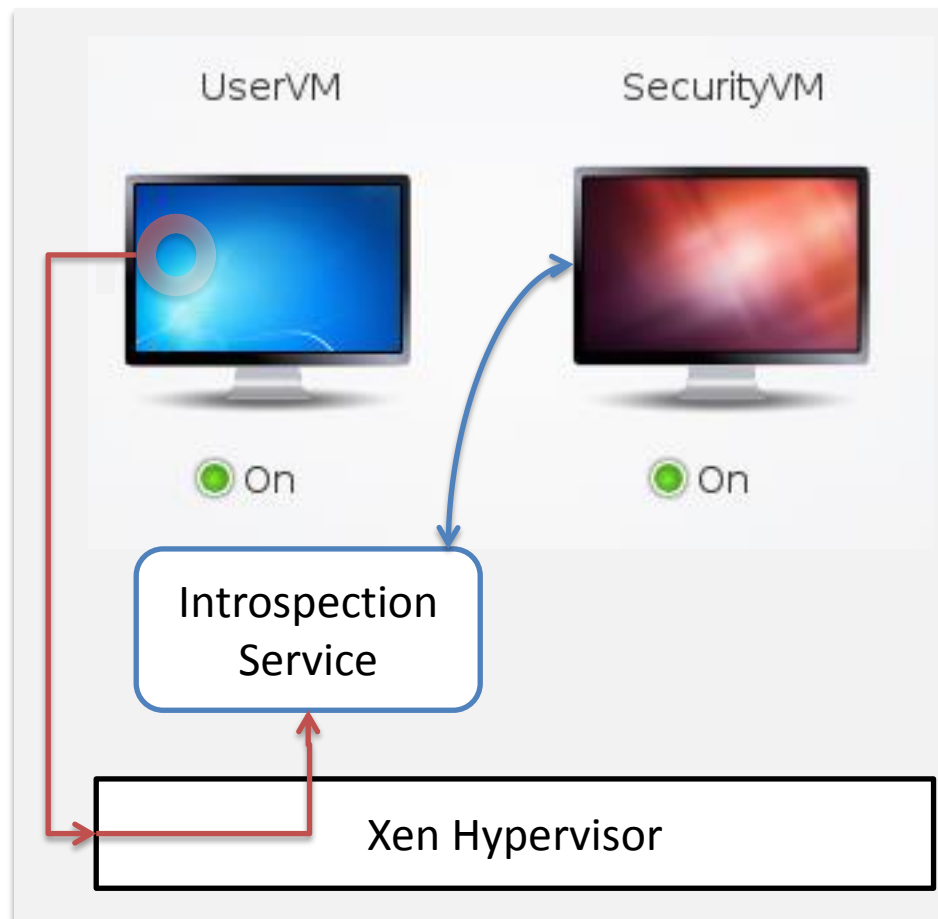
Virtual Machine Introspection

- Virtual machine introspection provides access to low-level details of a running virtual machine to agents running outside the guest.



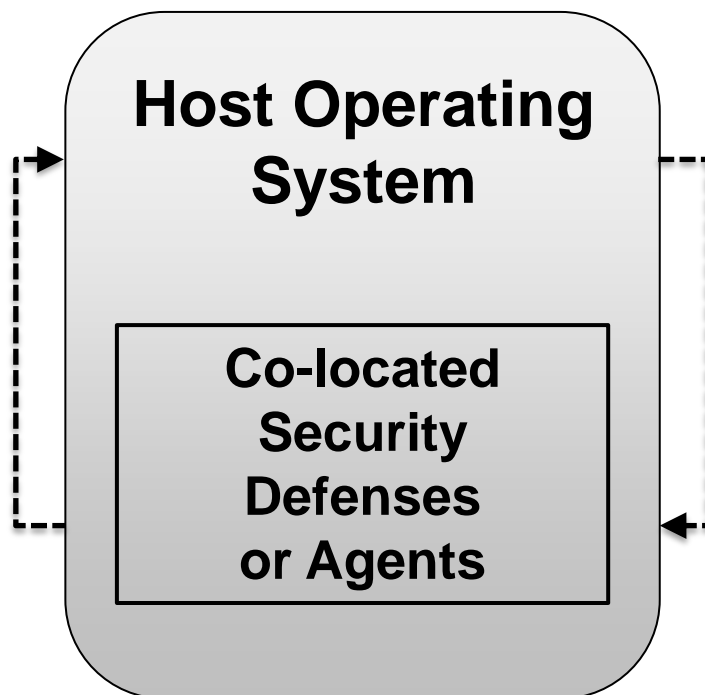
Applications of VM Introspection

- Applications
 - Provide system administrators with deeper visibility into running systems' state.
 - Enhance system security via agentless defenses.



Security as a Motivation for Agentless VM Introspection

- Host-based defenses: who defends the defender?



- Malware Analysis
 - Drop malware into a monitored guest and study its behavior.
- Malware Detection
 - Monitor a guest for indicators of malware.
- Malware Prevention
 - Intervene when malware is detected.

Three Challenges to Introspection

- Semantic Gap
 - Data as the guest OS sees it versus data as the hypervisor sees it.
- Performance
 - Introspection cycles should not detract from guest OS users' experience.
- Precision
 - Introspection cycles should have coherence over time.

Technologies: LibVMi

- LibVMi (<http://libvmi.com/>)
- C library with Python bindings
- View contents of memory and registers
- Event-based introspection
- Integration with Volatility

LibVM: “process-list”

The screenshot shows a Windows desktop environment. In the foreground, the Windows Task Manager is open, displaying a list of running processes. The background shows a terminal window with a list of processes and their memory addresses.

Windows Task Manager Processes:

Image Name	PID	User Name	CPU	Mem
calc.exe	1304	Windows	00	5
csrss.exe	292	SYSTEM	00	1
csrss.exe	352	SYSTEM	00	1
dwm.exe	1244	Windows	00	16
explorer.exe	1260	Windows	00	16
lsass.exe	412	SYSTEM	00	2
lsm.exe	420	SYSTEM	00	1
notepad.exe	1860	Windows	00	1
SearchIndexe...	1776	SYSTEM	00	1
services.exe	404	SYSTEM	00	3
smss.exe	220	SYSTEM	00	288 K
spoolsv.exe	416	SYSTEM	00	3,972 K
sppsvc.exe	1480	NETWO...	00	968 K
svchost.exe	240	NETWO...	00	4,024 K

Terminal Output (1. ssh):

```

[ 4] System (struct addr:fffffa800188e890)
[220] smss.exe (struct addr:fffffa80024fe910)
[292] csrss.exe (struct addr:fffffa8002582490)
[340] wininit.exe (struct addr:fffffa80025c07c0)
[352] csrss.exe (struct addr:fffffa80025c78c0)
[404] services.exe (struct addr:fffffa80023f8910)
[412] lsass.exe (struct addr:fffffa80023ffb30)
[420] lsm.exe (struct addr:fffffa80024004a0)
[448] winlogon.exe (struct addr:fffffa80023fab30)
[568] svchost.exe (struct addr:fffffa8003337060)
[636] svchost.exe (struct addr:fffffa8003598510)
[688] svchost.exe (struct addr:fffffa8003279890)
[788] svchost.exe (struct addr:fffffa80035d4640)
[816] svchost.exe (struct addr:fffffa80035ebb30)
[960] svchost.exe (struct addr:fffffa8003636b30)
[240] svchost.exe (struct addr:fffffa800363cb30)
[416] spoolsv.exe (struct addr:fffffa800365bb30)
[1000] svchost.exe (struct addr:fffffa80036ca890)
[1136] taskhost.exe (struct addr:fffffa8003771910)
[1244] dwm.exe (struct addr:fffffa800378bb30)
[1260] explorer.exe (struct addr:fffffa8003797b30)
[1776] SearchIndexer. (struct addr:fffffa80035bf630)
[1860] notepad.exe (struct addr:fffffa800269e740)
[1304] calc.exe (struct addr:fffffa8002730b30)
[1048] taskmgr.exe (struct addr:fffffa8004f52910)
[844] svchost.exe (struct addr:fffffa80026488c0)
[1480] sppsvc.exe (struct addr:fffffa800382d160)
  
```

Technologies: DRAKVUF

- DRAKVUF (<http://drakvuf.com/>)
- Agentless malware analysis system
- Uses LibVMI, Rekall, Volatility
- Detailed tracing and logging
- Process injection

DRAKVUF: Process Injection

```

File Edit View Search Terminal Help
Starting event loop
Ready to hijack thread of PID 2364 on vCPU 0!
CPA @ 0x77408840
GS: 0x7fffffffde000 RSP: 0x11eda8, RIP: 0x77381930, RCX: 0x357960
Stack base: 0x120000, Limit: 0x11b000
cmd.exe /K echo Hello World @ 0x11ed80.
pip @ 0x11ed68
sip @ 0x11ed00
Return address @ 0x11eca8 -> 0x77381930. Setting RSP: 0x11eca8.
Done with hijack routine
INT3 @ 0x26bb4930
RAX: 0x1
Restoring RSP to 0x11eda8
Restoring RAX to 0x0
Restoring RCX to 0x357960
Restoring RDX to 0x3579a0
Restoring R8 to 0x0
Restoring R9 to 0x0
-- CreateProcessA SUCCESS --
Process handle: 0x1c4, Thread handle: 0x1d0
PID: 2452, TID: 2336
Finished with test.
root@t0:/demo# ./injector 23 2364 "C:\\Program Files\\Internet Explorer\\iexplore.exe http://www.darpa.mil
Target PID 2364 to start C:\\Program Files\\Internet Explorer\\iexplore.exe http://www.darpa.mil
LibVMi Suggestion: set win_ntoskrnl=0x265e000 in libvmi.conf for faster startup.
LibVMi Suggestion: set win_kdbg=0x1f10a0 in libvmi.conf for faster startup.
LibVMi Suggestion: set win_kdvh=0xfffff8000284f0a0 in libvmi.conf for faster startup.
LibVMi Suggestion: set win_kdvh=0xfffff8000284f0a0 in libvmi.conf for faster startup.

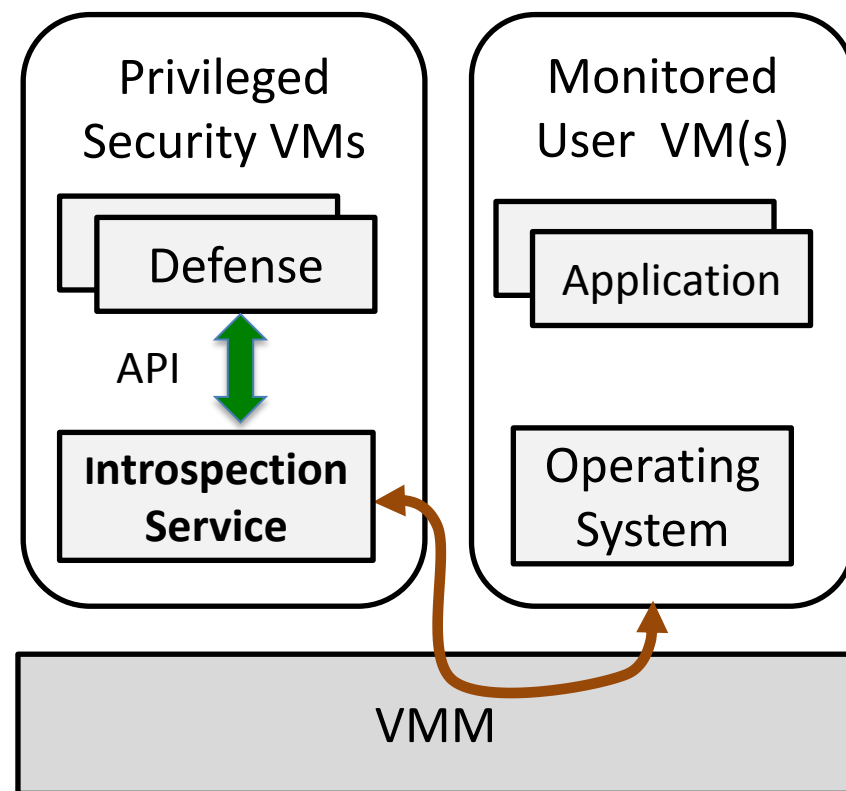
root@t0:/demo# ./injector 23 2364 "C:\\Program Files\\Internet Explorer\\iexplore.exe http://www.darpa.mil
Target PID 2364 to start C:\\Program Files\\Internet Explorer\\iexplore.exe http://www.darpa.mil
Stack base: 0x120000, Limit: 0x11b000
C:\\Program Files\\Internet Explorer\\iexplore.exe http://www.darpa.mil @ 0x11ed58.
pip @ 0x11ed40
sip @ 0x11ecd8
Return address @ 0x11ec80 -> 0x77381930. Setting RSP: 0x11ec80.
Done with hijack routine
INT3 @ 0x26bb4930
RAX: 0x1
Restoring RSP to 0x11eda8
Restoring RAX to 0x0
Restoring RCX to 0x3579a0
Restoring RDX to 0x374b80
Restoring R8 to 0x0
Restoring R9 to 0x0
-- CreateProcessA SUCCESS --
Process handle: 0x1cc, Thread handle: 0x1d4
PID: 2480, TID: 2688

```



Technologies: Adventium

- XIP (Adventium)
- Architecture for monitoring running guests from trusted vantage point
- Provides an OS-level interface (API) for introspection



XIP	<code>get_process_info(filter = {name, id})</code>
LibVMI	<code>vmi_read_va(pid=0, buf, 0xffffffffa80`80348ac3, 0x100)</code>
Xen	<code>xc_map_foreign_range(id=3, buf, 0x400, 0x100, ...)</code>


Adventium: XipWire and XipTop

Windows Server 2008 R2 (kernel 7601)

✓ Kernel Image (ntoskrnl)

✓ Interrupt Handler (IDTR)

✓ Syscall registers



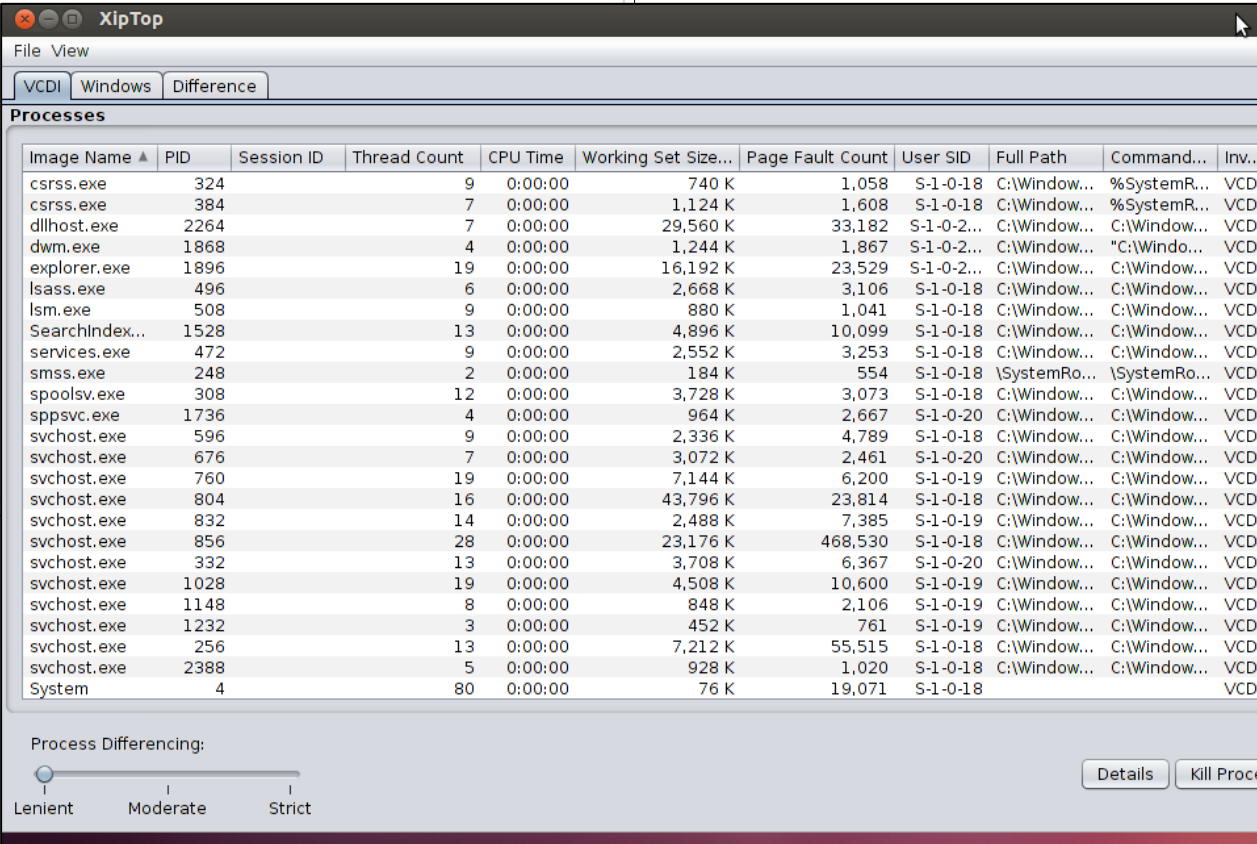


Image Name	PID	Session ID	Thread Count	CPU Time	Working Set Size...	Page Fault Count	User SID	Full Path	Command...	Inv..
csrss.exe	324		9	0:00:00	740 K	1,058	S-1-0-18	C:\Window...	%SystemR...	VCD
csrss.exe	384		7	0:00:00	1,124 K	1,608	S-1-0-18	C:\Window...	%SystemR...	VCD
dllhost.exe	2264		7	0:00:00	29,560 K	33,182	S-1-0-2...	C:\Window...	C:\Window...	VCD
dwm.exe	1868		4	0:00:00	1,244 K	1,867	S-1-0-2...	C:\Window...	"C:\Windo...	VCD
explorer.exe	1896		19	0:00:00	16,192 K	23,529	S-1-0-2...	C:\Window...	C:\Window...	VCD
lsass.exe	496		6	0:00:00	2,668 K	3,106	S-1-0-18	C:\Window...	C:\Window...	VCD
lsm.exe	508		9	0:00:00	880 K	1,041	S-1-0-18	C:\Window...	C:\Window...	VCD
Searchindex...	1528		13	0:00:00	4,896 K	10,099	S-1-0-18	C:\Window...	C:\Window...	VCD
services.exe	472		9	0:00:00	2,552 K	3,253	S-1-0-18	C:\Window...	C:\Window...	VCD
smss.exe	248		2	0:00:00	184 K	554	S-1-0-18	\SystemRo...	\SystemRo...	VCD
spoolsv.exe	308		12	0:00:00	3,728 K	3,073	S-1-0-18	C:\Window...	C:\Window...	VCD
spoolsv.exe	1736		4	0:00:00	964 K	2,667	S-1-0-20	C:\Window...	C:\Window...	VCD
svchost.exe	596		9	0:00:00	2,336 K	4,789	S-1-0-18	C:\Window...	C:\Window...	VCD
svchost.exe	676		7	0:00:00	3,072 K	2,461	S-1-0-20	C:\Window...	C:\Window...	VCD
svchost.exe	760		19	0:00:00	7,144 K	6,200	S-1-0-19	C:\Window...	C:\Window...	VCD
svchost.exe	804		16	0:00:00	43,796 K	23,814	S-1-0-18	C:\Window...	C:\Window...	VCD
svchost.exe	832		14	0:00:00	2,488 K	7,385	S-1-0-19	C:\Window...	C:\Window...	VCD
svchost.exe	856		28	0:00:00	23,176 K	468,530	S-1-0-18	C:\Window...	C:\Window...	VCD
svchost.exe	332		13	0:00:00	3,708 K	6,367	S-1-0-20	C:\Window...	C:\Window...	VCD
svchost.exe	1028		19	0:00:00	4,508 K	10,600	S-1-0-19	C:\Window...	C:\Window...	VCD
svchost.exe	1148		8	0:00:00	848 K	2,106	S-1-0-19	C:\Window...	C:\Window...	VCD
svchost.exe	1232		3	0:00:00	452 K	761	S-1-0-19	C:\Window...	C:\Window...	VCD
svchost.exe	256		13	0:00:00	7,212 K	55,515	S-1-0-18	C:\Window...	C:\Window...	VCD
svchost.exe	2388		5	0:00:00	928 K	1,020	S-1-0-18	C:\Window...	C:\Window...	VCD
System	4		80	0:00:00	76 K	19,071	S-1-0-18			VCD

Process Differencing:

☐ Lenient
 ☒ Moderate
 ☐ Strict

Conclusion and Final Remarks

- Virtualization, introspection, host-based defenses, challenges, and technologies.
- Agentless VM introspection provides a unique vantage point into a system's security.
- Adventium develops introspection-based security solutions for customers with high security requirements.